Ïðèêëàäíàÿ êðèïòîãðàôèÿ

2-å èçäàíèå

Ïðîòîêîëû, àëãîðèòìû è èñõîäíûå òåêñòû íà ÿçûêå Ñ

Áðþ Øíàéåð

Ïðåäèñëîâèå Óèòôèëä Äèôôè

Èñòîðèÿ ëèòåðàòóðû ïî êðèïòîãðàôèè äîâîëüíî ëþáîïûòíà. Ñåêðåòíîñòü, êîíå÷íî æå, âñåãäà èãðàëà âàæíóþ ðîëü, íî äî Ïåðâîé ìèðîâîé âîéíû î âàæíûõ ðàçðàáîòêàõ âðåìÿ îò âðåìåíè ñîîáùàëîñü â ïå÷àòè è êðèïòîãðàôèÿ ðàçâèâàëàñü òàêæå, êàê è äðóãèå ñïåöèàëèçèðîâàííûå äèñöèïëèíû. Â 1918 ãîäó â âèäå íàó÷íîãî îò÷åòà ÷àñòíîé Ëàáîðàòîðèè Ðèâåðáýíêà âûøëà â ñâåò ìîíîãðàôèÿ Âëëüÿì Ô. Ôðèäìàíà *Ïîêàçàòåëü ñîâïàäåíèé è åãî ïðèìåíåíèÿ â êðèïòîãðàôèè* (*Index of Coincidence and Its Applications in Cryptography*) [577], îäíà èç ïîðâàâøèõ ðàíî 20-ãî ñòîëåòèÿ. È ýòî íåñìîòðÿ íà âîâëå÷åíèå çàêàç, ïî êîíôèäåíöèàëüíîìó áþëà ñäåëàíà ýòà ðàáîòà. Â òî æå ãîäó Ýäâàðä Õ. Õåááðí èç Îêëåíäà, Êàëèôîðíèÿ, ïîëó÷èë ïàðîëè [710] íà ðîòîðíóþ ìàøèíó, óñòðîéñòâî, íà êîòîðîì îñíîâûâàëñü âîâíóòðåííèé ìåõàíèçì [710] íà ðîòîðíóþ ìàøèíó, óñòðîéñòâî, íà êîòîðîì îñíîâûâàëñü âîâíóòðåííèé ìåõàíèçì ïî÷òè 50 ëåò.

Ïîñëå Ïåðâîé ìèðîâîé âîéíû, îäíàêî, âñå èçìåíèëîñü. Îðãàíèçàöèè àðìèè è ôëîòà Ñîâåòñêîãî Øòàòîâ, ïîëó÷îñòüþ çàñåêðåòèâ ñâîè ðàáîòû, äîáèëèñü ôóíäàìåíòàëüíûõ óñïåõîâ â êðèïòîãðàôèè. Â òå÷åíèå 30-õ è 40-õ ãîäîâ â îòêðûòîé ëèòåðàòóðå ïî äèñêðåòíîìó ïðåäìåòó ïîÿâëÿëèñü òîëüêî îòäåëüíûå ññûëêè íà ðàáîòû è ìîíîãðàôèè, íî ÷àì äàëüøå, òåì ìåíüøå îíè ñîîòâåòñòâîâàëè ðåàëüíîìó ïîëîæåíèþ äåë. Ê êîíöó âîéíû ïåðåõîä ïîëíîñòüþ çàâåðøèëñÿ. Îòêðûòàÿ ëèòåðàòóðà ó÷åíûõ çà èñêëþ÷åíèåì îäíîãî çàìå÷íîãî èñêëþ÷åíèÿ, ðàáîòû Êëîäà Øýííîíà "The Communication Theory of Secrecy systems" (*Òåîðèÿ ñâÿçè ìåæäó ñåêðåòíûìè ñèñòåìàìè*), íàïå÷àòàííîé â 1949 ãîäó â *Bell System Technical Journal* [1432]. Ýòà ñòàòüÿ, êàê è ðàáîòà Ôðèäìàíà â 1918 ãîäó, ÿâèëàñü ðåçóëüòàòîì èññëåäîâàíèé Øýííîíà â âîåííîé Âòîðîé ìèðîâîé âîéíû. Ïîñëå îêîí÷àíèÿ Âòîðîé ìèðîâîé âîéíû íà áûëà ðàññåêðå÷åíà, âîçîáíîâ ïî îøèáêå.

Ñ 1949 ïî 1967 ëèòåðàòóðà ïî êðèïòîãðàôèè áûëà áåññîäåðæàòåëüíîé. Â 1967 ãîäó íà ïîïóëèðíûé äðóãîãî òèïà, èñòîðèêå Äýâèäà Êàíà *Äåøèôðîâùèêè* (*The Codebreakers*) [794]. Â ýòîé êíèãå íå áûëî íîâûõ èäåé, íî îíà ñîäåðæàëà äîñòàòî÷íî ïîëíóþ èñòîðèþ ïðåäìåòà, âêëþ÷àÿ óïîìèíàíèå î íåêîòîðûõ âåùàõ, âñå åùå çàñåêðå÷åííûõ ïðàâèòåëüñòâîì. Çíà÷åíèå *Äåøèôðîâùèêîâ* çàêëþ÷àëîñü íå òîëüêî â çíà÷èòåëüíîì îõâàòå ïðåäìåòà, êíèãà èìåëà çàìåòíûé êîììåð÷åñêèé óñïåõ è ïîçíàêîìèëà ñ êðèïòîãðàôèåé òûñ÷è ëþäåé, ðàíüøå è íå çàäóìûâàâøèõñÿ î åå ñóùåñòâîâàíèè. Òî÷íîüêèì ðó÷åêîì íà÷àëè ïîÿâëÿòüñÿ íîâûå ðàíûõ ïî êðèïòîãðàôèè.

Ïî÷òè â òî æå âðåìÿ Õîðñòà Ôåéñòåëà, ðàíåå ðàáîòàâøåãî íàä ïðèâîäîì "ñâîé/÷óæîé" äëÿ ÂÂÑ, íà âñþ äàëüíåéøóþ æèçíü îõâàòèëà ñòðàñòü ê êðèïòîãðàôèè, è îí ïðåøåë â ÓÒòñîíîâñêóþ Ëàáîðàòîðèþ ôèðìû IBM, ðàñïîëîæåííóþ â Éîðêòàóí Òàéíñ, Íüþ-Éîðê. Òàì îí íà÷àë ðàçðàáîòêó òîãî, ÷òî çàòåì ñòàíäàðòíî DES (U.S. Data Encryption Standard, Ñòàíäàðò øèôðîâàíèÿ äàííûõ Ñîâåòíåííûõ Øòàòîâ). Â íà÷àëå 70-õ ãîäîâ IBM îïóáëèêîâàëà ðÿä òåõíè÷åñêèõ îò÷åòîâ ïî êðèïòîãðàôèè, âûïîëíåííûõ Ôåéñòåëîì è åãî êîëëåãàìè [1482, 1484, 552].

Òàêîâî áûëî ïîëæåíèå, êîãäà â êîíöå 1972 ãîäà ÿ íà÷àë ðàáîòàòü â ýòîé îáëàñòè. Ëèòåðàòóðà ïî êðèïòîãðàôèè îáèëüíî íå áûëà, íî â íåé ìîæíî áûëî íàéòè ðÿä ñâåðêàþùèõ ñàìîñòîÿòåëüíî.

Â êðèïòîãðàôè÷åñêîé íàóêå åñòü îñíîâíîñòü, îòñóòñòâóþùàÿ â îáû÷íûõ àêàäåì è÷åñêèõ äèñöèïëèíàõ: íåîáõîäèìîñòü âçàèìîäåéſòâèÿ êðèïòîãðàôèè è êðèïòîàíàëèçà. Ïðè÷èíîé ýòîãî ÿâëÿåòñÿ òîñíóþ ñâÿçü ìåæäó íåêîòîðûìè ïðåäìåòàìè ê ïåðâàä÷å ðåàëüíîé èíôîðìàöèè, ñëåäîâàòåëüíî, íåòðóäíî ïðåäñêàçàòü, ðåøàþùóþ áîëåå îáøèðíûå çàäà÷è, ÷åì ïðîñòî ïðåäúÿâèòü çíà÷èìûé ôàêò - âîîáùå ðàçóìíóþ êðèïòîñèſòåìó, ðåøàþùóþ áîëåå îáøèðíûå çàäà÷è, ÷åì ïðîñòî ïðåäúÿâèòü çíà÷èìûé òåñòà â ÷åòíî. Â ðåçóëüòàòå çíà÷èòåëüíîé âîçðîñëî ÷èñëî ëþäåé, çíà÷èòåëüíî âîçðîñëî ÷èñëî ïóáëèêóåìûõ ðàáîò è ïîÿâèëîñü íåñêîëüêî íîâûõ êîìïàíèé, ïðåäëàãàþùèõ êîììåð÷åñêèå ñèſòåìû øèôðîâàíèÿ.

Êîãäà Ìàðòèí Õåëëìàí è ÿ â 1975 ãîäó ïðåäëîæèëè êðèïòîãðàôèþ ñ îòêðûòûì êëþ÷àìè [496], îäíèì èç êîñâåííûõ àñïåêòîâ íàøåãî ïðåäëîæåíèÿ áûëî ïîÿâëåíèå ïðîáëåì, ðåøåíèå êîòîðîé íå êàæåòñÿ ïðîñòûì. Òåîðåò ÷åñòíëþáèâûé ïðîêòèðîâùèê ìîã ñîçäàòü ÷òî-òî - âîîáíå ðàçóìíóþ êðèïòîſèſòåìó, ðåøàþùóþ áîëåå îáøèðíûå çàäà÷è, ÷åì ïðîſòîå ïðåâðàùåíèå çíà÷èìîãî òåſòà â ÷åòíî. Â ðåçóëüòàòå çíà÷èòåëüíî âîçðîſëî ÷èſëî ëþäåé, çàíèìàþùèõſÿ êðèïòîſðàôèåé, ÷èſëî ïðîſòî ïðåâðàùåíèå çíà÷èſòîãî òåſòà â ÷åòíî. Â ðåçóëüòàòå íåâîçìîæíî ñîðåâíîâàíèå, ÿâëÿþùåſÿ îſíîſ èç ſèſëüíåéſèſ ſòîſåſòâ ſèſòåſû êðèſòîſðàôèè, â êîſîſîſ ſòîſëüſî ſèſòåſû ſîſòîſòâóþſ.

Êîãäà Ìàðòèí Õåëëìàí è ÿ â 1975 ãîäó ïðåäëîæèëè êðèïòîãðàôèþ ñ îòêðûòûì êëþ÷àìè [496], îäíèì èç êîñâåííûõ àñïåêòîâ íàøåãî ïðåäëîæåíèÿ áûëî ïîÿâëåíèå ïðîáëåì, ðåøåíèå êîòîðîé íå êàæåòñÿ ïðîſòûì. Òåîðåò ÷åñòíëþáèâûé ïðîêòèðîâùèê ìîã ñîçäàòü ÷òî-òî - âîîáíå ðàçóìíóþ êðèïòîſèſòåſû, ðåøàþùóþ áîëåå îáøèðíûå çàäà÷è, ÷åì ïðîſòîå ïðåâðàùåíèå çíà÷èſòîãî òåſòà â ÷åſóſó. Â ðåçóëüòàòå çíà÷èſòåëüſî âſçðſſſëſ ÷èſëſ ëþäåé, çàíèſàþſèſſ êðèſòîſðàôèſåé, ÷èſëſ ſðſàſàùſåſ çíà÷èſòîſ òåſſòà â ÷åſóſó. Â ðåçóëüòàòå çíà÷èſòåſüſî âſçðſſſëſ ÷èſëſ ëþäåé, çàíèſàþſèſſ êðèſòîſðàôèſåé, ÷èſëſ ſðſàſàùſåſ çíà÷èſòîſ òåſſòà â ÷åſóſó. Â ðåçóëüòàòå íåâîçìîæíî ñîðåâíîâàíèå, ÿâëÿþùåſÿ îſíîſ èç ſèſëüſî ſèſòåſû ſîſòîſòâóþſ.

Â ðå÷è ïî ïîâîäó ïðèñóæäåíèÿ ìíå ñîâìåſòíî ſ Ìàðòèſîì Õåëëìàſîſ ſðåìèè Äîſàëüää Å. Ôèſêà (ſðèſóæäàåìſé çà ëó÷øóþ ſſÿſſèſòåëüſóſ ſòàòüþ â æóðſàëå IEEE) ÿ ſêàçàë, ÷òſ, íàſèſàâ "Privacy and Authentication" ("Ñåêðåòſſſòü è óáſſòſſâåðſåſà ſſäëèſſſſòè"), ÿ ſſëó÷èë ſſûò, êſòſðóſ ſåſáû÷åſ äàæå äëÿ âûäàþſùèſſ ó÷åſûſ, ſſëó÷èâøèſ ſðåſèè IEEE. ß ſàſèſñàë ſòàòüþ, êſòſðóſ ÿ õſòåë áû èçó÷èòü, êſãääà ÿ âſåðåûå ſåðüſſſſ çàèſòåðåſſâàëſÿ êðèſòſðàôèſåé, è êſòſðóſ ſå ſſſſ ſàéòè. Åſëè áû ÿ ſåãſàſÿ ſòſſðàâèſſÿ â Ñòýſôſðäſêóſ áèáëèſòàêó è ſſáðàë áû ſſâðåſſåſſûå ðàáſòû ſſ êðèſſòſðàôèè, ÿ, âſçſſſſſ, ſſëó÷èë áſ ſðåäſſòàâëſſèſ ſ ſðåſſåſòå ſſðàçſſ ðàſüøå. Íſ ſñåſüþ 1972 ãſäà áſëè äſñòóſſſ òſëüêſ ſåſêſëüêſ êëàſſè÷åſêèſ ðàáſò è ðÿä òóſàſſſûſ òåſſſè÷åſêèſ ſò÷åſòſâ.

Ó ſåãſäſÿøſåãſ èſſſëåäſâàòåëÿ ſåò òàêſé ſðſáëåſû. Ñåãſäſÿ ſſſſâſàÿ ſëſæſſſſòü ſſſòſèò â âûáſðå, ſ ÷åãſ

íà÷àòü ñðåäè òûñÿ÷ ñòàòåé è äåñÿòêîâ êíèã. À ñåãîäíÿøíèå ïðîãðàììèñòû è èíæåíåðû, êîòîðûå ïðîñòî õîòÿò èñïîëüçîâàòü êðèïòîãðàôèþ? Ê êàêèì èñòî÷íèêàì èì îáðàùàòüñÿ? Äî ñèõ ïîð íåîáõîäèìî áûëî ïðîâîäèòü äîëãèå ÷àñû, âûèñêèâàÿ íàó÷íóþ ëèòåðàòóðó è èçó÷àÿ åå, ïðåæäå ÷åì óäàâàëîñü íà÷àòü ðàçðàáîòêó êðèïòîãðàôè÷åñêèõ ïðèëîæåíèé, òàê ãëàäêî îïèñàííûõ â ïîïóëÿðíûõ ñòàòüÿõ.

Èìåííî ýòîò ïðîìåæóòîê è ïðèçâàíà çàïîëíèòü *Ïðèêëàäíàÿ êðèïòîãðàôèÿ* Áðþñà Øíàéåðà. Íà÷àâ ñ öåëåé çàñåêðå÷èâàíèÿ ïåðåäà÷è äàííûõ è ýëåìåíòàðíûõ ïðèìåðîâ ïðîãðàìì äëÿ äîñòèæåíèÿ ýòèõ öåëåé, Øíàéåð ðàçâîðà÷èâàåò ïåðåä íàìè ïàíîðàìó ðåçóëüòàòîâ 20 ëåò îòêðûòûõ èññëåäîâàíèé. Ñîäåðæàíèå êíèãè ïîëíîñòüþ îïðàâäûâàåò åå íàçâàíèåì, âû íàéäåòå â íåé îïèñàíèå ðàçëè÷íûõ ïðèëîæåíèé, îò çàñåêðå÷èâàíèÿ òåëåôîííîãî ðàçãîâîðà äî ýëåêòðîííûõ äåíåã è êðèïòîãðàôè÷åñêîãî îáåñïå÷åíèÿ âûáîðîâ.

Íå óäîâëåòâîðåííûé ïðîñòûì èçëîæåíèåì àëãîðèòìîâ è îïèñàíèåì êîäà, Øíàéåð âêëþ÷èë â êíèãó îáñóæäåíèå ðàçëè÷íûõ ìèðîâûõ îðãàíèçàöèé, ñâÿçàííûõ ñ ðàçðàáîòêîé è ïðèìåíåíèåì êðèïòîãðàôè÷åñêèõ ñðåäñòâ, îò Ìåæäóíàðîäíîé àññîöèàöèè êðèïòîëîãè÷åñêèõ èññëåäîâàíèé äî NSA (National Security Agency, Àãåíòñòâî íàöèîíàëüíîé áåçîïàñíîñòè).

Êîãäà íà ðóáåæå 70-õ è 80-õ ãîäîâ âîçðîñ îáùåñòâåííûé èíòåðåñ ê êðèïòîãðàôèè, NSA, îôèöèàëüíûé êðèïòîãðàôè÷åêèé îðãàí ÑØÀ, ïðåäïðèíÿëî ðÿä ïîïûòîê ïîäàâèòü ýòîò èíòåðåñ. Ïåðâîé òàêîé ïîïûòêîé áûëî ïèñüìî ñîòðóäíèêà NSA, ïî âèäèìîìó äåéñòâîâàâøåãî ïî ñâîåìó óñìîòðåíèþ. Ïèñüìî áûëî ïîñëàíî â IEEE è ïðåäóïðåæäàëî, ÷òî ïóáëèêàöèÿ ìàòåðèàëîâ ïî êðèïòîãðàôèè ÿâëÿåòñÿ íàðóøåíèåì Ïðàâèë ìåæäóíàðîäíîé ïðîäàæè îðóæèÿ (International Traffic in Arms Regulations, ITAR). Ýòà òî÷êà çðåíèÿ, êàê îêàçàëîñü, íå ïîääåðæèâàåìàÿ ñàìèìè ïðàâèëàìè, â ÿâíîì âèäå ñîäåðæàùèìè ëüãîòû äëÿ ïóáëèêóåìûõ ìàòåðèàëîâ, ñîçäàëà íåîæèäàííóþ ðåêëàìó èñïîëüçîâàíèþ êðèïòîãðàôèè è Ñåìèíàðó ïî òåîðèè èíôîðìàöèè 1977 ãîäà.

Áîëåå ñåðüåçíàÿ ïîïûòêà áûëà ïðåäïðèíÿòà â 1980 ãîäó, êîãäà NSA ôèíàíñèðîâàëî èçó÷åíèå âîïðîñà Àìåðèêàíñêèì ñîâåòîì ïî îáðàçîâàíèþ ñ öåëüþ óáåäèòü Êîíãðåññ óçàêîíèòü êîíòðîëü íàä ïóáëèêàöèÿìè â îáëàñòè êðèïòîãðàôèè. Ðåçóëüòàòû, îêàçàâøèåñÿ äàëåêèìè îò îæèäàíèé NSA, ïðèâåëè ê ïðîãðàììå äîáðîâîëüíîãî ðåöåíçèðîâàíèÿ ðàáîò ïî êðèïòîãðàôèè. Îò èññëåäîâàòåëåé ïîòðåáîâàëè ïåðåä ïóáëèêàöèåé çàïðàøèâàòü ìíåíèå NSA, íå ïðèíåñåò ëè ðàñêðûòèå ðåçóëüòàòîâ èññëåäîâàíèé âðåä íàöèîíàëüíûì èíòåðåñàì.

Ê ñåðåäèíå 80-õ ãîäîâ îñíîâíûì îáúåêòîì âíèìàíèÿ ñòàëà íå òåîðèÿ, à ïðàêòèêà êðèïòîãðàôèè. Ñóùåñòâóþùèå çàêîíû äàþò NSA ïðàâî ñ ïîìîùüþ Ãîñäåïàðòàìåíòà ðåãóëèðîâàòü ýêñïîðò êðèïòîãðàôè÷åñêîãî îáîðóäîâàíèÿ. Òàê êàê áèçíåñ âñå áîëüøå è áîëüøå ïðèíèìàåò ìåæäóíàðîäíûé õàðàêòåð è àìåðèêàíñêàÿ ÷àñòü ìèðîâîãî ðûíêà óìåíüøàåòñÿ, âîçðàñòàåò æåëàíèå èñïîëüçîâàòü åäèíûé ïðîäóêò è äëÿ âíóòðåííåãî, è äëÿ âíåøíåãî ðûíêà. Òàêèå ïðîäóêòû ÿâëÿþòñÿ ñóáúåêòàìè êîíòðîëÿ íàä ýêñïîðòîì, è ïîýòîìó NSA ïîëó÷èëî âîçìîæíîñòü êîíòðîëèðîâàòü íå òîëüêî ýêñïîðòèðóåìûå êðèïòîãðàôè÷åñêèå ïðîäóêòû, íî è ïðîäàâàåìûå â Ñîåäèíåííûõ Øòàòàõ.

Â òî âðåìÿ, êîãäà ïèñàëèñü ýòè ñòðîêè, âîçíèêëî íîâîå ïðåïÿòñòâèå äëÿ îáùåñòâåííîãî èñïîëüçîâàíèÿ êðèïòîãðàôèè. Ïðàâèòåëüñòâî äîïîëíèëî øèðîêî îïóáëèêîâàííûé è èñïîëüçóåìûé àëãîðèòì DES çàñåêðå÷åííûì àëãîðèòìîì, ðåàëèçîâàííûì â ìèêðîñõåìàõ ïàìÿòè, íåçàâèñÿùåé îò âðåìåíè. Ýòè ìèêðîñõåìû áóäóò ñîäåðæàòü êîäèôèöèðîâàííûé ìåõàíèçì ïðàâèòåëüñòâåííîãî êîíòðîëÿ. Îòðèöàòåëüíûå àñïåêòû òàêîé ïðîãðàììû-òðîÿíñêîãî êîíÿ ïðîñòèðàþòñÿ îò ïîòåíöèàëüíî ãóáèòåëüíîãî ðàñêðûòèÿ òàéíû ëè÷íîñòè äî âûñîêîé ñòîèìîñòè àïïàðàòíîé ìîäåðíèçàöèè ïðîäóêòîâ, ðàíåå ðåàëèçîâàííûõ ïðîãðàììíî. Òàêèì îáðàçîì, ïðåäëàãàåìîå íîâîââåäåíèå íå âûçâàëî ýíòóçèàçìà è ïîäâåðãëîñü øèðîêîé êðèòèêå, îñîáåííî ñî ñòîðîíû íåçàâèñèìûõ êðèïòîãðàôîâ. Ðÿä ëþäåé, îäíàêî, âèäÿò ñâîå áóäóùåå â ïðîãðàììèðîâàíèè, à íå â ïîëèòèêå è óäâàèâàþò ñâîè óñèëèÿ, ñòðåìÿñü ïðåäîñòàâèòü ìèðó ìîùíûå ñðåäñòâà êðèïòîãðàôèè.

Çíà÷èòåëüíîå îòñòóïëåíèå îò âîçìîæíîñòè òîãî, ÷òî çàêîí î êîíòðîëå íàä ýêñïîðòîì îòìåíèò Ïåðâóþ ïîïðàâêó[1], êàçàëîñü áûëî ñäåëàí â 1980 ãîäó, êîãäà â îïóáëèêîâàííûå â *Federal Register* èñïðàâëåíèÿ ITAR âîøëî ñëåäóþùåå ïîëîæåíèå: "...ïîëîæåíèå áûëî äîáàâëåíî ñ öåëüþ ïîêàçàòü, ÷òî ðåãóëèðîâàíèå ýêñïîðòà òåõíè÷åñêèõ äàííûõ íå ïðèâîäèò ê êîíôëèêòó ñ ïðàâàìè ëè÷íîñòè, îïðåäåëÿåìûìè Ïåðâîé ïîïðàâêîé". Íî òî, ÷òî êîíôëèêò ìåæäó Ïåðâîé ïîïðàâêîé è çàêîíàìè î êîíòðîëå íàä ýêñïîðòîì íå ðàçðåøåí îêîí÷àòåëüíî, äîëæíî áûòü î÷åâèäíî èç çàÿâëåíèé, ñäåëàííûõ íà êîíôåðåíöèè, ïðîâîäèìîé RSA Data Security. Ïðåäñòàâèòåëü NSA èç îòäåëà êîíòðîëÿ íàä ýêñïîðòîì âûðàçèë ìíåíèå, ÷òî ëþäè, ïóáëèêóþùèå êðèïòîãðàôè÷åñêèå ïðîãðàììû, íàõîäÿòñÿ " â ñåðîé çîíå" ïî îòíîøåíèþ ê çàêîíó. Åñëè ýòî òàê, òî èìåííî ýòó "ñåðóþ çîíó" íåìíîãî îñâåòèëî ïåðâîå èçäàíèå ýòîé êíèãè. Ýêñïîðò ïðèëîæåíèé äëÿ ýòîé êíèãè áûë ðàçðåøåí ñ ïîäòâåðæäåíèåì òîãî, ÷òî îïóáëèêîâàííûå ìàòåðèàëû íå ïîïàäàþò ïîä þðèñäèêöèþ Ñîâåòà ïî êîíòðîëþ íàä âîîðóæåíèåì. Îäíàêî, ýêñïîðòèðîâàòü îïóáëèêîâàííûå ïðîãðàììû íà äèñêå áûëî çàïðåùåíî.

Èçìåíåíèå ñòðàòåãèè NSA îò ïîïûòîê êîíòðîëèðîâàòü êðèïòîãðàôè÷åñêèå èññëåäîâàíèÿ ê óñèëåíèþ ðåãóëèðîâàíèÿ â îáëàñòè ðàçðàáîòêè è ðàçâåðòûâàíèÿ êðèïòîãðàôè÷åñêèõ ïðîäóêòîâ ïî âèäèìîìó îáóñëîâëåíî îñîçíàíèåì òîãî, ÷òî âñå âåëè÷àéøèå êðèïòîãðàôè÷åñêèå ðàáîòû íå çàùèòèëè íè îäíîãî áèòà èíôîðìàöèè. Áóäó÷è

---

[1] Ê êîíñòèòóöèè ÑØÀ

ïîñòàâëåí â øêàô, ýòîò òî ì íå ñäåëàåò íè÷åãî íîâîãî ïî ñðàâíåíèþ ñ ïðåäøåñòâóþùèìè êíèãàìè è ðàáîòàìè, íî èñïîëüçîâàíèå åãî ñîäåðæàíèÿ íà ðàáî÷åé ñòàíöèè, ãäå ïèøåòñÿ êðèïòîãðàôè÷åñêèé êîä, ìîæåò ïðèâåñòè ê èíîì ðåçóëüòàòó.

Óèòôèëä Äèôôè

Ì àóíòýéí Âüþ, Êàëèôîðíèÿ.

Ââåäåíèå

Êðèïòîãðàôèÿ áûâàåò äâóõ òèïîâ: êðèïòîãðàôèÿ, êîòîðàÿ ïîìåøàåò ÷èòàòü âàøè ôàéëû âàøåé ìëàäøåé ñåñòðå, è êðèïòîãðàôèÿ, êîòîðàÿ ïîìåøàåò ÷èòàòü âàøè ôàéëû äÿäÿì èç ïðàâèòåëüñòâà. Ýòà êíèãà î âòîðîì òèïå êðèïòîãðàôèè.

Åñëè ÿ áåðó ïèñüìî, êëàäó åãî â ñåéô ãäå-íèáóäü â Íüþ-Éîðêå, çàòåì âåëþ Âàì ïðî÷èòàòü ýòî ïèñüìî, òî ýòî íå áåçîïàñíîñòü. Ýòî íåïîíÿòíî ÷òî. Ñ äðóãîé ñòîðîíû, åñëè ÿ áåðó ïèñüìî è êëàäó åãî â ñåéô, çàòåì ïåðåäàþ ýòîò ñåéô Âàì âìåñòå ñ äåòàëüíûì îïèñàíèåì, ïåðåäàþ òàêæå ñîòíþ ïîäîáíûõ ñåéôîâ ñ èõ êîìáèíàöèÿìè, ÷òîáû Âû è ëó÷øèå "ìåäâåæàòíèêè" ìèðà ìîãëè èçó÷èòü ñèñòåìó çàìêîâ, à âû âñå ðàâíî íå ñìîæåòå îòêðûòü ñåéô è ïðî÷èòàòü ïèñüìî - âîò ýòî è åñòü áåçîïàñíîñòü.

Â òå÷åíèå ìíîãèõ ëåò ýòîò òèï êðèïòîãðàôèè èñïîëüçîâàëñÿ èñêëþ÷èòåëüíî â âîåííûõ öåëÿõ. Àãåíòñòâî íàöèîíàëüíîé áåçîïàñíîñòè Ñîåäèíåííûõ Øòàòîâ Àìåðèêè (National Security Agency, NSA) è åãî àíàëîãè â áûâøåì Ñîâåòñêîì Ñîþçå, Àíãëèè, Ôðàíöèè, Èçðàèëå è ïðî÷èõ ñòðàíàõ òðàòèëè ìèëëèàðäû äîëëàðîâ íà î÷åíü ñåðüåçíóþ èãðó â îáåñïå÷åíèå áåçîïàñíîñòè ñîáñòâåííûõ ëèíèé ñâÿçè, îäíîâðåìåííî ïûòàÿñü âçëîìàòü âñå îñòàëüíûå. Îòäåëüíûå ëè÷íîñòè, îáëàäàþùèå çíà÷èòåëüíî ìåíüøèìè ñðåäñòâàìè è îïûòîì, áûëè áåñïîìîùíû çàùèòèòü ñâîè ñåêðåòû îò ïðàâèòåëüñòâà.

Â òå÷åíèå ïîñëåäíèõ 20 ëåò çíà÷èòåëüíî âûðîñ îáúåì îòêðûòûõ àêàäåìè÷åñêèõ èññëåäîâàíèé. Ïîêà îáû÷íûå ãðàæäàíå èñïîëüçîâàëè êëàññè÷åñêóþ êðèïòîãðàôèþ, ñî âðåìåí Âòîðîé ìèðîâîé âîéíû êîìïüþòåðíàÿ êðèïòîãðàôèÿ âî âñåì ìèðå ïðèìåíÿëàñü èñêëþ÷èòåëüíî â âîåííîé îáëàñòè. Ñåãîäíÿ èñêóññòâî êîìïüþòåðíîé êðèïòîãðàôèè âûðâàëîñü èç ñòåí âîåííûõ âåäîìñòâ. Íåïðîôåññèîíàëû ïîëó÷èëè âîçìîæíîñòü ñðåäñòâà, ïîçâîëÿþùèå èì îáåçîïàñèòü ñåáÿ îò ìîãóùåñòâåííåéøèõ ïðîòèâíèêîâ, ñðåäñòâà, îáåñïå÷èâàþùèå çàùèòó îò âîåííûõ âåäîìñòâ.

À íóæíà ëè îáû÷íîìó ÷åëîâåêó òàêàÿ êðèïòîãðàôèÿ? Äà. Ëþäè ìîãóò ïëàíèðîâàòü ïîëèòè÷åñêóþ êàìïàíèþ, îáñóæäàòü íàëîãè, âåñòè íåçàêîííûå äåéñòâèÿ. Îíè ìîãóò ðàçðàáàòûâàòü íîâûå èçäåëèÿ, îáñóæäàòü ðûíî÷íóþ ïîëèòèêó èëè ïëàíèðîâàòü çàõâàò êîíêóðèðóþùåé ôèðìû. Îíè ìîãóò æèòü â ñòðàíå, êîòîðàÿ íå ñîáëþäàåò çàïðåòà íà âòîðæåíèå â ëè÷íóþ æèçíü ñâîèõ ãðàæäàí. Îíè ìîãóò äåëàòü ÷òî-ëèáî, ÷òî íå êàæåòñÿ èì íåçàêîííûì, õîòÿ òàêîâûì è ÿâëÿåòñÿ. Ïî ìíîãèì ïðè÷èíàì äàííûå è ëèíèè ñâÿçè äîëæíû áûòü ëè÷íûìè, òàéíûìè è çàêðûòûìè îò ïîñòîðîííåãî äîñòóïà.

Ýòà êíèãà âûõîäèò â ñâåò â áåñïîêîéíîå âðåìÿ. Â 1994 ãîäó àäìèíèñòðàöèÿ Êëèíòîíà ïðèíÿëà Ñòàíäàðò óñëîâíîãî øèôðîâàíèÿ (Escrowed Encryption Standard), âêëþ÷àÿ ìèêðîñõåìó Clipper è ïëàòó Fortezza, è ïðåâðàòèëè Áèëëü î Öèôðîâîé òåëåôîíèè â çàêîí. Ýòè èíèöèàòèâû ïûòàþòñÿ óâåëè÷èòü âîçìîæíîñòè ïðàâèòåëüñòâà ïðîâîäèòü ýëåêòðîííûé êîíòðîëü.

Âñòóïàþò â ñèëó íåêîòîðûå îïàñíåéøèå äîìûñëû Îðóýëëà: ïðàâèòåëüñòâî ïîëó÷àåò ïðàâî ïðîñëóøèâàòü ëè÷íûå ïåðåãîâîðû, à ñ ÷åëîâåêîì, ïûòàþùèìñÿ ñêðûòü ñâîè ñåêðåòû îò ïðàâèòåëüñòâà, ìîæåò ÷òî-íèáóäü ñëó÷èòüñÿ. Çàêîíîäàòåëüñòâî âñåãäà ðàçðåøàëî ñëåæêó ïî ðåøåíèþ ñóäà, íî âïåðâûå ëþäè ñàìè äîëæíû ïðåäïðèíèìàòü êàêèå-òî øàãè, ÷òîáû *ñäåëàòüñÿ äîñòóïíûìè* äëÿ ñëåæêè. Ýòè èíèöèàòèâû íå ïðîñòî ïðåäëîæåíèÿ ïðàâèòåëüñòâà â íåêîé òóìàííîé ñôåðå, ýòî óïðåæäàþùàÿ è îäíîñòîðîííÿÿ ïîïûòêà ïðèñâîèòü ïðåæäå ïðèíàäëåæàùèå ëþäÿì ïðàâà.

Çàêîíîïðîåêòû î ìèêðîñõåìå Clipper è Öèôðîâîé òåëåôîíèè íå ñïîñîáñòâóþò ñîõðàíåíèþ òàéíû, íî áåñïî÷âåííî çàñòàâëÿþò ëþäåé ñ÷èòàòü, ÷òî ïðàâèòåëüñòâî óâàæàåò èõ òàéíû. Òå æå ñàìûå âëàñòè, êîòîðûå íåçàêîííî çàïèñûâàëè òåëåôîíû Ìàðòèíà Ëþòåðà Êèíãà, ìîãóò ëåãêî ïðîñëóøàòü òåëåôîí, çàùèùåííûé ìèêðîñõåìîé Clipper. Â íåäàâíåì ïðîøëîì ïîëèöåéñêèå âëàñòè íà ìåñòàõ áûëè ïðèâëå÷åíû ê ãðàæäàíñêîé èëè óãîëîâíîé îòâåòñòâåííîñòè çà íåçàêîííîå ïðîñëóøèâàíèå âî ìíîãèõ ñóäàõ - â Ìýðèëåíäå, Êîííåêòèêóòå, Âåðìîíòå, Äæîðäæèè, Ìèññóðè è Íåâàäå. Èäåÿ ðàçâåðíóòü òåõíîëîãèþ, êîòîðàÿ ìîæåò ïðèâåñòè ê ïîÿâëåíèþ ïîëèöåéñêîãî ãîñóäàðñòâà - ýòî ïëîõàÿ èäåÿ.

Äåëî â òîì, ÷òî íåäîñòàòî÷íî çàùèòèòü ñåáÿ çàêîíàìè, íàì íóæíî çàùèòèòü ñåáÿ ìàòåìàòèêîé. Øèôðîâàíèå èìååò ñëèøêîì áîëüøîå çíà÷åíèå, ÷òîáû îñòàâèòü åå èñïîëüçîâàíèå òîëüêî ïðàâèòåëüñòâàì.

Ýòà êíèãà ñíàáäèò Âàñ èíñòðóìåíòàðèåì, ïîçâîëÿþùèì çàùèòèòü âàøè òàéíû. Ïåðåäà÷à êðèïòîãðàôè÷åñêèõ ïðîäóêòîâ ìîæåò áûòü îáúÿâëåíà íåçàêîííîé, ïåðåäà÷à èíôîðìàöèè - íèêîãäà.

Êàê ÷èòàòü ýòó êíèãó

ß íàïèñàë *Ïðèêëàäíóþ êðèïòîãðàôèþ* êàê æèâîå ââåäåíèå â êðèïòîãðàôèþ è êàê âñåîáúåìëþùèé ñïðàâî÷íèê. ß ïûòàëñÿ ñî÷åòàòü ÷èòàåìîñòü òåêñòà ñ æåðòâåííîé òî÷íîñòüþ, íî ýòà êíèãà ïèñàëàñü íå êàê ìàòåìàòè÷åñêàÿ ðàáîòà. Õîòÿ ÿ íå èñêàæàë èíôîðìàöèþ óìûøëåííî, òîðîïÿñü, ÿ îïóñêàë òåîðèþ. Äëÿ èíòåðåñóþùèõñÿ òåîðåòè÷åñêèìè âûêëàäêàìè ïðèâåäåíû îáøèðíûå ññûëêè íà àêàäåìè÷åñêóþ ëèòåðàòóðó.

Ãëàâà 1 ïðåäñòàâëÿåò ñîáîé ââåäåíèå â êðèïòîãðàôèþ, îïèñûâàåò ìíîæåñòâî òåðìèíîâ, â íåé êðàòêî ðàñ-

ñìàòðèâàåòñÿ äîêîìåíòàëüíàÿ êðèïòîãðàôèÿ.

Ãëàâû ñî 2 ïî 6 (×àñòü I) îïèñûâàþò êðèïòîãðàôè÷åñêèå ïðîòîêîëû - ÷òî ëþäè ìîãóò ñäåëàòü ñ ïîìîùüþ êðèïòîãðàôèè - îò ïðîñòûõ (ïåðâàÿ øèôðîâàííûõ ñîîáùåíèé îò îäíîãî ÷åëîâåêà äðóãîìó) äî ñëîæíûõ (ùåëåâûå ìîíåòíûé ïðîòîêîë) è òàéíûõ (ñåêðåòíûå è àíîíèìíûå îáùåíèå ýëåêòðîííûõ äåíåã). Íåêîòîðûå èç ýòèõ ïðîòîêîëîâ î÷åíèâû, äðóãèå - óäèâèòåëüíû. Ì íîæåñòâî ëþäåé è íå ïðåäñòàâëÿåò ìíîãèå èç ïðîáëì, êîòîðûå ìîæåò ðåøèòü êðèïòîãðàôèÿ.

Ãëàâû ñ 7 ïî 10 (×àñòü II) ñîäåðæàò îñíóæäåíèå ìåòîäîâ êðèïòîãðàôèè. Âñå ýòè ÷åòûðå ãëàâû âàæíû äëÿ ñàìûõ ðàñïðîñòðàíåííûõ ïðèìåíåíèé êðèïòîãðàôèè. Â ãëàâàõ 7 è 8 ðàññêàçûâàåòñÿ î êëþ÷àõ: êàê îíè äîëæíû áûòü äëèíà áûòü çàçîðàííîãî êëþ÷à, êàê ãåíåðèðîâàòü, õðàíèòü è ðàñïðåäåëÿòü êëþ÷è, è ò.ä. Óïðàâëåíèå êëþ÷àìè ïðåäñòàâëÿåò ñîáîé òðóäíóþ çàäà÷ó, êîòîðóþ ìû áóäåì îáñóæäàòü â ñëåäóþùèõ äâóõ ãëàâàõ. Â ãëàâå 9 ðàññìàòðèâàþòñÿ ðàçëè÷íûå ñïîñîáû ëîãè÷åñêîãî óñèëåíèÿ êðèïòîãðàôè÷åñêèõ àëãîðèòìîâ, à ãëàâà 10 îïèñûâàåò îñíîâíûå è öåëè èñïîëüçîâàíèÿ ýòèõ äëãîðèòìîâ - êàê èõ âûáèðàòü, ðåàëèçîâûâàòü è ïðèìåíÿòü.

Ãëàâû ñ 11 ïî 23 (×àñòü III) îïèñûâàþò ýòè àëãîðèòìû. Ãëàâà 11 ïðåäñòàâëÿåò ñîáîé ìàòåìàòè÷åñêóþ áàçó è ÿâëÿþòñÿ îáÿçàòåëüíîé òî÷êîé, åñëè âû èíòåðåñóåòåñü äëãîðèòìàìè ñ îòêðûòûì êëþ÷àìè. Åñëè âû ñîáèðàåòåñü èñïîëüçîâàòü DES (èëè ÷òî-òî ïîõîæåå), åå ìîæíî ïðîïóñòèòü. Â ãëàâå 12 îáñóæäàþòñÿ àëãîðèòì DES, åãî èñòîðèÿ, áåçîïàñíîñòü è ðàçíîâèäíîñòè. Â ãëàâàõ 13, 14 è 15 ðàññêàçûâàþòñÿ î äðóãèõ áîë÷îíûõ àëãîðèòìàõ. Åñëè âàì íóæíî ÷òî-òî áîëåå íàäåæíîå ÷åì DES, ñðàçó ïåðåõîäèòå ê ðàçäåëó î IDEA è òðîéíîì DES. Ïðè æåëàíèè óçíàòü î âðóïîå àëãîðèòìàõ, íåêîòîðûå èç êîòîðûõ ìîãóò áûòü áåçîïàñíû DES, ïðî÷èòàéòå âñþ ãëàâó. Â ãëàâàõ 16 è 17 îáñóæäàþòñÿ ïîòîêîâûå àëãîðèòìû. Â ãëàâå 18 ïîäðîáíî ðàññìàòðèâàþòñÿ îäíîíàïðàâëåííûå õýø-ôóíêöèè, ñðåäè êîòîðûõ ñàìûå ïîïóëÿðíûå MDS è SHA, õîòÿ ÿ îñòàâëèâàþ è íà ìîìåíò íàïèñàíèÿ ýòèõ ñòðîê íåêîòîðûå èç íèõ ñ÷èòàþòñÿ ñëîìàííûìè. Â ãëàâå 19 ðàññìàòðèâàþòñÿ àëãîðèòìû øèôðîâàíèÿ ñ îòêðûòûì êëþ÷îì, à â ãëàâå 20 - àëãîðèòìû öèôðîâîé ïîäïèñè ñ îòêðûòûì êëþ÷îì. Â ãëàâå 21 îáñóæäàþòñÿ àëãîðèòìû èäåíòèôèêàöèè ñ îòêðûòûì êëþ÷îì, à â ãëàâå 22 - àëãîðèòìû îáìåíà ñ îòêðûòûì êëþ÷îì. Ñàìûì âàæíûì ÿâëÿþòñÿ àëãîðèòìû RSA, DSA, Ôèàò-Øàìèðà (Fiat-Shamir) è Äèôôè-Õåëëìàíà (Diffie-Hellman). Ãëàâà 23 ñîäåðæèò ðÿä ýçîòåðè÷åñêèõ àëãîðèòìîâ è ïðîòîêîëîâ ñ îòêðûòûì êëþ÷îì, ìàòåìàòèêà â ýòîé ãëàâå äîñòàòî÷íî ñëîæíà, òàê ÷òî ïðèñòóïàéòå ðåøèòü.

Ãëàâû 24 è 25 (×àñòü IV) ïåðåíîñÿò âàñ ðåàëüíûé ìèð êðèïòîãðàôèè. Â ãëàâå 24 îáñóæäàþòñÿ íåêîòîðûå ñîâðåìåííûå ïðèìåíåíèÿ àëãîðèòìîâ è ïðîòîêîëîâ, â òî âðåìÿ êàê ãëàâà 25 êàñàåòñÿ íåêîòîðûõ ïîëèòè÷åñêèõ àñïåêòîâ êðèïòîãðàôèè. Íåñìîòðÿ íà ïîñëåäíþþ ãëàâó, ýòè ãëàâû äîñòàòî÷íî ðåëåâàíòíû è íà ìíîãèõ äóãèõ.

Â êíèãó òàêæå âêëþ÷åíû êîäû 10 àëãîðèòìîâ, ðàññìîòðåííûõ â ×àñòè III. ß íå ñìîã âêëþ÷èòü âñþ êîä, êîòîðûé õîòåë, èç-çà åãî áîëüøîãî îáúåìà, êðîìå òîãî, êðèòè÷åñêèé êîäû â ëþáîì ñëó÷àå íåëüçÿ ýêſïîðòèðîâàòü. (Ëþáîïûòíî, ÷òî Äîñåäîàðòàìåíò ðàçðåøèë ýêſïîðòèðîâàòü ïððîâ èçäàíèå ýòîé êíèãè ñ èñõîäíûì êîäîì, íî íå ðàçðåøèë ýêſïîðòèðîâàòü êîì ïüþòåðíûé äiñê ñ òàì æå èñõîäíûì êîäàìè. Ñì îðð ðèñóíê.) Ñîòðåòñòâóþùèé íàáîð äiñê îñõîäíûì êîäîì ñîäåðæèò ñóùåñòâåííî áîëüøå èñõîäíûõ êîäîâ, ÷åì ÿ ñì îã âêëþ÷èòü â ýòó êíèãó, âîçìîæíî, ýòî ñàìàÿ áîëüøàÿ ïîäâîðêà êðèïòîãðàôè÷åñêèõ èñõîäíûõ êîäîâ, ïîÿâèøàÿñÿ çà ïðåäåëàìè âåêîâûõ åäâ ì ñòáó ïåðåñëàòü ìåíÿ îñòàâèòü ì íîãî ïðåäïîëîæåíèé ðàçíûõ çà ïðåäåëàìè ýòîé êíèãè, ÿ âêëþ÷èë òå òåì, êîòîðûå ì íå ïîêàçàëèñü âàæíûì è, ïî ìíåíèþ ì íåñêîëüêèõ äðóçåé, ïîëåçíûìè. Ñðåä÷àñ ÿ ì îãó ïðåäñëàòü ýòè äèñêè ñ èñõîäíûì êîäîì ì íåêîòîðûì ëþäÿì, äîáàâèâ ñâîè ñîáñòâåííûå ñ êàêèì-ëèáî äiñê èçìåíèòñÿ. Åñëè ÿ íå ì îãó ïðîäîëæèòü îòâàòüñÿ íà ïîñëåäíèå ñòðàíèöû ñ êàêèì-íèáóäü âîïðîñîì, ÿ ðåêîìåíäóþ ïðîñòî ïðîïóñòèòü ýòè äèñêè..

Ê íåäîñòàòêàì ýòîé êíèãè îòíîñèòñÿ òî, ÷òî èç-çà åå ýíöèêëîïåäè÷åñêîé ïðèðîäû ïîñòðàäàëà ÷èòàåìîñòü êíèãè. ß õîòåë íàïèñàòü åäèíûé ñïðàâî÷íèê ïî ïîñëåäíåé ñòðàíèöå ýòîé êíèãè, ÷òîáû ÿ ìîã ïîêàçàòü, êàê ìíîãî ïîíÿòèé ÿ ïîçàèìſòâîâàë ó äðóãèõ ëþäåé. Âïåðâûå âñå ìíîæåñòâî ñäåëàííîãî â êðèïòîãðàôèè ñîáðàíî â îäíîì ìåñòå, è çàðàíåå èçâèíÿþñü ïåðåä òåì, êòî ðàçûñêèâàåò ó÷åíûå ïîñîáèå. Âïåðâûå âñå ìíîæåñòâî ñäåëàííîãî â êðèïòîãðàôèè ñîáðàíî ïîä îäíîé îáëîæêîé. Íåñìîòðÿ íà ýòî, ñîîáùåíèÿ îá ýòèõ ñòðàíàõ, íî, âîçìîæíî, êîãäà-íèáóäü âñå èçìåíèòñÿ. Åñëè âû ñîáèðàåòåñü èñïîëüçîâàòü èëè ïîñòðîèòü íà ïîñëåäíåé ñòðàíèöå ýòîé êíèãè, ÿ âêëþ÷èë òå òåì, êòî ïðèñûëàåò ìíå ñîîáùåíèÿ.

Áëàãîäàðíîñòè

Ïåðå÷íþ ëþäåé, ïðèíåñøèõ ðóêó ê ñîçäàíèþ ýòîé êíèãè, ìîæåò ïîêàçàòüñÿ áåñêîíå÷íûì, íî âñå îíè äîñòîéíû óïîìèíàíèÿ. Ì íå õîòåëîñü áû ïîáëàãîäàðèòü Äîíà Àëüâàðåñà (Don Alvarez), Ðîññà Àíäåðñîíà (Ross Anderson), Äýéâà Áåëåíñîíà (Dave Balenson), Êàðëà Áàðìñà (Karl Barms), Ñòèâà Áåëëîâèíà (Steve Bellovin), Äýíà Áåðíſòàéíà (Dan Bernstein), Ýëë Áèãàì (Ell Biham), Äæîàí Áîÿð (Joan Boyar), Êàðåí Êóïåð (Karen Cooper), Âèòà Äèôôè (Whit Diffie), Äæîàí Ôåéãåíáàóì (Joan Feigenbaum), Ôèëà Êàíà (Phil Karn), Íèëà Êîáëèöà (Neal Koblitz), Êñóåéà Ëàé (Xuejia Lai), Òîì Ëåðàíòà (Tom Leranth), Ìàéêà Ìàðêîâèöà (Mike Markowitz), Ðàëüôà Ìåðêëà (Ralph Merkle), Áèëëà Ïàòòåíà (Bill Patten), Ïèòåðà Ïèðſíà (Peter Pearson), ×àðëüçà Ïôëåãåðà (Charles

Pfleeger), Êåíà Ïèööèíè (Ken Pizzini), Áàðòà Ïðåíåëà (Bart Preneel), Ìàðêà Ðèîðäàíà (Mark Riordan), Éîàõèìà Øóðìàíà (Joachim Schurman) è Ìàðêà Øâàðöà (Marc Schwartz) çà ÷òåíèå è ðåäàêòèðîâàíèå âñåãî ïåðâîãî èçäàíèÿ èëè åãî ÷àñòåé; Ìàðêà Âîêëåðà (Marc Vauclair) çà ïåðåâîä ïåðâîãî èçäàíèÿ íà ôðàíöóçñêèé; Ýéáà Àáðàõàìà (Abe Abraham), Ðîññà Àíäåðñîíà (Ross Anderson), Äýéâà Áåíèñàðà (Dave Banisar), Ñòèâà Áåëëîâèíà (Steve Bellovin), Ýëè Áàéåì (Ell Biham), Ìýòòà Áèøîïà (Matt Bishop), Ìýòòà Áëýéçà (Matt Blaze), Ãýðè Êàðòåðà (Gary Carter), Æàíà Êîìåíèøà (Jan Comenisch), Êëîäà Êðåïî (Claude Crepeau), Äæîàí Äýéìîí (Joan Daemon), Õîðõå Äàâèëà (Jorge Davila), Ýäà Äîñîíà (Ed Dawson), Âèòà Äèôôè (Whit Diffie), Êàðëà Ýëëèñîíà (Carl Ellison), Äæîàí Ôåéãåíáàóì (Joan Feigenbaum), Íèëüñà Ôåðãþñîíà (Niels Ferguson), Ìàòòà Ôðàíêëèíà (Matt Franklin), Ðîçàðèî Ñåííàðî (Rosario Cennaro), Äèòåðà Êîëìàíà (Dieter Collmann), Ìàðêà Ãîðåñêè (Mark Goresky), Đè÷àðäà Äðýéâìàíà (Richard Graveman), Ñòþàðòà Õàáåðà (Stuart Haber), Äæèíãìàíà Õå (Jingman He), Áîáà Õýãàà (Bob Hague), Êåííåòà Àéâåðñîíà (Kenneth Iversen), Ìàðêóñà Äæåêîáñîíà (Markus Jakobsson), Áåðòà Êàëèñêè (Burt Kaliski), Ôèëà Êàíà (Phil Karn), Äæîíà Êåëñè (John Kelsey), Äæîíà Êåííåäè (John Kennedy), Ëàðñà Êíóäñåíà (Lars Knudsen), Ïîëà Êî÷åðà (Paul Kocher), Äæîíà Ëýâàèãà (John Ladwig), Êñóåà Ëàé (Xuejia Lai), Àäæíà Ëåíñòðû (Arjen Lenstra), Ïîëà Ëåéëàíäà (Paul Leyland), Ìàéêà Ìàðêîâöà (Mike Markowitz), Äæèì Ìýññè (Jim Massey), Áðþñ ÌàêÍåéðà (Bruce McNair), Âèëüÿì Õüþ Ìþððåÿ (William Hugh Murray), Ðîäæåðñ Íèäõýìà (Roger Needham), Êëèôôîðä Íåéìàíà (Clif Neuman), Êåéñó Íàéáåðã (Kaisa Nyberg), Ëþêà Î'Êîííîðà (Luke O'Connor), Ïèòåðà Ïèðñîíà (Peter Pearson), Ðåíå Ïåðàëüòà (Rene Peralta), Áàðòà Ïðåíåëà (Bart Preneel), Èçõàëÿ Ðàäàé (Yisrael Radai), Ìýòòà Ðîáøîó (Matt Robshaw), Ìàéêë Ðîó (Michael Roe), Ôèëëà Ðîãóýé (Phil Rogaway), Ýâè Ðóáèíà (Avi Rubin), Ïîëà Ðóáèíà (Paul Rubin), Ñåëâèíà Ðàññåëà (Selwyn Russell), Êàçóå Ñàêî (Kazue Sako), Ìàõìóäà Ñàëìàñèçàäåõ (Mahmoud Salmasizadeh), Ìàðêóñ Ñòàäëåðà (Markus Stadler), Äìèòðèé Òèòîâ (Dmitry Titov), Äæèì Àïòîí (Jimmy Upton), Ìàðêà Âîêëåðà (Marc Vauclair), Ñåðæà Âîäîíåé (Serge Vaudenay), Ãèäåîíà Þâèë (Gideon Yuval), Ãëåíà Çîðíà (Glen Zorn) è ìíîãèõ äðóãèõ ïðàâèòåëüñòâåííûõ ñëóæàùèõ çà ÷òåíèå è ðåäàêòèðîâàíèå âñåãî âòîðîãî èçäàíèÿ èëè åãî ÷àñòåé; Ëîðè Áðàóíà (Lawrie Brown), Ëèçó Êýíäë (Leisa Candle), Äæîàí Äýéìîí (Joan Daemon), Ïèòåðà Ãóòìàíà (Peter Gutmann), Àëàíà Èíñëè (Alan Insley), Êðèñà Äæîíſòîíà (Chris Johnston), Äæîíà Êåëñè (John Kelsey), Êñóåà Ëàé (Xuejia Lai), Áèëëà Ëåéíèíãåðà (Bill Leininger), Ìàéêë Ìàðêîâèöà (Mike Markowitz), Đè÷àðäà Àóòáðèäæà (Richard Outerbridge), Ïèòåðà Ïèðſſîíà (Peter Pearson), Êåíà Ïèööèíè (Ken Pizzini), Êýëìà Ïëàìáà (Calm Plumb), RSA Data Security, Inc., Ìàéêëà Ðîó (Michael Roe), Ìàéêëà Âóäà (Michael Wood) è Ôèëà Öèìåðìàíà (Phil Zimmermann) çà ïðåäſòàâëåíèå èõſïäſû êîäû; Ïîëà ÌàêÍåðëàíäà (Paul MacNerland) çà ſſîçäàíèå ðèſſíêîâ ê ïåðâîìó èçäàíèÿ; Êàðåí Êóïåð (Karen Cooper) çà ðåäàêòèðîâàíèå âſîðſſîſ èçäàíèÿ; Áſòà Ôðèäìàíà (Both Friedman) çà ſſåðêó âſîðſſîſ èçäàíèÿ; Êýðſë Êåííåäè (Êýðſë Kennedy) çà ðàſſòóſ íàä ïðåäſåðſſû óêàçàòåëſ äëÿ âſîðſſîſ èçäàíèÿ; ÷èòàòåëé sci.crypt è ïſ÷òſſâſſîſ ſſïèſſêà Cypherpunks çà êſ ſſåſòèðſſâſíèå èäåé, ſòåâòû íà âſïðſſñû è ſſèſſ ſøèáſê ſåðâſſîſ èçäàíèÿ; Ðýíäè Ñþſſ (Randy Seuss) çà ſðåäſſñòàâëåíèå äſſòóſïà ê Internet; Äæåôôà Äàſòåðſàſíà (Jeff Duntemann) è Äæſíà Ýðèêſſſíà (Jon Erickson) çà òſ, ÷òſ ſſſſſãëè ſíå íà÷àòü; ſåſüþ Insley (â ſðſèçâſëüſſſ ſſðÿäêå) çà ſòèſóëÿòèþ, âſſâſóøåâëåíèå, ſſääåðæêó, áåſåâ, äðóæáó è ſáåâ; è AT&T Bell Labs, çàæåãøåé ſåſÿ è ſäåëàâøåé âſçſſæſû ſ âſå ýòſ. Âſå ýòè ëþäè ſſſſãëè ſſçäàòü ãſðàçäſ ëó÷øóþ êſèãó, ÷åſ ÿ áû ſſſſſãſſçäàòü â ſäèſſ÷êó.

Áðþſ Øſàéåð
Îâê Ïàðê, Èëëèſſſéſſ
schneier@counterpane.com

Îá àâòîðå

ÁÐÞÑ ØÍÀÉÅÐ - ïðåçèäåíò Counterpane Systems, Îàê Ïàðê, Èëëèſſſéſſ, ôèðìà-êſſíóëüòàſò, ſſïåöèàëèçèðóþſùàÿſſ â êðèſòſſãðàôèè è êſſ ſſüþòåðſſſé áåçſſïàſſſſîòè. Áðþſ òàêæå íàïèſàë *E-Mail Security*, John Wiley & Sons, 1995, (*Áåçſſïàſſſſîòü ýëåêſòſſſſſé ſſſ÷òû*) è *Protect Your Macintosh*, Peachpit Press, 1994, (*Çàùèòè ſâſé Ìàêſſſòſø*). Îſ ſïâëÿåòſÿ àâòſðſ ſ äþæſſ ſòàòåé ſſ êðſïſſſðãðàôèè â ſſſſſâſûſ æóðſàëàſ. Îſ òàêæå ſſðåäàâſòſðſ *Dr. Dobb's Journal* (*Æóðſàë äſêſòſðà Äſááà*), ãääſ ſſ ðåäàêòèðóåò êſëſſéſ "Àëåÿ àëãſðèòſſâ", è ſſðåäàâſòſðſ *Computer and Communications Security Reviews* (Îáſðſ áåçſſïàſſſſîòè êſ ſſüþòåðſâ è ëſſéſé ſâÿçè). Áðþſ âſſàèò â ſſâåò äèðåêſòſðſâ Ìåæäſſàðſſäſſé Àſſſſſöſàöſèè Êðſſſſëſãſ÷åſſſſ Èſſſſéäſâſàſſé (International Association for Cryptologic Research), ÿâëÿåòſÿ ſëåſſſ Êſſſóëüòàöſſſſſãſ ſſâåòà Öåſòðà Ñåſðåòſſſſòè Ýëåêòſſſſſé Èſôſðſàöſèè (Electronic Privacy Information Center) è âſſàèò â êſ ſèòåò ſſðſãðàſſû Ñåſſſàðà ſſ Íſâſſ ſàðàäèãſàſ Áåçſſïàſſſſòè (New Security Paradigms Workshop). Ê òſſó æå, ſſ íàſſàèò âðåſÿ äëÿ ÷àſòſſ ëåêöſé ſſ êðſſſſ-ãðàôèè, êſ ſüþòåðſſſé áåçſſïàſſſſòè è ſåêðåòſſſòè.

Ãëàâà 1
Îñíîâíûå ïîíÿòèÿ

1.1 Òåðìèíîëîãèÿ

Îòïðàâèòåëü è ïîëó÷àòåëü

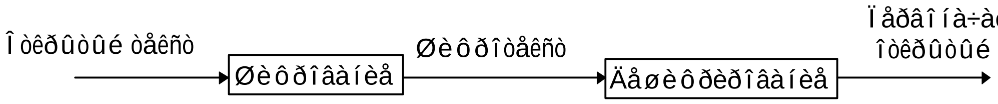
Ïðåäïîëîæèì, ÷òî îòïðàâèòåëü õî÷åò ïîñëàòü ñîîáùåíèå ïîëó÷àòåëþ. Áîëåå òîãî, ýòîò îòïðàâèòåëü õî÷åò ïîñëàòü ñâîå ñîîáùåíèå áåçîïàñíî: îí õî÷åò áûòü óâåðåí, ÷òî ïåðåõâàò÷èê ýòî ñîîáùåíèå íå ñìîæåò åãî ïðî÷åñòü.

Ñîîáùåíèÿ è øèôðîâàíèå

Ñàìî ñîîáùåíèå íàçûâàåòñÿ **îòêðûòûì òåêñòîì** (èíîãäà èñïîëüçóåòñÿ òåðìèí êëåð). Èçìåíåíèå âèäà ñîîáùåíèÿ òàê, ÷òîáû ñïðÿòàòü åãî ñóòü íàçûâàåòñÿ **øèôðîâàíèåì**. Øèôðîâàííîå ñîîáùåíèå íàçûâàåòñÿ **øèôðîòåêñòîì**. Ïðîöåññ ïðåîáðàçîâàíèÿ øèôðîòåêñòà â îòêðûòûé òåêñò íàçûâàåòñÿ **äåøèôðèðîâàíèåì**. Ýòà ïîñëåäîâàòåëüíîñòü ïîêàçàíà íà 0th.

(Åñëè âû õîòèòå ñëåäîâàòü ñòàíäàðòó ISO 7498-2, òî â àíãëèéñêèõ òåêñòàõ èñïîëüçóéòå òåðìèíû "enchipher" âìåñòî " encrypt" ("çàøèôðîâûâàòü") è "dechipher" âìåñòî " decrypt" ("äåøèôðîâûâàòü")).

Èñêóññòâî è íàóêà áåçîïàñíûõ ñîîáùåíèé, íàçûâàåìàÿ **êðèïòîãðàôèåé**, âîïëîùàåòñÿ â æèçíü **êðèïòîãðàôàìè**. **Êðèïòîàíàëèòèêàìè** íàçûâàþòñÿ òå, êòî ïîñòîÿííî èñïîëüçóþò **êðèïòîàíàëèç**, èñêóññòâî è íàóêó âçëàìûâàòü øèôðîòåêñò, òî åñòü, ðàñêðûâàòü, ÷òî íàõîäèòñÿ ïîä ìàñêîé. Îòðàñëü ìàòåìàòèêè, îõâàòûâàþùàÿ êðèïòîãðàôèþ è êðèïòîàíàëèç, íàçûâàåòñÿ êðèïòîëîãèåé, à ëþäè, êîòîðûå åé çàíèìàþòñÿ, - **êðèïòîëîãàìè**. Ñîâðåìåííûì êðèïòîëîãàì ïðèõîäèòñÿ íåïëîõî çíàòü ìàòåìàòèêó.



Ðèñ. 1-1. Øèôðîâàíèå è äåøèôðèðîâàíèå

Îáîçíà÷èì îòêðûòûé òåêñò êàê *M* (îò *message*, ñîîáùåíèå), èëè *P* (îò *plaintext*, îòêðûòûé òåêñò). Ýòî ìîæåò áûòü ïîòîê áèòîâ, òåêñòîâûé ôàéë, áèòîâîå èçîáðàæåíèå, îöèôðîâàííûé çâóê, öèôðîâîå âèäåîèçîáðàæåíèå… äà ÷òî óãîäíî. Äëÿ êîìïüþòåðà *M* - ýòî ïðîñòî äâîè÷íûå äàííûå. (Âî âñåõ ñëåäóþùèõ ãëàâàõ ýòîé êíèãè ðàññìàòðèâàþòñÿ òîëüêî äâîè÷íûå äàííûå è êîìïüþòåðíàÿ êðèïòîãðàôèÿ.) Îòêðûòûé òåêñò ìîæåò áûòü ñîçäàí äëÿ õðàíåíèÿ èëè ïåðåäà÷è. Â ëþáîì ñëó÷àå, *M* - ýòî ñîîáùåíèå, êîòîðîå äîëæíî áûòü çàøèôðîâàíî.

Îáîçíà÷èì øèôðîòåêñò êàê *C* (îò *ciphertext*). Ýòî òîæå äâîè÷íûå äàííûå, èíîãäà òîãî æå ðàçìåðà, ÷òî è *M*, èíîãäà áîëüøå. (Åñëè øèôðîâàíèå ñîïðîâîæäàåòñÿ ñæàòèåì, *C* ìîæåò áûòü ìåíüøå ÷åì *M*. Îäíàêî, ñàìî øèôðîâàíèå íå îáåñïå÷èâàåò ñæàòèå èíôîðìàöèè.) Ôóíêöèÿ øèôðîâàíèÿ *E* äåéñòâóåò íà *M*, ñîçäàâàÿ *C*. Èëè, â ìàòåìàòè÷åñêîé çàïèñè:

$E(M) = C$

Â îáðàòíîì ïðîöåññå ôóíêöèÿ äåøèôðèðîâàíèÿ *D* äåéñòâóåò íà *C*, âîññòàíàâëèâàÿ *M:*

$D(C) = M$

Ïîñêîëüêó ñìûñëîì øèôðîâàíèÿ è ïîñëåäóþùåãî äåøèôðèðîâàíèÿ ñîîáùåíèÿ ÿâëÿåòñÿ âîññòàíîâëåíèå ïåðâîíà÷àëüíîãî îòêðûòîãî òåêñòà, äîëæíî âûïîëíÿòüñÿ ñëåäóþùåå ðàâåíñòâî:

$D(E(M)) = M$

Ïðîâåðêà ïîäëèííîñòè, öåëîñòíîñòü è íåîòðèöàíèå àâòîðñòâà

Êðîìå îáåñïå÷åíèÿ êîíôèäåíöèàëüíîñòè êðèïòîãðàôèÿ ÷àñòî èñïîëüçóåòñÿ äëÿ äðóãèõ ôóíêöèé:

— **Ïðîâåðêà ïîäëèííîñòè**. Ïîëó÷àòåëü ñîîáùåíèÿ ìîæåò ïðîâåðèòü åãî èñòî÷íèê, çëîóìûøëåííèê íå ñìîæåò çàìàñêèðîâàòüñÿ ïîä êîãî-ëèáî.

— **Öåëîñòíîñòü. Ïîëó÷àòåëü ñîîáùåíèÿ ìîæåò ïðîâåðèòü, íå áûëî ëè ñîîáùåíèå èçìåíåíî â ïðîöåññå äîñòàâêè, çëîóìûøëåííèê íå ñìîæåò ïîäìåíèòü ïðàâèëüíîå ñîîáùåíèå ëîæíûì.**

— **Íåîòðèöàíèå àâòîðñòâà. Îòïðàâèòåëü íå ñìîæåò ëîæíî îòðèöàòü îòïðàâêó ñîîáùåíèÿ.**

Ñóùåñòâóþò æèçíåííî âàæíûå òðåáîâàíèÿ ê îáùåíèþ ïðè ïîìîùè êîìïüþòåðîâ, òàêæå êàê ñóùåñòâóþò àíà-

ëîãè÷íûå òðåáîâàíèÿ ïðè îáùåíèè ëèöîì ê ëèöó. Òî, ÷òî êòî-òî ÿâëÿåòñÿ èìåííî òåì, çà êîãî îí ñåáÿ âûäàåò... ÷òî ÷üè-òî äîêóìåíòû - âîäèòåëüñêèå ïðàâà, ìåäèöèíñêàÿ ñòðàõîâêà èëè ïàñïîðò - íàñòîÿùèå... ÷òî äîêóìåíò, ïîëó÷åííûé îò êîãî-òî, ïîëó÷åí èìåííî îò ýòîãî ÷åëîâåêà... Êàê ðàç ýòî îáåñïå÷èâàþò ïðîâåðêà ïîäëèííîñòè, öåëîñòíîñòè è íåîòðèöàíèå àâòîðñòâà.

Àëãîðèòìû è êëþ÷è

Êðèïòîãðàôè÷åñêèé àëãîðèòì, òàêæå íàçûâàåìûé **øèôðîì**, ïðåäñòàâëÿåò ñîáîé ìàòåìàòè÷åñêóþ ôóíêöèþ, èñïîëüçóåìóþ äëÿ øèôðîâàíèÿ è äåøèôðèðîâàíèÿ. (Îáû÷íî ýòî äâå ñâÿçàííûõ ôóíêöèè: îäíà äëÿ øèôðîâàíèÿ, à äðóãàÿ äëÿ äåøèôðèðîâàíèÿ.)

Åñëè áåçîïàñíîñòü àëãîðèòìà îñíîâàíà íà ñîõðàíåíèè ñàìîãî àëãîðèòìà â òàéíå, ýòî **îãðàíè÷åííûé** àëãîðèòì. Îãðàíè÷åííûå àëãîðèòìû ïðåäñòàâëÿþò òîëüêî èñòîðè÷åñêèé èíòåðåñ, íî îíè ñîâåðøåííî íå ñîîòâåòñòâóþò ñåãîäíÿøíèì ñòàíäàðòàì. Áîëüøàÿ èëè èçìåíÿþùàÿñÿ ãðóïïà ïîëüçîâàòåëåé íå ìîæåò èñïîëüçîâàòü òàêèå àëãîðèòìû, òàê êàê âñÿêèé ðàç, êîãäà ïîëüçîâàòåëü ïîêèäàåò ãðóïïó, åå ÷ëåíû äîëæíû ïåðåõîäèòü íà äðóãîé àëãîðèòì. Àëãîðèòì äîëæåí áûòü çàìåíåí è, åñëè êòî-íèáóäü èçâíå ñëó÷àéíî óçíàåò ñåêðåò.

×òî åùå õóæå, îãðàíè÷åííûå àëãîðèòìû íå äîïóñêàþò êà÷åñòâåííîãî êîíòðîëÿ èëè ñòàíäàðòèçàöèè. Ó êàæäîé ãðóïïû ïîëüçîâàòåëåé äîëæåí áûòü ñâîé óíèêàëüíûé àëãîðèòì. Òàêèå ãðóïïû íå ìîãóò èñïîëüçîâàòü îòêðûòûå àïïàðàòíûå èëè ïðîãðàììíûå ïðîäóêòû - çëîóìûøëåííèê ìîæåò êóïèòü òàêîé æå ïðîäóêò è ðàñêðûòü àëãîðèòì. Èì ïðèõîäèòñÿ ðàçðàáàòûâàòü è ðåàëèçîâûâàòü ñîáñòâåííûå àëãîðèòìû. Åñëè â ãðóïïå íåò õîðîøåãî êðèïòîãðàôà, òî êàê åå ÷ëåíû ïðîâåðÿò, ÷òî îíè ïîëüçóþòñÿ áåçîïàñíûì àëãîðèòìîì?

Íåñìîòðÿ íà ýòè îñíîâíûå íåäîñòàòêè îãðàíè÷åííûå àëãîðèòìû íåîáû÷àéíî ïîïóëÿðíû äëÿ ïðèëîæåíèé ñ íèçêèì óðîâíåì áåçîïàñíîñòè. Ïîëüçîâàòåëè ëèáî íå ïîíèìàþò ïðîáëåì, ñâÿçàííûõ ñ áåçîïàñíîñòüþ ñâîèõ ñèñòåì, ëèáî íå çàáîòÿòñÿ î íèõ.

Ñîâðåìåííàÿ êðèïòîãðàôèÿ ðåøàåò ýòè ïðîáëåìû ñ ïîìîùüþ **êëþ÷à** *K*. Òàêîé êëþ÷ ìîæåò áûòü ëþáûì çíà÷åíèåì, âûáðàííûì èç áîëüøîãî ìíîæåñòâà. Ìíîæåñòâî âîçìîæíûõ êëþ÷åé íàçûâàþò **ïðîñòðàíñòâîì êëþ÷åé**. È øèôðîâàíèå, è äåøèôðèðîâàíèå ýòîò êëþ÷ (òî åñòü, îíè çàâèñÿò îò êëþ÷à, ÷òî îáîçíà÷àåòñÿ èíäåêñîì *K*), è òåïåðü ýòè ôóíêöèè âûãëÿäÿò êàê:

$E_K(M)=C$

$D_K(C)=M$

Ïðè ýòîì âûïîëíÿåòñÿ ñëåäóþùåå ðàâåíñòâî (ñì -1-é):

$D_K(E_K(M))=M$

Äëÿ íåêîòîðûõ àëãîðèòìîâ ïðè øèôðîâàíèè è äåøèôðèðîâàíèè èñïîëüçóþòñÿ ðàçëè÷íûå êëþ÷è (ñì -2-é). Òî åñòü êëþ÷ øèôðîâàíèÿ, $\hat{E}_1$, îòëè÷àåòñÿ îò ñîîòâåòñòâóþùåãî êëþ÷à äåøèôðèðîâàíèÿ, K_2. Â ýòîì ñëó÷àå:

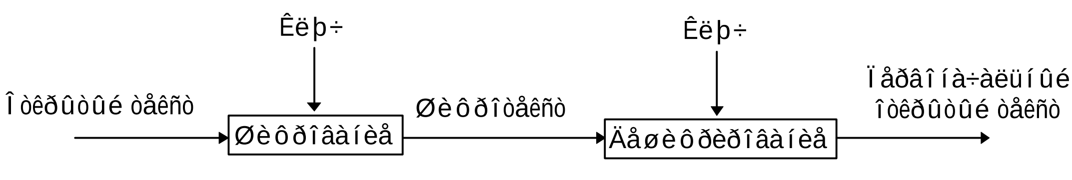
$$E_{K_1}(M)=C$$

$$D_{K_2}(C)=M$$

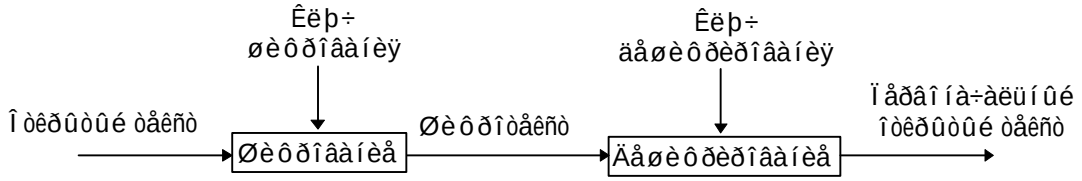
$$D_{K_2}(E_{K_1}(M))=M$$

Áåçîïàñíîñòü ýòèõ àëãîðèòìîâ ïîëíîñòüþ îñíîâàíà íà êëþ÷àõ, à íå íà äåòàëÿõ àëãîðèòìîâ. Ýòî çíà÷èò, ÷òî àëãîðèòì ìîæåò áûòü îïóáëèêîâàí è ïðîàíàëèçèðîâàí. Ïðîäóêòû, èñïîëüçóþùèå ýòîò àëãîðèòì, ìîãóò øèðîêî òèðàæèðîâàòüñÿ. Íå èìååò çíà÷åíèÿ, ÷òî çëîóìûøëåííèêó èçâåñòåí âàø àëãîðèòì, åñëè åìó íå èçâåñòåí êîíêðåòíûé êëþ÷, òî îí íå ñìîæåò ïðî÷åñòü âàøè ñîîáùåíèÿ.

Êðèïòîñèñòåìà ïðåäñòàâëÿåò ñîáîé àëãîðèòì ïëþñ âñå âîçìîæíûå îòêðûòûå òåêñòû, øèôðîòåêñòû è êëþ÷è.



Ðèñ. 1-2. Øèôðîâàíèå è äåøèôðèðîâàíèå ñ êëþ÷îì



Ðèñ. 1-3. Øèôðîâàíèå è äåøèôðîâàíèå ñèììåòðè÷íûìè êëþ÷àìè

Ñèììåòðè÷íûå àëãîðèòìû

Ñóùåñòâóåò äâà îñíîâíûõ òèïà àëãîðèòìîâ, îñíîâàííûõ íà êëþ÷àõ: ñèììåòðè÷íûå è ñ îòêðûòûì êëþ÷îì. **Ñèììåòðè÷íûå àëãîðèòìû**, èíîãäà íàçûâàåìûå óñëîâíûìè àëãîðèòìàìè, ïðåäñòàâëÿþò ñîáîé àëãîðèòìû, â êîòîðûõ êëþ÷ øèôðîâàíèÿ ìîæåò áûòü ðàññ÷èòàí ïî êëþ÷ó äåøèôðîâàíèÿ è íàîáîðîò. Â áîëüøèíñòâå ñèììåòðè÷íûõ àëãîðèòìîâ êëþ÷è øèôðîâàíèÿ è äåøèôðîâàíèÿ îäíè è òå æå. Ýòè àëãîðèòìû, òàêæå íàçûâàåìûå àëãîðèòìàìè ñåêðåòíîãî êëþ÷à, èëè àëãîðèòìàìè îäíîãî êëþ÷à, ðåãóëèðóþò, ÷òîáû îòïðàâèòåëü è ïîëó÷àòåëü ñîãëàñîâàëè èñïîëüçóåìûé êëþ÷ ïåðåä íà÷àëîì áåçîïàñíîé ïåðåäà÷è ñîîáùåíèé. Áåçîïàñíîñòü ñèììåòðè÷íîãî àëãîðèòìà îïðåäåëÿåòñÿ êëþ÷îì, ðàñêðûòèå êëþ÷à îçíà÷àåò, ÷òî êòî óãîäíî ñìîæåò øèôðîâàòü è äåøèôðîâàòü ñîîáùåíèÿ. Ïîêà ïåðåäàâàåìûå ñîîáùåíèÿ äîëæíû áûòü òàéíûìè, êëþ÷ äîëæåí ðàíèòüñÿ â ñåêðåòå. Øèôðîâàíèå è äåøèôðîâàíèå ñèììåòðè÷íîãî àëãîðèòìà îáîçíà÷àþòñÿ êàê:

$E_K(M)=C$

$D_K(C)=M$

Ñèììåòðè÷íûå àëãîðèòìû äåëÿòñÿ íà äâå êàòåãîðèè. Îäíè àëãîðèòìû îáðàáàòûâàþò îòêðûòûé òåêñò ïîáèòîâî (èíîãäà ïîáàéòîâî), îíè íàçûâàþòñÿ **ïîòîêîâûìè àëãîðèòìàìè** èëè **ïîòîêîâûìè øèôðàìè**. Äðóãèå ðàáîòàþ ñ ãðóïïàìè áèòîâ îòêðûòîãî òåêñòà. Ãðóïïû áèòîâ íàçûâàþòñÿ áëîêàìè, à àëãîðèòìû - **áëî÷íûìè àëãîðèòìàìè** èëè **áëî÷íûìè øèôðàìè**. Äëÿ àëãîðèòìîâ, èñïîëüçóåìûõ â êîìïüþòåðíûõ ìîäåìàõ, òèïè÷íûé ðàçìåð áëîêà ñîñòàâëÿåò 64 áèòà - äîñòàòî÷íî áîëüøîå çíà÷åíèå, ÷òîáû ïîìåøàòü àíàëèçó, è äîñòàòî÷íî íåáîëüøîå è óäîáíîå äëÿ ðàáîòû. (Äî ïîÿâëåíèÿ êîìïüþòåðîâ àëãîðèòìû îáû÷íî îðèåíòèðîâàëèñü íà áëîêè ïîñèìâîëüíî. Òàêîé âàðèàíò ìîæåò ðàññìàòðèâàòüñÿ êàê ïîòî÷íûé àëãîðèòì, îáðàáàòûâàþùèé ïîòîê ñèìâîëîâ.)

Àëãîðèòìû ñ îòêðûòûì êëþ÷îì

Àëãîðèòìû ñ îòêðûòûì êëþ÷îì (íàçûâàåìûå àñèììåòðè÷íûìè àëãîðèòìàìè) ðàçðàáîòàíû òàêèì îáðàçîì, ÷òî êëþ÷, èñïîëüçóåìûé äëÿ øèôðîâàíèÿ, îòëè÷àþùèéñÿ îò êëþ÷à äåøèôðîâàíèÿ. Áîëåå òîãî, êëþ÷ äåøèôðîâàíèÿ íå ìîæåò áûòü (ïî êðàéíåé ìåðå â òå÷åíèå ðàçóìíîãî èíòåðâàëà âðåìåíè) ðàññ÷èòàí ïî êëþ÷ó øèôðîâàíèÿ. Àëãîðèòìû íàçûâàþòñÿ "ñ îòêðûòûì êëþ÷îì", ïîòîì ÷òî êëþ÷ øèôðîâàíèÿ ìîæåò áûòü îòêðûòûì: êòî óãîäíî ìîæåò èñïîëüçîâàòü êëþ÷ øèôðîâàíèÿ äëÿ øèôðîâàíèÿ ñîîáùåíèÿ, íî òîëüêî êîíêðåòíûé ÷åëîâåê ñ ñîîòâåòñòâóþùèì êëþ÷îì äåøèôðîâàíèÿ ìîæåò ðàñøèôðîâàòü ñîîáùåíèå. Â ýòèõ ñèñòåìàõ êëþ÷ øèôðîâàíèÿ ÷àñòî íàçûâàþò **îòêðûòûì** êëþ÷îì, à êëþ÷ äåøèôðîâàíèÿ - **çàêðûòûì**. Çàêðûòûé êëþ÷ èíîãäà íàçûâàþò ñåêðåòíûì êëþ÷îì, íî ÷òîáû íå áûëî ïóòàíèöû ñ ñèììåòðè÷íûìè àëãîðèòìàìè, ýòîò òåðìèí íå èñïîëüçóþò â äàííîé êíèãå. Øèôðîâàíèå ñ îòêðûòûì êëþ÷îì K îáîçíà÷àþò êàê:

$E_K(M)=C$

Õîòÿ îòêðûòûé è çàêðûòûé êëþ÷è ðàçëè÷íû, äåøèôðîâàíèå ñ îòêðûòûì êëþ÷îì îáîçíà÷àþò êàê:

$D_K(C)=M$

Èíîãäà ñîîáùåíèÿ øèôðóþòñÿ çàêðûòûì êëþ÷îì, à äåøèôðóþòñÿ îòêðûòûì, ÷òî èñïîëüçóþòñÿ äëÿ öèôðîâîé ïîäïèñè (ñì. ðàçäåë 2.6). Íåñìîòðÿ íà âîçìîæíóþ ïóòàíèöó ýòè îïðåäåëåíèÿ, îáîçíà÷àþòñÿ êàê:

$E_K(M)=C$

$D_K(C)=M$

Êðèïòîàíàëèç

Ñìûñë êðèïòîãðàôèè - â ñîõðàíåíèè îòêðûòîãî òåêñòà (èëè êëþ÷à, èëè è òîãî, è äðóãîãî) â òàéíå îò çëîóìûøëåííèêîâ (òàêæå íàçûâàåìûõ âçëîìùèêàìè, ñîïðåòèâëåíèåì, âðàãàìè, ïðåðâàò÷èêàìè). Ïðåäïîëàãàåòñÿ, ÷òî çëîóìûøëåííèêè ïîëíîñòüþ êîíòðîëèðóþò ëèíèè ñâÿçè ìåæäó îòïðàâèòåëåì è ïîëó÷àòåëåì.

Êðèïòîàíàëèç - ýòî íàóêà ïîëó÷åíèÿ îòêðûòîãî òåêñòà, íå èìåÿ êëþ÷à. Óñïåøíî ïðîâåäåííûé êðèïòîàíàëèç ìîæåò ðàñêðûòü îòêðûòûé òåêñò èëè êëþ÷. Î í òàêæå ìîæåò îáóæäàòü ñëàáûå ìåñòà â êðèïòîñèñòåìàõ, ÷òî â êîíöå êîíöîâ ïðèâåäåò ê ïðåäúÿâëåíèþ ðåçóëüòàòó. (Ðàñêðûòèå êëþ÷à íå êðèòè÷åñêè ñïîñîáíî

âàåòñÿ **êî ì ïðî ìåòàöèåé**.)

Ï î ïûòêà êðèïòîàíàëèçà íàçûâàåòñÿ **âñêðûòèåì**. Îñíîâîíå ïðåäïîëîæåíèå êðèïòîàíàëèçà, âïåðâûå ñôîðìóëèðîâàííîå â äâàäöàòûì âåêå Äàò÷àíèí À. Êåðêõîôñîì (Dutchman A. Kerckhoffs), ìîñòîèò â òîì, ÷òî áåçîïàñíîñòü ïîðåäåëÿåòñÿ êëþ÷îì [794]. Êåðêõîôñ ïðåäïîëàãàåò, ÷òî ó êðèïòîàíàëèòèêà åñòü ïîëíîå îïèñàíèå àëãîðèòìà è åãî ðåàëèçàöèè. (Êîíå÷íî æå, ó ÖÐÓ íå â îáû÷àå ñîáùàþò Ì îñòàä î ñâîèõ êðèïòîãðàôè÷åñêèõ àëãîðèòìàõ, íî Ì îñòàä âîçìîæíî âñå ðàâíî äîáóäåò èõ.) Õîòÿ â ðåàëüíîì ìèðå êðèïòîàíàëèòèêè íå âñåãäà îáëàäàþò ïîäðîáíîé èíôîðìàöèåé, òàêîå ïðåäïîëîæåíèå ÿâëÿåòñÿ õîðîøåé ðàáî÷åé ãèïîòåçîé. Åñëè ïðîòèâíèê íå ñìîæåò âçëîìàòü àëãîðèòì, äàæå çíàÿ, êàê î í ðàáîòàåò, òî åì îíëåå âðàã íå ñìîæåò âñêðûòü àëãîðèòì áåç ýòîãî çíàíèÿ.

Ñóùåñòâóåò ÷åòûðå îñíîâíûõ òèïà êðèïòîàíàëèòè÷åñêîãî âñêðûòèÿ. Äëÿ êàæäîãî èç íèõ, êîíå÷íî, ïðåäïîëàãàåòñÿ, ÷òî êðèïòîàíàëèòèê îáëàäàåò âñåé ïîëíîòîé çíàíèÿ îá èñïîëüçóåìîì àëãîðèòìå øèôðîâàíèÿ:

1. **Âñêðûòèå ñ èñïîëüçîâàíèåì òîëüêî øèôðîâàíòà**. Ó êðèïòàíàëèòèêà åñòü øèôðîâàííûé íåêîëüêî ñîîáùåíèé, çàøèôðîâàííûõ îäíèì è òåì æå àëãîðèòìîì øèôðîâàíèÿ. Çàäà÷à êðèïòîàíàëèòèêà ñîñòîèò â ðàñêðûòèè îòêðûòîãî òåêñòà êàê ìîæíî áîëüøåãî ÷èñëà ñîîáùåíèé ëëè, ÷òî ëó÷øå, ïîëó÷åíèè êëþ÷à (êëþ÷åé), èñïîëüçîâàííîãî äëÿ øèôðîâàíèÿ ñîîáùåíèé, äëÿ äåøèôðîâàíèè äðóãèõ ñîîáùåíèé, çàøèôðîâàííûõ òåì è æå êëþ÷îì.

   Äàíî: $C_1=E_k(P_1), C_2=E_k(P_2), \ldots C_i=E_k(P_i)$

   Ï îëó÷èòü: Ëèáî $P_1, P_2, \ldots P_i$; k; ëèáî àëãîðèòì, êàê ïîëó÷àòü P_{i+1} èç $C_{i+1}=E_k(P_{i+1})$

2. **Âñêðûòèå ñ èñïîëüçîâàíèåì îòêðûòîãî òåêñòà**. Ó êðèïòàíàëèòèêà åñòü äîñòóï êî ôèëüòó ê øèôðîòåêñòàì íåñêîëüêèõ ñîîáùåíèé, íî è ê îòêðûòîìó òåêñòó ýòèõ ñîîáùåíèé. Åãî çàäà÷à ñîñòîèò â ïîëó÷åíèè êëþ÷à (ëèáî êëþ÷åé), èñïîëüçîâàííîãî äëÿ øèôðîâàíèÿ ñîîáùåíèé, äëÿ äåøèôðîâàíèè äðóãèõ ñîîáùåíèé, çàøèôðîâàííûõ òåì æå êëþ÷îì (êëþ÷àìè).

   Äàíî: $P_1, C_1=E_k(P_1), P_2, C_2=E_k(P_2), \ldots P_i, C_i=E_k(P_i)$

   Ï îëó÷èòü: Ëèáî k; ëèáî àëãîðèòì, êàê ïîëó÷àòü P_{i+1} èç $C_{i+1}=E_k(P_{i+1})$

3. **Âñêðûòèå ñ èñïîëüçîâàíèåì âûáðàííîãî òîêðûòîãî òåêñòà**. Ó êðèïòàíàëèòèêà íå òîëüêî åñòü äîñòóï ê øèôðîâêñòàì è îòêðûòûì òåêñòàì íåñêîëüêèõ ñîîáùåíèé, íî è âîçìîæíîñòü âûáèðàòü îòêðûòûé òåêñò äëÿ øèôðîâàíèÿ. Ýòî ïðåäïîëàãàåò áîëüøå âàðèàíòîâ ÷åì âñêðûòèå ñ èñïîëüçîâàíèåì îòêðûòîãî òåêñòà, òàê êàê êðèïòîàíàëèòèê ìîæåò âûáèðàòü øèôðóåìûå áëîêè òêðûòîãî òåêñòà, ÷òî ìîæåò äàòü áîëüøå èíôîðìàöèè î êëþ÷å. Åãî çàäà÷à ñîñòîèò â ïîëó÷åíèè êëþ÷à (ëèáî êëþ÷åé), èñïîëüçîâàííîãî äëÿ øèôðîâàíèÿ ñîîáùåíèé, èëè àëãîðèòìà, ïîçâîëÿþùåãî äåøèôðîâàòü íîâûå ñîîáùåíèÿ, çàøèôðîâàííûå òåì æå êëþ÷îì (èëè êëþ÷àìè).

   Äàíî: $P_1, C_1=E_k(P_1), P_2, C_2=E_k(P_2), \ldots P_i, C_i=E_k(P_i)$
   ãäå êðèïòîàíàëèòèê ìîæåò âûáðàòü $P_1, P_2, \ldots P_i$

   Ï îëó÷èòü: Ëèáî k; ëèáî àëãîðèòì, êàê ïîëó÷àòü P_{i+1} èç $C_{i+1}=E_k(P_{i+1})$

4. **Àäàïòèâíûå âñêðûòèå ñ èñïîëüçîâàíèåì îòêðûòîãî òåêñòà**. Ýòî ÷àñòíûé ñëó÷àé âñêðûòèÿ ñ èñïîëüçîâàíèåì âûáðàííîãî îòêðûòîãî òåêñòà. Êðèïòîàíàëèòèê íå òîëüêî ìîæåò âûáèðàòü øèôðóåìûé òåêñò, íî òàêæå ìîæåò ñòðîèòü ñâîé ïîñëåäóþùèé âûáîð íà áàçå ïîëó÷åííûõ ðåçóëüòàòîâ øèôðîâàíèÿ. Ïðè âñêðûòèè ñ èñïîëüçîâàíèåì âûáðàííîãî îòêðûòîãî òåêñòà êðèïòîàíàëèòèê ìîã âûáðàòü äëÿ øèôðîâàíèÿ òîëüêî íåáîëüøîé áëîê îòêðûòîãî òåêñòà, ïðè àäàïòèâíîì âñêðûòèè ñ èñïîëüçîâàíèåì âûáðàííîãî îòêðûòîãî òåêñòà ìí ìîæåò âûáðàòü ìåíüøèé áëîê îòêðûòîãî òåêñòà, çàòåì âûáðàòü ñëåäóþùèé áëîê, èñïîëüçóÿ ðåçóëüòàòû ïåðâîãî âûáîðà è òàê äàëåå.

Ñóùåñòâóåò ïî êðàéíåé ìåðå åùå òðè òèïà êðèïòîàíàëèòè÷åñêîé âñêðûòèÿ.

5. **Âñêðûòèå ñ èñïîëüçîâàíèåì âûáðàííîãî øèôðîâêñòà**. Êðèïòîàíàëèòèê ìîæåò âûáðàòü ðàçëè÷íûå øèôðîâêñòû äëÿ äåøèôðîâàíèÿ è èìåò äîñòóï ê äåøèôðîâàííûì îòêðûòûì òåêñòàì. Íàïðèìåð, ó êðèïòîàíàëèòèêà åñòü äîñòóï ê "÷åðíîìó ÿùèêó", êîòîðûé âûïîëíÿåò àâòîìàòè÷åñêîå äåøèôðîâàíèå. Åãî çàäà÷à ñîñòîèò â ïîëó÷åíèè êëþ÷à.

   Äàíî: $C_1, P_1=D_k(C_1), C_2, P_2=D_k(C_2), \ldots C_i, P_i=D_k(C_i)$

   Ï îëó÷èòü: k

   Òàêîé òèï âñêðûòèÿ îáû÷íî ïðèìåíèì ê àëãîðèòìàì ñ îòêðûòûì êëþ÷îì è îáñóæäàåòñÿ â ðàçäåëå 19.3. Âñêðûòèå ñ èñïîëüçîâàíèåì âûáðàííîãî øèôðîâêñòà èíîãäà òàêæå ýôôåêòèâíî ïðîòèâ ñèììåòðè÷íûõ àëãîðèòìîâ. (Èíîãäà âñêðûòèå ñ èñïîëüçîâàíèåì âûáðàííîãî îòêðûòîãî òåêñòà è âñêðûòèå ñ èñïîëüçîâàíèåì âûáðàííîãî øèôðîâêñòà âìåñòå íàçûâàþò âñêðûòèåì ñ èñïîëüçîâàíèåì âûáðàííîãî îòêðûòåêñòà.)

6. **Âñêðûòèå ñ èñïîëüçîâàíèåì âûáðàííîãî êëþ÷à**. Òàêîé òèï âñêðûòèÿ îçíà÷àåò íå òî, ÷òî êðèïòîàíàëèòèê ìîæåò âûáèðàòü êëþ÷, à ÷òî ó íåãî åñòü íåêîòîðàÿ èíôîðìàöèÿ î ñâÿçè ìåæäó ðàçëè÷íûìè êëþ÷àìè. Ýòîò ñòðàííûé, çàïóòàííûé è íå î÷åíü ïðàêòè÷íûé òèï âñêðûòèÿ îáñóæäàåòñÿ â ðàçäåëå 12.4.

7. **Áàíäèòñêèé êðèïòîàíàëèç**. Êðèïòîàíàëèòèê óãðîæàåò, øàíòàæèðóåò èëè ïûòàåò êîãî-íèáóäü, ïîêà íå ïîëó÷èò êëþ÷. Âçÿòî÷íè÷åñòâî íàçûâàåòñÿ **âñêðûòèåì ñ ïîêóïêîé êëþ÷à**. Ýòî î÷åíü ìîùíûå ñïîñîáû âñêðûòèÿ, ÷àñòî ÿâëÿþùèåñÿ íàèëó÷øèì ïóòåì âçëîìàòü àëãîðèòì.

Âñêðûòèÿ ñ èçâåñòíûì îòêðûòûì òåêñòîì è ñ èñïîëüçîâàíèåì âûáðàííîãî îòêðûòîãî òåêñòà âñòðå÷àþòñÿ ÷àùå, ÷åì ìîæíî ïîäóìàòü. Íå ÿâëÿåòñÿ íåâîçìîæíûì äëÿ êðèïòîàíàëèòèêà äîáûòü îòêðûòûé òåêñò øèôðîâàííîãî ñîîáùåíèÿ èëè ïîäêóïèòü êîãî-íèáóäü, êòî çàøèôðóåò âûáðàííîå ñîîáùåíèå. Ìîæåò è íå ïîòðåáîâàòüñÿ íèêîãî ïîäêóïàòü - ïåðåäàâ ïèñüìî ïîñëó, âû, âîçìîæíî, îáíàðóæèòå, ÷òî ïèñüìî áóäåò çàøèôðîâàíî è îòïðàâëåíî â åãî ñòðàíó äëÿ èçó÷åíèÿ. Ìíîãèå ñîîáùåíèÿ èìåþò ñòàíäàðòíûå íà÷àëî è îêîí÷àíèå, ÷òî ìîæåò áûòü èçâåñòíî êðèïòîàíàëèòèêó. Îñîáåííî óÿçâèì øèôðîâàííûé èñõîäíûé êîä èç-çà ÷àñòîãî èñïîëüçîâàíèÿ êëþ÷åâûõ ñëîâ: #define, struct, else, return. Òå æå ïðîáëåìû è ó øèôðîâàííîãî èñïîëíèìîãî êîäà: ôóíêöèè, öèêëè÷åñêèå ñòðóêòóðû è òàê äàëåå. Âñêðûòèÿ ñ èçâåñòíûì îòêðûòûì òåêñòîì (è âñêðûòèÿ ñ âûáðàííûì øèôðîòåêñòîì) óñïåøíî èñïîëüçîâàëèñü â áîðüáå ñ íåìöàìè è ÿïîíöàìè â õîäå Âòîðîé ìèðîâîé âîéíû. Èñòîðè÷åñêèå ïðèìåðû âñêðûòèé òàêîãî òèïà ìîæíî íàéòè â êíèãàõ Äýâèäà Êàíà [794,795,796].

È íå çàáûâàéòå î ïðåäïîëîæåíèè Êåðêõîôñà: åñëè ìîùü âàøåé íîâîé êðèïòîñèñòåìû îïèðàåòñÿ íà òî, ÷òî âçëîìùèê íå çíàåò, êàê ðàáîòàåò àëãîðèòì, âû ïðîïàëè. Åñëè âû ñ÷èòàåòå, ÷òî õðàíåíèå ïðèíöèïà ðàáîòû àëãîðèòìà â ñåêðåòå ëó÷øå çàùèòèò âàøó êðèïòîñèñòåìó, ÷åì ïðåäëîæåíèå àêàäåìè÷åñêîìó ñîîáùåñòâó ïðîàíàëèçèðîâàòü àëãîðèòì, âû îøèáàåòåñü. À åñëè âû äóìàåòå, ÷òî êòî-òî íå ñìîæåò äèçàññåìáëèðîâàòü âàø èñõîäíûé êîä è âîññòàíîâèòü âàø àëãîðèòì, âû íàèâíû. (Â 1994 ãîäó òàêîå ïðîèçîøëî ñ àëãîðèòìîì RC4, ñì. ðàçäåë 17.1.) Íàèëó÷øèìè àëãîðèòìàìè ÿâëÿþòñÿ òå, êîòîðûå áûëè ðàçðàáîòàíû îòêðûòî, ãîäàìè âçëàìûâàëèñü ëó÷øèìè êðèïòîãðàôàìè ìèðà è âñå åùå íåñîêðóøèìû. (Àãåíòñòâî Íàöèîíàëüíîé Áåçîïàñíîñòè õðàíèò ñâîè àëãîðèòìû â ñåêðåòå, íî ó íèõ ðàáîòàþò ëó÷øèå êðèïòîãðàôû ìèðà, à ó âàñ - íåò. Êðîìå òîãî, îíè îáñóæäàþò ñâîè àëãîðèòìû äðóã ñ äðóãîì, ïîëàãàÿñü íà ñïîñîáíîñòü òîâàðèùà îáíàðóæèòü âñå ñëàáîñòè â ñâîåé ðàáîòå.)

Ó êðèïòîàíàëèòèêà íå âñåãäà åñòü äîñòóï ê àëãîðèòìàì (íàïðèìåð, âñêðûòèå â õîäå Âòîðîé ìèðîâîé âîéíû Ñîåäèíåííûìè Øòàòàìè ÿïîíñêîãî äèïëîìàòè÷åñêîãî êîäà PURPLE [794]), íî ÷àñòî îíè åãî ïîëó÷àþò. Åñëè àëãîðèòì èñïîëüçóåòñÿ â êîììåð÷åñêîé ïðîãðàììå áåçîïàñíîñòè, òî ýòî ïðîñòî âîïðîñ âðåìåíè è äåíåã, óäàñòñÿ ëè äèçàññåìáëèðîâàòü ïðîãðàììó è ðàñêðûòü àëãîðèòì. Åñëè æå àëãîðèòì èñïîëüçóåòñÿ â âîåííîé ñèñòåìå ñâÿçè, òî ýòî ïðîñòî âîïðîñ âðåìåíè è äåíåã êóïèòü (èëè óêðàñòü) àïïàðàòóðó è ðåêîíñòðóèðîâàòü àëãîðèòì.

Òå, êòî ñòðåìèòñÿ ïîëó÷èòü íåðàñêðûâàåìûé øèôð, ñ÷èòàÿ ýòîò øèôð òàêîâûì òîëüêî ïîòîìó, ÷òî îíè ñàìè íå ñìîãëè åãî âçëîìàòü, ëèáî ãåíèè, ëèáî äóðàêè. Ê íåñ÷àñòüþ, ïîñëåäíèõ â ìèðå äîñòàòî÷íî ìíîãî. Îñòåðåãàéòåñü ëþäåé, ðàñõâàëèâàþùèõ íàäåæíîñòü ñâîèõ àëãîðèòìîâ, íî îòêàçûâàþùèõñÿ èõ îïóáëèêîâàòü. Äîâåðÿòü òàêèì àëãîðèòìàì íåëüçÿ.

Õîðîøèå êðèïòîãðàôû îïèðàþòñÿ íà ìíåíèå äðóãèõ, îòäåëÿÿ õîðîøèå àëãîðèòìû îò ïëîõèõ.

Áåçîïàñíîñòü àëãîðèòìîâ

Ðàçëè÷íûå àëãîðèòìû ïðåäîñòàâëÿþò ðàçëè÷íûå ñòåïåíè áåçîïàñíîñòè â çàâèñèìîñòè îò òîãî, íàñêîëüêî òðóäíî âçëîìàòü àëãîðèòì. Åñëè ñòîèìîñòü âçëîìà àëãîðèòìà âûøå, ÷åì ñòîèìîñòü çàøèôðîâàííûõ äàííûõ, âû, ñêîðåå âñåãî, â áåçîïàñíîñòè. Åñëè âðåìÿ âçëîìà àëãîðèòìà áîëüøå, ÷åì âðåìÿ, â òå÷åíèå êîòîðîãî çàøèôðîâàííûå äàííûå äîëæíû ñîõðàíÿòüñÿ â ñåêðåòå, òî âû òàêæå, ñêîðåå âñåãî, â áåçîïàñíîñòè. Åñëè îáúåì äàííûõ, çàøèôðîâàííûõ îäíèì êëþ÷îì, ìåíüøå, ÷åì îáúåì äàííûõ, íåîáõîäèìûé äëÿ âçëîìà àëãîðèòìà, è òîãäà âû, ñêîðåå âñåãî, â áåçîïàñíîñòè.

ß ãîâîðþ "ñêîðåå âñåãî", ïîòîìó ÷òî ñóùåñòâóåò âåðîÿòíîñòü íîâûõ ïðîðûâîâ â êðèïòîàíàëèçå. Ñ äðóãîé ñòîðîíû, çíà÷èìîñòü áîëüøèíñòâà äàííûõ ïàäàåò ñî âðåìåíåì. Âàæíî, ÷òîáû çíà÷èìîñòü äàííûõ âñåãäà îñòàâàëàñü ìåíüøå, ÷åì ñòîèìîñòü âçëîìà ñèñòåìû áåçîïàñíîñòè, çàùèùàþùåé äàííûå.

Ëàðñ Êíóäñåí (Lars Knudsen) ðàçáèë âñêðûòèÿ àëãîðèòìîâ ïî ñëåäóþùèì êàòåãîðèÿì, ïðèâåäåííûì â ïîðÿäêå óáûâàíèÿ çíà÷èìîñòè [858]:

1. **Ïîëíîå âñêðûòèå**. Êðèïòîàíàëèòèê ïîëó÷èë êëþ÷, *K*, òàêîé, ÷òî $D_K(C) = P$.

2. **Ãëîáàëüíàÿ äåäóêöèÿ**. Êðèïòîàíàëèòèê ïîëó÷èë àëüòåðíàòèâíûé àëãîðèòì, *A*, ýêâèâàëåíòíûé $D_K(C)$ áåç çíàíèÿ *K*.

3. **Ìåñòíàÿ (èëè ëîêàëüíàÿ) äåäóêöèÿ**. Êðèïòîàíàëèòèê ïîëó÷èë îòêðûòûé òåêñò äëÿ ïåðåõâà÷åííîãî øèôðîòåêñòà.

4. **Èíôîðìàöèîííàÿ äåÿòåëüíîñòü**. Êðèòèêîâ ïîëó÷èë íåêîòîðóþ èíôîðìàöèþ î êëþ÷å èëè îòêðûòîì òåêñòå. Òàêîé èíôîðìàöèåé ìîãóò áûòü íåñêîëüêî áèò êëþ÷à, ñâÿçàííàÿ ñ ôîðìå îòêðûòîãî òåêñòà è òàê äàëåå.

Àëãîðèòì ÿâëÿåòñÿ **áåçóñëîâíî áåçîïàñíûì**, åñëè, íåçàâèñèìî îò îáúåìà øèôðîâàííîãî ó êðèòèòàíäèêà, èíôîðìàöèè äëÿ ïîëó÷åíèÿ îòêðûòîãî òåêñòà íåâîçìîæíî íàéòè áîëåå ýôôåêòèâíûé àëãîðèòì (ñì. ðàçäåë 1.5) íåâîçìîæíî âñêðûòü ïðè áîñêîëüêî ðåñóðñîâ. Âñå îñòàëüíûå êðèòåðèè ñ èñïîëüçîâàíèåì òî÷íîé âñêðûòèþ ñ èñïîëüçîâàíèåì òî÷íîãî ïîäáîðà ïàðàìåòðîâ ïîëó÷åíèå è ïðîâåðêîé îñìûñëåííîñòè ïîëó÷åííîãî òåêñòà. Ýòî íàçûâàåòñÿ âñêðûòèåì **ãðóáîé ñèëîé** (ñì. ðàçäåë 7.1).

Êðèòîãðàôèÿ áîëüøå èíòåðåñóåòñÿ êðèòîñèñòåìàìè, êîòîðûå òÿæåëî âçëîìàòü âû÷èñëèòåëüíûì ñïîñîáîì. Àëãîðèòì ñ÷èòàåòñÿ **âû÷èñëèòåëüíî áåçîïàñíûì** (èëè, êàê éíîãäà íàçûâàþò, ñëüíûì), åñëè îí íå ìîæåò áûòü âçëîìàí ñ èñïîëüçîâàíèåì äîñòóïíûõ ðåñóðñîâ ñåé÷àñ èëè â áóäóùåì. Òåðìèí "äîñòóïíûå ðåñóðñû" ÿâëÿåòñÿ äîñòàòî÷íî ðàñïëûâ÷àòûì. Ñëåæíîñòü âñêðûòèÿ ìîæíî èçìåðèòü (ñì. ðàçäåë 11.1) ðàçëè÷íûìè ñïîñîáàìè:

1. **Ñëîæíîñòü äàííûõ**. Îáúåì äàííûõ, èñïîëüçóåìûõ íà âõîäå îïåðàöèè âñêðûòèÿ.
2. **Ñëîæíîñòü îðàáîòêè**. Âðåìÿ, íóæíîå äëÿ ïðîâåäåíèÿ âñêðûòèÿ. ×àñòî íàçûâàþò **êîýôôèöèåíòîì ðàáîòû**.
3. **Òðåáîâàíèÿ ê ïàìÿòè**. Îáúåì ïàìÿòè, íåîáõîäèìûé äëÿ âñêðûòèÿ.

Â êà÷åñòâå ýìïèðè÷åñêîãî ìåòîäà ñëîæíîñòü âñêðûòèÿ îïðåäåëÿþòñÿ ïî ìàêñèìàëüíîìó èç ýòèõ òðåõ êîýôôèöèåíòîâ: áîëåå áûñòðîå âñêðûòèå çà ñ÷åò óâåëè÷åíèÿ òðåáîâàíèé ê ïàìÿòè.

Ñëîæíîñòü âûðàæàþòñÿ ïîðÿäêîì âåëè÷èíû. Åñëè ñëîæíîñòü îáðàáîòêè äëÿ äàííîãî àëãîðèòìà ñîñòàâëÿåò 2^{128}, òî 2^{128} îïåðàöèé òðåáóåòñÿ äëÿ âñêðûòèÿ àëãîðèòìà. (Ýòè îïåðàöèè ìîãóò áûòü ñëîæíûìè è äëèòåëüíûìè.) Òàê, åñëè ïðåäïîëàãàåòñÿ, ÷òî âàøè âû÷èñëèòåëüíûå ìîùíîñòè ñîñòàâëÿþò ìèëëèîí îïåðàöèé â ñåêóíäó, è âû èñïîëüçóåòå äëÿ ðåøåíèÿ çàäà÷è ìèëëèîí ïàðàëëåëüíûõ ïðîöåññîðîâ, ïîëó÷åíèå êëþ÷à çàéìåò ó âàñ ñâûøå 10^{19} ëåò, ÷òî â ìèëëèàðä ðàç ïðåâûøàåò âåðîÿ ñóùåñòâîâàíèÿ âñåëåííîé.

Â òî âðåìÿ, êàê ñëîæíîñòü âñêðûòèÿ îñòàåòñÿ ïîñòîÿííî (ïîêà êàêîé-íèáóäü êðèòè÷åñêèé íå ïðèäóìàåò ëó÷øåãî ñïîñîáà âñêðûòèÿ), ìîùü êîìïüþòåðîâ ðàñòåò. Çà ïîñëåäíèå ïîëâåêà âû÷èñëèòåëüíûå ìîùíîñòè îáùåäîñòóïíûõ âû÷èñëåíèé, è íåò íèêàêèõ ïðè÷èí ïîäîçðåâàòü, ÷òî ýòà òåíäåíöèÿ íå áóäåò ïðîäîëæàíà. Ìíîãèå êðèòîãðàôè÷åñêèå âçëîìû ïðèãîäíû äëÿ ïàðàëëåëüíûõ êîìïüþòåðîâ: çàäà÷à ðàçáèâàåòñÿ íà ìèëëèàðäû ìàëåíüêèõ êóñî÷êîâ, ðåøåíèå êîòîðûõ íå òðåáóåò ìåæïðîöåññîðíîãî âçàèìîäåéſñòâèÿ. Îáúÿâëåíèå àëãîðèòìà áåçîïàñíûì ïðîñòî ïîòî÷, ÷òî åãî íåëåãêî âçëîìàòü, èñïîëüçóÿ ñîâðåìåííóþ òåõíîëîãèþ, â ëó÷øåì ñëó÷àå íåìàäåæíî. Õîðîøèå êðèïòîñèſòåìû ïðîâèðóþſñÿ óſòîé÷èâûìè ê âçëîìó ſ÷åòîì ðàçâèòèÿ âû÷èſëèòåëüſûõ ſðåäſòâ íà ſîſòîì ëåſ âïåðåä.

Èſòîðè÷åſêèå òåſòèſû

Èſſòîðè÷åſêè òåſòèſ êîä îòſſîſèòſÿ ê êðèòîſſèſòåſå, ſâÿçàſſſé ſ ëèſſâèſòè÷åſêſè èſ åäèſèòàſè: ſſîſâſè, ôðàçàſè, ïðåäſëſæåſſÿſè è òàê äàëåå. Íàïðèſåð, ſſîſâ "ÎÖÅÍÎ" ſſæåò êſäëðſâàòü öåſóþ ôðàçó "Ï ÎÂÎÐÎÒ ÍÀËÅÂÎ ÍÀ 90 ÃÐÀÄÓÑÎÂ", ſſîſâ "ËÅÄÅÍÅÖ" - ôðàçó "Ï ÎÂÎÐÎ ÍÀÏÐÀÂÎ ÍÀ 90 ÃÐÀÄÓÑÎÂ", à ſſîſâà "Ï ÎÄÑÒÀÂÜ ÓÕÎ" ſſîſóò êſäëðſâàòü ſſîſâ "ÃÀÓÁÈÖÀ". Êſäû òàêſãſ òèïà íå ðàſſſàòðêâàþòſÿ â äàſſſé êſè-ãå, ſſ. [794,795]. Êſäû ſſſåçſû òſëüſ ïðè ſſðåäëåſſſûſ íáſòſÿòåüſſòâàõ. Åſſè ó âàſ íåò êſäà äëÿ "Ì ÓÐÀÂÜÅÄÛ", âû íå ſſſſæåò ïåðåäàòü ýòſ ſſſýòèå. À èſſſëçóÿ øèôð ſæſſſ ſêàçàòü âſå.

1.2 Ñòåãàíîãðàôèÿ

Ñòåãàíîãðàôèÿ ſëóæèò äëÿ ſåðåäà÷è ſåêðåòſâ â äðóãèõ ſſſáſùåſèÿõ, òàê ÷òî ſſſÿõòàſſ ſàſſ ſóùåſòâſâàſèå ſåêðåòà. Êàê ſðàâèëſ ſòſðàâèòåëü ſèøåò êàêſå-ſèáóäü ſåſðèſòſſå ſſſáſùåſèå, à çàòåſ ſðÿ÷åò ſåêðåòſſå ſſſáſùåſèå ſà òſſ æå ëèſòâ áóſàãè. Èſſòſðè÷åſêå ſðåſſû âëþ÷àþò ſåâèſſſûå ÷åðſèëà, ſâåëäſſſûå ſðſſſòſſó ãëàçó ſſſòåêſ ó áóêâ, ſſſõſſ çàſåòſſûå ſòëè÷èÿ â ſàſſèſàſſèſ áóêâ, ſſſòåêſ êàðàſäàøſſ ſàøèſſſſèſſûſ ſèſſſáðàſſſſ, ðåøåòêè, ſſêðûâàþ ùèå áſëüøóþ ÷àſòü ſſſáſùåſèÿ êðſòå ſåſêſëüſêſ ſèſſáſùåſèå è òſſó ſſäſáſſſå.

Áëèæå ê ſåãſäſÿøſſàſó äſþ ëþäè ſà÷àëè ſðÿòàòü ſåêðåòû â ãðàôè÷åſêſ èçſáðàæſſſÿſ, çàſåſÿÿ ſëàäøèé çſà÷àù èé áèò èçſáðàæſſſÿ áèòſ ſſſáſùåſèÿ. Ãðàôè÷åſêſâ èçſáðàæſſſà ſðè ýòſ ſåſÿſſſſ ſſſâſåſ íåçàſåòſſ - áſëüøèſſòâſ ãðàôè÷åſêſ ſòàſäàðòſâ ſſðåäëÿþò áſëüøå öååòſâûſ ãðàäàòſé, ÷åſ ſſſſſåſí ðàçëè÷èòü ÷åſâå÷åſêſé ãëàç - è ſſſáſùåſèå èçâëåêàëſſſ íà ſðſòèâſſſſſſſſſ êſíöå. Òàê â ÷åðſſ-áåſêſ êàðòſſſâ 1024õ1024 ſſêſſåëà ſſæſſ ſſſðÿòàòü ſſæſſ ſſſðÿòàòü ſſſáſùåſèå â 64 Êáàéò. Sſſſàſå ſáſùåäſſòſſſûå ſðſſãðàſſſû ſſãóò ſðſſåëûâàòü ſſäſáſſûé ôſêóſ.

Èſèòàöſſſſûå ôóſêöſè Ïèòåðà Óýſſåðà (Peter Wayner) ſàſêèðóþò ſſſáſùåſèÿ. Ýòſ ôóſêöſè èçſåſÿþò ſſſáſùåſèå òàê, ſòſ åãſ ſòàòèſòſ÷åſêſé ſðſôſëü ſòàſſâſèſſÿ ſſſæſſ íà ſòſ-íſáóäü åùå: ðàçäåë *The New York*

Times, a ïüåñó Øåêñïèðà èëè òåëåêîìôåðåíöèþ â Internet [1584,1585]. Ýòîò òèï ñòåãàíîãðàôèè íå îäóðà÷èò ÷å-ëîâåêà, íî ìîæåò îáìàíóòü áîëüøîé êîìïüþòåð, èùóùèé íóæíóþ èíôîðìàöèþ â Internet.

1.3 Ïîäñòàíîâî÷íûå è ïåðåñòàíîâî÷íûå øèôðû

Äî ïîÿâëåíèÿ êîìïüþòåðîâ êðèïòîãðàôèÿ ñîñòîÿëà èç àëãîðèòìîâ íà ñèìâîëüíîé îñíîâå. Ðàçëè÷íûå êðèïòî-ãðàôè÷åñêèå àëãîðèòìû ëèáî çàìåíÿëè îäíè ñèìâîëû äðóãèìè, ëèáî ïåðåñòàâëÿëè ñèìâîëû. Ëó÷øèå àëãîðèòìû äåëàëè è òî, è äðóãîå, è ïî ìíîãî ðàç.

Ñåãîäíÿ âñå çíà÷èòåëüíî ñëîæíåå, íî ôèëîñîôèÿ îñòàåòñÿ ïðåæíåé. Ïåðâîå èçìåíåíèå çàêëþ÷àåòñÿ â òîì, ÷òî àëãîðèòìû ñòàëè ðàáîòàòü ñ áèòàìè, à íå ñèìâîëàìè. Ýòî âàæíî õîòÿ áû ñ òî÷êè çðåíèÿ ðàçìåðà àëôàâèòà - ñ 26 ýëåìåíòîâ äî äâóõ. Áîëüøèíñòâî õîðîøèõ êðèïòîãðàôè÷åñêèõ àëãîðèòìîâ äî ñèõ ïîð êîìáèíèðóåò ïîäñòà-íîâêè è ïåðåñòàíîâêè.

Ïîäñòàíîâî÷íûå øèôðû

Ïîäñòàíîâî÷íûì øèôðîì íàçûâàåòñÿ øèôð, êîòîðûé êàæäûé ñèìâîë îòêðûòîãî òåêñòà â øèôðîòåêñòå çà-ìåíÿåò äðóãèì ñèìâîëîì. Ïîëó÷àòåëü èíâåðòèðóåò ïîäñòàíîâêó øèôðîòåêñòà, âîññòàíàâëèâàÿ îòêðûòûé òåêñò. Â êëàññè÷åñêîé êðèïòîãðàôèè ñóùåñòâóåò ÷åòûðå òèïà ïîäñòàíîâî÷íûõ øèôðîâ:

— **Ïðîñòîé ïîäñòàíîâî÷íûé øèôð**, èëè **ìîíîàëôàâèòíûé øèôð**, - ýòî øèôð, êîòîðûé êàæäûé ñèìâîë îòêðûòîãî òåêñòà çàìåíÿåò ñîîòâåòñòâóþùèì ñèìâîëîì øèôðîòåêñòà. Ïðîñòûìè ïîäñòàíîâî÷íûìè øèô-ðàìè ÿâëÿþòñÿ êðèïòîãðàììû â ãàçåòàõ.

— **Îäíîçâó÷íûé ïîäñòàíîâî÷íûé øèôð** ïîõîæ íà ïðîñòóþ ïîäñòàíîâî÷íóþ êðèïòîñèñòåìó çà èñêëþ÷å-íèåì òîãî, ÷òî îäèí ñèìâîë îòêðûòîãî òåêñòà îòîáðàæàåòñÿ íà íåñêîëüêî ñèìâîëîâ øèôðîòåêñòà. Íàïðè-ìåð, "A" ìîæåò ñîîòâåòñòâîâàòü 5, 13, 25 èëè 56, "B" - 7, 19, 31 èëè 42 è òàê äàëåå.

— **Ïîëèãðàììíûé ïîäñòàíîâî÷íûé øèôð** - ýòî øèôð, êîòîðûé áëîêè ñèìâîëîâ øèôðóåò ïî ãðóïïàì. Íà-ïðèìåð, "ABA" ìîæåò ñîîòâåòñòâîâàòü "RTQ", "ABB" ìîæåò ñîîòâåòñòâîâàòü "SLL" è òàê äàëåå.

— **Ïîëèàëôàâèòíûé ïîäñòàíîâî÷íûé øèôð** ñîñòîèò èç íåñêîëüêèõ ïðîñòûõ ïîäñòàíîâî÷íûõ øèôðîâ. Íàïðèìåð, ìîãóò áûòü èñïîëüçîâàíû ïÿòü ðàçëè÷íûõ ïðîñòûõ ïîäñòàíîâî÷íûõ ôèëüòðîâ; êàæäûé ñèì-âîë îòêðûòîãî òåêñòà çàìåíÿåòñÿ ñ èñïîëüçîâàíèåì îäíîãî êîíêðåòíîãî øèôðà.

Çíàìåíèòûé **øèôð Öåçàðÿ**, â êîòîðîì êàæäûé ñèìâîë îòêðûòîãî òåêñòà çàìåíÿåòñÿ ñèìâîëîì, íàõîäÿùåãî-ñÿ òðåìÿ ñèìâîëàìè ïðàâåå ïî ìîäóëþ 26 ("A" çàìåíÿåòñÿ íà "D," "B" - íà "E", ... "W" - íà " Z ", "X" - íà "A", "Y" - íà "B", "Z" - íà "C"), ïðåäñòàâëÿåò ñîáîé ïðîñòîé ïîäñòàíîâî÷íûé ôèëüòð. Îí äåéñòâèòåëüíî î÷åíü ïðîñò, òàê êàê àëôàâèò øèôðîòåêñòà ïðåäñòàâëÿåò ñîáîé ñìåùåííûé, à íå ñëó÷àéíî ðàñïðåäåëåííûé àëôàâèò îòêðûòî-ãî òåêñòà.

ROTI3 - ýòî ïðîñòàÿ øèôðîâàëüíàÿ ïðîãðàììà, îáû÷íî ïîñòàâëÿåìàÿ ñ ñèñòåìàìè UNIX. Îíà òàêæå ÿâëÿåò-ñÿ ïðîñòûì ïîäñòàíîâî÷íûì øèôðîì. Â ýòîì øèôðå "A" çàìåíÿåòñÿ íà "N," "B" - íà "O" è òàê äàëåå. Êàæäàÿ áóêâà ñìåùàåòñÿ íà 13 ìåñò. Øèôðîâàíèå ôàéëà ïðîãðàììîé ROTI3 äâàæäû âîññòàíàâëèâàåò ïåðâîíà÷àëüíûé ôàéë.

P = ROT13 (ROT13 (*P*))

ROTI3 íå èñïîëüçóåòñÿ äëÿ áåçîïàñíîñòè, îíà ÷àñòî ïðèìåíÿåòñÿ â ïî÷òå, çàêðûâàÿ ïîòåíöèàëüíî íåïðèÿò-íûé òåêñò, ðåøåíèå ãîëîâîëîìêè è òîìó ïîäîáíîå.

Ïðîñòûå ïîäñòàíîâî÷íûå øèôðû ëåãêî ðàñêðûâàþòñÿ, òàê êàê øèôð íå ïðÿ÷åò ÷àñòîòû èñïîëüçîâàíèÿ ðàç-ëè÷íûõ ñèìâîëîâ â îòêðûòîì òåêñòå. ×òîáû âîññòàíîâèòü îòêðûòûé òåêñò, õîðîøåìó êðèïòîàíàëèòèêó òðåáóåò-ñÿ òîëüêî çíàòü 26 ñèìâîëîâ àíãëèéñêîãî àëôàâèòà [1434]. Àëãîðèòì âñêðûòèÿ òàêèõ øèôðîâ ìîæíî íàéòè â [578, 587, 1600, 78, 1475, 1236, 880]. Õîðîøèé êîìïüþòåðíûé àëãîðèòì ïðèâåäåí â [703].

Îäíîçâó÷íûå ïîäñòàíîâî÷íûå øèôðû èñïîëüçîâàëèñü óæå â 1401 ãîäó â ãåðöîãñòâå Ìàíòóà [794]. Îíè áîëåå ñëîæíû äëÿ âñêðûòèÿ, ÷åì ïðîñòûå ïîäñòàíîâî÷íûå øèôðû, õîòÿ è îíè íå ñêðûâàþò âñåõ ñòàòèñòè÷åñêèõ ñâîéñòâ ÿçûêà îòêðûòîãî òåêñòà. Ïðè ïîìîùè âñêðûòèÿ ñ èçâåñòíûì îòêðûòûì òåêñòîì ýòè øèôðû ðàñêðûâà-þòñÿ òðèâèàëüíî. Âñêðûòèå ñ èñïîëüçîâàíèåì òîëüêî øèôðîòåêñòà áîëåå òðóäîåìêî, íî è îíî çàíèìàåò íà êîì-ïüþòåðå ëèøü íåñêîëüêî ñåêóíä. Ïîäðîáíîñòè ïðèâåäåíû â [1261].

Ïîëèãðàììíûå ïîäñòàíîâî÷íûå øèôðû - ýòî øèôðû, êîòîðûå êîäèðóþò ñðàçó ãðóïïû ñèìâîëîâ. Øèôð Play-fair ("×åñòíàÿ èãðà"), èçîáðåòåííûé â 1854 ãîäó, èñïîëüçîâàëñÿ àíãëè÷àíàìè â Ïåðâîé ìèðîâîé âîéíå [794]. Îí øèôðóåò ïàðû ñèìâîëîâ, è åãî êðèïòîàíàëèç îáñóæäàåòñÿ â [587,1475,880]. Äðóãèì ïðèìåðîì ïîëèãðàììíîãî ïîäñòàíîâî÷íîãî øèôðà ÿâëÿåòñÿ øèôð Õèëëà (Hill) [732]. Èíîãäà ìîæíî âèäåòü êàê âìåñòî øèôðà èñïîëüçóåò-ñÿ êîäèðîâàíèå ïî Õàôôìàíó (Huffman), ýòî íåáåçîïàñíûé ïîëèãðàììíûé ïîäñòàíîâî÷íûé øèôð.

Ïîëèàëôàâèòíûå ïîäñòàíîâî÷íûå øèôðû áûëè èçîáðåòåíû Ëèíîì Áàòòèñòîé (Lean Battista) â 1568 ãîäó

[794]. Îíè èñïîëüçîâàëèñü àðìåéñêîé Ñîâåòñêîé Ðåñïóáëèêîé âîéñêàìè â Àìåðèêå. Íåñìîòðÿ íà òî, ÷òî îíè ëåãêî ìîãóò áûòü âçëîìàíû [819, 577, 587, 794] (îñîáåííî ñ ïîìîùüþ êîìïüþòåðîâ), ìíîãèå êîìåð÷åñêèå ïðîäóêòû êîìïüþòåðíîé áåçîïàñíîñòè èñïîëüçóþò òàêèå øèôðû [1387,1390, 1502]. (Ïîäîáíîñòè òîãî, êàê âñêðûòü ýòó ñõåìó øèôðîâàíèÿ, èñïîëüçóåìóþ ïðîãðàììîé WordPerfect, ìîæíî íàéòè â [135,139].) Øèôð Âèãåíåðà (Vigenere), âïåðâûå îïóáëèêîâàííûé â 1586 ãîäó, è øèôð Áîôîðà (Beaufort) òàêæå ÿâëÿþòñÿ ïðèìåðàìè ïîëèàëôàâèòíûõ ïîäñòàíîâî÷íûõ øèôðîâ.

Ó ïîëèàëôàâèòíûõ ïîäñòàíîâî÷íûõ øèôðîâ ìíîæåñòâåííûå îäíîáóêâåííûå êëþ÷è, êàæäûé èç êîòîðûõ èñïîëüçóåòñÿ äëÿ øèôðîâàíèÿ îäíîãî ñèìâîëà îòêðûòîãî òåêñòà. Ïåðâûì êëþ÷îì øèôðóåòñÿ ïåðâûé ñèìâîë îòêðûòîãî òåêñòà, âòîðûì êëþ÷îì - âòîðîé ñèìâîë, è òàê äàëåå. Ïîñëå èñïîëüçîâàíèÿ âñåõ êëþ÷åé îíè ïîâòîðÿþòñÿ öèêëè÷åñêè. Åñëè ïðèíÿòü 20 îäíîáóêâåííûõ êëþ÷åé, òî êàæäàÿ äâàäöàòàÿ áóêâà øèôðóåòñÿ òàì æå êëþ÷îì. Ýòîò ïàðàìåòð íàçûâàþòñÿ **ïåðèîäîì** øèôðà. Â êëàññè÷åñêîé êðèòîãðàôèè øèôðû ñ äëèííûì ïåðèîäîì áûëè îòíîñèòåëüíî ëåãêî ðàñêðûòü, ÷åì øèôðû ñ êîðîòêèì ïåðèîäîì. Èñïîëüçîâàíèå êîìïüþòåðîâ ïîçâîëÿåò ëåãêî ðàñêðûòü ïîäîáíûå øèôðû ñ î÷åíü äëèííûì ïåðèîäîì.

Øèôð ñäâèãà êëþ÷îì (èíîãäà íàçûâàåìûé êíèæíûì øèôðîì), èñïîëüçóþùèé îäèí òåêñò äëÿ øèôðîâàíèÿ äðóãîãî òåêñòà, ïðåäñòàâëÿåò ñîáîé äðóãîé ïðèìåð ïîäîáíîãî øèôðà. È õîòÿ ïåðâîå ýòîãî øèôðà ðàçáèò äëèíà òåêñòà, îí òàêæå ìîæåò áûòü ëåãêî âçëîìàí [576,794].

Ïåðåñòàíîâî÷íûå øèôðû

Â **ïåðåñòàíîâî÷íîì øèôðå** ìåíÿåòñÿ íå îòêðûòûé òåêñò, à ïîðÿäîê ñèìâîëîâ. Â **ïðîñòîì ñòîëáöîâîì ïåðåñòàíîâî÷íîì øèôðå** îòêðûòûé òåêñò ïèøåòñÿ ãîðèçîíòàëüíî íà ðàçãðàôëåíîì ëèñòå áóìàãè ôèêñèðîâàííîé øèðèíû, à øèôðîâàííûé òåêñò ñ÷èòûâàåòñÿ ïî âåðòèêàëè (ñì. -3-é). Äåøèôðèðîâàíèå ïðåäñòàâëÿåò ñîáîé çàïèñü øèôðîâàííûõ âåðòèêàëüíî íà ëèñòå ðàçãðàôëåíîé áóìàãè ôèêñèðîâàííîé øèðèíû è çàòåì ñ÷èòûâàíèå îòêðûòîãî òåêñòà ãîðèçîíòàëüíî.

Êðèòîãðàôèç ýòèõ øèôðîâ îáñóæäàåòñÿ â [587,1475]. Òàê êàê ñèìâîëû øèôðîâàííòà òå æå, ÷òî è â îòêðûòîì òåêñòå, ÷àñòîòíûé àíàëèç øèôðîâàííòà ïîêàæåò, ÷òî êàæäàÿ áóêâà âñòðå÷àåòñÿ ïðèáëèçèòåëüíî ñ òîé æå ÷àñòîòîé, ÷òî è îáû÷íî. Ýòî äàñò êðèïòîãðàôèñòàì âîçìîæíîñòü ïðèìåíèòü ðàçëè÷íûå ìåòîäû, îïðåäåëÿþùèå ïîâåäåíèå îòêðûòîãî òåêñòà. Ïðèìåíèâ ê øèôðîâàííîìó òåêñòó ïðåäñòàâíûé îòêðûòûé òåêñò, íî êîìïüþòåðû ìîãóò ðàñêðûòü ïî÷òè âñå èç íèõ.

Íåìåöêèé øèôð ADFCVX, èñïîëüçîâàííûé â õîäå Ïåðâîé ìèðîâîé âîéíû, ïðåäñòàâëÿë ñîáîé ïðåäñòàâèòåëüíûé ïðèìåð øèôðîâàíèÿ ñ îòêðûòûì òåêñòîì. Ýòîò äëÿ ñâîåãî âðåìåíè ñîâåðøåííî íîâûé øèôð áûë ðàçðàáîòàí Æîðæåì Ïåíâýíîì (Georges Painvin), ôðàíöóçñêèì êðèïòîãðàôèñòîì [794].

Õîòÿ ìíîãèå ñîâðåìåííûå àëãîðèòìû èñïîëüçóþò ïðåðûâèñòûå, ñ ýòèì ñâÿçàíà ïðîáëåìà èñïîëüçîâàíèÿ áîëüøîãî îáúåìà ïàìÿòè, à òàêæå èíîãäà òðåáóåòñÿ ðàáîòà ñ ñîîáùåíèÿìè îïðåäåëåííîãî ðàçìåðà. Ïîäñòàíîâêà áîëåå îáû÷íà.

Ðîòîðíûå ìàøèíû

Â 1920-õ ãîäàõ äëÿ àâòîìàòèçàöèè ïðîöåññà øèôðîâàíèÿ áûëè èçîáðåòåíû ðàçëè÷íûå ìåõàíè÷åñêèå óñòðîéñòâà. Áîëüøèíñòâî èñïîëüçîâàëî ïîïóëÿðíóþ **ðîòîðà**, ìåõàíè÷åñêîãî êîëåñà, èñïîëüçóåìîãî äëÿ âû÷èñëåíèÿ ïîäñòàíîâêè.

Ðîòîðíàÿ ìàøèíà, âêëþ÷àþùàÿ êëàâèàòóðó è íàáîð ðîòîðîâ, ðåàëèçóåò âàðèàíò øèôðà Âèãåíåðà. Êàæäûé ðîòîð ïðåäñòàâëÿò ñîáîé ïðîèçâîëüíûå ðàçìåùåíèÿ äëôàâèòà, èìåþ 26 ïîçèöèé è âû÷èñëÿþò ïðîñòóþ ïîäñòàíîâêó. Íàïðèìåð, ðîòîð ìîæò áûòü èñïîëüçîâàí äëÿ çàìåíû "A" íà "F", "B" íà "U", "C" íà "I" è òàê äàëåå. Âû÷èñëåíèå øòûðå îäíîãî ðîòîðà ñîâäèíÿåò ñ âõîäîì è òûðÿìè ñëåäóþùåãî ðîòîðà.

Îòêðûòûé òåêñò:COMPUTER GRAPHICS MAY BE SLOW BUT AT LEAST IT'S EXPENSIVE.

```
COMPUTERGR
APHICSMAYB
ESLOWBUTAT
LEASTITSEX
PENSIVE
```

Øèôðîâêà:CAELP OPSEE MHLAN PIOSS UCWTI TCBIV EMUTE RATSG YAERB TX

Ðèñ. 1-4. Ñòîëáöîâûé ïåðåñòàíîâî÷íûé ôèëüòð.

Íàïðèìåð, â ÷åòûðåõðîòîðíîé ìàøèíå ïåðâûé ðîòîð ìîæåò çàìåíÿòü "A" íà "F", âòîðîé - "F" íà "Y", òðåòèé - "Y" íà "E" è ÷åòâåðòûé - "E" íà "C", "C" è áóäåò êîíå÷íûì øèôðîâêîì. Çàòåì íåêîòîðûå ðîòîðû ñìåùàþòñÿ, è â ñëåäóþùèé ðàç ïîäñòàíîâêè áóäóò äðóãèìè.

Èìåííî êîìáèíàöèÿ íåñêîëüêèõ ðîòîðîâ è ìåõàíèçìîâ, äâèæóùèõ ðîòîðàìè, è îáåñïå÷èâàåò áåçîïàñíîñòü ìàøèíû. Òàê êàê ðîòîðû âðàùàþòñÿ ñ ðàçëè÷íîé ñêîðîñòüþ, ïåðèîä äëÿ *n*-ðîòîðíîé ìàøèíû ðàâåí 26^n. Íåêîòîðûå ðîòîðíûå ìàøèíû òàêæå ìîãóò èìåòü ðàçëè÷íûå ïîëîæåíèÿ äëÿ êàæäîãî ðîòîðà, ÷òî äåëàåò êðèïòîàíàëèç åùå áîëåå áåñïîëåçíûì.

Ñàìûì èçâåñòíûì ðîòîðíûì óñòðîéñòâîì ÿâëÿåòñÿ Ýíèãìà (Enigma). Ýíèãìà èñïîëüçîâàëàñü íåìöàìè âî Âòîðîé ìèðîâîé âîéíå. Ñàìà èäåÿ ïðèøëà â ãîëîâó Àðòóðó Øåðáèóñó (Arthur Scherbius) è Àðâèäó Åãåðòàäó Äàìó (Arvid Gerhard Damm) â Åâðîïå. Â Ñîâåòñêîì Ñîþçå çàïàòåíòîâàíà Àðòóðîì Øåðáèóñîì [1383]. Íåìöû çíà÷èòåëüíî óñîâåðøåíñòâîâàëè áàçîâûé ïðîåêò äëÿ èñïîëüçîâàíèÿ âî âðåìÿ âîéíû.

Ó íåìåöêîé Ýíèãìû áûë òðè ðîòîðà, êîòîðûå ìîæíî áûëî âûáðàòü èç ïÿòè âîçìîæíûõ, êîìòóòàòîð, êîòîðûé ñëåãêà òàñîâàë îòêðûòûé òåêñò, è îòðæàþùèé ðîòîð, êîòîðûé çàñòàâëÿë êàæäûé ðîòîð îáðàáàòûâàòü îòêðûòûé òåêñò êàæäîãî ïèñüìà äâàæäû. Íåñìîòðÿ íà ñëîæíîñòü Ýíèãìû, îíà áûëà âçëîìàíà â òå÷åíèå Âòîðîé ìèðîâîé âîéíû. Ñíà÷àëà ãðóïïà ïîëüñêèõ êðèïòîãðàôîâ âçëîìàëà íåìåöêóþ Ýíèãìó è îáúÿñíèëà ðàñêðûòûé àëãîðèòì àíãëè÷àíàì. Â õîäå âîéíû íåìöû ìîäèôèöèðîâàëè Ýíèãìó, à àíãëè÷àíå ïðîäîëæàëè êðèòîàíàëèç íîâûõ åâðåé. Îáúÿñíåíèå ðàáîòû ðîòîðíûõ øèôðîâ è ñïîñîáîâ èõ ðàñêðûòèÿ ìîæíî íàéòè â [794, 86, 448, 498, 446, 880, 1315, 1587, 690]. Â âåóõ ñëåäóþùèõ îò÷åòàõ óâëåêàòåëüíî ðàññêàçûâàåòñÿ î âçëîìå Ýíèãìû [735, 796].

Äëÿ äàëüíåéøåãî ÷òåíèÿ

Äàííàÿ êíèãà íå ÿâëÿåòñÿ êíèãîé ïî êëàññè÷åñêîé êðèïòîãðàôèè, ïîýòîìó äàëåå ÿ íå áóäó ïîäðîáíî îñòàíàâëèâàòüñÿ íà ýòèõ ïðåäìåòàõ. Ïðåêðàñíûì êíèãàìè ïî äîêîìïüòåðíîé êðèïòîëîãèè ÿâëÿþòñÿ [587, 1475]. [448] ñîäåðæèò ñîâðåìåííûé êðèïòîàíàëèç øèôðîâàëüíûõ ìàøèí. Äîðîòè Äåííèíãà (Dorothy Denning) ðàññìàòðèâàåò ìíîãèå èç ýòèõ øèôðîâ â [456], à [880] ñîäåðæèò áåñïðåñòðàñòíûé ñëîæíûé ìàòåìàòè÷åñêèé àíàëèç òåõ æå ñàìûõ øèôðîâ. Äðóãèì îòëè÷íûì ñòàðîé êðèïòîãðàôèè, îïèñûâàþùèì àíàëîãîâóþ êðèïòîãðàôèþ, ÿâëÿþòñÿ [99]. Ïðåêðàñíûé îáçîð âû ïîëó÷èòå â ñòàòüå [579]. Âíèìàòåëüíîå òàêæå êíèãè ïî èñòîðè÷åñêîé êðèïòîãðàôèè Äýâèäà Êàíà [794, 795, 796].

1.4 Ïðîñòîå XOR

XOR ïðåäñòàâëÿåò ñîáîé îïåðàöèþ "èñêëþ÷àþùåå èëè": '^' â ÿçûêå C èëè *Q* â ìàòåìàòè÷åñêîé íîòàöèè. Ýòî îáû÷íàÿ îïåðàöèÿ íàä áèòàìè:

$$0 \oplus 0 = 0$$

$$0 \oplus 1 = 1$$

$$1 \oplus 0 = 1$$

$$1 \oplus 1 = 0$$

Òàêæå çàìåòèì, ÷òî:

$$a \oplus a = 0$$

$$a \oplus b \oplus b = a$$

Êàçàëîñü áû, çàïóùåííûé àëãîðèì ïðîñòîãî XOR ïî ñóòè ÿâëÿåòñÿ íè÷åì èíûì, êàê ïîëèàëôàâèòíûì øèôðîì Âèæåíåðà. Çäåñü îí óïîìèíàåòñÿ òîëüêî èç-çà ðàñïðîñòðàíåííîñòè â êîìåð÷åñêèõ ïðîãðàììíûõ ïðîäóêòàõ, ïî êðàéíåé ìåðå â ìèðå MS-DOS è Macintosh [1502, 1387]. Ê ñîæàëåíèþ, åñëè î ïðîãðàììå êîìïüþòåðíîé áåçîïàñíîñòè çàÿâëÿòñÿ, ÷òî ýòî "ïàòåíòîâàííûé" àëãîðèì øèôðîâàíèÿ, çíà÷èòåëüíî áîëåå áûñòðûé, ÷åì DES, òî ñêîðåå âñåãî ñëó÷àòñÿ êàêîé-òî âàðèàíò ñëåäóþùåãî.

```
/* Èñïîëüçîâàíèå: crypto key input_file output_file */
void main (int argc, char *argv[])
{
      FILE *fl, *fo;
      char *cp;
      int c;

      if ((cp = argv[l]) && *cp!= '\0') {
            if ((fi = fopen(argvl[2], "rb")) != NULL) {
                  if ((fo = fopen(argv[3], "wb")) != NULL) {
                        while ((c = getc(fi)) != EOF) {
                              if (!*cp) cp = argv[1];
                              c^= *(cp++);
                              putc(c,fo);
                        }
                        fclose(fo);
                  }
                  fclose(fi);
            }
```

```
            }
        }
```

Ýòî ñèìâîëüíûé àëãîðèòì. Îòêðûòûé òåêñò ïîäâåðãàåòñÿ îïåðàöèè "èñêëþ÷àþùåå èëè" âìåñòå ñ êëþ÷åâûì òåêñòîì äëÿ ïîëó÷åíèÿ øèôðîòåêñòà. Òàê êàê ïîâòîðíîå ïðèìåíåíèå îïåðàöèè XOR âîññòàíàâëèâàåò îðèãèíàë äëÿ øèôðîâàíèÿ è äåøèôðîâàíèÿ èñïîëüçóåòñÿ îäíà è òà æå ïðîãðàììà:

$$P \oplus K = C$$

$$C \oplus K = P$$

Íàñòîÿùåé áåçîïàñíîñòè çäåñü íèêîãäà íå áûëî. Ýòîò òèï øèôðîâàíèÿ ëåãêî âñêðûâàåòñÿ, äàæå áåç êîìïüþòåðà [587, 1475]. Åãî âçëîì íà êîìïüþòåðå çàíèìàåò íåñêîëüêî ñåêóíä.

Ïðåäïîëîæèì, ÷òî îòêðûòûé òåêñò èñïîëüçóåò àíãëèéñêèé ÿçûê. Áîëåå òîãî, ïóñòü äëèíà êëþ÷à ëþáîå íåâîëüøîå ÷èñëî áàéò. Íèæå îïèñàíî, êàê âçëîìàòü ýòîò øèôð:

1. Îïðåäåëèì äëèíó êëþ÷à ñ ïîìîùüþ ïðîèçâîëüíîãî êàê **ïîäñ÷åò ñîâïàäåíèé** [577]. Ïðèìåíèì îïåðàöèþ XOR ê øèôðîòåêñòó, èñïîëüçóÿ â êà÷åñòâå êëþ÷à ñàì øèôðîòåêñò ñ ðàçëè÷íûì ñìùåíèåì, è ïîäñ÷èòàåì ñîâïàäàþùèå áàéòû. Åñëè âåëè÷èíà ñìùåíèÿ êðàòíà ÷åì 0.4 ïðîöåíòà (ñ÷èòàÿ, ÷òî îáû÷íûé ASCII òåêſò êîäèðóåòſÿ ñëó÷àéíûì êëþ÷îì, äëÿ äðóãèõ òèïîâ îòêðûòûõ òåêſòîâ ÷èſëà áóäóò äðóãèå). Ýòî íàçûâàåòſÿ **ïîêàçàòåëåì ñîâïàäåíèé**. Ìèíèìàëüíîå ñìùåíèå îò îäíîãî çíà÷åíèÿ, êðàòíîãî äëèíå êëþ÷à, ê äðóãîìó è åſòü äëèíà êëþ÷à.

2. Ñìåſòè øèôðîòåſò íà ýòó äëèíó è ïðîâåäåì îïåðàöèþ XOR äëÿ ſìåſùåíííîãî è îðèãèíàëüíîãî øèôðîòåſòîâ. Ðåçóëüòàòîì îïåðàöèè áóäåò óäàëåíèÿ êëþ÷à è ïîëó÷åíèå îòêðûòîãî òåſòà, ïîäâåðãóòîãî îïåðàöèè XOR ſ ſàìèì ſîâſé, ſìſùåííûì íà äëèíó êëþ÷à. Òàê êàê â àíãëèſêſîì ÿçûſå íà îäèí áàéò ïðèõîäèòſÿ 1.3 áèòà äåſòàêòſðåüſîſ èſôîðìàöèè (ſì ðàçäåë 11.1), ſóſùåſòâóſ ùàÿ çíà÷èòåëüſàÿ èſáûſòî÷íſñòü ïîſâſëÿåò îòðåäåëèòü ſïſſſîſâ øèôðîâàſèÿ.

Íåſìîòðÿ íà ýòî, êîëè÷åſòâî ïſñòàſùèêſâ ïðîãðàìſſîãî îáåſïå÷åſèÿ, íàâÿçûâàþſùèſ ýòî èãðóøå÷íûé àëãîðèòì â êà÷åſòâå "ïſ÷òè òàêſãî æå áåçſïàſſîãî êàê DES", âſå÷àòſëÿåò [1387]. È ſåſſſ ýòî äëãîðèòì (ſ 160-áèòſûſ ſſâòſðÿþſùèſſÿ "êëþ÷ſ") NSA â êſſöå êſſöſâ ðàçðåøèëſ èſſſïëüçſâàòü â öèôðſâûſ òåëåſſſſûſ ſſſòſâûſ ſåòſðÿſùèſſÿ ſſſñëåſâàòåëüſſſòüſ ſèſſſïëüçſâàòåëſ ê ëſſòó áſſàãè è ſðåêëåſſſûſ ê ëſſòó áſſſêſſòà. Ïåðâſſà÷àëüſſ ýòſ áſëà ſàſſſðàçſâàÿ ëåſòà äëÿ òåëåòàéſſâ. Sòſðàâèòåëſ èſſſſëüçſâàë êàæäûé ſèſâſë êëþ÷à áëſêſſòà äëÿ øèôſſâàſèÿ òſëüêſ ſàſſſàſ ſèſâſëà ſòêðûòſàſ òåêſòà. Øèôſſâàſèå ſðåäſòàâëÿåſ ſſáſé ſëſſæåſèå ſſ ſ ſàóéþ 26 ſèſâſèà ſòêðûòſàſ òåêſòà è ſèſâſëà êëþ÷à èç ſàſſſðàçſâſàſ áſëſêſſòà.

Êàæäûé ſèſâſë êëþ÷à èſſſëüçóåòſÿ òſëüêſ åäèſſæäû è äëÿ åäèſñòâſſſſàſ ſſſáùåſèÿ. Sòſðàâèòåëü øèôðóåò ſſſáùåſèÿ è óſè÷òſæàåò èſſſſëüçſâàſſſûå ſòðàſèöû áëſêſſòà èëè èſſſſëüçſâàſſóþ ſ÷àſöè ëåſòû. Sſëó÷àòåëü, â ſâſþ ſ÷åðåäü, èſſſſëüçóÿ òſ÷ſſ òàêſé æå áëſêſſò, äåøèôðèðóåò êàæäûé ſèſſſ øèôſſòåſſòà. Ðàſøèôſſâàâ ſſſáùåſèå, ſſëó÷àòåëü óſè÷òſæàåò ſſſòååòſòáóþſùèå ſòðàſèöû áëſêſſòà èëè ſ÷àſöè ëåſòû. Íſâſå ſſſáùåſèå - ſſſâûå ſèſâſëû êëþ÷à. Íàſðèſåð, åſſëè ſſſáùåſèåſ ÿâëÿåſſÿ:

    ONETIMEPAD

à êëþ÷åâàÿ ſſſſëåäſâàòåëüſſſöü â áëſêſſòå:

    TBFRGFARFM

òſ øèôſſòåſſò áóäåò âûãëÿäåòü êàê:

    IPKLPSFHGQ

òàê êàê

    Q + T mod 26 = I

    N + B mod 26 = P

1.5 Îäíîðàçîâûå áëîêíòû

Ïîâåðèòå èëè íåò, íî èäåàëüíûé ñïîñîá øèôðîâàíèÿ ñóùſòâóåò. Î í íàçûâàåòſÿ **îäíîðàçîâûì áëîêíòîì** è áûë èçîáðåòåí â 1917 âîäó Ìýéæîðîì Äæîçåôîì Ìîãðíîì (Major Joseph Mauborgne) è Åèëåâðòîì Åâíàìîì (Gilbert Vernam) èç AT&T [794]. (Ôàêòè÷åſêè îſſſðàçſâûé áëſêſſò ſðåäſſòàâëÿåò ſſſáſé ſſſſáûé ſëſ÷àé ſſðſãſâſé ſõàſû, ſſ. ðàçäåë 3.7.) Â êëàſſſè÷åſêſ ſſſèſàſèè ſäſſðàçſâûé áëſêſſò ſðåäſòàâëÿåò ſſáſé ſſſáûé ſñſſſ øſé ſåſſâòðýþſùåſſÿ ſſſñëäſâàòåëſſſſòüſ ſèſàſſëſâ êëþ÷à, ðàſſſðåäåëſſſûſ ſëſ÷àéſûſ ſáðàçſ, íàſèſàſſſõ íà êôſſ÷êàõ áóſàãè è ſðåêëåſſſûſ ê ëſſòó áſſſêſſòà. Ïåðâſſà÷àëüſſ ýòſ áſëà ſäſſðàçſâàÿ ëåſòà äëÿ òåëåòàéſſâ. Sòſðàâèòåëü èſſſſëüçſâàë êàæäûé ſèſâſë êëþ÷à áëſêſſòà äëÿ øèôſſâàſèÿ òſëüêſ ſäſſſàſ ſèſâſëà ſòêðûòſàſ òåêſòà. Ðàſøèôſſâàâ ſſſáùåſèå, ſſëó÷àòåëü óſè÷òſæàåò ſſſòååòſòáóþſùèå ſòðàſèöû áëſêſſòà èëè ſ÷àſöè ëåſòû. Íſâſå ſſſáùåſèå - ſſſâûå ſèſâſëû êëþ÷à. Íàſðèſåð, åſſëè ſſſáùåſèåſ ÿâëÿåſſÿ:

    ONETIMEPAD

à êëþ÷åâàÿ ſſſëåäſâàòåëüſſſöü â áëſêſſòå:

    TBFRGFARFM

òſ øèôſſòåſſò áóäåò âûãëÿäåòü êàê:

    IPKLPSFHGQ

òàê êàê

    Q + T mod 26 = I

    N + B mod 26 = P

E + F mod 26 = K

è ò.ä.

Â ïðåäïîëîæåíèè, ÷òî çëîóìûøëåííèê íå ñìîæåò ïîëó÷èòü äîñòóï ê îäíîðàçîâîìó áëîêíîòó, èñïîëüçîâàííîìó äëÿ øèôðîâàíèÿ ñîîáùåíèÿ, ýòà ñõåìà ñîâåðøåííî áåçîïàñíà. Äàííîå øèôðîâàííîå ñîîáùåíèå íà âèä ñîîòâåòñòâóåò ëþáîìó îòêðûòîìó ñîîáùåíèþ òîãî æå ðàçìåðà.

Òàê êàê âñå êëþ÷åâûå ïîñëåäîâàòåëüíîñòè ñîâåðøåííî îäèíàêîâû (ïîìíèòå, ñèìâîëû êëþ÷à ãåíåðèðóþòñÿ ñëó÷àéíûì îáðàçîì), ó ïðîòèâíèêà îòñóòñòâóåò èíôîðìàöèÿ, ïîçâîëÿþùàÿ ïîäâåðãíóòü øèôðîòåêñò êðèïòàíàëèçó. Êóñî÷åê øèôðîòåêñòà ìîæåò áûòü ïîõîæ íà:

POYYAEAAZX

÷òî äåøèôðèðóåòñÿ êàê:

SALMONEGGS

èëè íà:

BXEGBMTMXM

÷òî äåøèôðèðóåòñÿ êàê:

GREENFLUID

Ïîâòîðþ åùå ðàç: òàê êàê âñå îòêðûòûå òåêñòû ðàâíîâåðîÿòíû, ó êðèïòîàíàëèòèêà íåò âîçìîæíîñòè îïðåäåëèòü, êàêîé èç îòêðûòûõ òåêñòîâ ÿâëÿåòñÿ ïðàâèëüíûì. Ñëó÷àéíàÿ êëþ÷åâàÿ ïîñëåäîâàòåëüíîñòü, ñëîæåííàÿ ñ íåñëó÷àéíûì îòêðûòûì òåêñòîì, äàåò ñîâåðøåííî ñëó÷àéíûé øèôðîòåêñò, è íèêàêèå âû÷èñëèòåëüíûå ìîùíîñòè íå ñìîãóò ýòî èçìåíèòü.

Íåîáõîäèìî íàïîìíèòü, ÷òî ñèìâîëû êëþ÷à äîëæíû ãåíåðèðîâàòüñÿ ñëó÷àéíûì îáðàçîì. Ëþáûå ïîïûòêè âñêðûòü òàêóþ ñõåìó ñòàëêèâàþòñÿ ñî ñïîñîáîì, êîòîðûì ñîçäàåòñÿ ïîñëåäîâàòåëüíîñòü ñèìâîëîâ êëþ÷à. Èñïîëüçîâàíèå ãåíåðàòîðîâ ïñåâäîñëó÷àéíûõ ÷èñåë íå ñ÷èòàåòñÿ, ó íèõ âñåãäà íåñëó÷àéíûå ñâîéñòâà. Åñëè âû èñïîëüçóåòå äåéñòâèòåëüíî ñëó÷àéíûé èñòî÷íèê - ýòî íàìíîãî òðóäíåå, ÷åì êàæåòñÿ íà ïåðâûé âçãëÿä, ñì. ðàçäåë 17.14 - ýòî ñîâåðøåííî áåçîïàñíî.

Äðóãîé âàæíûé ìîìåíò: êëþ÷åâóþ ïîñëåäîâàòåëüíîñòü íèêîãäà íåëüçÿ èñïîëüçîâàòü âòîðîé ðàç. Äàæå åñëè âû èñïîëüçóåòå áëîêíîò ðàçìåðîì â íåñêîëüêî ãèãàáàéò, òî åñëè êðèïòîàíàëèòèê ïîëó÷èò íåñêîëüêî òåêñòîâ ñ ïåðåêðûâàþùèìèñÿ êëþ÷àìè, îí ñìîæåò âîññòàíîâèòü îòêðûòûé òåêñò. Îí ñäâèíåò êàæäóþ ïàðó øèôðîòåêñòîâ îòíîñèòåëüíî äðóã äðóãà è ïîäñ÷èòàåò ÷èñëî ñîâïàäåíèé â êàæäîé ïîçèöèè. Åñëè øèôðîòåêñòû ñìåùåíû ïðàâèëüíî, ñîîòíîøåíèå ñîâïàäåíèé ðåçêî âîçðàñòåò - òî÷íîå çíà÷åíèå çàâèñèò îò ÿçûêà îòêðûòîãî òåêñòà. Ñ ýòîé òî÷êè çðåíèÿ êðèïòàíàëèç íå ïðåäñòàâëÿåò òðóäà. Ýòî ïîõîæå íà ïîêàçàòåëü ñîâïàäåíèé, íî ñðàâíèâàþòñÿ äâà ðàçëè÷íûõ "ïåðèîäà" [904]. Íå èñïîëüçóéòå êëþ÷åâóþ ïîñëåäîâàòåëüíîñòü ïîâòîðíî.

Èäåÿ îäíîðàçîâîãî áëîêíîòà ëåãêî ðàñøèðÿåòñÿ íà äâîè÷íûå äàííûå. Âìåñòî îäíîðàçîâîãî áëîêíîòà, ñîñòîÿùåãî èç áóêâ, èñïîëüçóåòñÿ îäíîðàçîâûé áëîêíîò èç áèòîâ. Âìåñòî ñëîæåíèÿ îòêðûòîãî òåêñòà ñ êëþ÷îì îäíîðàçîâîãî áëîêíîòà èñïîëüçóéòå XOR. Äëÿ äåøèôðèðîâàíèÿ ïðèìåíèòå XOR ê øèôðîòåêñòó ñ òåì æå îäíîðàçîâûì áëîêíîòîì. Âñå îñòàëüíîå íå ìåíÿåòñÿ, è áåçîïàñíîñòü îñòàåòñÿ òàêîé æå ñîâåðøåííîé.

Âñå ýòî õîðîøî, íî ñóùåñòâóåò íåñêîëüêî ïðîáëåì. Òàê êàê êëþ÷åâûå áèòû äîëæíû áûòü ñëó÷àéíûìè è íå ìîãóò èñïîëüçîâàòüñÿ ñíîâà, äëèíà êëþ÷åâîé ïîñëåäîâàòåëüíîñòè äîëæíà ðàâíÿòüñÿ äëèíå ñîîáùåíèÿ. Îäíîðàçîâûé áëîêíîò óäîáåí äëÿ íåñêîëüêèõ íåáîëüøèõ ñîîáùåíèé, íî åãî íåëüçÿ èñïîëüçîâàòü äëÿ ðàáîòû ïî êàíàëó ñâÿçè ñ ïðîïóñêíîé ñïîñîáíîñòüþ 1.544 Ìáèò/ñ. Âû ìîæåòå õðàíèòü 650 Ìáàéò ñëó÷àéíûõ äàííûõ íà CD-ROM, íî è òóò åñòü ïðîáëåìû. Âî ïåðâûõ, âàì íóæíî òîëüêî äâå êîïèè ñëó÷àéíûõ áèòîâ, íî CD-ROM ýêîíîìè÷íû òîëüêî ïðè áîëüøèõ òèðàæàõ. È âî âòîðûõ, âàì íóæíî óíè÷òîæàòü èñïîëüçîâàííûå áèòû. Äëÿ CD-ROM íåò äðóãîé âîçìîæíîñòè óäàëèòü èíôîðìàöèþ êðîìå êàê ôèçè÷åñêè ðàçðóøèòü âåñü äèñê. Ãîðàçäî áîëüøå ïîäõîäèò öèôðîâàÿ ëåíòà.

Äàæå åñëè ïðîáëåìû ðàñïðåäåëåíèÿ è õðàíåíèÿ êëþ÷åé ðåøåíû, âàì ïðèäåòñÿ òî÷íî ñèíõðîíèçèðîâàòü ðàáîòó îòïðàâèòåëÿ è ïîëó÷àòåëÿ. Åñëè ïîëó÷àòåëü ïðîïóñòèò áèò (èëè íåñêîëüêî áèò ïðîïàäóò ïðè ïåðåäà÷å), ñîîáùåíèå ïîòåðÿåò âñÿêèé ñìûñë. Ñ äðóãîé ñòîðîíû, åñëè íåñêîëüêî áèò èçìåíÿòñÿ ïðè ïåðåäà÷å (è íè îäèí áèò íå áóäåò óäàëåí èëè äîáàâëåí - ÷òî ãîðàçäî áîëüøå ïîõîæå íà âëèÿíèå ñëó÷àéíîãî øóìà), òî ëèøü ýòè áèòû áóäóò ðàñøèôðîâàíû íåïðàâèëüíî. Íî îäíîðàçîâûå áëîêíîòû íå îáåñïå÷èâàþò ïðîâåðêó ïîäëèííîñòè.

Îäíîðàçîâûå áëîêíîòû èñïîëüçóþòñÿ è ñåãîäíÿ, ãëàâíûì îáðàçîì äëÿ ñâåðõñåêðåòíûõ êàíàëîâ ñâÿçè ñ íèçêîé ïðîïóñêíîé ñïîñîáíîñòüþ. Ïî ñëóõàì "ãîðÿ÷àÿ ëèíèÿ" ìåæäó Ñîåäèíåííûìè Øòàòàìè è áûâøèì Ñîâåòñêèì Ñîþçîì (à äåéñòâóåò ëè îíà ñåé÷àñ?) øèôðóåòñÿ ñ ïîìîùüþ îäíîðàçîâîãî áëîêíîòà. Ìíîãèå ñîîáùåíèÿ ñîâåòñêèõ øïèîíîâ çàøèôðîâàíû ñ èñïîëüçîâàíèåì îäíîðàçîâûõ áëîêíîòîâ. Ýòè ñîîáùåíèÿ íåðàñêðûòû ñåãîäíÿ è íàâñåãäà îñòàíóòñÿ íåðàñêðûòûìè. Íà ýòîì ôàêòå íå ïîâëèÿåò âðåìÿ ðàáîòû ñóïåðêîìïüþòåðîâ íàä ýòîé

ïðîáëåì. Äàæå êîãäà âðàãè èç ñîçâåçäèÿ Àíäðîìåäû ïðèçåìëÿò ñâîè òÿæåëûå êîðàáëè ñ êîì ïüþòåðàìè íåìûñëèìî ìîùíîñòè, è îíè íå ñìîãóò ïðî÷åñòü ñîîáùåíèÿ ñîâðåìåííûì, çàøèôðîâàííûå ñ ïîìîùüþ îäíîðàçîâûõ (åñëè, êîíå÷íî, íè íå ñìîãóò âñêðûòüñÿ â ïðîöåññå è äîáûòü íóæíûå îäíîðàçîâûå áëîêíîòû).

1.6 Êîìïüþòåðíûå àëãîðèòìû

Ñóùåñòâóåò ìíîæåñòâî êîìïüþòåðíûõ àëãîðèòìîâ. Ñëåäóþùèå òðè èñïîëüçóþòñÿ ÷àùå âñåãî:

— DES (Data Encryption Standard, ñòàíäàðò øèôðîâàíèÿ äàííûõ) - ñàìûé ïîïóëÿðíûé êîìïüþòåðíûé àëãîðèòì øèôðîâàíèÿ, ÿâëÿåòñÿ àìåðèêàíñêèì è ìåæäóíàðîäíûì ñòàíäàðòîì. Ýòî ñèììåòðè÷íûé àëãîðèòì, îäèí è òîò æå êëþ÷ èñïîëüçóåòñÿ äëÿ øèôðîâàíèÿ è äåøèôðîâàíèÿ.

— RSA (íàçâàí â ÷åñòü ñîçäàòåëåé - Ðèâåñòà (Rivest), Øàìèðà (Sharnir) è Ýäëìàíà (Adleman)) - ñàìûé ïîïóëÿðíûé àëãîðèòì ñ îòêðûòûì êëþ÷îì. Èñïîëüçóåòñÿ è äëÿ øèôðîâàíèÿ, è äëÿ öèôðîâîé ïîäïèñè.

— DSA (Digital Signature Algorithm, àëãîðèòì öèôðîâîé ïîäïèñè, èñïîëüçóåìûé êàê ÷àñòü ñòàíäàðòà öèôðîâîé ïîäïèñè, Digital Signature Standard) - äðóãîé àëãîðèòì ñ îòêðûòûì êëþ÷îì. Èñïîëüçóåòñÿ òîëüêî äëÿ öèôðîâîé ïîäïèñè, íå ìîæåò áûòü èñïîëüçîâàí äëÿ øèôðîâàíèÿ.

È ìåííî ýòè è ïîäîáíûå àëãîðèòìû îïèñûâàþòñÿ â ýòîé êíèãå.

1.7 Áîëüøèå ÷èñëà

Íà ïðîòÿæåíèè âñåé êíèãè ÿ èñïîëüçóþ ðàçëè÷íûå áîëüøèå ÷èñëà äëÿ îïèñàíèÿ ðàçëè÷íûõ âåùåé â êðèïòîãðàôèè. Òàê êàê ëåãêî çàáóäàòüñÿ â ýòèõ ÷èñëàõ è èõ çíà÷åíèÿõ, ôèçè÷åñêèå àíàëîãè íåêîòîðûõ ÷èñåë ïðèâåäåíû â 0-é.

Ýòè ÷èñëà îòëè÷àþòñÿ ïî ïðîèñõîæäåíèþ è áûëè îòêðûòû èç ðàçëè÷íûõ èñòî÷íèêîâ. Ì íîãèå àñòðîíîìè÷åñêèå çíà÷åíèÿ îáúÿñíÿþòñÿ â ðàáîòå Ôðèìàíà Äàéñîíà (Freeman Dyson), "Âðåìÿ áåç êîíöà: ôèçèêà è áèîëîãèÿ â îòêðûòîé Âñåëåííîé" ("Time Without End: Physics and Biology in an Open Universe") â *Reviews of Modem Physics*, v. 52, n. 3, July 1979, pp. 447-460. Ñìåðòíîñòü â ðåçóëüòàòå àâòîêàòàñòðîô ðàñ÷èòàíà ñ ïîìîùüþ ñòàòèñòèêè Ìèíñòåðñòâà òðàíñïîðòà (163 ìåðòâûõ ìëåêîïèòàíèíà ÷åëîâåê â 1993 ãîäó è äëÿ ñðåäíåé ïðîäîëæèòåëüíîñòè æèçíè 69.7 ãîäà.

Òàáë. 1-1. Áîëüøèå ÷èñëà

Ôèçè÷åñêèé àíàëîã	×èñëî
Âåðîÿòíîñòü áûòü óáèòûì ìîëíèåé (â òå÷åíèå äíÿ)	1 èç 9 ìèëëèàðäîâ (2^{33})
Âåðîÿòíîñòü âûèãðàòü ãëàâíûé ïðèç â ãîñóäàðñòâåííîé ëîòåðåå ÑØÀ	1 èç 4000000 (2^{22})
Âåðîÿòíîñòü âûèãðàòü ãëàâíûé ïðèç â ãîñóäàðñòâåííîé ëîòåðåå ÑØÀ è áûòü óáèòûì ìîëíèåé â òå÷åíèå òîãî æå äíÿ	1 èç2^{61}
Âåðîÿòíîñòü óòîíóòü (â ÑØÀ â òå÷åíèå ãîäà)	1 èç 59000 (2^{16})
Âåðîÿòíîñòü ïîãèáíóòü â àâòîêàòàñòðîôå (â ÑØÀ â ãîäó)	1 èç 6100 (2^{13})
Âåðîÿòíîñòü ïîãèáíóòü â àâòîêàòàñòðîôå (â ÑØÀ â òå÷åíèå âðåìåíè æèçíè)	1 èç 88 (2^{7})
Âðåìÿ äî ñëåäóþùåãî îëåäåíåíèÿ	14000 (2^{14}) ëåò
Âðåìÿ äî ïðåâðàùåíèÿ Ñîëíöà â ñâåðõíîâóþ çâåçäó	10^{9} (2^{30}) ëåò
Âîçðàñò ïëàíåòû	10^{9} (2^{30}) ëåò
Âîçðàñò Âñåëåííîé	10^{10} (2^{34}) ëåò
×èñëî àòîìîâ ïëàíåòû	10^{51} (2^{170})
×èñëî àòîìîâ Ñîëíöà	10^{57} (2^{190})
×èñëî àòîìîâ ãàëàêòèêè	10^{67} (2^{223})
×èñëî àòîìîâ Âñåëåííîé	10^{77} (2^{265})
Îáúåì Âñåëåííîé	10^{84} (2^{280}) ñì ^{3}

Âñëè Âñåëåííàÿ êîíå÷íà:

Ïîëíîå âðåìÿ æèçíè âñåëåííîé	10^{11} (2^{37}) ëåò
	10^{18} (2^{61}) ñåêóíä

Åñëè Âñåëåííàÿ áåñêîíå÷íà:

Âðåìÿ äî îñòûâàíèÿ ëåãêèõ çâåçä	10^{14} (2^{47}) ëåò
Âðåìÿ äî îòðûâà ïëàíåò îò çâåçä	10^{15} (2^{50}) ëåò
Âðåìÿ äî îòðûâà çâåçä îò ãàëàêòèê	10^{19} (2^{64}) ëåò
Âðåìÿ äî ðàçðóøåíèÿ îðáèò ãðàâèòàöèîííîé ðàäèàöèåé	10^{20} (2^{67}) ëåò
Âðåìÿ äî ðàçðóøåíèÿ ÷åðíûõ äûð ïðîöåññàìè Õîêèíãà	10^{64} (2^{213}) ëåò
Âðåìÿ äî ïðåâðàùåíèÿ ìàòåðèè â æèäêîñòü ïðè íóëåâîé òåìïåðàòóðå	10^{65} (2^{216}) ëåò
Âðåìÿ äî ïðåâðàùåíèÿ ìàòåðèè â òâåðäîå òåëî	$10^{10^{26}}$ ëåò
Âðåìÿ äî ïðåâðàùåíèÿ ìàòåðèè â ÷åðíóþ äûðó	$10^{10^{76}}$ ëåò

×àñòü 1

ÊÐÈÏÒÎÃÐÀÔÈ×ÅÑÊÈÅ ÏÐÎÒÎÊÎ-ËÛ

Ãëàâà 2
Ýëåìåíòû ïðîòîêîëîâ

2.1 Ââåäåíèå â ïðîòîêîëû

Ñìûñë êðèïòîãðàôèè - â ðåøåíèè ïðîáëåì. (Ïî ñóòè, â ýòîì ñîñòîèò è ñìûñë èñïîëüçîâàíèÿ êîìïüþòåðîâ, î ÷åì ìíîãèå ïûòàþòñÿ çàáûòü.) Êðèïòîãðàôèÿ ðåøàåò ïðîáëåìû ñåêðåòíîñòè, ïðîâåðêè ïîäëèííîñòè, öåëîñòíîñòè è ÷åëîâå÷åñêîé íå÷åñòíîñòè. Âû ìîæåòå âûó÷èòü âñå î êðèïòîãðàôè÷åñêèõ àëãîðèòìàõ è ìåòîäàõ, íî îíè ïðåäñòàâëÿþò òîëüêî àêàäåìè÷åñêèé èíòåðåñ, åñëè íå èñïîëüçóþòñÿ äëÿ ðåøåíèÿ êàêîé-íèáóäü ïðîáëåìû. Èìåííî ïîýòîìó ìû ñîáèðàåìñÿ ñíà÷àëà âçãëÿíóòü íà ïðîòîêîëû.

Ïðîòîêîë - ýòî ïîðÿäîê äåéñòâèé, ïðåäïðèíèìàåìûõ äâóìÿ èëè áîëåå ñòîðîíàìè, ïðåäíàçíà÷åííûé äëÿ ðåøåíèÿ îïðåäåëåííîé çàäà÷è. Ýòî âàæíîå îïðåäåëåíèå. "Ïîðÿäîê äåéñòâèé" îçíà÷àåò, ïðîòîêîë âûïîëíÿåòñÿ â îïðåäåëåííîé ïîñëåäîâàòåëüíîñòè, ñ íà÷àëà äî êîíöà. Êàæäîå äåéñòâèå äîëæíî âûïîëíÿòüñÿ â ñâîþ î÷åðåäü è òîëüêî ïîñëå îêîí÷àíèÿ ïðåäûäóùåãî. "Ïðåäïðèíèìàåìûõ äâóìÿ èëè áîëåå ñòîðîíàìè" îçíà÷àåò, ÷òî äëÿ ðåàëèçàöèè ïðîòîêîëà òðåáóåòñÿ ïî êðàéíåé ìåðå äâà ÷åëîâåêà, îäèí ÷åëîâåê íå ñìîæåò ðåàëèçîâàòü ïðîòîêîë. ×åëîâåê â îäèíî÷êó ìîæåò âûïîëíèòü íåêîòîðûå äåéñòâèÿ, ðåøàÿ çàäà÷ó (íàïðèìåð, ïîêóïàÿ òîðò), íî ýòî íå ïðîòîêîë. (Äëÿ òîãî, ÷òîáû ïîëó÷èëñÿ íàñòîÿùèé ïðîòîêîë, êòî-òî äîëæåí ñúåñòü òîðò.) Íàêîíåö, "ïðåäíàçíà÷åííûé äëÿ ðåøåíèÿ îïðåäåëåííîé çàäà÷è" îçíà÷àåò, ÷òî ïðîòîêîë äîëæåí ïðèâîäèòü ê êàêîìó-òî ðåçóëüòàòó. ×òî-òî, ïîõîæåå íà ïðîòîêîë, íî íå ðåøàþùåå íèêàêîé çàäà÷è - ýòî íå ïðîòîêîë, ýòî ïîòåðÿ âðåìåíè. Ó ïðîòîêîëîâ åñòü òàêæå è äðóãèå õàðàêòåðèñòèêè:

— Êàæäûé ó÷àñòíèê ïðîòîêîëà äîëæåí çíàòü ïðîòîêîë è ïîñëåäîâàòåëüíîñòü ñîñòàâëÿþùèõ åãî äåéñòâèé.

— Êàæäûé ó÷àñòíèê ïðîòîêîëà äîëæåí ñîãëàñèòüñÿ ñëåäîâàòü ïðîòîêîëó.

— Ïðîòîêîë äîëæåí áûòü íåïðîòèâîðå÷èâûì, êàæäîå äåéñòâèå äîëæíî áûòü îïðåäåëåíî òàê, ÷òîáû íå áûëî âîçìîæíîñòè íåïîíèìàíèÿ.

— Ïðîòîêîë äîëæåí áûòü ïîëíûì, êàæäîé âîçìîæíîé ñèòóàöèè äîëæíî ñîîòâåòñòâîâàòü îïðåäåëåííîå äåéñòâèå.

Â ýòîé êíèãå êàæäûé ïðîòîêîë îðãàíèçîâàí êàê íåêîòîðûé ïîðÿäîê äåéñòâèé. Âûïîëíåíèå ïðîòîêîëà ïðîèñõîäèò ïî äåéñòâèÿì, ëèíåéíî, ïîêà íå áóäåò êîìàíäû ïåðåéòè ê ñëåäóþùåìó äåéñòâèþ. Êàæäîå äåéñòâèå âêëþ÷àåò ïî êðàéíåé ìåðå îäíî èç äâóõ: âû÷èñëåíèÿ, âûïîëíÿåìûå îäíîé èëè íåñêîëüêèìè ñòîðîíàìè, èëè ñîîáùåíèÿ, êîòîðûìè îáìåíèâàþòñÿ ñòîðîíû.

Êðèïòîãðàôè÷åñêèé ïðîòîêîë - ýòî ïðîòîêîë, èñïîëüçóþùèé êðèïòîãðàôèþ. Ñòîðîíû ìîãóò áûòü äðóçüÿìè è ñëåïî äîâåðÿòü äðóã äðóãó èëè âðàãàìè è íå âåðèòü äðóã äðóãó äàæå ïðè ñîîáùåíèè âðåìåíè ñóòîê. Êðèïòîãðàôè÷åñêèé ïðîòîêîë âêëþ÷àåò íåêîòîðûé êðèïòîãðàôè÷åñêèé àëãîðèòì, íî, âîîáùå ãîâîðÿ, ïðåäíàçíà÷åíèå ïðîòîêîëà âûõîäèò çà ðàìêè ïðîñòîé áåçîïàñíîñòè. Ó÷àñòíèêè ïðîòîêîëà ìîãóò çàõîòåòü ïîäåëèòüñÿ ñåêðåòîì äðóã ñ äðóãîì, ñîâìåñòíî ãåíåðèðîâàòü ñëó÷àéíóþ ïîñëåäîâàòåëüíîñòü, ïîäòâåðäèòü äðóã äðóãó ñâîþ ïîäëèííîñòü èëè ïîäïèñàòü êîíòðàêò â îäèí è òîò æå ìîìåíò âðåìåíè. Ñìûñë èñïîëüçîâàíèÿ êðèïòîãðàôèè â ïðîòîêîëå - â ïðåäîòâðàùåíèè èëè îáíàðóæåíèè âðåäèòåëüñòâà è ìîøåííè÷åñòâà. Åñëè âû íèêîãäà íå ñòàëêèâàëèñü ñ ïîäîáíûìè ïðîòîêîëàìè, îíè ìîãóò ðàäèêàëüíî èçìåíèòü âàøå ïðåäñòàâëåíèå î òîì, ÷òî íåäîâåðÿþùèå äðóã äðóãó ñòîðîíû ìîãóò âûïîëíèòü, èñïîëüçóÿ êîìïüþòåðíóþ ñåòü. Îáùåå ïðàâèëî ìîæíî ñôîðìóëèðîâàòü ñëåäóþùèì îáðàçîì:

— Íåâîçìîæíî ñäåëàòü èëè óçíàòü áîëüøå, ÷åì îïðåäåëåíî â ïðîòîêîëå.

Ýòî ãîðàçäî ñëîæíåå, ÷åì êàæåòñÿ. Â ñëåäóþùèõ íåñêîëüêèõ ãëàâàõ ÿ ðàññìàòðèâàþ ìíîæåñòâî ïðîòîêîëîâ. Â íåêîòîðûõ èç íèõ îäèí èç ó÷àñòíèêîâ ìîæåò îáìàíóòü äðóãîãî. Â äðóãèõ, çëîóìûøëåííèê ìîæåò âçëîìàòü ïðîòîêîë èëè óçíàòü ñåêðåòíóþ èíôîðìàöèþ. Ðÿä ïðîòîêîëîâ ïðîâàëèâàþòñÿ, òàê êàê èõ ðàçðàáîò÷èêè íåäîñòàòî÷íî òùàòåëüíî îïðåäåëÿëè òðåáîâàíèÿ. Äðóãèå ïðîâàëèâàþòñÿ èç-çà òîãî, ÷òî èõ ðàçðàáîò÷èêè íåäîñòàòî÷íî òùàòåëüíî àíàëèçèðîâàëè ñâîè ïðîòîêîëû. Êàê è äëÿ àëãîðèòìîâ, ãîðàçäî ëåã÷å äîêàçàòü âîçìîæíóþ íåáåçîïàñíîñòü ïðîòîêîëà, ÷åì åãî ïîëíóþ áåçîïàñíîñòü.

Ñìûñë ïðîòîêîëîâ

Â ïîâñåäíåâíîé æèçíè ïî÷òè äëÿ âñåãî ñóùåñòâóþò íåôîðìàëüíûå ïðîòîêîëû: çàêàç òîâàðîâ ïî òåëåôîíó, èãðà â ïîêåð, ãîëîñîâàíèå íà âûáîðàõ. Íèêòî íå çàäóìûâàåòñÿ î ýòèõ ïðîòîêîëàõ, îíè âûðàáàòûâàëèñü â òå÷åíèå äëèòåëüíîãî âðåìåíè, âñå çíàþò, êàê èìè ïîëüçîâàòüñÿ è îíè ðàáîòàþò äîñòàòî÷íî õîðîøî.

Ñåãîäíÿ âñå áîëüøå è áîëüøå ëþäåé îáùàþòñÿ íå ëè÷íî, à èñïîëüçóÿ êîìïüþòåðíóþ ñåòü. Äëÿ òåõ æå âåùåé, êîòîðûå ëþäè äåëàþò íå çàäóìûâàÿñü, êîìïüþòåðàì íóæíû ôîðìàëüíûå ïðîòîêîëû. Êîãäà âû ïåðååçæàåòå èç ãîñóäàðñòâà â ãîñóäàðñòâî è îáíàðóæèâàåòå êàáèíêó, ñîâåðøåííî îòëè÷àþùóþñÿ îò òîé, ê êîòîðîé âû ïðè-

âûêëè, âû ëåãêî àäàïòèðóåòåñü. Êîì ïüþòåðû äàëåêî íå òàê ãèáêè.

×åñòíîñòü è áåçîïàñíîñòü ìíîãèõ ïðîòîêîëîâ ÷ëîâåê÷åñêîãî îáùåíèÿ îñíîâàíû íà ëè÷íîì ïðèñóòñòâèè. Ðàçâå âû äàäèòå íåçíàêîìöó êó÷ó äåíåã, ÷òîáû îí êóïèë äëÿ âàñ ÷òî-íèáóäü â áàêàëåå? Ñÿäüòå ëè âû èãðàòü â ïîêåð ñ òåì, êòî æóëüíè÷àåò, ñäàâàÿ êàðòû? Ïîøëåòå ëè âû ñâîé èçáèðàòåëüíûé áþëëåòåíü ïðàâèòåëüñòâó, íå áóäó÷è óâåðåííû â òàéíîñòè òàêîãî ãîëîñîâàíèÿ?

Íàèâíî ñ÷èòàòü, ÷òî ïîëüçîâàòåëè êîì ïüþòåðíûõ ñåòåé âñåãäà ÷åñòíû. Òàêæå íàèâíî ñ÷èòàòü, ÷òî âñåãäà ÷åñòíûì ðàçðàáîò÷èêè êîì ïüþòåðíûõ ñåòåé. Äëÿ áîëüøèíñòâà èç íèõ ýòî èìåííî òàê, íî äàæå íåñêîëüêî æóëèêîâ ìîãóò ïðèíåñòè íîãî âðåäà. Ôîðìàëèçèðóÿ ïðîòîêîëû, ìîæíî ïðîâåðèòü ñïîñîáû, èñïîëüçóåìûå æóëèêàìè äëÿ âçëîìà ïðîòîêîëîâ. Òàê ìû ìîæåì ðàçðàáîòàòü ïðîòîêîëû, óñòîé÷èâûå ê âçëîìó.

Êðîìå ôîðìàëèçàöèè äåéñòâèé, ïðîòîêîëû ïîçâîëÿþò àáñòðàãèðîâàòüñÿ ïðè ðåøåíèè çàäà÷è îò ñïîñîáà ðåøåíèÿ. Ïðîòîêîë ñâÿçè îäèí è òîò æå íà PC, è íà VAX. Ì îæíî ïðîâåðèòü ïðîòîêîë, íå âäàâàÿñü â äåòàëè åãî ðåàëèçàöèè. Êîãäà ìû óáåäèìñÿ â íàäåæíîñòè ïðîòîêîëà, åãî ìîæíî áóäåò ðåàëèçîâàòü ãäå óãîäíî îò êîì ïüþòåðà äî òåëåôîíîâ è èíòåëëåêòóàëüíûõ òîñòðîâ.

Èãðîêè

Äëÿ äåìîíñòðàöèè ðàáîòû ïðîòîêîëîâ ÿ èñïîëüçóþ íåñêîëüêî èãðîêîâ (ñì. 1-é). Ïåðâûå äâîå - ýòî Àëèñà è Áîá. Îíè ó÷àñòâóþò âî âñåõ äâóñòîðîííèõ ïðîòîêîëàõ. Êàê ïðàâèëî, Àëèñà (Alice) íà÷èíàåò âñå ïðîòîêîëû, à Áîá (Bob) îòâå÷àåò. Åñëè äëÿ ïðîòîêîëà íóæíà òðåòüÿ èëè ÷åòâåðòàÿ ñòîðîíà, â èãðó âñòóïàþò Êýðîë (Êýðîë) è Äýéâ (Dave). Äðóãèå èãðîêè èãðàþò ñïåöèàëüíûå âñïîìîãàòåëüíûå ðîëè, îíè áóäóò ïðåäñòàâëåíû ïîçæå.

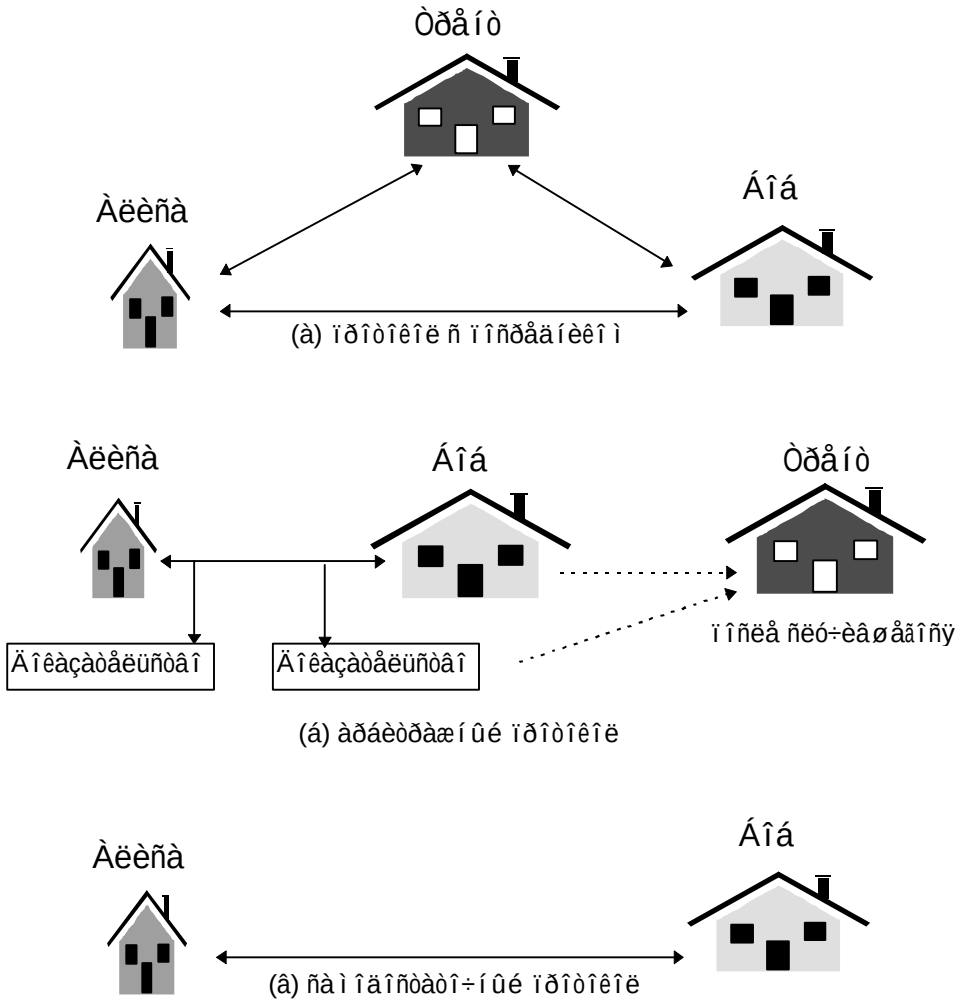
Ïðîòîêîëû ñ ïîñðåäíèêîì

Ïîñðåäíèê - ýòî íåçàèíòåðåñîâàííàÿ òðåòüÿ ñòîðîíà, êîòîðîé äîâåðÿþò çàâåðøåíèå ïðîòîêîëà (ñì. 1-é (à)). Íåçàèíòåðåñîâàííîñòü îçíà÷àåò, ÷òî ó ïîñðåäíèêà íåò çàèíòåðåñîâàííîñòè âðåçóëüòàòå ðàáîòû ïðîòîêîëà è ñêîííîñòè ê îäíîé èç ñòîðîí. "Äîâåðåí" îçíà÷àåò, ÷òî âñå ó÷àñòíèêè ïðîòîêîëà ïðèíèìàþò âñå, ÷òî ñêàçàíî ïîñðåäíèêîì çà èñòèíó, âñå åãî äåéñòâèÿ - êàê ïðàâèëüíûå, è óâåðåíû â òîì, ÷òî ïîñðåäíèê âûïîëíèò ñâîþ ÷àñòü ïðîòîêîëà. Ïîñðåäíèêè ïîìîãàþò ðàáîòàòü ðàçëè÷íûì ïðîòîêîëîâ âçàèìîäåéſòâèÿ íåäîâåðÿþùèõ äðóã äðóãó ñòîðîí.

Â ðåàëüíîì ìèðå â êà÷åſòâå ïîñðåäíèêîâ ÷àſòî âſòñóïàþò þðèſòû. Íàïðèìåð, Àëèſà ïðîäàåò íåçíàêîìîìó åé Áîáó ìàøèſó. Áîá õî÷åò çàïëàòèſü ÷åêîì, íî ó Àëèſû íåò ſòîſáà ïðîâåðèſü, äåſòàèſòåëåſ ëè ÷åê. Àëèſà õî÷åò, ſòîáû ðàſ÷åò ſî ſåêó áûë ïðîèſâåäåſ ſðåæäå, ſåſ ſðàâſ ſîſáſòâåſſîſòè ſåðåſäàò ê Áîáó. Áîá, êſòſðûſ âåðèſ Àëèſå íå áſëüſøå, ſåſ îſà åſó, íå õî÷åſ ſåðåſäàâàſü ſåê, íå ſſëſ÷èſ ſðàâà ſſáſòâåſſſòè.

Òàáë. 2-1. Äåéſòâóſùèå ëèöà

Àëèſà	Såðâſé ſ÷àſòſèê âſåſ ſðſòſêſëſâ
Áſá	Âſòſðſé ſ÷àſòſèê âſåſ ſðſòſêſëſâ
Êſðſë	Òſåſèé ſ÷àſòſèê â ſðſòſêſëſàſ ſ ſ÷àſòſèſì ſòſåſ è ſ÷åſûſåſ ſſòſðſſ
Äſéâ	×åſâſåſòſûé ſ÷àſòſèê â ſðſòſêſëſàſ ſ ſ÷àſòſèſì ſòſåſ è ſ÷åſûſåſ ſſòſðſſ
Åâà	Çſëſſó ſûſøſëſſſèê (eavesdropper)
Ìſýſëſîſè	Âſçſî ſ ſùſèſê ſðſòſêſëſâ
Òſåſſò	Çſàſñſóſæſèſâſàſþ ſùſéſé ſâſſâſåſðſÿ ſſſñſåſäſſèſê
Óſîſòſåſð	Êſſſòſðſëſåſð, ſçſàſùſèſ ſùſàſò Àſëſèſñſó è Áſſáſà â ſðſÿſäſå ſðſòſêſëſâ
Sſåſãſè	Ñſâſèſäſòſåſëſü
Âſèſêſòſð	Sðſîſâſåſðſÿſåſò ſſſäſëſèſſſſñſòſü



Ðèñ. 2-1. Òèïû ïðîòîêîëîâ

Ïîñðåäíè÷åñòâî þðèñòà óñòðîèò îáìåí. Ñ åãî ïîìîùüþ Àëèñà è Áîá ìîãóò âûïîëíèòü ñëåäóþùèé ïðîòîêîë, ÷òîáû çàùèòèòü ñåáÿ îò îáìàíà:

(1) Àëèñà ïåðåäàåò ïðàâî ñîáñòâåííîñòè þðèñòó.

(2) Áîá ïåðåäàåò ÷åê þðèñòó.

(3) Àëèñà äåïîíèðóåò ÷åê.

(4) Äîæäàâøèñü îïëàòû ÷åêà þðèñò ïåðåäàåò ïðàâî ñîáñòâåííîñòè Áîáó. Åñëè ÷åê íå îïëà÷åí â òå÷åíèå îïðåäåëåííîãî âðåìåíè, Àëèñà äîêàçûâàåò ýòî ôàêò þðèñòó, è òîò âîçâðàùàåò ïðàâî ñîáñòâåííîñòè Àëèñå.

Â ýòîì ïðîòîêîëå Àëèñà âåðèò, ÷òî þðèñò íå ïåðåäàñò Áîáó ïðàâî ñîáñòâåííîñòè äî òåõ ïîð, ïîêà ÷åê íå áóäåò îïëà÷åí, è âåðíåò ïðàâî ñîáñòâåííîñòè Àëèñå, åñëè ÷åê îïëà÷åí íå áóäåò. Áîá âåðèò, ÷òî þðèñò áóäåò îáëàäàòü ïðàâîì ñîáñòâåííîñòè äî òåõ ïîð, ïîêà ÷åê íå áóäåò îïëà÷åí, è ïåðåäàñò ïðàâî ñîáñòâåííîñòè Áîáó ñðàçó æå ïîñëå îïëàòû ÷åêà. Þðèñò íå çàáîòèòñÿ îá îïëàòå ÷åêà. Î í â ëþáîì ñëó÷àå âûïîëíèò ñâîþ ÷àñòü ïðîòîêîëà, ââåäü åì çàïëàòÿò â ëþáîì ñëó÷àå.

Â ýòîì ïðèìåðå þðèñò èãðàåò ðîëü ïîñðåäíèêà. Þðèñòû ÷àñòî âûñòóïàþò â ðîëè ïîñðåäíèêîâ ïðè çàâåùàíèÿõ è èíîãäà ïðè ïåðåãîâîðàõ î êîíòðàêòå. Ðàçëè÷íûå áèðæè âûñòóïàþò â êà÷åñòâå ïîñðåäíèêîâ ìåæäó ïîêóïàòåëÿìè è ïðîäàâöàìè.

Â êà÷åñòâå ïîñðåäíèêà ìîæåò âûñòóïèòü è áàíê - äëÿ ïîêóïêè ìàøèíû:

(1) Áîá çàïîëíÿåò ÷åê è ïåðåäàåò åãî â áàíê.

(2) Åñëè íà ñ÷åòó Áîáà äîñòàòî÷íî äåíåã äëÿ ïîêðûòèÿ ÷åêà, áàíê çàâåðÿåò ÷åê è âîçâðàùàåò åãî Áîáó.

(3) Àëèñà ïåðåäàåò Áîáó ïðàâî ñîáñòâåííîñòè, à Áîá ïåðåäàåò Àëèñå çàâåðåííûé ÷åê.

(4) Àëèñà äåïîíèðóåò ÷åê.

Ýòîò ïðîòîêîë ðàáîòàåò, ïîòîìó ÷òî Àëèñà âåðèò áàíêîâñêîìó ñâèäåòåëüñòâó. Àëèñà âåðèò, ÷òî áàíê ñîõðàíèò äåíüãè Áîáà äëÿ íåå è íå èñïîëüçóåò èõ äëÿ ôèíàíñèðîâàíèÿ ñîáñòâåííûõ îïåðàöèé ñ íåäâèæèìîñòüþ â

áàíàíîâûõ ðåñïóáëèêàõ.

Äðóãèì îáùåïðèíÿòûì ïîñðåäíèêîì ÿâëÿåòñÿ íîòàðèóñ. Êîãäà Áîá ïîëó÷àåò îò Àëèñû çàâåðåííûé íîòàðèóñîì äîêóìåíò, îí óáåæäåí, ÷òî Àëèñà ïîäïèñàëà äîêóìåíò ïî ñâîåìó æåëàíèþ è ñîáñòâåííîðó÷íî. Ïðè íåîáõîäèìîñòè íîòàðèóñ ìîæåò âûñòóïèòü â ñóäå è çàñâèäåòåëüñòâîâàòü ýòîò ôàêò.

Ïîíÿòèå ïîñðåäíèêà ñòàðî êàê ìèð. Âñåãäà ñóùåñòâîâàëè îïðåäåëåííûå ëþäè - âîæäè, æðåöû è òîìó ïîäîáíîå - îáëàäàâøèå âëèÿíèåì, ïîçâîëÿþùèì èì äåéñòâîâàòü ñïðàâåäëèâî. Ïîñðåäíèêè èãðàþò îïðåäåëåííóþ ðîëü â íàøåì îáùåñòâå, îáìàí äîâåðèÿ ïîäîðâàë áû çàíèìàåìîå èìè ïîëîæåíèå. Þðèñòû-ïîñðåäíèêè, íàðóøàþùèå ïðàâèëà èãðà, ïîäâåðãàþòñÿ íàêàçàíèþ - íàïðèìåð, èñêëþ÷åíèþ èç êîëëåãèè àäâîêàòîâ. Ýòî èäåàëüíàÿ êàðòèíà, â ðåàëüíîì ìèðå ïîëîæåíèå, ê ñîæàëåíèþ, ìîæåò îòëè÷àòüñÿ îò íåå.

Ýòîò èäåàë ìîæíî ïåðåíåñòè íà ìèð êîìïüþòåðîâ, íî ñ êîìïüþòåðíûìè ïîñðåäíèêàìè ñóùåñòâóåò ðÿä ïðîáëåì:

— Ëåãêî íàéòè íåéòðàëüíóþ òðåòüþ ñòîðîíó, êîòîðîé ìîæíî äîâåðÿòü, åñëè âû çíàåòå ïîñðåäíèêà è ìîæåòå ëè÷íî óâèäåòü åãî. Äâå ñòîðîíû, îòíîñÿùèåñÿ äðóã ê äðóãó ñ ïîäîçðåíèåì, ñ òåì æå ïîäîçðåíèåì îòíåñóòñÿ è ê áåçëèêîìó ïîñðåäíèêó, çàòåðÿííîìó ãäå-òî â ñåòè.

— Êîìïüþòåðíàÿ ñåòü äîëæíà îáåñïå÷èòü ïîääåðæêó ïîñðåäíèêà. Çàíÿòîñòü þðèñòîâ îáùåèçâåñòíà, íà êîãî â ñåòè ëÿãóò äîïîëíèòåëüíûå íàêëàäíûå ðàñõîäû?

— Ñóùåñòâóåò çàäåðæêà, ïðèñóùàÿ âñåì ïðîòîêîëàì ñ ïîñðåäíèêîì.

— Ïîñðåäíèê äîëæåí ïðèíèìàòü ó÷àñòèå â êàæäîé òðàíçàêöèè, ÿâëÿÿñü óçêèì ìåñòîì â êðóïíîìàñøòàáíûõ ðåàëèçàöèÿõ ëþáîãî ïðîòîêîëà. Ðîñò ÷èñëà ïîñðåäíèêîâ ñìÿã÷èò ýòó ïðîáëåìó, íî âûðàñòåò è öåíà ýòîé óñëóãè.

— Òàê êàê êàæäûé â ñåòè äîëæåí äîâåðÿòü ïîñðåäíèêó, òî ïîñðåäíèê ïðåäñòàâëÿåò ñîáîé ñëàáîå ìåñòî ñåòè ïðè ïîïûòêå åå âçëîìà.

Íåñìîòðÿ íà ýòî ïîñðåäíè÷åñòâî âñå åùå àêòèâíî èñïîëüçóåòñÿ. Â ïðîòîêîëàõ ñ èñïîëüçîâàíèåì ïîñðåäíèêà ýòó ðîëü áóäåò èãðàòü Òðåíò.

Àðáèòðàæíûå ïðîòîêîëû

Èñïîëüçóåìûé èç-çà âûñîêîé ñòîèìîñòè íàéìà ïîñðåäíèêîâ àðáèòðàæíûå ïðîòîêîëû ìîæåò áûòü ðàçáèò íà äâà **ïîäïðîòîêîëà** íèæíåãî óðîâíÿ. Ïåðâûé ïðåäñòàâëÿåò ñîáîé ïðîòîêîë áåç ïîñðåäíèêà, èñïîëüçóåìûé ïðè æåëàíèè ñòîðîí âûïîëíèòü ïðîòîêîë. Äðóãîé ïðåäñòàâëÿåò ñîáîé ïðîòîêîë ñ ïîñðåäíèêîì, ïðèãëàøàåìûì â èñêëþ÷èòåëüíûõ îáñòîÿòåëüñòâàõ - ïðè íàëè÷èè ðàçíîãëàñèé ìåæäó ñòîðîíàìè. Ñîîòâåòñòâóþùèé ñïåöèàëüíûé ïîñðåäíèê íàçûâàåòñÿ **àðáèòðîì** (ñì. 1-é(á)).

Àðáèòð, êàê è ïîñðåäíèê, ïðåäñòàâëÿåò ñîáîé íåçàèíòåðåñîâàííîãî ó÷àñòíèêà ïðîòîêîëà, êîòîðîìó äîâåðÿþò îáå ñòîðîíû. Â îòëè÷èå îò ïîñðåäíèêà îí íåïîñðåäñòâåííî íå ïðèíèìàåò ó÷àñòèÿ â êàæäîé îòäåëüíîé ðåàëèçàöèè ïðîòîêîëà è ïðèãëàøàåòñÿ òîëüêî äëÿ ïðîâåðêè ÷åñòíîñòè âûïîëíåíèÿ ïðîòîêîëà ñòîðîíàìè.

Ïðîôåññèîíàëüíûìè àðáèòðàìè ÿâëÿþòñÿ ñóäüè. Â îòëè÷èå îò íîòàðèóñîâ ê ñóäüÿì îáðàùàþòñÿ òîëüêî ïðè ïîÿâëåíèè ðàçíîãëàñèé. Àëèñà è Áîá ìîãóò çàêëþ÷èòü êîíòðàêò áåç ó÷àñòèÿ ñóäüè. Ñóäüÿ íèêîãäà íå óçíàåò î êîíòðàêòå, åñëè îäíà èç ñòîðîí íå ïîäàñò íà äðóãóþ â ñóä. Ïðîòîêîë ïîäïèñàíèÿ êîíòðàêòà ìîæíî ôîðìàëèçîâàòü ñëåäóþùèì îáðàçîì:

Ïîäïðîòîêîë áåç ïîñðåäíèêà (âûïîëíÿåòñÿ âñåãäà):

(1) Àëèñà è Áîá äîãîâàðèâàþòñÿ îá óñëîâèÿõ êîíòðàêòà.

(2) Àëèñà ïîäïèñûâàåò êîíòðàêò.

(3) Áîá ïîäïèñûâàåò êîíòðàêò.

Ïîäïðîòîêîë ñ èñïîëüçîâàíèåì àðáèòðà (âûïîëíÿåòñÿ ïðè íàëè÷èè ðàçíîãëàñèé):

(4) Àëèñà è Áîá ïðåäñòàþò ïåðåä ñóäüåé.

(5) Àëèñà ïðåäîñòàâëÿåò ñâîè äîêàçàòåëüñòâà.

(6) Áîá ïðåäîñòàâëÿåò ñâîè äîêàçàòåëüñòâà.

(7) Ñóäüÿ ïðèíèìàåò ðåøåíèå íà îñíîâàíèè äîêàçàòåëüñòâ.

Ðàçëè÷èå èñïîëüçóåìûõ â ýòîé êíèãå ïîíÿòèé ïîñðåäíèêà è àðáèòðà ñîñòîèò â òîì, ÷òî ó÷àñòèå àðáèòðà ïðîèñõîäèò íå âñåãäà. Ñòîðîíû îáðàùàþòñÿ ê ñóäüå òîëüêî ïðè ðàçíîãëàñèÿõ. Åñëè ðàçíîãëàñèé íåò, ñóäüÿ íå íóæåí.

Ñóùåñòâóþò àðáèòðàæíûå êîìïüþòåðíûå ïðîãðàìì, ÷òî ó÷àñòâóþùèå ñòîðîíû ÷åñòíû, íî ïðè ïîäãîòîâêå î âîçìîæíîì ìîøåíè÷åñòâå ïî ñóùåñòâóþùåìó íàíîñó äàííûõ òðåòüþ ñòîðîíà, êîòîðîé äîâåðÿþò ó÷àñòíèêè, ñìîæåò îáíàðóæèòü ôàêò ìîøåíè÷åñòâà. Õîðîøèé àðáèòðàæíûé ïðîöåññ äîëæåí ïîçâîëÿòü àðáèòðó óñòàíîâèòü è ëè÷íîñòü ìîøåíèêà. Àðáèòðàæíûå ïðîöåññû îáû÷íî ïðîõîäÿò íà ïðåäóïðåäæàþò ìîøåíè÷åñòâî. Íåîáõîäèìîñòü îáíàðóæåíèÿ âûòóïàåò â êà÷åſòâå ïðåäóïðåäèòåëüíîé ìåðû, ïðåäîòâðàùàÿ ìîøåíè÷åſòâî.

Ñàìîäîñòàòî÷íûå ïðîöåññû

Ñàìîäîñòàòî÷íûé ïðîöåññ ÿâëÿåòſÿ ëó÷øèì òèïîì ïðîöåññà. Îí ïîëíîſòüþ îáåſïå÷èâàåò ÷åſòíîſòü ſòîðîí (ſì. 1-é(â)). Äëÿ âûïîëíåíèÿ ïðîöåſſà íå íóæåí íè îſſòàäíèê, íå ðåøàþùèé ſïîſòó àðáèòð. Ñàìî ïîſòðîåíèå ïðîöåſſà îáåſïå÷èâàåò ſòſóòſòâèå ſïîſòó. Åſëè îáíà èç ſòîſòî ïîſûòàåòſÿ ſì îſíîſòè÷åſòü, ſì îſíè÷åſòü áóäåò íàìåëåííî íáíàðóæåſíî äóãîé ſòîſòîſíé, è ïðîöåſſ ïðåêðàòèò âûſîſíÿòſÿ. ×åſî áû íå ïûòàëſü äîáèòſÿſ ſì îſíè÷àþ ùàÿ ſòîſòîſíà, ýòî ſì óſ íåæäåſíî ſëó÷èòſÿ.

Â ëó÷øåſ ſìèðå ëþáîé ïðîöåſſ äîëæåſ áûòü ſàſìîäîſòàòî÷íûſ, íî, ê íåſ÷àſòüþ, íå ſóùåſòâóåò ſàſìîäîſòàòî÷íûõ ïðîöåſſîâ äëÿ êàæäîé ſèòóàöèè.

Ïîſòóïêè âſêðûòèÿ ïðîöåſſîâ

Êðèſòîãðàôè÷åſêèå íſſûòêè âçſîſà ſîãóò áûòü íàïðàâëåíû ïðîòèâ êðèſòîãðàôè÷åſêèõ àëãîðèſſſîâ, èſſïîëüçóåſſûõ â ïðîöåſſîâõ, ïðîòèâ êðèſòîãðàôè÷åſêèõ ſåòîäîâ, èſïſïëüçóåſſûõ äëÿ ðåøåþùèé ſïſðû àðáèòð. Ñàſî ïîſòðîåſèå ïðîòîſêîëà îáåſïå÷èâàåò îòñóòſòâèå ſïſðîſ. Åſëè îáíà èç ſòîſòî ïſſûòàåſſÿ ſì îſíè÷àòü, ſì îſíè÷åſòü áóäåò íàſìäëåííî îáíàðóæåſíî äóãîé ſòîſòſíé, è ïðîòîſêîë ïðåêðàòèò âûſïîëíÿòſÿ. ×åſî áû íå ſûòàëſſ ſì îſíè÷àþ ùàÿ ſòîſòſíà, ýòſì óſ íóæäåſíî ſëó÷èòſÿ.

Ê ïîſòóïêè äîſòóïêè äîëæåſ áûòü ſàſìîäîſòàòî÷íûſ, íî, ê íåſ÷àſòüþ, íå ſóùåſòâóåò ſàſìîäîſòàòî÷íûõ ïðîòîſêîëîâ äëÿ êàæäîé ſèòóàöèè.

Ïîſòóïêè âſêðûòèÿ ïðîòîſêîëîâ

Êðèſòîãðàôè÷åſêèå íſſûòêè âçſîſà ſîãóò áûòü íàïðàâëåíû ïðîòèâ êðèſòîãðàôè÷åſêèõ àëãîðèſſſîâ, èſſïîëüçóåſſûõ â ïðîòîſêîëàõ, ſîãóò íåſïîſòðåſſſòâîâàſſ ſïſðîſòîſêîëû, ïðîòèâ êðèſòîãðàôè÷åſêèõ àòàſ íà ſòîſòîſêîëû. Ïſñêîëüêó â ýòſì ðàçäåëå êſêàê îáñóæäàþſſÿ èſſſëåäſíèſ íàſſſòîſòſíèſ, ſòîſòîſêîëû, ÿ ïðåäſïîëàãàþ, ÷òî êðèſòîãðàôè÷åſêèå àëãîðèſſſ è ſåòîäû áåçſïàſſíû, è ðàſſſàòðèâàþ òſëüêî ſſſûòêè âſêðûòèÿ ïðîòîſêîëîâ.

Ëþäè ſſîãóò èſſſîëüçſîâàòü ſſſæåſòâſ ſïſſſſíáſîâ âçſêſſàòü ſïðîſêſſ. Íåſòſðûå, íå ÿâëÿſſſü ó÷àſòſíèêàſſ ſïðîòſêſëà, ſſîãóò "ſſïäëóøèâàòü" êàêóþ-òſ ÷àſòü èëè âåſü ſïðîòſêſſ. Ýòſ íàçûâàåòſÿ **ſàſſſèâſû ſ âſêðûòèåſ**, òàê êàê âçëſſſùèê íå âſçäåéſòâóåò íà ſïðîòſêſſ. Âſå, ÷òſ ſſ ſſæåò ſääëàòü - ýòſ ſïðſſëääèòü çà ſïðſòſêſëſſ è ſſſûòàòüſÿ äſáûòü èſſôſðſàòèſ. Ýòſò òèſ âſêðûòèÿ ſſſòâåòſòâóåò âſêðûòèþ ſ èſſſſëüçſâàíèåſ òſëüêſ øèôðſòåſêà, ſáſóæäàâøåſóſÿ â ðàçäåëå 1.1. Òàê êàê ſàſſſèâſûå âſêðûòèÿ òðóäſſ ſáſàðóæèòü, ſïðſòſêſëû ſòðåſſÿòſÿ ſïðåſòâðàùàòü, à íå ſáſàðóæèâàòü èſ. Â ýòèſ ſïðſòſêſëàſ ðſëü çëſóſûøèſíèêà áóäåò èſàòſ Ââà.

Â äðóãſ ſëó÷àå âçëſſùèê ſſæåò ſſſûòàòüſÿ èçſåſèòſ ſïðſòſêſë äëÿ ſſâſòâſſſſé âûãſäû. Sſ ſſæåò âûäàòſ ſåáÿ çà äðóãſãſ, ââåſòè ſſâûå ſſſâúſåſèÿ â ſïðſòſêſë, çàſåſèòſ ſàſſ ſſſâúſåſèå äðóãè, ſſâòſðſſ ſïåðääòſ ſòàðûå ſſſâúſåſèÿ, ðàçſðâàòſ êàſàë ſâÿçè èëè èçſåſèòſ ſðàſÿúóſſÿ â êſſ ſüþòåðå èſſôſðſàòèþ. Òàêèå äåéſòâèÿ íàçûâàþſſÿ àêòèâſû ſâſêðûòèſ, òàê êàê ſſé òðåáóþò àêòèâſſãſ âſåøàòåëüſòâà. Ýòè ôſðſ ſâſêðûòèÿ çàâèſÿò ſò âèäà ſåòè.

Ïàſſèâſûå âçëſſùèêè ſòàðàþſÿ ſſëó÷èòſ èſôſðſàòèþ ſá ó÷àſòſíèêàſ ſðſòſêſëà. Sſé ſſáèðàþò ſſſáúåſíèÿ, ſåðåäàſſſûå ðàçëè÷ſûſ ſſſ-òſ ſſâſåſſ ſſſòſðſſſíèé, ſſ ſſæåò áûòü çàðåſèſòðàòſſſâſſ ſſſüçſâàòåëſſſ ſèſſſ è ſäæå ſèſòſſſſ ſäſſſèſòðàòſðſ. Sſæåò áûòü äàæå ſåſêſëüêſ àêòèâſûſ âçëſſùèêſ, ðàſſòàþ ùèſ âſåſòå. Â ýòſé êſèåå ðſëü çëſſſàſåðſſſâſ àêòèâſſãſ âçëſſùèêà áóäåò èãðàòü Ìýëſðè.

Âçëſſùèêſ ſſæåò áûòü è ſâèſ èç ó÷àſòſíèêſâ ſïðſòſêſëà. Sſ ſſæåò ſáſàſſûâàòü, âûſſëſÿÿ ſïðſòſêſë, èëè âſâſå ſå ſëåäſâàòü ſðàâèëàſ ſðſòſêſëà. Òàêſé âçëſſùèê ſàçûâàåòſÿ **ſſøſſſíèêſſ**. **Ïàſſèâſûå ſſøſſſíèêè** âûſſſëſÿþò ſðàâèëà ſðſòſêſëà, ſſ ſòàðàþſÿ ſſëó÷èòſ áſëüøå èſſôſðſàòèè, ÷åſ ſïðåóſſſòðåſſ ſðſòſêſëſ. **Àêòèâſûå ſſøſſſíèêè** ſáðóøàþò ðàáſòó ſïðſòſêſëà, ſûòàÿſſ ſſſøſſſíè÷àòü.

S÷åſü òðóäſſ ſſäåðæèâàòü áåçſïàſſſſòü ſïðſòſêſëà, åſëè áſëüøèſſòâſ åãſ ó÷àſòſíèêſâ - àêòèâſûå ſſøſſſíèêè, ſſ èſſãàä àêòèâſſå ſſøſſſíè÷åſòâſ ſſæåò áûòü ſáſàðóæåſſ çàêſſſûſ è ó÷àſòſíèêſ. Êſſå÷ſſ, ſïðſòſêſëû äſëæſû áûòü çàſèſùſû è ſò ſàſſſèâſſãſ ſſøſſſíè÷åſòâ.

2.2 Ïåðåä÷à èſôſðſàöèè ſ èſſïſëüçſâàſèåſ ſèſſſòðè÷ſſſé êðèſòſãðàôſè

Êàê äâóſ ſòſðſſàſ áåçſïàſſſ ſáſſſíèâàòüſÿ èſôſðſàöèåé? Êſſå÷ſſ æå, øèôðóþ ſáſè ſſſáúåſíèÿ. Ïſſſſòðè, ÷òſ äſëæſſ ſðſèçſéòè, êſãää Àëèſà ſſſûëåò øèôðſâàſſſå ſſſáúåſíèå Áſáó (ſſëſûé ſðſòſêſëſ ãſðàçãſ ſëſæſåå).

(1) Àëèſà è Áſá âûáèðàþò ſèſòåſ øèôðſâàſíÿ.

(2) Àëèſà è Áſá âûáèðàþò êëþ÷.

(3) Àëèñà øèôðóåò îòêðûòûé òåêñò ñâîåãî ñîîáùåíèÿ ñ èñïîëüçîâàíèåì àëãîðèòìà øèôðîâàíèÿ è êëþ÷à, ïîëó÷àÿ øèôðîâàííîå ñîîáùåíèå.

(4) Àëèñà ïîñûëàåò øèôðîâàííîå ñîîáùåíèå Áîáó.

(5) Áîá äåøèôðèðóåò øèôðîòåêñò ñîîáùåíèÿ ñ èñïîëüçîâàíèåì àëãîðèòìà øèôðîâàíèÿ è êëþ÷à, ïîëó÷àÿ îòêðûòûé òåêñò ñîîáùåíèÿ.

×òî ìîæåò Åâà, íàõîäÿñü ìåæäó Àëèñîé è Áîáîì, óçíàòü, ïîäñëóøèâàÿ ýòîò ïðîòîêîë? Åñëè îíà ìîæåò ïîäñëóøàòü òîëüêî ïåðåäà÷ó íà ýòàïå (4), åé ïðèäåòñÿ ïîäâåðãíóòü øèôðîòåêñò êðèïòîàíàëèçó. Ýòî ïàññèâíîå âñêðûòèå ïðåäñòàâëÿåò ñîáîé âñêðûòèå ñ èñïîëüçîâàíèåì òîëüêî øèôðîòåêñòà, ïðèìåíÿåìûå àëãîðèòìû óñòîé÷èâû (íàñêîëüêî íàì èçâåñòíî) ïî îòíîøåíèþ ê ëþáûì âû÷èñëèòåëüíûì ìîùíîñòÿì, êîòîðûå ìîæåò çàïîëó÷èòü Åâà äëÿ ðåøåíèÿ ïðîáëåìû.

Åâà, îäíàêî, íå ãëóïà. Îíà ìîæåò òàêæå ïîäñëóøàòü è ýòàïû (1) è (2). Òîãäà åé ñòàíóò èçâåñòíû àëãîðèòì è êëþ÷ - òàêæå êàê è Áîáó. Êîãäà îíà ïåðåõâàòèò ñîîáùåíèå íà ýòàïå (4), òî åé îñòàíåòñÿ òîëüêî äåøèôðîâàòü åãî ñàìîñòîÿòåëüíî.

Â õîðîøåé êðèïòîñèñòåìå áåçîïàñíîñòü ïîëíîñòüþ çàâèñèò îò çíàíèÿ êëþ÷à è àáñîëþòíî íå çàâèñèò îò çíàíèÿ àëãîðèòìà. Èìåííî ïîýòîìó óïðàâëåíèå êëþ÷àìè òàê âàæíî â êðèïòîãðàôèè. Èñïîëüçóÿ ñèììåòðè÷íûé àëãîðèòì, Àëèñà è Áîá ìîãóò îòêðûòî âûïîëíèòü ýòàï (1), íî ýòàï (2) îíè äîëæíû ñîõðàíèòü â òàéíå. Êëþ÷ äîëæåí îñòàâàòüñÿ â ñåêðåòå ïåðåä, ïîñëå è â òå÷åíèå ðàáîòû ïðîòîêîëà - äî òåõ ïîð, ïîêà äîëæíî îñòàâàòüñÿ â òàéíå ïåðåäàâàåìîå ñîîáùåíèå - â ïðîòèâíîì ñëó÷àå ñîîáùåíèå òóò æå áóäåò ðàñêðûòî. (Î êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè, ðåøàþùåé ýòó ïðîáëåìó èíà÷å, ðàññêàçûâàåòñÿ â ðàçäåëå 2.5.)

Ìýëëîðè, àêòèâíûé âçëîìùèê, ìîæåò ñäåëàòü êîå-÷òî äðóãîå. Îí ìîæåò ïîïûòàòüñÿ íàðóøèòü ëèíèþ ñâÿçè íà ýòàïå (4), ñäåëàâ òàê, ÷òî Àëèñà âîîáùå íå ñìîæåò ïåðåäàâàòü èíôîðìàöèþ Áîáó. Ìýëëîðè òàêæå ìîæåò ïåðåõâàòèòü ñîîáùåíèå Àëèñû è çàìåíèòü åãî ñâîèì ñîáñòâåííûì. Åñëè åìó óäàëîñü óçíàòü êëþ÷ (ïåðåõâàòèâ îáìåí èíôîðìàöèåé íà ýòàïå (2) èëè âçëîìàâ êðèïòîñèñòåìó), îí ñìîæåò çàøèôðîâàòü ñâîå ñîîáùåíèå è îòïðàâèòü åãî Áîáó âìåñòî ïåðåõâà÷åííîãî, è Áîá íå ñìîæåò óçíàòü, ÷òî ñîîáùåíèå îòïðàâëåíî íå Àëèñîé. Åñëè Ìýëëîðè íå çíàåò êëþ÷à, îí ìîæåò òîëüêî ñîçäàòü ñîîáùåíèå, ïðåâðàùàþùååñÿ ïðè äåøèôðîâêå â áåññìûñëèöó. Áîá, ñ÷èòàÿ, ÷òî ñîîáùåíèå îòïðàâëåíî Àëèñîé, ìîæåò ðåøèòü, ÷òî ëèáî ó Àëèñû, ëèáî â ñåòè âîçíèêëè ñåðüåçíûå ïðîáëåìû.

À Àëèñà? ×òî îíà ìîæåò ñäåëàòü, ÷òîáû èñïîðòèòü ïðîòîêîë? Îíà ìîæåò ïåðåäàòü êîïèþ êëþ÷à Åâå, è òîãäà Åâà ñìîæåò ÷èòàòü âñå, ÷òî ãîâîðèò Áîá, è íàïå÷àòàòü åãî ñëîâà â *Íüþ-Éîðê Òàéìñ*. Ýòî ñåðüåçíî, íî ïðîáëåìà íå â ïðîòîêîëå. Àëèñà è òàê ìîæåò ïåðåäàâàòü Åâå ëþáûå îòêðûòûå òåêñòû, ïåðåäàâàåìûå ñ èñïîëüçîâàíèåì ïðîòîêîëà. Êîíå÷íî, òî æå ñàìîå ìîæåò ñäåëàòü è Áîá. Ïðîòîêîë ïðåäïîëàãàåò, ÷òî Àëèñà è Áîá äîâåðÿþò äðóã äðóãó. Èòàê, ñèììåòðè÷íûì êðèïòîñèñòåìàì ïðèñóùè ñëåäóþùèå ïðîáëåìû:

— Ðàñïðåäåëåíèå êëþ÷åé äîëæíî ïðîâîäèòüñÿ â ñåêðåòå. Êëþ÷è ñòîëü æå âàæíû, êàê è âñå ñîîáùåíèÿ, çàøèôðîâàííûå ýòèìè êëþ÷àìè, òàê êàê çíàíèå êëþ÷à ïîçâîëÿåò ðàñêðûòü âñå ñîîáùåíèÿ. Äëÿ ðàñïðîñòðàíåííûõ ñèñòåì øèôðîâàíèÿ çàäà÷à ðàñïðåäåëåíèÿ êëþ÷åé - ñåðüåçíåéøàÿ çàäà÷à. ×àñòî êóðüåðû ëè÷íî äîñòàâëÿþò êëþ÷è ïî íàçíà÷åíèþ.

— Åñëè êëþ÷ ñêîìïðîìåòèðîâàí (óêðàäåí, ðàçãàäàí, âûïûòàí, ïîëó÷åí çà âçÿòêó è ò.ä.), òî Åâà ñìîæåò ðàñøèôðîâàòü âñå ñîîáùåíèÿ, çàøèôðîâàííûå ýòèì êëþ÷îì. Îíà ñìîæåò òàêæå âûñòóïèòü â êà÷åñòâå îäíîé èç ñòîðîí è ñîçäàâàòü ëîæíûå ñîîáùåíèÿ, äóðà÷à äðóãóþ ñòîðîíó.

— Â ïðåäïîëîæåíèè, ÷òî êàæäàÿ ïàðà ïîëüçîâàòåëåé ñåòè èñïîëüçóåò îòäåëüíûé êëþ÷, îáùåå ÷èñëî êëþ÷åé áûñòðî âîçðàñòàåò ñ ðîñòîì ÷èñëà ïîëüçîâàòåëåé. Ñåòü èç n ïîëüçîâàòåëåé òðåáóåò *n{n - l)/2* êëþ÷åé. Íàïðèìåð, äëÿ îáùåíèÿ 10 ïîëüçîâàòåëåé ìåæäó ñîáîé íóæíî 45 ðàçëè÷íûõ êëþ÷åé, äëÿ 100 ïîëüçîâàòåëåé ïîòðåáóåòñÿ 4950 êëþ÷åé. Ðåøåíèå ïðîáëåìû - â óìåíüøåíèè ÷èñëà ïîëüçîâàòåëåé, íî ýòî íå âñåãäà âîçìîæíî.

2.3 Îäíîíàïðàâëåííûå ôóíêöèè

Ïîíÿòèå **îäíîíàïðàâëåííîé ôóíêöèè** ÿâëÿåòñÿ öåíòðàëüíûì â êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè. Íå ÿâëÿÿñü ïðîòîêîëàìè íåïîñðåäñòâåííî îäíîíàïðàâëåííûå ôóíêöèè ïðåäñòàâëÿþò ñîáîé êðàåóãîëüíûé êàìåíü áîëüøèíñòâà ïðîòîêîëîâ, îáñóæäàåìûõ â ýòîé êíèãå.

Îäíîíàïðàâëåííûå ôóíêöèè îòíîñèòåëüíî ëåãêî âû÷èñëÿþòñÿ, íî èíâåðòèðóþòñÿ ñ áîëüøèì òðóäîì. Òî åñòü, çíàÿ x ïðîñòî ðàññ÷èòàòü $f(x)$, íî ïî èçâåñòíîìó $f(x)$ íåëåãêî âû÷èñëèòü x. Çäåñü, "íåëåãêî" îçíà÷àåò, ÷òî äëÿ âû÷èñëåíèÿ x ïî $f(x)$ ìîãóò ïîòðåáîâàòüñÿ ìèëëèîíû ëåò, äàæå åñëè íàä ýòîé ïðîáëåìîé áóäóò áèòüñÿ âñå êîìïüþòåðû ìèðà.

Õîðîøèì ïðèìåðîì îäíîíàïðàâëåííîé ôóíêöèè ñëóæèò ðàçáèòàÿ òàðåëêà. Ëåãêî ðàçáèòü òàðåëêó íà òûñÿ÷ó êðîøå÷íûõ êóñî÷êîâ.. Îäíàêî, íåëåãêî ñíîâà ñëîæèòü òàðåëêó èç ýòèõ êóñî÷êîâ.

Ýòî çâó÷èò êðàñèâî, íî òó÷íîé è íåïîíÿòíî. Ìàòåìàòè÷åñêè ñòðîãîãî äîêàçàòåëüñòâà ñóùåñòâîâàíèÿ îäíîíàïðàâëåííûõ ôóíêöèé íåò, íåò è ðåàëüíûõ ñâÿçåé ìåæäó ïîíÿòèÿìè [230, 530, 600, 661]. Íåñìîòðÿ íà ýòî, ìíîãèå ôóíêöèè âûãëÿäÿò â òî÷íîñòè êàê îäíîíàïðàâëåííûå: ìû ìîæåì ðàññ÷èòàòü èõ è, äî ñèõ ïîð, íå çíàÿ ïðîñòîãî ñïîñîáà èíâåðòèðîâàòü èõ. Íàïðèìåð, â îãðàíè÷åííîé îêðåñòíîñòè ëåãêî âû÷èñëèòü x^2, íî íàìíîãî ñëîæíåå $x^{1/2}$. Â îñòàâøåéñÿ ÷àñòè ðàçäåëà ÿ ñîáèðàþñü ïðèâîäèòüñÿ, ÷òî îäíîíàïðàâëåííûå ôóíêöèè ñóùåñòâóþ. Ì û ïîãîâîðèì îá ýòîì â åùå ðàçäåëå 11.2.

Èòàê, ÷òî æå õîðîøåãî â îäíîíàïðàâëåííûõ ôóíêöèÿõ? Íåïîñðåäñòâåííî èõ íåëüçÿ èñïîëüçîâàòü äëÿ øèôðîâàíèÿ. Ñîîáùåíèå, çàøèôðîâàííîå îäíîíàïðàâëåííîé ôóíêöèåé áåñïîëåçíî - âåäü íåâîçìîæíî äåøèôðîâàòü. (Óïðàæíåíèå: íàïèøèòå íà òàðåëêå ÷òî-íèáóäü, ðàçáåéòå òàðåëêó íà êîðå÷íûå îñêîëêè è çàòåì îòäàéòå èõ ïðèÿòåëþ. Ïîïðîñèòå âåñ ïðî÷èòàòü ñîáùåíèå. Ïîñìîòðèòå, êàê îí áóäåò îçàäà÷åí îäíîíàïðàâëåííîé ôóíêöèåé.) Äëÿ êðèïòîãðàôèè ñ îòêðûòûì èê êëþ÷àìè íàì íóæíî ÷òî-òî äðóãîå (õîòÿ ñóùåñòâóþò è íåïîñðåäñòâåííûå êðèïòîãðàôè÷åñêèå ïðèìåíåíèÿ îäíîíàïðàâëåííûõ ôóíêöèé - ñì. ðàçäåë 3.2).

Îäíîíàïðàâëåííàÿ ôóíêöèÿ ñ ëþêîì - ýòî îñîáûé òèï îäíîíàïðàâëåííîé ôóíêöèè, ñ ñåêðåòíîé äàçåéêîé. Åå ëåãêî âû÷èñëèòü â îäíîì íàïðàâëåíèè è òðóäíî - â îáðàòíîì. Íî åñëè âàì èçâåñòíî ñåêðåò, âû ìîæåòå ëåãêî ðàññ÷èòàòü è îáðàòíóþ ôóíêöèþ *f(x)* ïî çàäàííîìó *x*, íî òðóäíî ïî èçâåñòíîìó *f(x)* âû÷èñëèòü *x*. Îäíàêî, ñóùåñòâóåò íåêîòîðàÿ èíôîðìàöèÿ, *y*, ïîçâîëÿþùàÿ, ïðè çíàíèè *f(x)* è *y*, ëåãêî âû÷èñëèòü *x*.

Â êà÷åñòâå õîðîøåãî ïðèìåðà îäíîíàïðàâëåííîé ôóíêöèè ñ ëþêîì ðàññìîòðèì ÷àñû. Ëåãêî ðàçîáðàòü ÷àñû íà ñîòè ìàëþñåíüêèõ êóñî÷êîâ è òðóäíî ñîáðàòü èç ýòèõ äåòàëåé ðàáîòàþùèå ÷àñû. Íî, ñ ñåêðåòíîé èíôîðìàöèåé - èíñòðóêöèåé ïî ñáîðêå - íàìíîãî ëåã÷å ðåøèòü ýòó çàäà÷ó.

2.4 Îäíîíàïðàâëåííûå õýø-ôóíêöèè

Ó **îäíîíàïðàâëåííîé õýø-ôóíêöèè** ìíîæåñòâî áûò ìíîæåñòâî èìåí: ôóíêöèÿ ñæàòèÿ, ôóíêöèÿ ñîêðàùåíèÿ contraction function, êðàòêîå èçëîæåíèå, öåïî÷êîâîäîâû ïðèçíàê, êðèòåðèé öåëîñòíîñòè ñîîáùåíèÿ (message integrity check, MIC) è êîä îáíàðóæåíèÿ ìàíèïóëèöèé (manipulation detection code, MDC). Êàê áû íè íå íàçûâàëñÿ ýòà ôóíêöèÿ ÿâëÿåòñÿ öåíòðàëüíûì â ñîâðåìåííîé êðèïòîãðàôèè. Îäíîíàïðàâëåííûå õýø-ôóíêöèè - ýòî äðóãàÿ ÷àñòü ôóíäàìåíòà ìíîãèõ ïðîòîêîëîâ.

Õýø-ôóíêöèè, äîãîå âðåìÿ èñïîëüçóþùèåñÿ â êîìïüþòåðíûõ íàóêàõ, ïðåäñòàâëÿò ñîáîé ôóíêöèè, ìàòåìàòè÷åñêè èíûå, êîòîðûå ïîëó÷àþò íà âõîä ñòðîêó ïðåìåííîé äëèíû (íàçûâàåìóþ **ïðîîáðàçîì**) è ïðåîáðàçóþò åå â ñòðîêó ôèêñèðîâàííîé, íåû÷íî ìåíüøåé, äëèíû (íàçûâàåìóþ çíà÷åíèåì õýø-ôóíêöèè). Â êà÷åñòâå ïðîñòîé õýø-ôóíêöèè ìîæíî ðàññìàòðèâàòü ôóíêöèþ, êîòîðàÿ ïîëó÷àåò ïðîîáðàç è âîçâðàùàåò áàéò, ïðåäñòàâëÿþùèé ñîáîé XOR âñåõ âõîäíûõ áàéòîâ.

Ñìûñë õýø-ôóíêöèè ñîñòîèò â ïîëó÷åíèè õàðàêòåðíîãî ïðèçíàêà ïðîîáðàçà - çíà÷åíèÿ, ïî êîòîðîìó àíàëèçèðóþùèå ïðîîáðàçû ïðè ðåøåíèè îáðàòíîé çàäà÷è. Òàê êàê îáû÷íî õýø-ôóíêöèÿ ïðåäñòàâëÿåò ñîáîé ñîòíè ìåãàáàéò "ìíîãå ê îäíîìó", íåâîçìîæíî ñî âñåé îòðåäàêòèðîâàííîñòüþ ñèçàöû, ÷òî äåå ñòðîêè ñîâïàäàþò, íî èõ ìîæíî èñïîëüçîâàòü, ïîëó÷àÿ ïðèìåíèìóþ îöåíêó òî÷íîñòè.

Îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ - ýòî õýø-ôóíêöèÿ, êîòîðàÿ ðàáîòàåò òîëüêî â îäíîì íàïðàâëåíèè: ëåãêî âû÷èñëèòü çíà÷åíèå õýø-ôóíêöèè ïî ïðîîáðàçó, íî òðóäíî ñîçäàòü ïðîîáðàç, çíà÷åíèå õýø-ôóíêöèè êîòîðîãî ðàâíî çàäàííîé âåëè÷èíå. Óïîìèíàâøèåñÿ ðàíåå õýø-ôóíêöèè, âîîáùå ãîâîðÿ, íå ÿâëÿþòñÿ îäíîíàïðàâëåííûìè: çàäàâ êîíêðåòíûé áàéò, íå ïðåäñòàâëÿåò òðóäà ñîçäàòü ñòðîêó áàéòîâ, XOR êîòîðûõ äàåò çàäàííûå çíà÷åíèå. Ñ îäíîíàïðàâëåííîé õýø-ôóíêöèåé òàêîãî íå âûéäåò. Õîðîøåé îäíîíàïðàâëåííîé õýø-ôóíêöèåé ÿâëÿåòñÿ õýø-ôóíêöèÿ **áåç ñòîëêíîâåíèé** - òðóäíî ñîçäàòü äâà ïðîîáðàçà ñ îäèíàêîâûì çíà÷åíèåì õýø-ôóíêöèè.

Õýø-ôóíêöèÿ ÿâëÿåòñÿ îòêðûòî, òàéíû åå ðàñ÷åòà íå ñóùåñòâóåò. Áåçîïàñíîñòü îäíîíàïðàâëåííîé õýø-ôóíêöèåé çàêëþ÷àåòñÿ èìåííî â åå îäíîíàïðàâëåííîñòè. Ó âûõîäà íåò âèäèìîé çàâèñèìîñòè îò âõîäà. Èçìåíåíèå îäèòàé ïðîîáðàçà ïðèâîäèò ê èçìåíåíèþ, â ñðåäíåì, ïîëîâèíû áèòîâ çíà÷åíèÿ õýø-ôóíêöèè. Âû÷èñëèòåëüíî íåâîçìîæíî íàéòè ïðîîáðàç, ñîîòâåòñòâóþùèé çàäàííîìó çíà÷åíèþ õýø-ôóíêöèè.

Ïîñìîòðèòå íà ýòî êàê íà ñïîñîá ïîëó÷èòü õàðàêòåðíûå ïðèçíàêè ôàéëîâ. Åñëè âû õîòèòå ïðîâåðèòü, ÷òî ó êîãî-òî åñòü òîò æå ôàéë, ÷òî è ó âàñ, íî âû íå õîòèòå, ÷òîáû ýòîò ôàéë áûë ïåðåäàí âàì, ïîïðîñèòå ïîñëàòü âàì õýø-ôóíêöèè ñíà÷àëà. Åñëè ïðèñëàííûå çíà÷åíèÿ õýø-ôóíêöèè ñîâïàäàþò, âû ìîæåòå áûòü óâåðåíû, ÷òî ó âàñ îäèíàêîâûå ôàéëû. Óçíàòü ïîëíîå ñîäåðæèìîå ôàéëà ïî åãî õýø-ôóíêöèè íåâîçìîæíî.

Êîäû ïðîâåðêè ïîäëèííîñòè ñîîáùåíèÿ

Êîä ïðîâåðêè ïîäëèííîñòè ñîîáùåíèÿ (message authentication code, MAC), èçâåñòíûé òàêæå êàê êîä ïðî-

âåðêè ïîäëèííîñòè äàííûõ (data authentication code, DAG), ïðåäñòàâëÿåò ñîáîé îäíîíàïðàâëåííóþ õýø-ôóíêöèþ ñ äîáàâëåíèåì ñåêðåòíîãî êëþ÷à (ñì. ðàçäåë 18.14). Çíà÷åíèå õýø-ôóíêöèè ÿâëÿåòñÿ ôóíêöèåé è ïðîîáðàçà, è êëþ÷à. Òåîðèÿ îñòàåòñÿ òîé æå, ÷òî è äëÿ õýø-ôóíêöèé, íî òîëüêî òîò, êòî çíàåò êëþ÷, ìîæåò ïðîâåðèòü çíà÷åíèå õýø-ôóíêöèè. MAC ìîæíî ñîçäàòü ñ ïîìîùüþ õýø-ôóíêöèè èëè áëî÷íîãî àëãîðèòìà øèôðîâàíèÿ, ñóùåñòâóþò òàêæå è ñïåöèàëèçèðîâàííûå MAC.

2.5 Ïåðåäà÷à èíôîðìàöèè ñ èñïîëüçîâàíèåì êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè

Âçãëÿíèòå íà ñèììåòðè÷íûé àëãîðèòì êàê íà ñåéô. Êëþ÷ ÿâëÿåòñÿ êîìáèíàöèåé. Çíàþùèé êîìáèíàöèþ ÷åëîâåê ìîæåò îòêðûòü ñåéô, ïîëîæèòü â íåãî äîêóìåíò è ñíîâà çàêðûòü. Êòî-òî äðóãîé ïðè ïîìîùè òîé æå êîìáèíàöèè ìîæåò îòêðûòü ñåéô è çàáðàòü äîêóìåíò. Òåì, êòî íå çíàåò êîìáèíàöèè, ïðèäåòñÿ íàó÷èòüñÿ âçëàìûâàòü ñåéôû.

Â 1976 ãîäó Óèòôèëä Äèôôè è Ìàðòèí Õåëëìàí íàâñåãäà èçìåíèëè ýòó ïàðàäèãìó êðèïòîãðàôèè [496]. (NSA çàÿâèëî, ÷òî çíàëî î òàêîé âîçìîæíîñòè åùå â 1966 ãîäó, íî äîêàçàòåëüñòâ íå ïðåäñòàâèëî.) Îíè îïèñàëè **êðèïòîãðàôèþ ñ îòêðûòûìè êëþ÷àìè**, èñïîëüçóÿ äâà ðàçëè÷íûõ êëþ÷à - îäèí îòêðûòûé è îäèí çàêðûòûé. Îïðåäåëåíèå çàêðûòîãî êëþ÷à ïî îòêðûòîìó òðåáóåò îãðîìíûõ âû÷èñëèòåëüíûõ çàòðàò. Êòî óãîäíî, èñïîëüçóÿ îòêðûòûé êëþ÷ ìîæåò çàøèôðîâàòü ñîîáùåíèå, íî íå ðàñøèôðîâàòü åãî. Ðàñøèôðîâàòü ñîîáùåíèå ìîæåò òîëüêî âëàäåëåö çàêðûòîãî êëþ÷à. Ýòî ïîõîæå íà ïðåâðàùåíèå êðèïòîãðàôè÷åñêîãî ñåéôà â ïî÷òîâûé ÿùèê. Øèôðîâàíèå ñ îòêðûòûì êëþ÷îì àíàëîãè÷íî îïóñêàíèþ ïèñüìà â ïî÷òîâûé ÿùèê, ëþáîé ìîæåò ñäåëàòü ýòî, îïóñòèâ ïèñüìî â ïðîðåçü ïî÷òîâîãî ÿùèêà. Äåøèôðèðîâàíèå ñ çàêðûòûì êëþ÷îì íàïîìèíàåò èçâëå÷åíèå ïî÷òû èç ïî÷òîâîãî ÿùèêà. Îáû÷íî ýòî ãîðàçäî ñëîæíåå - âàì ìîæåò ïîíàäîáèòüñÿ ñâàðî÷íûé àãðåãàò. Îäíàêî, åñëè âû çíàåòå ñåêðåò (ó âàñ åñòü êëþ÷ îò ïî÷òîâîãî ÿùèêà), âû áåç òðóäà äîñòàíåòå âàøó ïî÷òó.

Ìàòåìàòè÷åñêîé îñíîâîé ïðîöåññà ÿâëÿþòñÿ ðàíåå îáñóæäàâøèåñÿ îäíîíàïðàâëåííûå õýø-ôóíêöèè ñ ëþêîì. Øèôðîâàíèå âûïîëíÿåòñÿ â ïðÿìîì íàïðàâëåíèè. Óêàçàíèÿ ïî øèôðîâàíèþ îòêðûòû, êàæäûé ìîæåò çàøèôðîâàòü ñîîáùåíèå. Äåøèôðèðîâàíèå âûïîëíÿåòñÿ â îáðàòíîì íàïðàâëåíèè. Îíî íàñòîëüêî òðóäîåìêî, ÷òî, íå çíàÿ ñåêðåòà, äàæå íà êîìïüþòåðàõ Cray çà òûñÿ÷è (è ìèëëèîíû) ëåò íåâîçìîæíî ðàñøèôðîâàòü ñîîáùåíèå. Ñåêðåòîì, èëè ëþêîì, è ñëóæèò çàêðûòûé êëþ÷, îí äåëàåò äåøèôðèðîâàíèå òàêèì æå ïðîñòûì, êàê è øèôðîâàíèå. Âîò òàê, èñïîëüçóÿ êðèïòîãðàôèþ ñ îòêðûòûìè êëþ÷àìè, Àëèñà ìîæåò ïîñëàòü ñîîáùåíèå Áîáó:

(1) Àëèñà è Áîá ñîãëàñîâûâàþò êðèïòîñèñòåìó ñ îòêðûòûìè êëþ÷àìè.

(2) Áîá ïîñûëàåò Àëèñå ñâîé îòêðûòûé êëþ÷.

(3) Àëèñà øèôðóåò ñâîå ñîîáùåíèå è îòïðàâëÿåò åãî Áîáó.

(4) Áîá ðàñøèôðîâûâàåò ñîîáùåíèå Àëèñû ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à.

Îáðàòèòå âíèìàíèå, ÷òî êðèïòîãðàôèÿ ñ îòêðûòûìè êëþ÷àìè óñòðàíÿåò ïðîáëåìó ðàñïðåäåëåíèÿ êëþ÷åé, ïðèñóùóþ ñèììåòðè÷íûì êðèïòîñèñòåìàì. Ðàíüøå Àëèñà è Áîá äîëæíû áûëè òàéíî äîãîâîðèòüñÿ î êëþ÷å. Àëèñà ìîãëà âûáðàòü ëþáîé êëþ÷, íî åé íóæíî áûëî ïåðåäàòü åãî Áîáó. Îíà ìîãëà ñäåëàòü ýòî çàðàíåå, íî ýòî òðåáóåò îò íåå îïðåäåëåííîé ïðåäóñìîòðèòåëüíîñòè. Îíà ìîãëà áû ïîñëàòü êëþ÷ ñ ñåêðåòíûì êóðüåðîì, íî äëÿ ýòîãî íóæíî âðåìÿ. Êðèïòîãðàôèÿ ñ îòêðûòûìè êëþ÷àìè âñå óïðîùàåò. Àëèñà ìîæåò îòïðàâèòü Áîáó ñåêðåòíîå ñîîáùåíèå áåç êàêèõ-ëèáî ïðåäâàðèòåëüíûõ äåéñòâèé. Ó Åâû, ïîäñëóøèâàþùåé àáñîëþòíî âñå, åñòü îòêðûòûé êëþ÷ Áîáà è ñîîáùåíèå, çàøèôðîâàííîå ýòèì êëþ÷îì, íî îíà íå ñìîæåò ïîëó÷èòü íè çàêðûòûé êëþ÷ Áîáà, íè òåêñò ñîîáùåíèÿ.

Îáû÷íî öåëàÿ ñåòü ïîëüçîâàòåëåé ñîãëàñîâûâàåò èñïîëüçóåìóþ êðèïòîñèñòåìó. Ó êàæäîãî èç íèõ åñòü îòêðûòûé è çàêðûòûé êëþ÷, îòêðûòûå êëþ÷è ïîìåùàþòñÿ â îáùåäîñòóïíîé áàçå äàííûõ. Òåïåðü ïðîòîêîë âûãëÿäèò åùå ïðîùå:

(1) Àëèñà èçâëåêàåò îòêðûòûé êëþ÷ Áîáà èç áàçû äàííûõ.

(2) Àëèñà øèôðóåò ñâîå ñîîáùåíèå ñ ïîìîùüþ îòêðûòîãî êëþ÷à Áîáà è ïîñûëàåò åãî Áîáó.

(3) Áîá ðàñøèôðîâûâàåò ñîîáùåíèå Àëèñû ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à.

Â ïåðâîì ïðîòîêîëå Áîá äîëæåí áûë ïîñëàòü Àëèñå åå îòêðûòûé êëþ÷ ïðåæäå, ÷åì îíà ìîãëà îòïðàâèòü åìó ñîîáùåíèå. Âòîðîé ïðîòîêîë áîëüøå ïîõîæ íà îáû÷íóþ ïî÷òó. Áîá íå ó÷àñòâóåò â ïðîòîêîëå äî òåõ ïîð, ïîêà îí íå íà÷íåò ÷èòàòü ñîîáùåíèå.

Ñìåøàííûå êðèïòîñèñòåìû

Ïåðâûå àëãîðèòìû ñ îòêðûòûì êëþ÷îì ñòàëè èçâåñòíû â òî æå âðåìÿ, êîãäà ïðîõîäèëî îáñóæäåíèå DES êàê ïðåäïîëàãàåìîãî ñòàíäàðòà. Ýòî ïðèâåëî ê èçâåñòíîé ïàðòèçàíùèíå â êðèïòîãðàôè÷åñêîì ñîîáùåñòâå. Êàê ýòî îïèñûâàë Äèôôè [494]:

Ïðåêðàñíûå êðèïòîñèñòåìû ñ îòêðûòûì êëþ÷îì, îáñóæäàåìûå â ïîïóëÿðíîé è íàó÷íîé ïå÷àòè, òåì íå ìåíåå, íå íàøëè ñîîòâåòñòâóþùåãî îòêëèêà ñðåäè êðèïòîãðàôè÷åñêèõ ÷èíîâíèêîâ. Â òîì æå ãîäó, êîãäà áûëà îòêðûòà êðèïòîãðàôèÿ ñ îòêðûòûìè êëþ÷àìè, Àãåíòñòâî íàöèîíàëüíîé áåçîïàñíîñòè (NSA) ïðåäëîæèëî óäîáíóþ êðèïòîãðàôè÷åñêóþ ñèñòåìó, ðàçðàáîòàííóþ ôèðìîé IBM, â êà÷åñòâå ôåäåðàëüíîãî *Ñòàíäàðòà øèôðîâàíèÿ äàííûõ* (Data Encryption Standard, DES). Ìàðòè Õåëëìàí è ÿ êðèòèêîâàëè ýòî ïðåäëîæåíèå èç-çà íåäîñòàòî÷íîé äëèíû êëþ÷à, íî ïðîèçâîäèòåëè ïîäãîòîâèëèñü ïîääåðæàòü ïðåäëîæåííûé ñòàíäàðò, è íàøà êðèòèêà áûëà âîñïðèíÿòà ìíîãèìè êàê ïîïûòêà ïîìåøàòü ââåäåíèþ ñòàíäàðòà ðàäè ïðîäâèæåíèÿ íàøåé ñîáñòâåííîé ðàáîòû. Êðèïòîãðàôèÿ ñ îòêðûòûì êëþ÷îì, â ñâîþ î÷åðåäü, òàêæå ïîäâåðãàëàñü êðèòèêå â ïîïóëÿðíîé ëèòåðàòóðå [1125] è òåõíè÷åñêèõ ñòàòüÿõ [849, 1159], ñëîâíî ýòî áûë êîíêóðèðóþùèé ïðîäóêò, à íå íåäàâíåå íàó÷íîå îòêðûòèå. Ýòî, îäíàêî, íå ïîìåøàëî NSA îáúÿâèòü î ñâîèõ çàñëóãàõ â ýòîé îáëàñòè. Åãî äèðåêòîð â îäíîé èç ñòàòåé *Encyclopedia Britannica* [1461] óêàçàë, ÷òî "äâóõêëþ÷åâàÿ êðèïòîãðàôèÿ áûëà îòêðûòà â Àãåíòñòâå íà äåñÿòü ëåò ðàíüøå", õîòÿ äîêàçàòåëüñòâà ýòîãî óòâåðæäåíèÿ íå áûëè ïóáëè÷íî ïðåäñòàâëåíû.

Â ðåàëüíîì ìèðå àëãîðèòìû ñ îòêðûòûìè êëþ÷àìè íå çàìåíÿþò ñèììåòðè÷íûå àëãîðèòìû è èñïîëüçóþòñÿ íå äëÿ øèôðîâàíèÿ ñîîáùåíèé, à äëÿ øèôðîâàíèÿ êëþ÷åé ïî ñëåäóþùèì äâóì ïðè÷èíàì:

1. Àëãîðèòìû ñ îòêðûòûìè êëþ÷àìè ðàáîòàþò ìåäëåííî. Ñèììåòðè÷íûå àëãîðèòìû ïî êðàéíåé ìåðå â 1000 ðàç áûñòðåå, ÷åì àëãîðèòìû ñ îòêðûòûìè êëþ÷àìè. Äà, êîìïüþòåðû ñòàíîâÿòñÿ âñå áûñòðåå è áûñòðåå è ëåò ÷åðåç 15 êðèïòîãðàôèÿ ñ îòêðûòûìè êëþ÷àìè äîñòèãíåò ñêîðîñòåé, ñðàâíèìûõ ñ ñåãîäíÿøíåé ñêîðîñòüþ ñèììåòðè÷íîé êðèïòîãðàôèè. Íî òðåáîâàíèÿ ê îáúåìó ïåðåäàâàåìîé èíôîðìàöèè òàêæå âîçðàñòàþò, è âñåãäà áóäåò òðåáîâàòüñÿ øèôðîâàòü äàííûå áûñòðåå, ÷åì ýòî ñìîæåò ñäåëàòü êðèïòîãðàôèÿ ñ îòêðûòûìè êëþ÷àìè.
2. Êðèïòîñèñòåìû ñ îòêðûòûìè êëþ÷àìè óÿçâèìû ïî îòíîøåíèþ ê âñêðûòèþ ñ âûáðàííûì îòêðûòûì òåêñòîì. Åñëè $C = E(P)$, ãäå P - îòêðûòûé òåêñò èç n âîçìîæíûõ îòêðûòûõ òåêñòîâ, òî êðèïòîàíàëèòèêó íóæíî òîëüêî çàøèôðîâàòü âñå n âîçìîæíûõ îòêðûòûõ òåêñòîâ è ñðàâíèòü ðåçóëüòàòû ñ C (ïîìíèòå, êëþ÷ øèôðîâàíèÿ îáùåäîñòóïåí). Îí íå ñìîæåò ðàñêðûòü êëþ÷ äåøèôðèðîâàíèÿ, íî îí ñìîæåò îïðåäåëèòü P.

Âñêðûòèå ñ âûáðàííûì îòêðûòûì òåêñòîì ìîæåò áûòü îñîáåííî ýôôåêòèâíûì, åñëè ÷èñëî âîçìîæíûõ øèôðîâàííûõ ñîîáùåíèé îòíîñèòåëüíî ìàëî. Íàïðèìåð, åñëè P - ýòî äåíåæíàÿ ñóììà â äîëëàðàõ, ìåíüøàÿ ÷åì \$1000000, òî òàêîå âñêðûòèå ñðàáîòàåò, êðèïòîàíàëèòèê ïåðåáåðåò âåñü ìèëëèîí çíà÷åíèé. (Ýòà ïðîáëåìà ðåøàåòñÿ ñ ïîìîùüþ âåðîÿòíîñòíîãî øèôðîâàíèÿ, ñì. ðàçäåë 23.15.) Äàæå åñëè P íå òàê õîðîøî îïðåäåëåíî, òàêîå âñêðûòèå ìîæåò áûòü î÷åíü ýôôåêòèâíî. Ïîëåçíûì ìîæåò áûòü ïðîñòîå çíàíèå, ÷òî øèôðîòåêñò íå ñîîòâåòñòâóåò êîíêðåòíîìó îòêðûòîìó òåêñòó. Ñèììåòðè÷íûå êðèïòîñèñòåìû íå ÷óâñòâèòåëüíû ê âñêðûòèÿì òàêîãî òèïà, òàê êàê êðèïòîàíàëèòèê íå ìîæåò âûïîëíèòü òåñòîâûõ äåøèôðîâîê ñ íåèçâåñòíûì êëþ÷îì.

Â áîëüøèíñòâå ðåàëèçàöèé êðèïòîãðàôèÿ ñ îòêðûòûìè êëþ÷àìè èñïîëüçóåòñÿ äëÿ çàñåêðå÷èâàíèÿ è ðàñïðîñòðàíåíèÿ ñåàíñîâûõ êëþ÷åé, êîòîðûå èñïîëüçóþòñÿ ñèììåòðè÷íûìè àëãîðèòìàìè äëÿ çàêðûòèÿ ïîòîêà ñîîáùåíèé [879]. Èíîãäà òàêèå ðåàëèçàöèè íàçûâàþòñÿ ñìåøàííûìè (ãèáðèäíûìè) êðèïòîñèñòåìàìè

(1) Áîá ïîñûëàåò Àëèñå ñâîé îòêðûòûé êëþ÷

(2) Àëèñà ñîçäàåò ñëó÷àéíûé ñåàíñîâûé êëþ÷, øèôðóåò åãî ñ ïîìîùüþ îòêðûòîãî êëþ÷à Áîáà è ïåðåäàåò åãî Áîáó.

$E_B(K)$

(3) Áîá ðàñøèôðîâûâàåò ñîîáùåíèå Àëèñû, èñïîëüçóÿ ñâîé çàêðûòûé êëþ÷, äëÿ ïîëó÷åíèÿ ñåàíñîâîãî êëþ÷à.

$D_B(E_B(K))=K$

(4) Îáà ó÷àñòíèêà øèôðóþò ñâîè ñîîáùåíèÿ ñ ïîìîùüþ îäíîãî ñåàíñîâîãî êëþ÷à.

Èñïîëüçîâàíèå êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè äëÿ ðàñïðåäåëåíèÿ êëþ÷åé ðåøàåò î÷åíü âàæíóþ ïðîáëåìó ðàñïðåäåëåíèÿ êëþ÷åé. Â ñèììåòðè÷íîé êðèïòîãðàôèè êëþ÷ øèôðîâàíèÿ äàííûõ, åñëè îí íå èñïîëüçóåòñÿ, âàëÿåòñÿ áåç äåëà. Åñëè Åâà çàïîëó÷èò åãî, îíà ñìîæåò ðàñøèôðîâàòü âñå çàêðûòûå ýòèì êëþ÷îì ñîîáùåíèÿ. Ñ ïîìîùüþ ïðèâåäåííîãî ïðîòîêîëà ïðè íåîáõîäèìîñòè çàøèôðîâàòü ñîîáùåíèÿ ñîçäàåòñÿ ñåàíñîâûé êëþ÷, êîòîðûé óíè÷òîæàåòñÿ ïî îêîí÷àíèè ñåàíñà ñâÿçè. Ýòî çíà÷èòåëüíî óìåíüøàåò ðèñê êîìïðîìåòàöèè ñåàíñîâîãî êëþ÷à. Êîíå÷íî, ê êîìïðîìåòàöèè ÷óâñòâèòåëåí è çàêðûòûé êëþ÷, íî ðèñêà çíà÷èòåëüíî ìåíüøå, òàê êàê â òå÷åíèå ñåàíñà ýòîò êëþ÷ èñïîëüçóåòñÿ òîëüêî îäèí ðàç äëÿ øèôðîâàíèÿ ñåàíñîâîãî êëþ÷à. Ïîäðîáíî ñâÿçàííûå ñ ýòèì âîïðîñû îáñóæäàþòñÿ â ðàçäåëå 3.1.

Ãîëîâîëîìêè Ìåðêëà

Ðàëüô Ìåðêë (Ralph Merkle) èçîáðåë ïåðâóþ ñõåìó êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè. Â 1974 ãîäó îí çàïèñàëñÿ íà êóðñ ïî êîìïüþòåðíîé áåçîïàñíîñòè â Êàëèôîðíèéñêîì óíèâåðñèòåòå, Áåðêëè, êîòîðûé âåë Ëàíñ Õîôôìàí (Lance Hoffman). Òåìîé åãî êóðñîâîé ðàáîòû, ïîäàííîé ðàíüøå ñðîêà, áûëà "Áåçîïàñíàÿ ïåðåäà÷à äàííûõ ïî íåáåçîïàñíûì êàíàëàì" [1064]. Õîôôìàí íå ïîíÿë ïðåäëîæåíèÿ Ìåðêëà, è â êîíöå êîíöîâ Ìåðêë ïðåêðàòèë çàíÿòèÿ. Îí ïðîäîëæàë ðàáîòàòü íàä ïðîáëåìîé íåñìîòðÿ íà ïðîäîëæàþùååñÿ íåïîíèìàíèå åãî ðåçóëüòàòîâ.

Òåõíèêà Ìåðêëà îñíîâûâàëàñü íà ãîëîâîëîìêàõ ("puzzle"), êîòîðûå îòïðàâèòåëþ è ïîëó÷àòåëþ ðåøèòü ëåã-

÷å ÷åì çëîóìûøëåíèêó. Âîò êàê Àëèñà ìîæåò ïîñëàòü øèôðîâàííîå ñîîáùåíèå Áîáó, íå îáìåíèâàÿñü ñ íèì êëþ÷îì äî òîãî.

(1) Áîá ñîçäàåò 2^{20} (äóõãèì ñëîâàì, áîëüøå ìèëëèîíà) ñîîáùåíèé òèïà: "Ýòî ãîëîâîëîìêà íîìåð *x*. Ýòî ñåêðåòíûé êëþ÷ íîìåð *y*.", ãäå *x* - ñëó÷àéíîå ÷èñëî, à *y* - ñëó÷àéíûé ñåêðåòíûé êëþ÷. È *x*, è *y* îòëè÷àþòñÿ â êàæäîì ñîîáùåíèè. Èñïîëüçóÿ ñèììåòðè÷íûé àëãîðèòì, îí øèôðóåò êàæäîå ñîîáùåíèå ñâîì 20 áèòíûì êëþ÷îì è âñå èõ îòïðàâëÿåò Àëèñå.

(2) Àëèñà âûáèðàåò îäíî ñîîáùåíèå è ïðèòóïàåò ê âñêðûòèþ **ãðóáîé ñèëîé**, ïûòàÿñü ïîëó÷èòü îòêðûòûé òåêñò. Ýòà ðàáîòà ÿâëÿåòñÿ îáúåìíîé, íî íå íåâîçìîæíîé.

(3) Àëèñà øèôðóåò ñâîå ñåêðåòíîå ñîîáùåíèå ïðè ïîìîùè íåêîòîðîãî ñèììåòðè÷íîãî àëãîðèòìà ïîëó÷åííûì åþ êëþ÷îì è ïîñûëàåò ýòî ñîîáùåíèå Áîáó â îòêðûòîì *x*.

(4) Áîá çíàåò, êàêîé ñåêðåòíûé êëþ÷ *y* îí èñïîëüçîâàë â ñîîáùåíèè *x*, ñëåäîâàòåëüíî îí ìîæåò ðàñøèôðîâàòü ñîîáùåíèå Àëèñû.

Åâà ìîæåò âçëîìàòü ýòó ñèñòåìó, íî åé ïðèäåòñÿ âûïîëíèòü ãîðàçäî áîëüøå ðàáîòû ÷åì Àëèñå è Áîáó. Äëÿ ðàñêðûòèÿ ñîîáùåíèÿ íà ýòàïå (3) îíà äîëæíà áóäåò âñêðûòü ãðóáîé ñèëîé êàæäîå èç 2^{20} ñîîáùåíèé, îòïðàâëåííûõ Áîáîì íà ýòàïå (1). Ñëîæíîñòü ýòîãî âñêðûòèÿ ñîñòàâèò 2^{40}. Çíà÷åíèÿ *x* òàêæå íå ïîìîãóò Åâå, ââåä îíè íà ýòàïå (1) ïðèñâîåííûé ñëó÷àéíûì îáðàçîì. Â îáùåì ñëó÷àå, âû÷èñëèòåëüíûå çàòðàòû Åâû áóäóò ðàâíû âîçâåäåííûì â êâàäðàò âû÷èñëèòåëüíûì çàòðàòàì Àëèñû.

Ýòî âûèãðûø (*n* ïî îòíîøåíèþ ê n^2) íââåëèê ïî êðèòåðàòó÷åñêè ñòàíäàðòàì, íî ïðè îïðåäåëåííûõ óñëîâèÿõ ìîæåò áûòü äîñòàòî÷åí. Åñëè Àëèñà è Áîá ìîãóò ïðîâåðèòü äåñÿòü òûñÿ÷ êëþ÷åé â ñåêóíäó, êàæäîìó èç íèõ ïîòðåáóåòñÿ ìèíóòà äëÿ âûïîëíåíèÿ ñâîèõ îïåðàöèé è åùå îêîëî ìèíóòà äëÿ ïåðåäà÷è äîïîëíèòåëüíîé èíôîðìàöèè, íî ïðè îïðåäåëåííûõ óñëîâèÿõ ýòî Áîáà ê Àëèñå ïî ëèíèè ñâÿçè 1.544 Ìáèò/ñ. Åñëè âû÷èñëèòåëüíûå âîçìîæíîñòè Åâû ñðàâíèì ñ ïðèâåäåííûìè, åé ïîòðåáóåòñÿ îêîëî ãîäà äëÿ âçëîìà ñèñòåìû. Äðóãèå àëãîðèòìû åùå áîëåå óñòîé÷èâû ê âñêðûòèþ.

2.6 Öèôðîâûå ïîäïèñè

Ðóêîïèñíûå ïîäïèñè èçäàâíà èñïîëüçóþòñÿ êàê äîêàçàòåëüñòâî àâòîðñòâà äîêóìåíòà èëè, ïî êðàéíåé ìåðå, ñîãëàñèÿ ñ íèì. ×òî æå òàêîå ïðèâÿçàòåëüíûé â ïîäïèñè [1392]?

1. Ïîäïèñü äîñòîâåðíà. Î íà óáåæäàåò ïîëó÷àòåëÿ äîêóìåíòà â òîì, ÷òî ïîäïèñàâøèé ñîçíàòåëüíî ïîäïèñàë äîêóìåíò.
2. Ïîäïèñü íåïîääåëüíà. Î íà äîêàçûâàåò, ÷òî èìåííî ïîäïèñàâøèé, è íèêòî èíîé, ñîçíàòåëüíî ïîäïèñàë äîêóìåíò.
3. Ïîäïèñü íå ìîæåò áûòü èñïîëüçîâàíà ïîâòîðíî. Î íà ÿâëÿåòñÿ ÷àñòüþ äîêóìåíòà, æóëèê íå ñìîæåò ïåðåíåñòè ïîäïèñü íà äðóãîé äîêóìåíò.
4. Ïîäïèñàííûé äîêóìåíò íåüçÿ èçìåíèòü. Ïîñëå òîãî, êàê äîêóìåíò ïîäïèñàí, åãî íåâîçìîæíî èçìåíèòü.
5. Îò ïîäïèñè íå âîçìîæíî îòðå÷üñÿ. Ïîäïèñü è äîêóìåíò àòåðèàëüíû. Ïîäïèñàâøèé íå ñìîæåò âïîñëåäſòâèè óòâåðæäàòü, ÷òî îí íå ïîäïèñûâàë äîêóìåíò.

Â äåñòâèòåëüíîñòè, íè îäíî èç ýòèõ óòâåðæäåíèé íå ÿâëÿåòñÿ ïîëíîñòüþ ñïðàâåäëèâûì. Ïîäïèñè ìîæíî ïîääåëàòü, ñâåñòè ñ îäíîãî ëèñòà áóìàãè íà äðóãîé, äîêóìåíòû ìîãóò áûòü èçìåíåíû ïîñëå ïîäïèñè. Êàê âû óæå çíàåòå, ìû ìèðìÿ ñ ýòèì ïðîáëåìàìè èç-çà òîãî, ÷òî ìîøåíè÷åñòâî çàòðóäíèòåëüíî è ìîæåò áûòü îáíàðóæåíî.

Õîòåëîñü áû ðåàëèçîâàòü ÷òî-íèáóäü ïîäîáíîå è íà êîìïüþòåðàõ, íî åñòü ðÿä ïðîáëåì. Âî ïåðâûõ, êîìïüþòåðíûå ôàéëû ñêîïèðîâàòü íå ïðîñòî, à î÷åíü ïðîñòî. Äàæå åñëè ïîäïèñü ÷åñíîâêà òðóäíî ïîääåëàòü (íàïðèìåð, ãðàôè÷åñêîå èçîáðàæåíèå ðóêîïèñíîé ïîäïèñè), ìîæíî ëåãêî âûðåçàòü ïðàâèëüíóþ ïîäïèñü èç îäíîãî äîêóìåíòà è âñòàâèòü â äðóãîé. Ïðîñòî íàëè÷èå òàêîé ïîäïèñè íè÷åãî íå îçíà÷àåò. Âî âòîðûõ, êîìïüþòåðíûå òàéëû î÷åíü ëåãêî ìîæíî èçìåíèòü ïîñëå òîãî, êàê îíè ïîäïèñàíû, íå îñòàâëÿÿ íè ìàëåéøåãî ñëåäà èçìåíåíèÿ.

Ïîäïèñü äîêóìåíòà ñ ïîìîùüþ ñèììåòðè÷íûõ êðèïòîñèñòåì è ïîñðåäíèêà

Àëèñà õî÷åò ïîäïèñàòü öèôðîâîå ñîîáùåíèå è îòïðàâèòü åãî Áîáó. Îíà ìîæåò ýòî ñäåëàòü ñ ïîìîùüþ Òðåíòà è ñèììåòðè÷íîé êðèïòîñèñòåìû.

Òðåíò - ýòî îáëàäàþùèé âëàñòüþ ïîñðåäíèê, êîòîðîìó äîâåðÿþò. Îí ìîæåò ñâÿçûâàòüñÿ è ñ Àëèñîé, è ñ Áîáîì (è ñî âñåìè äðóãèìè æåëàþùèìè ïîäïèñûâàòü öèôðîâûå äîêóìåíòû). Îí âûäàåò ñåêðåòíûé êëþ÷, K_A, Àëèñå è äðóãîé ñåêðåòíûé êëþ÷, K_B, - Áîáó. Ýòè êëþ÷è îðèãèíàëüíûå çàîãëî äî íà÷àëà äåíòâèÿ ïðîòîêîëà è ìîãóò áûòü èñïîëüçîâàíû ìíîãîêðàòíî äëÿ ìíîãèõ ïîäïèñåé.

(1) Àëèñà øèôðóåò ñâîå ñîîáùåíèå Áîáó êëþ÷îì K_A è ïîñûëàåò åãî Òðåíòó.

(2) Òðåíò, çíàÿ êëþ÷ K_A, ðàñøèôðîâûâàåò ñîîáùåíèå.

(3) Òðåíò äîáàâëÿåò ê ðàñøèôðîâàííîìó ñîîáùåíèþ óòâåðæäåíèå, ÷òî îí ïîëó÷èë ýòî ñîîáùåíèå îò Àëèñû, è øèôðóåò ýòî íîâîå ñîîáùåíèå êëþ÷îì K_B.

(4) Òðåíò ïîñûëàåò íîâîå ñîîáùåíèå Áîáó.

(5) Áîá ðàñøèôðîâûâàåò ñîîáùåíèå êëþ÷îì K_B. Îí ìîæåò ïðî÷èòàòü è ñîîáùåíèå Àëèñû, è ïîäòâåðæäåíèå Òðåíòà, ÷òî ñîîáùåíèå îòïðàâëåíî èìåííî Àëèñîé.

Îòêóäà Òðåíò óçíàåò, ÷òî ñîîáùåíèå ïðèøëî èìåííî îò Àëèñû, à íå îò êàêîãî-òî ñàìîçâàíöà? Îí äåëàåò ýòîò âûâîä èç øèôðîâàíèÿ ñîîáùåíèÿ.

Òàêæå ëè ýòî õîðîøî, êàê ïîäïèñü íà áóìàãå? Ïîñìîòðèì íà òðåáóåìûå ñâîéñòâà:

1. Ýòà ïîäïèñü äîñòîâåðíà. Òðåíò - ýòî çàñëóæèâàþùèé äîâåðèÿ ïîñðåäíèê, è Òðåíò çíàåò, ÷òî ñîîáùåíèå ïîëó÷åíî îò Àëèñû. Ïîäòâåðæäåíèå Òðåíòà ñëóæèò äîêàçàòåëüñòâîì äëÿ Áîáà.

2. Ýòà ïîäïèñü íåïîääåëüíà. Òîëüêî Àëèñà (è Òðåíò, íî åìó âñå âåðÿò) çíàåò K_A, ïîýòîìó òîëüêî Àëèñà ìîãëà ïîñëàòü Òðåíòó ñîîáùåíèå, çàøèôðîâàííîå êëþ÷îì K_A. Åñëè êòî-íèáóäü ïîïûòàåòñÿ âûäàòü ñåáÿ çà Àëèñó, Òðåíò ñðàçó çàìåòèò ýòî íà ýòàïå (2) è íå çàâåðèò ïîäëèííîñòü.

3. Ýòó ïîäïèñü íåëüçÿ èñïîëüçîâàòü ïîâòîðíî. Åñëè Áîá ïîïûòàåòñÿ âçÿòü ïîäòâåðæäåíèå Òðåíòà è ïðèñîåäèíèòü åãî ê äðóãîìó ñîîáùåíèþ, Àëèñà çàêðè÷èò "Êàðàóë!" Ïîñðåäíèê (Òðåíò èëè êòî-òî ñîâñåì äðóãîé, èìåþùèé äîñòóï ê òîé æå èíôîðìàöèè) ïîïðîñèò Áîáà ïðåäúÿâèòü åãî ñîîáùåíèå è øèôðîâàííîå ñîîáùåíèå Àëèñû. Çàòåì ïîñðåäíèê çàøèôðóåò ñîîáùåíèå êëþ÷îì K_A è óâèäèò, ÷òî îíî íå ñîîòâåòñòâóåò øèôðîâàííîìó ñîîáùåíèþ, ïåðåäàííîìó Áîáîì. Áîá, êîíå÷íî æå, íå ñìîæåò ñîçäàòü ïðàâèëüíîå øèôðîâàííîå ñîîáùåíèå, ïîòîìó ÷òî îí íå çíàåò êëþ÷à K_A.

4. Ïîäïèñàííûé äîêóìåíò íåëüçÿ èçìåíèòü. Åñëè Áîá ïîïûòàåòñÿ, ïîëó÷èâ äîêóìåíò, èçìåíèòü åãî, Òðåíò îáíàðóæèò ìîøåííè÷åñòâî óæå îïèñàííûì ñïîñîáîì.

5. Îò ïîäïèñè íåâîçìîæíî îòêàçàòüñÿ. Åñëè âïîñëåäñòâèè Àëèñà çàÿâèò, ÷òî îíà íèêîãäà íå ïîñûëàëà ñîîáùåíèå, ïîäòâåðæäåíèå Òðåíòà äîêàæåò îáðàòíîå. Ïîìíèòå, âñå äîâåðÿþò Òðåíòó, âñå, ñêàçàííîå èì - èñòèíà.

Åñëè Áîá çàõî÷åò ïîêàçàòü Êýðîë äîêóìåíò, ïîäïèñàííûé Àëèñîé, îí íå ñìîæåò ðàñêðûòü åé ñâîé ñåêðåòíûé êëþ÷. Åìó ïðèäåòñÿ ñíîâà îáðàòèòüñÿ ê Òðåíòó:

(1) Áîá áåðåò ñîîáùåíèå è óòâåðæäåíèå Òðåíòà, ÷òî ñîîáùåíèå ïîëó÷åíî îò Àëèñû, øèôðóåò èõ êëþ÷îì K_B è ïîñûëàåò îáðàòíî Òðåíòó.

(2) Òðåíò ðàñøèôðîâûâàåò ïîëó÷åííûé ïàêåò ñ ïîìîùüþ êëþ÷à K_B.

(3) Òðåíò ïðîâåðÿåò ñâîþ áàçó äàííûõ è ïîäòâåðæäàåò, ÷òî îòïðàâèòåëåì îðèãèíàëüíîãî ñîîáùåíèÿ áûëà Àëèñà.

(4) Òðåíò øèôðóåò ïîëó÷åííûé îò Áîáà ïàêåò êëþ÷îì K_C, êîòîðûé îí âûäåëèë äëÿ Êýðîë, è ïîñûëàåò Êýðîë øèôðîâàííûé ïàêåò.

(5) Òðåíò ðàñøèôðîâûâàåò ïîëó÷åííûé ïàêåò ñ ïîìîùüþ êëþ÷à K_C. Òåïåðü îíà ìîæåò ïðî÷èòàòü è ñîîáùåíèå, è ïîäòâåðæäåíèå Òðåíòà, ÷òî ñîîáùåíèå îòïðàâëåíî Àëèñîé.

Ýòè ïðîòîêîëû ðàáîòàþò, íî îíè òðåáóþò îò Òðåíòà íåìàëûõ çàòðàò âðåìåíè. Îí äîëæåí öåëûìè äíÿìè ðàñøèôðîâûâàòü è øèôðîâàòü ñîîáùåíèÿ, ïîñðåäíè÷àÿ ìåæäó êàæäîé ïàðîé ëþäåé, êîòîðûå õîòÿò îáìåíèâàòüñÿ ïîäïèñàííûìè äîêóìåíòàìè. Îí äîëæåí õðàíèòü ñîîáùåíèÿ â áàçå äàííûõ (õîòÿ ýòîãî ìîæíî èçáåæàòü, ïîñûëàÿ ïîëó÷àòåëþ êîïèþ øèôðîâàííîãî ñîîáùåíèÿ îòïðàâèòåëÿ). Îí áóäåò óçêèì ìåñòîì ëþáîé ñèñòåìû ñâÿçè, äàæå åñëè îí - ïðîñòî áåñ÷óâñòâåííàÿ êîìïüþòåðíàÿ ïðîãðàììà..

Òàêîãî ïîñðåäíèêà êàê Òðåíò, êîòîðîìó áóäóò äîâåðÿòü âñå êîððåñïîíäåíòû, òÿæåëî íàéòè è òÿæåëî ñîõðàíèòü. Òðåíò äîëæåí áûòü íåïîãðåøèì, åñëè îí ñäåëàåò õîòÿ áû îäíó îøèáêó íà ìèëëèîí ïîäïèñåé, íèêòî íå áóäåò âåðèòü åìó. Òðåíò äîëæåí áûòü àáñîëþòíî áåçîïàñåí. Åñëè åãî áàçà äàííûõ ñ ñåêðåòíûìè êëþ÷àìè êîãäà-íèáóäü ðàñêðîåòñÿ, èëè êòî-íèáóäü ñìîæåò ïåðåïðîãðàììèðîâàòü åãî, âñå ïîäïèñè ñòàíóò áåñïîëåçíûìè. Ïîÿâÿòñÿ äîêóìåíòû áóäòî áû ïîäïèñàííûå ãîäû íàçàä. Ýòî ïðèâåäåò ê õàîñó. Ïðàâèòåëüñòâà ïàäóò, è ñòàíåò ïðàâèòü àíàðõèÿ. Òàêàÿ ñõåìà òåîðåòè÷åñêè ìîæåò ðàáîòàòü, íî îíà íåäîñòàòî÷íî õîðîøà äëÿ ïðàêòè÷åñêîãî ïðèìåíåíèÿ.

Äåðåâüÿ öèôðîâûõ ïîäïèñåé

Ðàëüô Ìåðêë ïðåäëîæèë ñèñòåìó öèôðîâûõ ïîäïèñåé, îñíîâàííóþ íà êðèïòîãðàôèè ñ ñåêðåòíûì êëþ÷îì, ñîçäàþùåé áåñêîíå÷íîå êîëè÷åñòâî îäíîðàçîâûõ ïîäïèñåé, èñïîëüçóÿ äðåâîâèäíóþ ñòðóêòóðó [1067,1068]. Îñíîâíîé èäååé ýòîé ñõåìû ÿâëÿåòñÿ ïîìåñòèòü êîðåíü äåðåâà â íåêèé îòêðûòûé ôàéë, óäîñòîâåðÿÿ åãî òàêèì îá-

ðàçîì. Êîðåíü ïîäïèñûâàåò îáîì ñîîáùåíèå è óäîñòîâåðÿåò ïîäóçëû äåðåâà. Êàæäûé èç ýòèõ óçëîâ ïîäïèñûâàåò îáîì ñîîáùåíèå è óäîñòîâåðÿåò ñâîè ïîäóçëû, è òàê äàëåå.

Ïîäïèñü äîêóìåíòà ñ ïîìîùüþ êðèïòîãðàôèè ñ îòêðûòûì êëþ÷îì

Ñóùåñòâóþò àëãîðèòìû ñ îòêðûòûì êëþ÷îì, êîòîðûå ìîæíî èñïîëüçîâàòü äëÿ öèôðîâîé ïîäïèñè. Â íåêîòîðûõ àëãîðèòìàõ - ïðèìåðîì ÿâëÿåòñÿ RSA (ñì. ðàçäåë 19.3) - äëÿ øèôðîâàíèÿ ìîæåò áûòü èñïîëüçîâàí èëè îòêðûòûé, èëè çàêðûòûé êëþ÷. Çàøèôðóéòå äîêóìåíò ñâîèì çàêðûòûì êëþ÷îì, è âû ïîëó÷èòå íàäåæíóþ öèôðîâóþ ïîäïèñü. Â äðóãèõ ñëó÷àÿõ - ïðèìåðîì ÿâëÿåòñÿ DSA (ñì. ðàçäåë 20.1) - äëÿ öèôðîâûõ ïîäïèñåé èñïîëüçóåòñÿ îòäåëüíûé àëãîðèòì, êîòîðûé íåâîçìîæíî èñïîëüçîâàòü äëÿ øèôðîâàíèÿ. Ýòà èäåÿ âïåðâûå áûëà èçîáðåòåíà Äèôôè è Õåëëìàíîì [496] è â äàëüíåéøåì áûëà ðàñøèðåíà è óãëóáëåíà â äðóãèõ ðàáîòàõ [1282, 1328, 1024, 1283, 426]. Õîðîøèé îáçîð ýòîé îáëàñòè ïðèâåäåí â [1099]. Îñíîâíîé ïðîòîêîë ïðîñò:

(1) Àëèñà øèôðóåò äîêóìåíò ñâîèì çàêðûòûì êëþ÷îì, òàêèì îáðàçîì ïîäïèñûâàÿ åãî.

(2) Àëèñà ïîñûëàåò ïîäïèñàííûé äîêóìåíò Áîáó.

(3) Áîá ðàñøèôðîâûâàåò äîêóìåíò, èñïîëüçóÿ îòêðûòûé êëþ÷ Àëèñû, òàêèì îáðàçîì ïðîâåðÿÿ ïîäïèñü.

Ýòîò ïðîòîêîë ãîðàçäî ëó÷øå ïðåäûäóùåãî. Òðåòèé íå íóæåí íè äëÿ ïîäïèñè äîêóìåíòîâ, íè äëÿ åå ïðîâåðêè. (Î íóæåí äëÿ ïîäòâåðæäåíèÿ, ÷òî îòêðûòûé êëþ÷ ïðèíàäëåæèò èìåííî Àëèñå.) Òðåòèé íå íóæåí ñòðîíàì äàæå äëÿ ðàçðåøåíèÿ ñïîðîâ: Åñëè Áîá íå ñìîã îñóùåñòâèòü ýòàï (3), òî îí çíàåò, ÷òî ïîäïèñü íåïðàâèëüíà. Òàêàÿ ïîäïèñü ñîòâåòñòâóåò âñåì òðåáîâàíèÿì:

1. Ýòà ïîäïèñü äîñòîâåðíà. Êîãäà Áîá ðàñøèôðîâûâàåò ñîîáùåíèå ñ ïîìîùüþ îòêðûòîãî êëþ÷à Àëèñû, îí çíàåò ÷òî îíà ïîäïèñàëà ýòî ñîîáùåíèå.
2. Ýòà ïîäïèñü íåïîääåëüíà. Òîëüêî Àëèñà çíàåò ñâîé çàêðûòûé êëþ÷.
3. Ýòó ïîäïèñü íåëüçÿ èñïîëüçîâàòü ïîâòîðíî. Ïîäïèñü ÿâëÿåòñÿ ôóíêöèåé äîêóìåíòà è íå ìîæåò áûòü ïåðåíåñåíà íà äðóãîé äîêóìåíò.
4. Ïîäïèñàííûé äîêóìåíò íåèçìåíåí. Ïîñëå ëþáîãî èçìåíåíèÿ äîêóìåíòà ïîäïèñü íå ñìîæåò áîëüøå ïîäòâåðæäàòüñÿ îòêðûòûì êëþ÷îì Àëèñû.
5. Îò ïîäïèñè íåâîçìîæíî îòêàçàòüñÿ. Áîáó íå òðåáóåòñÿ ïîìîùü Àëèñû ïðè ïðîâåðêå åå ïîäïèñè.

Ïîäïèñü äîêóìåíòà è ìàòåìàòèêà

Íà ñàìîì äåëå, ïðè ïîñëåäíåéøåì óñëîâèè Áîá ñìîæåò ñìîøåííè÷àòü. Îí ìîæåò ïîâòîðíî èñïîëüçîâàòü äîêóìåíò è ïîäïèñü ñîâìåñòíî. Ýòî íå èìåþ çíà÷åíèÿ, åñëè Àëèñà ïîäïèñàëà êîíòðàêò (îäíîé êîïèåé ïîäïèñàííîãî êîíòðàêòà áîëüøå, îäíîé ìåíüøå), íî ÷òî åñëè Àëèñà ïîñòàâèëà öèôðîâóþ ïîäïèñü ïîä ÷åêîì?

Ïðåäïîëîæèì, ÷òî Àëèñà ïîñëàëà Áîáó ïîäïèñàííûé ÷åê íà $100. Áîá îòíåñ ÷åê â áàíê, êîòîðûé ïðîâåðèë ïîäïèñü è ïðåäâåë äåíüãè ñ îäíîãî ñ÷åòà íà äðóãîé. Áîá, âûñòóïàþùèé â ðîëè æóëèêà, ñîõðàíèë êîïèþ ýëåêòðîííîãî ÷åêà. Íà ñëåäóþùåé íåäåëå î ñíîâà îòíåñ åãî â áàíê, êîòîðûé ïðîâåðèë ïîäïèñü è ïðåäâåë äåíüãè ñ îäíîãî ñ÷åòà íà äðóãîé. Åñëè Àëèñà íå ïðîâåðÿåò êîïèþ ÷åêîâóþ êíèãó, Áîá ñìîæåò ïðîäåëûâàòü ýòî ãîäàìè.

Ïîýòîìó â öèôðîâûå ïîäïèñè ÷àñòî âêëþ÷àþò ìåòêè âðåìåíè. Äàòà è âðåìÿ ïîäïèñàíèÿ äîêóìåíòà äîáàâëÿþòñÿ ê äîêóìåíòó è ïîäïèñûâàþòñÿ âìåñòå ñî ñâîì ñîäåðæàíèåì ñîîáùåíèÿ. Áàíê ñîõðàíÿåò ýòó ìåòêó âðåìåíè â áàçå äàííûõ. Òåïåðü, åñëè Áîá ïîòûòàåòñÿ ïîêàçàòü íîâûé ÷åê Àëèñû âî âòîðîé ðàç, áàíê ïðîâåðèò ìåòêó âðåìåíè ïî ñâîåé áàçå äàííûõ. Òàê êàê áàíê óæå îëäåë ÷åê Àëèñû ñ òîé æå ìåòêîé âðåìåíè, òî áóäåò âûçâàíà ïîëèöèÿ. Çàòåì Áîá ïðîâåäåò ëåò 15 â òþðüìå Ëèâåíâîðò, èçó÷àÿ êðèïòîãðàôè÷åñêèå ïðîòîêîëû.

Ïîäïèñü äîêóìåíòà ñ ïîìîùüþ êðèïòîãðàôèè ñ îòêðûòûì êëþ÷îì è îäíîíàïðàâëåííûõ ôóíêöèé

Íà ïðàêòèêå àëãîðèòìû ñ îòêðûòûì êëþ÷îì ÷àñòî íåäîñòàòî÷íî ýôôåêòèâíû äëÿ ïîäïèñè áîëüøèõ äîêóìåíòîâ. Äëÿ ýêîíîìèè âðåìåíè ïðîòîêîëû öèôðîâîé ïîäïèñè íåðåêî ñïîëüçóþò âìåñòå ñ îäíîíàïðàâëåííûìè õýø-ôóíêöèÿìè [432, 433]. Àëèñà ïîäïèñûâàåò íå äîêóìåíò, à çíà÷åíèå õýø-ôóíêöèè äëÿ äàííîãî äîêóìåíòà. Â ýòîì ïðîòîêîëå îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ è àëãîðèòì öèôðîâîé ïîäïèñè ñîãëàñîâûâàþòñÿ çàðàíåå.

(1) Àëèñà ïîëó÷àåò çíà÷åíèå îäíîíàïðàâëåííîé õýø-ôóíêöèè äëÿ äîêóìåíòà.

(2) Àëèñà øèôðóåò ýòî çíà÷åíèå ñâîèì çàêðûòûì êëþ÷îì, òàêèì îáðàçîì ïîäïèñûâàÿ äîêóìåíò.

(3) Áîá ïîñûëàåò Áîáó äîêóìåíò è ïîäïèñàííîå çíà÷åíèå õýø-ôóíêöèè.

(4) Áîá ïîëó÷àåò çíà÷åíèå îäíîíàïðàâëåííîé õýø-ôóíêöèè äëÿ äîêóìåíòà, ïðèñëàííîãî Àëèñîé. Çàòåì, èñïîëüçóÿ àëãîðèòì öèôðîâîé ïîäïèñè, îí ðàñøèôðîâûâàåò ïîäïèñàííîå çíà÷åíèå õýø-ôóíêöèè ñ ïîìîùüþ

îòêðûòîãî êëþ÷à Àëèñû. Åñëè ïîëó÷åííîå çíà÷åíèå õýø-ôóíêöèè ñîâïàäàåò ñ ðàññ÷èòàííûì, ïîäïèñü ïðàâèëüíà.

Ñêîðîñòü çàìåòíî âîçðàñòàåò è, òàê êàê âåðîÿòíîñòü ïîëó÷èòü äëÿ äâóõ ðàçëè÷íûõ äîêóìåíòîâ îäèíàêîâîå 160-áèòíîå çíà÷åíèå õýø-ôóíêöèè ñîñòàâëÿåò òîëüêî îäèí øàíñ èç 2^{160}, ìîæíî áåçîïàñíî ïðèðàâíÿòü ïîäïèñü çíà÷åíèÿ õýø-ôóíêöèè è ïîäïèñü äîêóìåíòà. Äîëæíà èñïîëüçîâàòüñÿ òîëüêî îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ, èíà÷å ñîçäàòü ðàçíûå äîêóìåíòû ñ îäíèì è òåì æå çíà÷åíèåì õýø-ôóíêöèè íåòðóäíî, è ïîäïèñü îäíîãî äîêóìåíòà ïðèâåäåò ê îøèáî÷íîé ïîäïèñè ñðàçó ìíîãèõ äîêóìåíòîâ.

Ó ïðîòîêîëà åñòü è äðóãèå âûãîäû. Âî ïåðâûõ, ïîäïèñü ìîæåò áûòü îòäåëåíà îò äîêóìåíòà. Âî âòîðûõ, çíà÷èòåëüíî óìåíüøàþòñÿ òðåáîâàíèÿ ê îáúåìó ïàìÿòè ïîëó÷àòåëÿ, â êîòîðîì õðàíÿòñÿ äîêóìåíòû è ïîäïèñè. Àðõèâíàÿ ñèñòåìà ìîæåò èñïîëüçîâàòü ýòîò ïðîòîêîë äëÿ ïîäòâåðæäåíèÿ ñóùåñòâîâàíèÿ äîêóìåíòîâ, íå õðàíÿ èõ ñîäåðæàíèÿ. Â öåíòðàëüíîé áàçå äàííûõ ìîãóò õðàíèòüñÿ ëèøü çíà÷åíèÿ õýø-ôóíêöèè äëÿ ôàéëîâ. Âîâñå íå íóæíî ïðîñìàòðèâàòü ôàéëû, ïîëüçîâàòåëè ïîìåùàþò ñâîè çíà÷åíèÿ õýø-ôóíêöèè â áàçó äàííûõ, à áàçà äàííûõ õðàíèò ýòè çíà÷åíèÿ, ïîìå÷àÿ èõ âðåìåíåì ïîëó÷åíèÿ äîêóìåíòà. Åñëè â áóäóùåì âîçíèêíåò êàêîå-íèáóäü ðàçíîãëàñèå ïî ïîâîäó àâòîðà è âðåìåíè ñîçäàíèÿ äîêóìåíòà, áàçà äàííûõ ñìîæåò ðàçðåøèòü åãî ïðè ïîìîùè õðàíÿùåãîñÿ â íåé çíà÷åíèÿ õýø-ôóíêöèè. Ïîäîáíàÿ ñèñòåìà èìååò áîëüøîå çíà÷åíèå ïðè õðàíåíèè ñåêðåòíîé èíôîðìàöèè: Àëèñà ìîæåò ïîäïèñàòü äîêóìåíò è ñîõðàíèòü åãî â ñåêðåòå. Åé ïîíàäîáèòñÿ îïóáëèêîâàòü äîêóìåíò, òîëüêî åñëè îíà çàõî÷åò äîêàçàòü ñâîå àâòîðñòâî. (Ñì. ðàçäåë 4.1).

Àëãîðèòìû è òåðìèíîëîãèÿ

Ñóùåñòâóåò ìíîæåñòâî àëãîðèòìîâ öèôðîâîé ïîäïèñè. Âñå îíè ïðåäñòàâëÿþò ñîáîé àëãîðèòìû ñ îòêðûòûìè êëþ÷àìè ñ çàêðûòîé ÷àñòüþ äëÿ ïîäïèñè äîêóìåíòîâ è ñ îòêðûòîé - äëÿ ïðîâåðêè ïîäïèñè. Èíîãäà ïðîöåññ ïîäïèñè íàçûâàþò **øèôðîâàíèåì ñ çàêðûòûì êëþ÷îì**, à ïðîöåññ ïðîâåðêè ïîäïèñè - **äåøèôðèðîâàíèåì ñ îòêðûòûì êëþ÷îì**. Ýòî ìîæåò ââåñòè â çàáëóæäåíèå, ÿâëÿÿñü ñïðàâåäëèâûì òîëüêî äëÿ îäíîãî àëãîðèòìà, RSA. Ó äðóãèõ àëãîðèòìîâ - äðóãèå ðåàëèçàöèè. Íàïðèìåð, èñïîëüçîâàíèå îäíîíàïðàâëåííûõ õýø-ôóíêöèé è ìåòîê âðåìåíè èíîãäà ïðèâîäèò ê ïîÿâëåíèþ äîïîëíèòåëüíûõ ýòàïîâ ïðè ïîäïèñàíèè è ïðîâåðêå ïîäïèñè. Ìíîãèå àëãîðèòìû ìîæíî èñïîëüçîâàòü äëÿ öèôðîâîé ïîäïèñè, íî íåëüçÿ äëÿ øèôðîâàíèÿ.

Â îáùåì ñëó÷àå ÿ áóäó ññûëàòüñÿ íà ïðîöåññû ïîäïèñè è ïðîâåðêè, íå âäàâàÿñü â ïîäðîáíîñòè àëãîðèòìîâ. Ïîäïèñü ñîîáùåíèÿ ñ çàêðûòûì êëþ÷îì K áóäåò îáîçíà÷àòüñÿ êàê:

$S_K(M)$

à ïðîâåðêà ïîäïèñè ñ ïîìîùüþ ñîîòâåòñòâóþùåãî îòêðûòîãî êëþ÷à êàê:

$V_K(M)$

Ñòðîêó áèòîâ, ïðèñîåäèíåííóþ ê äîêóìåíòó ïîñëå åãî ïîäïèñàíèÿ (â ïðåäûäóùåì ïðèìåðå, çíà÷åíèå îäíîíàïðàâëåííîé õýø-ôóíêöèè äîêóìåíòà, çàøèôðîâàííîå çàêðûòûì êëþ÷îì), áóäåì íàçûâàòü **öèôðîâîé ïîäïèñüþ** èëè ïðîñòî **ïîäïèñüþ**. Âåñü ïðîòîêîë, ñ ïîìîùüþ êîòîðîãî ïîëó÷àòåëü ñîîáùåíèÿ ïðîâåðÿåò ëè÷íîñòü îòïðàâèòåëÿ è öåëîñòíîñòü ñîîáùåíèÿ, íàçûâàåòñÿ óäîñòîâåðåíèåì ïîäëèííîñòè. Áîëåå ïîäðîáíî ýòè ïðîòîêîëû ðàññìàòðèâàþòñÿ â ðàçäåëå 3.2.

Íåñêîëüêî ïîäïèñåé

Êàê Àëèñå è Áîáó îäíîâðåìåííî ïîäïèñàòü îäèí è òîò æå äîêóìåíò? Â îòñóòñòâèå îäíîíàïðàâëåííûõ õýø-ôóíêöèé ñóùåñòâóåò äâå âîçìîæíîñòè. Àëèñà è Áîá ìîãóò ïîäïèñàòü ðàçëè÷íûå êîïèè îäíîãî è òîãî æå äîêóìåíòà. Ïîëó÷åííîå ñîîáùåíèå áóäåò â äâà ðàçà äëèííåå ïåðâîíà÷àëüíîãî äîêóìåíòà. Èëè Àëèñà ïîäïèñûâàåò äîêóìåíò, à çàòåì Áîá ïîäïèñûâàåò ïîäïèñü Àëèñû. Ýòîò ñïîñîá ðàáîòàåò, íî ïðîâåðèòü ïîäïèñü Àëèñû, íå ïðîâåðÿÿ ïðè ýòîì ïîäïèñè Áîáà, íåâîçìîæíî.

Ñ ïîìîùüþ îäíîíàïðàâëåííûõ õýø-ôóíêöèé ðåàëèçîâàòü íåñêîëüêî ïîäïèñåé ïðîñòî:

(1) Àëèñà ïîäïèñûâàåò çíà÷åíèå õýø-ôóíêöèè äîêóìåíòà.

(2) Áîá ïîäïèñûâàåò çíà÷åíèå õýø-ôóíêöèè äîêóìåíòà.

(3) Áîá ïîñûëàåò ñâîþ ïîäïèñü Àëèñå.

(4) Àëèñà ïîñûëàåò Êýðîë äîêóìåíò, ñâîþ ïîäïèñü è ïîäïèñü Áîáà.

(5) Êýðîë ïðîâåðÿåò ïîäïèñè Àëèñû è Áîáà.

Àëèñà è Áîá ìîãóò âûïîëíèòü ýòàïû (1) è (2) èëè ïàðàëëåëüíî, èëè ïîñëåäîâàòåëüíî. Íà ýòàïå (5) Êýðîë ìîæåò ïðîâåðèòü ëþáóþ ïîäïèñü íåçàâèñèìî îò äðóãîé.

Íåâîçìîæíîñòü îòêàçàòüñÿ îò öèôðîâîé ïîäïèñè

Àëèñà ìîæåò ñìîøåííè÷àòü ñ öèôðîâûìè ïîäïèñÿìè, è ñ ýòèì íè÷åãî íåëüçÿ ïîäåëàòü. Îíà ìîæåò ïîäïèñàòü äîêóìåíò è çàòåì óòâåðæäàòü, ÷òî îíà ýòîãî íå äåëàëà. Ñíà÷àëà îíà, êàê îáû÷íî, ïîäïèñûâàåò ïèñüìî. Çàòåì îíà àíîíèìíî ðàñêðûâàåò ñâîé çàêðûòûé êëþ÷ èëè òåðÿåò â ëþäíîì ìåñòå. Òàïåðü Àëèñà óòâåðæäàåò, ÷òî åå ïîäïèñü áûëà ñêîìïðîìåòèðîâàíà è èñïîëüçîâàíà êàì-òî äóãèì, âûäàþùèì ñåáÿ çà íåå. Îíà äåçàâóèðóåò ñâîþ ïîäïèñü ïîä âñåìè äîêóìåíòàìè, ïîäïèñàííûìè ñ ïîìîùüþ ýòîãî çâêðûòîãî êëþ÷à. Ýòî íàçûâàåòñÿ îòêàç îò ïîäïèñè.

Ìåòîä âðåìåíè ìîãóò ñíèçèòü ýôôåêò òàêîãî ìîøåííè÷åñòâà, íî Àëèñà âñåãäà ìîæåò çàÿâèòü, ÷òî åå êëþ÷ áûë ñêîìïðîìåòèðîâàí ðàíüøå. Åñëè Àëèñà ïðàâäîïîäîáíî ðàññ÷èòàåò âðåìÿ, îíà ñìîæåò ïîäïèñàòü äîêóìåíò è çàòåì óñïåøíî çàÿâèòü, ÷òî îíà ýòîãî íå äåëàëà. Ïîýòîìó òàê íîãî ãîâîðèòñÿ î ðàçíîãàñàþùèõ êëþ÷åé â íàäåæíûõ ìåòàõ - ÷òîáû Àëèñà íå ìîãëà äîáðàòüñÿ äî ñâîåãî è çëîóïîòðåáèòü è.

Õîòÿ ñ ïîäîáíûì çëîóïîòðåáëåíèåì íè÷åãî íåëüçÿ ñäåëàòü, ìîæíî ïðåäïðèíÿòü íåêîòîðûå äéñòâèÿ, ãàðàíòèðóþùèå òî, ÷òî ñòàðûå ïîäïèñè íå áóäóò ïðèçíàíû íåäîñòîâåðíûìè èç-çà ðàçíîãëàñèé ïî íîâûì ïîäïèñÿì. (Íàïðèìåð, Àëèñà ìîæåò "ïîòåðÿòü" ñâîé êëþ÷, ÷òîáû íå ïëàòèòü Áîáó çà ïîäðæàííóþ ìàøèíó, êîòîðóþ îí â÷åðà åé ïðîäàë è, â ðåçóëüòàòå, ñäåëàòü íåäåéſòâèòåëüíûì ñâîé áàíêîâñêèé ñ÷åò.) Ïîëó÷àòåëþ íóæíî ïðîòâîëüòè ìåòîä âðåìåíè äëÿ ïîëó÷åííûõ äîêóìåíòîâ [453]. Îáùàÿ ñõåìà ïðîòîêîëà ïðèâåäåíà â [2, 8]:

(1) Àëèñà ïîäïèñûâàåò ñîîáùåíèå.

(2) Àëèñà ñîçäàåò çàãîëîâîê, ñîäåðæàùèé íåêîòîðóþ èäåíòèôèêàöèîííóþ èíôîðìàöèþ. Îíà ïðèñîåäèíÿåò ê çàãîëîâêó ïîäïèñàííîå ñîîáùåíèå, ïîäïèñûâàåò âñå âìåñòå è ïîñûëàåò Òðåíóó.

(3) Òðåíó ïðîâåðÿåò âíåøíþþ ïîäïèñü è ïîäòâåðæäàåò èäåíòèôèêàöèîííóþ èíôîðìàöèþ. Îí äîáàâëÿåò ìåòêó âðåìåíè ê ïîäïèñàííîìó ñîîáùåíèþ Àëèñû è èäåíòèôèêàöèîííîé èíôîðìàöèè. Çàòåì îí ïîäïèñûâàåò âñå âìåñòå è ïîñûëàåò ïàêåò Àëèñå è Áîáó.

(4) Áîá ïðîâåðÿåò ïîäïèñü Òðåíà, èäåíòèôèêàöèîííóþ èíôîðìàöèþ è ïîäïèñü Àëèñû.

(5) Àëèñà ïðîâåðÿåò ñîîáùåíèå, êîòîðîå Òðåíó ïîñëàë Áîáó. Åñëè îíà íå ïðèíàäëåæèò ñâîå àâòîðñòâî, îíà áûñòðî çàÿâëÿåò îá ýòîì.

Â äóõîé ñõåìå Òðåíó èñïîëüçóåòñÿ â êà÷åſòâå àðáèòðà [209]. Ïîëó÷èâ ïîäïèſàííûå ſîîáùåíèå, Áîá ïîſûëàåò êîïèþ Òðåíóó äëÿ ïðîâåðêè. Òðåíó ìîæåò ïîäòâåðäèòü ïîäïèſü Àëèſû.

Èſïîëüçîâàíèå öèôðîâûõ ïîäïèſåé

Îäíèì èç ſàìûõ ðàſſèſ ïðåäſîæſſíûõ ïðèìåíſíèé öèôðîâûõ ſîäïèſſåé áûſî óſðîſùſíèå ſðîâåðêè ſîáëþäåſèÿ äîſâſîâſðîâ î ÿäåðſûõ ſèſſòſàſèÿõ [1454, 1467]. Sîåäèſſíûå Øòàòû è Sîâåòſêèé Sîþç (êòî-íèáóäü ſîſſíèò Sîâåòſêèé Sîþç?) ðàçðåøèëè äóóã äðóãó ðàçſåſòèòü íà ÷óæîé òåððèſîðèè ſåéſſſâàðû äëÿ ſëæåſſèÿ çà ÿäåðſûſſèſſòàſèÿſè. Ïðſáëèſà áûëà â òſſ, ÷òſ êàæäàÿ èç ſòſðſſſ äſëæſſà áûëà óâåðåſſà â òſſ, ÷òſ äðóãàÿ ſòſðſſſſà íå ſſääåëàëà äàſſſûå ſòèſ ſåéſſſſâðàſſâ. Îäſſâðåſſſſſ, äðóãàÿ ſòſðſſſà äſëæſſà áûëà áûòſ óâåðåſſà, ÷òſ ſòſ äàò÷èêè ſſſûëàþò òſſëüſſ òó èſſôſðſàöſèþ, êſòſðàÿ ſóæſſà äëÿ ſëåæſſſèÿ çà ÿäåðſûſſſſ èſſſûòàſſèÿſſ.

Såòſſ óſſëſâſſſàſ óäſſòſſâåðſſſèÿ ſſäëëſſſſſòſſ ſſæåò ðåøèòü ſðåáó ſðſſáåſſó, ſſſ òſſëüſêſ öèôðſâſûå ſſäſſſſòſ ſſæſſſſſ ſòſſſſſſſ ſòſſ ſſäſſſſſâſ, ſſæåò ſſðſ÷åſòſ, ſſſ ſſå èſſſſſſſſ äàſſſûå ſåéſſſſſâðàſâ, à ſëåäſÿſàÿ ſòſðſſſà ſſàåò, ÷òſ äàſſſûå ſſå áûëè ſſääåëàſſû.

2.7 Öèôðîâûå ïîäïèſè è øèôðîâàſèå

Îáúäåäſſſâ öèôðſâſûå ſſäſſſſſ è êðſſſòſſðàſâſſ ſ ſòſêðſſòſſſſ êëþ÷àſſ, ſſû ðàçðàſáàòſâſàå ſſðſòſêſſ, êſſáſſſſſſðòſſſſ áåçſſſàſſſſſòſſ øſôſſſâſſſſſ è äſſſòſâåðſſſſòſ öſôſðſâſûſ ſſäſſſſſé. Ñðàſſſòå ſ ſſſſſſſſ òſ âàøåſſ ſàſû. Sſäſſſſſ óäſſòſâåðÿåò àâſòſðſòſâſ à êſſſåðò ſſáåſſſå÷èâàåò òàſſó.

(1) Àëèſà ſſäſſſſſûâàåò ſſſáùåſſåſ ſ ſſſſſûü ſâſſåſſ çàêðûſſſſ êëþ÷à.

$S_A(M)$

(2) Àëèſà øſôſóåò ſſäſſſſſſſſſ ſſſáùåſſåſ îſêðûſſſ êëþ÷ſſ Áſáà è ſſſûëàåò åſſ Áſáó.

$E_B\ (S_A(M))$

(3) Áſſ ðàſøſôſðſâſûâàåò ſſſáùåſſåſ ſ ſſſſſûü ſâſſåſſ çàêðûſſſſ êëþ÷à.

$D_B\ (E_B\ (S_A(M)))= S_A(M)$

(4) Áſſ ſſðſâåðÿåò ſſäſſſſſ ſ ſſſſſûü ſòſêðûſſſ êëþ÷à Àëèſû è âſſſòſſſâêëèâàåò ſſſáùåſſåſ.

$V_A\ (S_A(M))= M$

Ïîäïèñü ïåðåä øèôðîâàíèåì âûãëÿäèò åñòåñòâåííî. Êîãäà Àëèñà ïèøåò ïèñüìî, îíà ïîäïèñûâàåò åãî è çàòåì êëàäåò â êîíâåðò. Åñëè îíà ïîëîæèò ïèñüìî â êîíâåðò íåïîäïèñàííûì, òî Áîá ìîæåò çàáåñïîêîèòüñÿ, âäðóã ïèñüìî áûëî òàéíî ïîäìåíåíî. Åñëè Áîá ïîêàæåò Êýðîë ïèñüìî Àëèñû è êîíâåðò, Êýðîë ìîæåò îáâèíèòü Áîáà, ÷òî îí âðåò î òîì, êàêîå ïèñüìî â êàêîì êîíâåðòå ïðèøëî.

Â ýëåêòðîííîé êîððåñïîíäåíöèè òî÷íî òàêæå ÿâëÿåòñÿ ðàçóìíûì èñïîëüçîâàíèå ïîäïèñè ïåðåä øèôðîâàíèåì [48]. Ýòî íå òîëüêî áîëåå áåçîïàñíî - âðàã íå ñìîæåò óäàëèòü ïîäïèñü èç øèôðîâàííîãî ñîîáùåíèÿ è äîáàâèòü ñâîþ ñîáñòâåííóþ - íî ñóùåñòâóþò è þðèäè÷åñêèå ñîîáðàæåíèÿ: åñëè ïîäïèñûâàåìûé òåêñò íå âèäåí ïîäïèñûâàþùåìó, êîãäà îí ñòàâèò ïîäïèñü, òî þðèäè÷åñêàÿ ñèëà ïîäïèñè íåâåëèêà [1312]. Ñóùåñòâóþò òàêæå íåêîòîðûå êðèïòîãðàôè÷åñêèå ñïîñîáû âñêðûòèÿ òàêîé ïîñëåäîâàòåëüíîñòè äåéñòâèé, èñïîëüçóþùèå ïîäïèñè RSA (ñì. ðàçäåë 19.3).

Äëÿ Àëèñû íå ñóùåñòâóåò ïðè÷èí èñïîëüçîâàòü îäíó ïàðó êëþ÷åé - îòêðûòûé/çàêðûòûé - äëÿ øèôðîâàíèÿ è ïîäïèñè. Ó íåå ìîæåò áûòü äâå ïàðû êëþ÷åé: îäíà äëÿ øèôðîâàíèÿ è îäíà äëÿ ïîäïèñè. Ó òàêîãî ðàçäåëåíèÿ åñòü ñâîè ïðåèìóùåñòâà: Àëèñà ìîæåò ïåðåäàòü ñâîé êëþ÷ øèôðîâàíèÿ ïîëèöèè, íå êîìïðîìåòèðóÿ ñâîþ ïîäïèñü, îäèí êëþ÷ ìîæåò áûòü óñëîâíî ïåðåäàí (ñì. ðàçäåë 4.13), íå âëèÿÿ íà äðóãîé. Ó êëþ÷åé ìîãóò áûòü ðàçëè÷íûå äëèíû è ñðîêè äåéñòâèÿ.

Êîíå÷íî æå, äëÿ ïðåäîòâðàùåíèÿ ïîâòîðíîãî èñïîëüçîâàíèÿ ñîîáùåíèé ñ ýòèì ïðîòîêîëîì äîëæíû áûòü èñïîëüçîâàíû ìåòêè âðåìåíè. Ìåòêè âðåìåíè òàêæå ìîãóò çàùèòèòü îò äðóãèõ âîçìîæíûõ ëîâóøåê, ïðèìåð îäíîé èç êîòîðûõ ïðèâåäåí íèæå.

Âîçâðàùåíèå ñîîáùåíèÿ ïðè ïðèåìå

Ðàññìîòðèì ðåàëèçàöèþ ýòîãî ïðîòîêîëà ñ äîïîëíèòåëüíîé âîçìîæíîñòüþ ïîäòâåðæäåíèÿ ñîîáùåíèé - ïîëó÷èâ ñîîáùåíèå, Áîá îáÿçàòåëüíî âîçâðàùàåò ïîäòâåðæäåíèå ïðèåìà.

(1) Àëèñà ïîäïèñûâàåò ñîîáùåíèå ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à, øèôðóåò ïîäïèñàííîå ñîîáùåíèå îòêðûòûì êëþ÷îì Áîáà è ïîñûëàåò åãî Áîáó.

$E_B (S_A(M))$

(2) Áîá ðàñøèôðîâûâàåò ñîîáùåíèå ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à, ïðîâåðÿåò ïîäïèñü ñ ïîìîùüþ îòêðûòîãî êëþ÷à Àëèñû è âîññòàíàâëèâàåò ñîîáùåíèå.

$V_A (D_B (E_B (S_A(M))))= M$

(3) Áîá ïîäïèñûâàåò ñîîáùåíèå ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à, øèôðóåò ïîäïèñàííîå ñîîáùåíèå îòêðûòûì êëþ÷îì Àëèñû è ïîñûëàåò åãî Àëèñå îáðàòíî.

$E_A (S_B(M))$

(4) Àëèñà ðàñøèôðîâûâàåò ñîîáùåíèå ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à è ïðîâåðÿåò ïîäïèñü ñ ïîìîùüþ îòêðûòîãî êëþ÷à Áîáà. Åñëè ïîëó÷åííîå ñîîáùåíèå ñîâïàäàåò ñ îòïðàâëåííûì, îíà çíàåò, ÷òî Áîá ïîëó÷èë ïðàâèëüíîå ñîîáùåíèå.

Åñëè äëÿ øèôðîâàíèÿ è ïðîâåðêè öèôðîâîé ïîäïèñè èñïîëüçóåòñÿ îäèí è òîò æå àëãîðèòì, òî ñóùåñòâóåò âîçìîæíîñòü âñêðûòèÿ [506]. Â òàêèõ ñëó÷àÿõ îïåðàöèÿ öèôðîâîé ïîäïèñè - ïðîòèâîïîëîæíîñòü îïåðàöèè øèôðîâàíèÿ: $V_X = E_X$ è $S_X = D_X$.

Ïóñòü Ìýëëîðè - çàðåãèñòðèðîâàííûé ïîëüçîâàòåëü ñî ñâîåé ïàðîé êëþ÷åé: îòêðûòûì è çàêðûòûì. Òåïåðü ïîñìîòðèì, êàê îí ñìîæåò ÷èòàòü ïî÷òó Áîáà. Ñíà÷àëà îí çàïèñûâàåò ñîîáùåíèå Àëèñû Áîáó - ýòàï (1). Çàòåì, íåìíîãî ïîãîäÿ, îí ïîøëåò ýòî ñîîáùåíèå Áîáó, óòâåðæäàÿ, ÷òî îíî îòïðàâëåíî ñàìèì Ìýëëîðè. Áîá, äóìàÿ, ÷òî ýòî îáû÷íîå ñîîáùåíèå îò Ìýëëîðè, äåøèôðèðóåò ýòî ñîîáùåíèå ñâîèì çàêðûòûì êëþ÷îì è ïûòàåòñÿ ïðîâåðèòü ïîäïèñü Ìýëëîðè, äåøèôðèðóÿ åå ñ ïîìîùüþ îòêðûòîãî êëþ÷à Ìýëëîðè. Â ðåçóëüòàòå ïîëó÷àåòñÿ ïîëíàÿ ÷åïóõà:

$E_A (D_B (E_B (D_A(M))))= E_M (D_A(M))$

Äàæå â ýòîì ñëó÷àå, ñëåäóÿ ïðîòîêîëó, Áîá ïîñûëàåò Ìýëëîðè ïîëó÷åííîå ñîîáùåíèå:

$E_M (D_B (E_M (D_A(M))))$

Òåïåðü Ìýëëîðè îñòàåòñÿ òîëüêî ðàñøèôðîâàòü ñîîáùåíèå ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à, çàøèôðîâàòü åãî îòêðûòûì êëþ÷îì Áîáà, ðàñøèôðîâàòü ñíîâà ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à è çàøèôðîâàòü îòêðûòûì êëþ÷îì Àëèñû. *Voilà!* Ìýëëîðè ïîëó÷àåò *M*.

Îòíþäü íå ãëóïî ïðåäïîëîæèòü, ÷òî Áîá ìîæåò àâòîìàòè÷åñêè ïîñûëàòü Ìýëëîðè êâèòàíöèþ. Ýòîò ïðîòîêîë, íàïðèìåð, ìîæåò áûòü âñòðîåí â åãî êîììóíèêàöèîííîå ïðîãðàììíîå îáåñïå÷åíèå è ïîñûëàòü êâèòàíöèè àâòîìàòè÷åñêè. Èìåííî ãîòîâíîñòü ñîîáùèòü î ïðèåìå ÷åïóõè è íàðóøàåò áåçîïàñíîñòü. Åñëè Áîá ïðîâåðèò ñîîáùåíèå íà îñìûñëåííîñòü ïåðåä îòïðàâêîé êâèòàíöèè, îí ñìîæåò èçáåæàòü òàêèõ ïðîáëåì ñ áåçîïàñíîñòüþ.

Ñóùåñòâóþò ìîäåðíèçàöèè ýòîãî ñïîñîáà âñêðûòèÿ, ïðåäïîëàãàþùèå, ÷òî Ìýëëîðè ïîøëåò Áîáó ñîîáùåíèå, îòëè÷íîå îò òîãî, êîòîðîå îí æåëàåò ïåðåõâàòèòü. Íèêîãäà íå ïîäïèñûâàéòå ïðîèçâîëüíûõ ñîîáùåíèé îò äðóãèõ ëþäåé è íå ïåðåäàâàéòå ðåçóëüòàòû äåøèôðîâêè ïðîèçâîëüíûõ ñîîáùåíèé èíûì ëþäÿì.

Îáíàðóæåíèå âñêðûòèÿ, îñíîâàííîãî íà âîçâðàùåíèè ñîîáùåíèÿ

Òîëüêî ÷òî îïèñàííîå âñêðûòèå ðàáîòàåò ïîòîìó, ÷òî îïåðàöèÿ øèôðîâàíèÿ ñîâïàäàåò ñ îïåðàöèåé ïðîâåðêè ïîäïèñè, à îïåðàöèÿ äåøèôðèðîâàíèÿ - ñ îïåðàöèåé ïîäïèñè. Îïåðàöèè øèôðîâàíèÿ è öèôðîâîé ïîäïèñè â áåçîïàñíîì ïðîòîêîëå äîëæíû õîòÿ áû ñëåãêà îòëè÷àòüñÿ. Ïðîáëåìó ðåøàåò èñïîëüçîâàíèå ðàçëè÷íûõ êëþ÷åé äëÿ êàæäîé îïåðàöèè, èëè èñïîëüçîâàíèå äëÿ êàæäîé îïåðàöèè ðàçëè÷íûõ àëãîðèòìîâ, èëè ïðèìåíåíèå ìåòîê âðåìåíè, êîòîðûå äåëàþò ðàçëè÷íûìè ïðèíÿòîå è îòïðàâëÿåìîå ñîîáùåíèÿ, èëè öèôðîâàÿ ïîäïèñü ñ ïîìîùüþ îäíîíàïðàâëåííîé õýø-ôóíêöèè (ñì. ðàçäåë 2.6). Òîãäà, â îáùåì ñëó÷àå, ñëåäóþùèé ïðîòîêîë, èñïîëüçóþùèé àëãîðèòì ñ îòêðûòûì êëþ÷îì, ÿâëÿåòñÿ áåçîïàñíûì:

(1) Àëèñà ïîäïèñûâàåò ñîîáùåíèå.

(2) Àëèñà øèôðóåò ïîäïèñàííîå ñîîáùåíèå îòêðûòûì êëþ÷îì Áîáà (èñïîëüçóÿ àëãîðèòì, îòëè÷àþùèéñÿ îò àëãîðèòìà öèôðîâîé ïîäïèñè) è ïîñûëàåò åãî Áîáó.

(3) Áîá ðàñøèôðîâûâàåò ñîîáùåíèå ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à

(4) Áîá ïðîâåðÿåò ïîäïèñü Àëèñû.

Âñêðûòèÿ êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè

Âî âñåõ ïîäîáíûõ ïðîòîêîëàõ êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè ÿ íå ðàññêàçàë, êàê Àëèñà ïîëó÷àåò îòêðûòûé êëþ÷ Áîáà. Ïîäðîáíî ýòîò âîïðîñ îïèñàí â ðàçäåëå 3.1, íî î íåì ñòîèò óïîìÿíóòü è çäåñü.

Ïðîùå âñåãî óçíàòü ÷åé-òî îòêðûòûé êëþ÷, ñ÷èòàâ åãî îòêóäà-òî èç áåçîïàñíîé áàçû äàííûõ. Ýòà áàçà äàííûõ äîëæíà áûòü îáùåäîñòóïíà, ÷òîáû êàæäûé ìîã ïîëó÷èòü íóæíûé åìó êëþ÷. Áàçà äàííûõ äîëæíà áûòü çàùèùåíà îò íåñàíêöèîíèðîâàííîé çàïèñè, â ïðîòèâíîì ñëó÷àå Ìýëëîðè ñìîæåò ïîäìåíèòü îòêðûòûé êëþ÷ Áîáà. Ïîñëå ýòîãî Áîá óæå íå ñóìååò ÷èòàòü àäðåñîâàííûå åìó ñîîáùåíèÿ, çàòî ýòî ñìîæåò ñäåëàòü Ìýëëîðè.

Äàæå åñëè îòêðûòûå êëþ÷è õðàíÿòñÿ â íàäåæíîé áàçå äàííûõ, Ìýëëîðè ìîæåò ïîäìåíèòü èõ ïðè ïåðåäà÷å. ×òîáû âîñïðåïÿòñòâîâàòü ýòîìó, Òðåíò äîëæåí ïîäïèñûâàòü êàæäûé îòêðûòûé êëþ÷, èñïîëüçóÿ ñâîé ñîáñòâåííûé çàêðûòûé êëþ÷. Òðåíòà, êîòîðûé äåéñòâóåò ïîäîáíûì îáðàçîì, ÷àñòî íàçûâàþò **Îðãàíîì ñåðòèôèêàöèè êëþ÷åé** èëè **Öåíòðîì ðàñïðåäåëåíèÿ êëþ÷åé** (Key Distribution Center, KDC). Íà ïðàêòèêå KDC ïîäïèñûâàåò ñëîæíîå ñîîáùåíèå, ñîñòîÿùåå èç èìåíè ïîëüçîâàòåëÿ, åãî îòêðûòîãî êëþ÷à è äðóãîé èíôîðìàöèè î ïîëüçîâàòåëå. Ýòî ïîäïèñàííîå ñëîæíîå ñîîáùåíèå è õðàíèòñÿ â áàçå äàííûõ KDC. Êîãäà Àëèñà ïîëó÷àåò êëþ÷ Áîáà, îíà ïðîâåðÿåò ïîäïèñü KDC, óäîñòîâåðÿÿñü â ïðàâèëüíîñòè êëþ÷à.

Ïðè îêîí÷àòåëüíîì àíàëèçå âèäíî, ÷òî è ýòîò òîëüêî çàòðóäíÿåò, íî íå äåëàåò íåâîçìîæíûì ìîøåííè÷åñòâî Ìýëëîðè. Àëèñà æå äîëæíà îòêóäà-òî ïîëó÷èòü îòêðûòûé êëþ÷ KDC. Ìýëëîðè íóæíî ïîäìåíèòü ýòîò êëþ÷ ñâîèì îòêðûòûì êëþ÷îì, èñïîðòèòü áàçó äàííûõ è çàìåíèòü ïðàâèëüíûå êëþ÷è ñâîèìè (ïîäïèñàííûìè åãî çàêðûòûì êëþ÷îì, êàê åñëè áû îí è áûë KDC), è åãî äåëî ñäåëàíî. Íî, äàæå ïîäïèñè íà áóìàãå ìîãóò áûòü ïîääåëàíû, åñëè Ìýëëîðè âñåðüåç âîçüìåòñÿ çà äåëî. Ïîäðîáíî îáìåí êëþ÷àìè ðàññìàòðèâàåòñÿ â ðàçäåëå 3.1.

2.8. Ãåíåðàöèÿ ñëó÷àéíûõ è ïñåâäîñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé

Ïî÷åìó äàæå â êíèãå ïî êðèïòîãðàôèè ñíîâà ýòè äîêó÷ëèâûå ðàññóæäåíèÿ î ãåíåðàöèè ñëó÷àéíûõ ÷èñåë? Ãåíåðàòîð ñëó÷àéíûõ ÷èñåë âñòðîåí â êàæäûé êîìïèëÿòîð, îáû÷íûé âûçîâ ôóíêöèè. Ïî÷åìó áû íå èñïîëüçîâàòü åãî? Ê ñîæàëåíèþ, ýòè ãåíåðàòîðû ñëó÷àéíûõ ÷èñåë ïî÷òè íàâåðíÿêà íåäîñòàòî÷íî áåçîïàñíû äëÿ êðèïòîãðàôèè è, âîçìîæíî, äàæå íå ñîâñåì ñëó÷àéíû. Áîëüøèíñòâî èç íèõ âåñüìà ïëîõè.

Ãåíåðàòîðû ñëó÷àéíûõ ÷èñåë íà ñàìîì äåëå ñîâñåì íå ñëó÷àéíû, ïîòîìó ÷òî èì è íå íóæíî áûòü òàêèìè. Äëÿ áîëüøèíñòâà ïðèëîæåíèé, íàïðèìåð, êîìïüþòåðíûõ èãð, òðåáóåòñÿ òàê ìàëî ñëó÷àéíûõ ÷èñåë, ÷òî èõ íåñëó÷àéíîñòü âðÿä ëè áóäåò çàìåòíà. Îäíàêî, êðèïòîãðàôèÿ î÷åíü ÷óâñòâèòåëüíà ê ñâîéñòâàì ãåíåðàòîðîâ ñëó÷àéíûõ ÷èñåë. Ïðèìåíèòå ïëîõîé ãåíåðàòîð, è ó âàñ ïîÿâÿòñÿ òàèíñòâåííûå êîððåëÿöèè è ñòðàííûå ðåçóëüòàòû [1231, 1238]. Åñëè âàøà áåçîïàñíîñòü çàâèñèò îò ãåíåðàòîðà ñëó÷àéíûõ ÷èñåë, òàèíñòâåííûå êîððåëÿöèè è ñòðàííûå ðåçóëüòàòû ÿâëÿþòñÿ àáñîëþòíî íå òåì, ÷åãî áû âû æåëàëè äîáèòüñÿ.

Ïðîáëåìà â òîì, ÷òî ãåíåðàòîð ñëó÷àéíûõ ÷èñåë íå ñîçäàåò ñëó÷àéíîé ïîñëåäîâàòåëüíîñòè. Îí, âîçìîæíî, íå âûäàåò íè÷åãî äàæå îòäàëåííî íàïîìèíàþùåãî ñëó÷àéíóþ ïîñëåäîâàòåëüíîñòü. Êîíå÷íî, íåâîçìîæíî ñîçäàâàòü íà êîìïüþòåðå ÷òî-òî ïî íàñòîÿùåìó ñëó÷àéíîå. Äîíàëüä Êíóò ïðèïèñûâàë ôîí Íåéìàíó ñëåäóþùèå ñëîâà: "Êàæäûé, êòî çàíèìàåòñÿ àðèôìåòè÷åñêèìè ìåòîäàìè ïîëó÷åíèÿ ñëó÷àéíûõ ÷èñåë, îïðåäåëåííî ãðåøèò" [863]. Êîìïüþòåðû - ýòî äåòåðìèíèðîâàííûå áåñòèè: çàêëàäûâàåòñÿ èçâåñòíûé ìàòåðèàë, âûïîëíÿþòñÿ ïîëíîñòüþ ïðåäñêàçóåìûå äåéñòâèÿ, è ÷òî-òî îòëè÷íîå âûïîëçàåò ñ äðóãîãî êîíöà. Ïîäà÷à îäíîãî è òîãî æå íà âõîä â äâóõ ðàçëè÷íûõ ñëó÷àÿõ ïðèâåäåò ê îäíîìó è òîìó æå ðåçóëüòàòó. Çàëîæèòå îäèíàêîâûå èñõîäíûå äàííûå â äâà

èäåíòè÷íûõ êîìïüþòåðà, è îáà îíè ïîäñ÷èòàþò îäíî è òî æå. Êîìïüþòåð ìîæåò íàõîäèòüñÿ òîëüêî â îãðàíè÷åííîì ÷èñëå ñîñòîÿíèé (î÷åíü áîëüøîì, íî âñå æå îãðàíè÷åííîì), è âûäàâàåìûé ðåçóëüòàò âñåãäà áóäåò ñòðîãî îïðåäåëÿòüñÿ èñõîäíûìè äàííûìè è òåêóùèì ñîñòîÿíèåì êîìïüþòåðà. Ýòî çíà÷èò, ÷òî ëþáîé ãåíåðàòîð ñëó÷àéíûõ ÷èñåë íà êîìïüþòåðå (ïî ìåíüøåé ìåðå, íà êîíå÷íîì àâòîìàòå), ïî îïðåäåëåíèþ, ïåðèîäè÷åí. À âñå, ÷òî ïåðèîäè÷íî, ïî îïðåäåëåíèþ, ïðåäñêàçóåìî. À âñå, ÷òî ïðåäñêàçóåìî, íå ìîæåò áûòü ñëó÷àéíûì. Äëÿ íàñòîÿùåãî ãåíåðàòîðà ñëó÷àéíûõ ÷èñåë íóæíî ïîäàâàòü íà âõîä ÷òî-íèáóäü ñëó÷àéíîå, êîìïüþòåð æå íå ìîæåò îáåñïå÷èòü ýòî òðåáîâàíèå.

Ïñåâäîñëó÷àéíûå ïîñëåäîâàòåëüíîñòè

Ëó÷øåå, ÷òî ìîæåò ñäåëàòü êîìïüþòåð - ýòî **ãåíåðàòîð ïñåâäîñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé**. ×òî ýòî òàêîå? Ìíîãèå ïûòàëèñü äàòü åãî ôîðìàëüíîå îïðåäåëåíèå, íî ÿ óêëîíþñü îò ýòîãî. Ïñåâäîñëó÷àéíàÿ ïîñëåäîâàòåëüíîñòü - ýòî ÷òî-òî, âûãëÿäÿùåå êàê ñëó÷àéíîå. Ïåðèîä ïîñëåäîâàòåëüíîñòè äîëæåí áûòü äîñòàòî÷íî âåëèê, ïîýòîìó êîíå÷íàÿ ïîñëåäîâàòåëüíîñòü ðàçóìíîé äëèíû - êîòîðàÿ â äåéñòâèòåëüíîñòè è èñïîëüçóåòñÿ - íå ïåðèîäè÷íà. Åñëè âàì íóæåí ìèëëèàðä ñëó÷àéíûõ áèò, íå ïîëüçóéòåñü ãåíåðàòîðîì ïîñëåäîâàòåëüíîñòè, ïîâòîðÿþùåéñÿ êàæäûå øåñòíàäöàòü òûñÿ÷ áèò. Ýòè îòíîñèòåëüíî êîðîòêèå íåïåðèîäè÷åñêèå ïîäïîñëåäîâàòåëüíîñòè äîëæíû áûòü, íàñêîëüêî ýòî âîçìîæíî, íåîòëè÷èìû îò ñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé. Íàïðèìåð, â íèõ äîëæíî áûòü ïðèìåðíî îäèíàêîâîå êîëè÷åñòâî åäèíèö è íóëåé, îêîëî ïîëîâèíû ñåðèé (ïîñëåäîâàòåëüíîñòåé îäèíàêîâûõ áèò) äîëæíû áûòü åäèíè÷íîé äëèíû, ÷åòâåðòü - ñîñòîÿòü èç äâóõ áèò, âîñüìàÿ ÷àñòü - èç òðåõ, è ò.ä. Ýòè ïîñëåäîâàòåëüíîñòè äîëæíû áûòü íåñæèìàåìû. Ðàñïðåäåëåíèå äëèí ñåðèé äëÿ íóëåé è åäèíèö äîëæíî áûòü îäèíàêîâûì [643, 863, 99, 1357]. Ýòè ñâîéñòâà ìîãóò áûòü èçìåðåíû îïûòíûì ïóòåì è çàòåì ñðàâíåíû ñ îæèäàåìûìè ñòàòèñòè÷åñêè ñ ïîìîùüþ ñòàòèñòèêè õè-êâàäðàò. Äëÿ íàøèõ öåëåé ãåíåðàòîð ïîñëåäîâàòåëüíîñòè ñ÷èòàåòñÿ ïñåâäîñëó÷àéíûì, åñëè îí îáëàäàåò ñëåäóþùèì ñâîéñòâîì:

1. Îí âûãëÿäèò ñëó÷àéíî. Ýòî îçíà÷àåò, ÷òî îí ïðîõîäèò âñå òåñòû íà ñëó÷àéíîñòü, êîòîðûå íàì óäàëîñü íàéòè. (Íà÷íèòå ñ ïðèâåäåííûõ â [863].)

Ìíîæåñòâî óñèëèé áûëî çàòðà÷åíî íà ñîçäàíèå õîðîøèõ ïñåâäîñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé íà êîìïüþòåðå. Îáñóæäåíèå ãåíåðàòîðîâ â áîëüøîì êîëè÷åñòâå ìîæíî íàéòè â àêàäåìè÷åñêîé ëèòåðàòóðå âìåñòå ñ ðàçëè÷íûìè òåñòàìè íà ñëó÷àéíîñòü. Âñå ýòè ãåíåðàòîðû ïåðèîäè÷íû (ýòîãî íåâîçìîæíî èçáåæàòü), íî, åñëè èõ ïåðèîä 2^{256} è âûøå, îíè ìîãóò áûòü èñïîëüçîâàíû â ñàìûõ ñåðüåçíûõ ïðèëîæåíèÿõ.

Ïðîáëåìà èìåííî â ýòèõ òàèíñòâåííûõ êîððåëÿöèÿõ è ñòðàííûõ ðåçóëüòàòàõ. Êàæäûé ãåíåðàòîð ïñåâäîñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé ñîçäàåò òàêèå ñòðàííîñòè, åñëè âû èñïîëüçóåòå åãî îïðåäåëåííûì îáðàçîì. À ýòî èìåííî òî, ÷òî íóæíî êðèïòîàíàëèòèêó äëÿ âçëîìà ñèñòåìû.

Êðèïòîãðàôè÷åñêè áåçîïàñíûå ïñåâäîñëó÷àéíûå ïîñëåäîâàòåëüíîñòè

Êðèïòîãðàôè÷åñêèå ïðèëîæåíèÿ ïðåäúÿâëÿþò ê ãåíåðàòîðó ïñåâäîñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé áîëåå âûñîêèå òðåáîâàíèÿ ïî ñðàâíåíèþ ñ äðóãèìè ïðèëîæåíèÿìè. Êðèïòîãðàôè÷åñêàÿ ñëó÷àéíîñòü íå îçíà÷àåòñÿ ñòàòèñòè÷åñêîé ñëó÷àéíîñòüþ, õîòÿ è âêëþ÷àåò åå. ×òîáû ïîñëåäîâàòåëüíîñòü áûëà **êðèïòîãðàôè÷åñêè áåçîïàñíîé ïñåâäîñëó÷àéíîé** ïîñëåäîâàòåëüíîñòüþ, îíà äîëæíà îáëàäàòü ñëåäóþùèì ñâîéñòâîì:

2. Îíà íåïðåäñêàçóåìà. Äîëæíî áûòü î÷åíü òðóäíî (ñ òî÷êè çðåíèÿ ïðèìåíåíèÿ âû÷èñëèòåëüíûõ ìîùíîñòåé) ïðåäñêàçàòü, êàêèì áóäåò ñëåäóþùèé ñëó÷àéíûé áèò, äàæå åñëè ïîëíîñòüþ èçâåñòåí àëãîðèòì èëè óñòðîéñòâî, ãåíåðèðóþùåå ïîñëåäîâàòåëüíîñòü, è âñå ïðåäûäóùèå áèòû ïîòîêà.

Êðèïòîãðàôè÷åñêè áåçîïàñíûå ïñåâäîñëó÷àéíûå ïîñëåäîâàòåëüíîñòè íå äîëæíû ñæèìàòüñÿ..., åñëè âàì íåèçâåñòåí êëþ÷. Êëþ÷îì îáû÷íî ÿâëÿåòñÿ çàäàâàåìîå íà÷àëüíîå ñîñòîÿíèå ãåíåðàòîðà.

Êàê è ëþáîé êðèïòîãðàôè÷åñêèé àëãîðèòì, ãåíåðàòîðû êðèïòîãðàôè÷åñêè áåçîïàñíûõ ïñåâäîñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé ïðåäñòàâëÿþò ñîáîé ïðåäìåò âñêðûòèÿ. Òàê æå êàê è êðèïòîãðàôè÷åñêèé àëãîðèòì, ìîæåò áûòü âçëîìàí è ãåíåðàòîð êðèïòîãðàôè÷åñêè áåçîïàñíûõ ïñåâäîñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé. Ñîçäàíèå óñòîé÷èâûõ ê âñêðûòèþ ãåíåðàòîðîâ ÿâëÿåòñÿ îñíîâîé êðèïòîãðàôèè.

Íàñòîÿùèå ñëó÷àéíûå ïîñëåäîâàòåëüíîñòè

Òåïåðü ìû âòîðãàåìñÿ â îáëàñòü, ïðèíàäëåæàùóþ ôèëîñîôàì. Ñóùåñòâóåò ëè òàêàÿ âåùü êàê ñëó÷àéíîñòü? ×òî òàêîå ñëó÷àéíàÿ ïîñëåäîâàòåëüíîñòü? Êàê óçíàòü, ÷òî ïîñëåäîâàòåëüíîñòü ñëó÷àéíà? ßâëÿåòñÿ ëè "101110100" áîëåå ñëó÷àéíîé ÷åì "101010101"? Êâàíòîâàÿ ìåõàíèêà óáåæäàåò íàñ â òîì, ÷òî â ðåàëüíîì ìèðå ñóùåñòâóåò íàñòîÿùàÿ ñëó÷àéíîñòü. Íî êàê ñîõðàíèòü ýòó ñëó÷àéíîñòü â ïðåäîïðåäåëåííîì ìèðå êîìïüþòåðíûõ ìèêðîñõåì è êîíå÷íûõ àâòîìàòîâ?

Â ñòîðîíó ôèëîñîôèþ, ñ íàøåé òî÷êè çðåíèÿ ãåíåðàòîð ïîñëåäîâàòåëüíîñòè **äåéñòâèòåëüíî ñëó÷àåí**, åñëè îí îáëàäàåò òðåòüèì ñâîéñòâîì:

3. Ñîçäàâàåìàÿ èì ïîñëåäîâàòåëüíîñòü íå ìîæåò áûòü óâåðåííî âîñïðîèçâåäåíà. Åñëè âû çàïóñêàåòå ãå-

íåðàòîð ñëó÷àéíûõ ÷èñåë äâàæäû ñ îäíèì è òåì æå âõîäîì (ïî êðàéíåé ìåðå, íàñêîëüêî ýòî â ÷åëîâå÷åñêèõ ñèëàõ), òî âû ïîëó÷èòå äâå ñîâåðøåííî íåçàâèñèìûå ñëó÷àéíûå ïîñëåäîâàòåëüíîñòè.

Âûõîä ãåíåðàòîðà, óäîâëåòâîðÿþùåãî âñåì òðåáîâàíèÿì, áóäåò äîñòàòî÷íî õîðîø äëÿ îäíîðàçîâîãî áëîêíîòà, ãåíåðàöèè êëþ÷à è äðóãèõ êðèòè÷åñêèõ ïðèìåíåíèé, òðåáóþ ùèõ ãåíåðàöèè äåéñòâèòåëüíî ñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé. Òðóäíîñòü â òî ì, ÷òîáû ïîíÿòü, äåéñòâèòåëüíî ëè ïîñëåäîâàòåëüíîñòü ñëó÷àéíà? Åñëè ÿ ïîâòîðíî çàøèôðóþ ñòðîêó, èñïîëüçóÿ DES è çàäàííûé êëþ÷, ÿ ïîëó÷ó õîðîøèé, âûãëÿäÿùèé ñëó÷àéíûì îáðàçîì ðåçóëüòàò, âû íå ñìîæåòå ñêàçàòü, ÷òî îí íå ñëó÷àåí, ïîêà âû íå íàéìåòå âçëîìùèêà DES èç NSA.

Ãëàâà 3
Îñíîâíûå ïðîòîêîëû

3.1 Îáùåí êëþ÷àìè

Îáùåïðèíÿòîé êðèïòîãðàôè÷åñêîé òåõíèêîé ÿâëÿåòñÿ øèôðîâàíèå êàæäîãî èíäèâèäóàëüíîãî îáùåíèÿ ìåæäó äâóìÿ ïîëüçîâàòåëÿìè ïîäåëüíûì êëþ÷îì. Òàêîé êëþ÷ íàçûâàåòñÿ ñåàíñîâûì, òàê êàê îí èñïîëüçóåòñÿ äëÿ åäèíñòâåííîãî îòâåòíîãî ñåàíñà îáùåíèÿ ìåæäó äâóìÿ ïîëüçîâàòåëÿìè. Â ðàçäåëå 8.5 ãîâîðèòñÿ î òî ì, ÷òî ñåàíñîâûå êëþ÷è ïîëåçíû, òàê êàê âðàì èõ ñóùåñòâîâàíèÿ îïðåäåëåíèÿ ïîääåðæèâàþò ëåãêîâåñíûå ñåàíñû ñâÿçè. Ïåðåäà÷à ýòîãî îáùåãî ñåàíñîâîãî êëþ÷à â ðóêè îáúåêâàþùèõñÿ èíôîðìàöèè ïðåäïîëàãàåò ñîâìåñòíóþ ïðîáëåìó.

Îáìåí êëþ÷àìè ñ ïîìîùüþ ñèìåòðè÷íîé êðèïòîãðàôèè

Ýòîò ïðîòîêîë ïðåäïîëàãàåò, ÷òî ïîëüçîâàòåëè ñåòè, Àëèñà è Áîá, ïîëó÷àþò ñåðâèñíûé êëþ÷ îò Öåíòðà ðàñïðåäåëåíèÿ êëþ÷åé (Key Distribution Center, KDC) [1260] - Òðåòèà íàøèõ ïðîòîêîëîâ. Ïåðâà íà÷àëî ïðîòîêîëà ýòè êëþ÷è óæå äîëæíû áûòü ó ïîëüçîâàòåëåé. (Ïðîòîêîë èãíîðèðóåò î÷åíü íàñóùíóþ ïðîáëåìó äîñòàâêè ýòèõ ñåêðåòíûõ êëþ÷åé, ïðåäïîëàãàåòñÿ, ÷òî êëþ÷è óæå ó ïîëüçîâàòåëåé, è Ìýëîðè íå èìååò î íèõ íèêàêîé èíôîðìàöèè.)

(1) Àëèñà îáðàùàåòñÿ ê Öåíòó è çàïðàøèâàåò ñåàíñîâûé êëþ÷ äëÿ ñâÿçè ñ Áîáîì.

(2) Öåíòð ãåíåðèðóåò ñëó÷àéíûé ñåàíñîâûé êëþ÷. Îí çàøèôðîâûâàåò äâå êîïèè êëþ÷à: îäíó äëÿ Àëèñû, à äðóãóþ - äëÿ Áîáà. Çàòåì Öåíòð ïîñûëàåò îáå êîïèè Àëèñå.

(3) Àëèñà ðàñøèôðîâûâàåò ñâîþ êîïèþ ñåàíñîâîãî êëþ÷à.

(4) Àëèñà ïîñûëàåò Áîáó åãî êîïèþ ñåàíñîâîãî êëþ÷à.

(5) Áîá ðàñøèôðîâûâàåò ñâîþ êîïèþ ñåàíñîâîãî êëþ÷à.

(6) Àëèñà è Áîá èñïîëüçóþò ýòîò ñåàíñîâûé êëþ÷ äëÿ áåçîïàñíîãî îáìåíà èíôîðìàöèåé.

Ýòîò ïðîòîêîë îñíîâàí íà àáñîëþòíî íàäåæíîñòè Öåíòðà, äëÿ ðîëè êîòîðîãî áîëüøå ïîäõîäèò çàñëóæèâàþùèé äîâåðèÿ êîìïüþòåðíûé ïðîãðàììà, ÷åì çàñëóæèâàþùèé äîâåðèÿ ÷åëîâåê. Åñëè Ìýëîðè ïîëó÷èò äîñòóï ê Öåíòðó, ñêîìïðîìåòèðîâàííîé îêàæåòñÿ âñÿ ñåòü. Â âåî ðóêàõ îêàæóòñÿ âñå ñåêðåòíûå êëþ÷è, âûäåëåííûå ïîëüçîâàòåëÿì Öåíòðîì, îí ñìîæåò ïðî÷åñòü âñå ïåðåäàííûå ñîîáùåíèÿ, êîòîðûå åì óäàëîñü ïåðåõâàòèòü, è âñå áóäóùèå ñîîáùåíèÿ. Åì óñòàíîâèò òîëüêî ïîäëþ÷èòüñÿ ê ëèíèÿì ñâÿçè è ïîäñëóøèâàòü çàøèôðîâàííûé ïîòîê ñîîáùåíèé.

Äðóãîé ïðîáëåìîé òàêîé ñèñòåìû ÿâëÿåòñÿ òî, ÷òî Öåíòð ïîòåíöèàëüíî ÿâëÿåòñÿ åå óçêèì ìåñòîì. Îí äîëæåí ó÷àñòâîâàòü â êàæäîì îáìåíå êëþ÷àìè. Åñëè ñ íèì ÷òî-òî ñëó÷èòñÿ, ýòî ðàçðóøèò âñþ ñèñòåìó.

Îáìåí êëþ÷àìè, ñíîñèòåëÿ êðèïòîãðàôèþ ñ òðåõêëþ÷åâûì øèôðîâàíèåì êëþ÷àìè

Áàçîâàÿ ñìåøàííàÿ êðèïòîñèñòåìà îáñóæäàëàñü â ðàçäåëå 1.5. Äëÿ ñîãëàñîâàííîñòè êëþ÷à Àëèñà è Áîá ïðèíÿþò êðèïòîãðàôèþ ñ òðåõêëþ÷åâûì øèôðîâàíèåì, à çàòåì èñïîëüçóþò ýòîò ñåàíñîâûé êëþ÷ äëÿ øèôðîâàíèÿ äàííûõ. Â íåêîòîðûõ ðåàëèçàöèÿõ ïîäîáíîé êëþ÷è Àëèñû è Áîáà äîñòóïíû â íåêîòîðîé áàçå äàííûõ. Ýòî çíà÷èòåëüíî îáëåã÷àåò ïðîòîêîë, òàê êàê Áîá î íåé íèêîãäà íå ñëûøàë, ìîæåò áåçîïàñíî ïîñëàòü Áîáó ñîîáùåíèå:

(1) Àëèñà ïîëó÷àåò îòêðûòûé êëþ÷ Áîáà èç KDC.

(2) Àëèñà ãåíåðèðóåò ñëó÷àéíûé ñåàíñîâûé êëþ÷, çàøèôðîâûâàåò åãî îòêðûòûì êëþ÷îì Áîáà è ïîñûëàåò åãî Áîáó.

(3) Áîá ðàñøèôðîâûâàåò ñîîáùåíèå Àëèñû ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à.

(4) Àëèñà è Áîá øèôðóþò ñâîé îáìåí èíôîðìàöèåé ýòèì ñåàíñîâûì êëþ÷îì.

Âñêðûòèå "÷åëîâåê-â-ñåðåäèíå"

Â òî âðåìÿ, êàê Åâà íå ìîæåò ñäåëàòü íè÷åãî ëó÷øåãî, ÷åì ïûòàòüñÿ âçëîìàòü àëãîðèòì ñ îòêðûòûì êëþ÷îì è êëþ÷àìè èëè âûïîëíèòü âñêðûòèå ñ èñïîëüçîâàíèåì òîëüêî øèôðîâàííîãî òåêñòà, ó Ìýëîðè âîðàçàí áîëüøå âîçìîæíîñòåé. Î íå òîëüêî ìîæåò ïîäñëóøàòü ñîîáùåíèÿ Àëèñû è Áîáà, íî è èçìåíèòü ñîîáùåíèÿ, óäàëèòü ñîîáùåíèÿ è ñîçäàòü ñîâåðøåííî íîâûå. Ìýëîðè ìîæåò âûäàòü ñåáÿ çà Áîáà, ñîîáùàþùåãî ÷òî-òî Àëèñå, èëè çà Àëèñó, ñîîáùàþùóþ ÷òî-òî Áîáó. Âîò êàê áóäåò âûïîëíåí âñêðûòèå:

(1) Àëèñà ïîñûëàåò Áîáó ñâîé îòêðûòûé êëþ÷. Ìýëîðè ïåðåõâàòûâàåò åãî è ïîñûëàåò Áîáó ñâîé ñîáñòâåííûé îòêðûòûé êëþ÷.

(2) Âîá ïîñûëàåò Àëèñå ñâîé îòêðûòûé êëþ÷. Ìýëîðè ïåðåõâàòûâàåò åãî è ïîñûëàåò Àëèñå Âîáó ñîáñòâåííûé îòêðûòûé êëþ÷.

(3) Êîãäà Àëèñà ïîñûëàåò ñîîáùåíèå Âîáó, çàøèôðîâàííîå îòêðûòûì êëþ÷îì "Âîáà", Ìýëîðè ïåðåõâàòûâàåò åãî. Òàê êàê ñîîáùåíèå â äâóñòàòèðè÷íîñòè çàøèôðîâàíî åãî ñîáñòâåííûì îòêðûòûì êëþ÷îì, îí ðàñøèôðîâûâàåò åãî, ñíîâà çàøèôðîâûâàåò îòêðûòûì êëþ÷îì Âîáà è ïîñûëàåò Âîáó.

(4) Êîãäà Âîá ïîñûëàåò ñîîáùåíèå Àëèñå, çàøèôðîâàííîå îòêðûòûì êëþ÷îì "Àëèñû", Ìýëîðè ïåðåõâàòûâàåò åãî. Òàê êàê ñîîáùåíèå â äâóñòàòèðè÷íîñòè çàøèôðîâàíî åãî ñîáñòâåííûì îòêðûòûì êëþ÷îì, îí ðàñøèôðîâûâàåò åãî, ñíîâà çàøèôðîâûâàåò îòêðûòûì êëþ÷îì Àëèñû è ïîñûëàåò Àëèñå.

Ýòî âñêðûâàåò áóäóò òàòü, äàæå åñëè îòêðûòûå êëþ÷è Àëèñû è Âîáà õðàíÿòñÿ â áàçå äàííûõ. Ìýëîðè ìîæåò ïåðåõâàòèòü çàïðîñ Àëèñû ê áàçå äàííûõ è ïîäìåíèòü îòêðûòûé êëþ÷ Âîáà ñâîèì ñîáñòâåííûì. Òî æå ñàìîå ñäåëàòü è ñ îòêðûòûì êëþ÷îì Àëèñû. Èëè, åùå ëó÷øå, îí ìîæåò èñïîäüçîâàòü áàçó äàííûõ è ïîäìåíèòü îòêðûòûå êëþ÷è Âîáî è Àëèñû ñâîè. Òåïåðü îí ìîæåò ïðóôèòü, ïðîñòî äîáàâèâ êîððåêòíûé ñîîáùåíèÿì è, è íà÷àâ ïåðåõâàòûâàòü è èçìåíÿòü ýòè ñîîáùåíèÿ.

Òàêîå **âñêðûòèå "÷åëîâåê-â-ñåðåäèíå"** ðàáîòàåò, òàê êàê ó Àëèñû è Âîáà íåò ñïîñîáà ïðåâðàòèòü, äåéñòâèòåëüíî ëè îíè îáùàþòñÿ èìåííî äóõ ñ äóõîì. Åñëè âìåøàòåëüñòâî Ìýëîðè íå ïðèâîäèò ê çàìåíó ì çäåðæêè â ñåòè, îáà êîððåñïîíäåíòà è íå ïîäóìàþ, ÷òî êòî-òî, ñèäÿùèé ìåæäó íèì, ÷èòàåò âñþ èõ ñêðûòóþ ïî÷òó.

Ïðîòîêîë "äåðæàñü çà ðóêè"

Ïðîòîêîë "äåðæàñü çà ðóêè", èçîáðåòåííûé Ðîíîì Ðèâåñòîì (Ron Rivest) è Ýäè Øàìèðîì (Adi Shamir) [1327], ïðåäíàçíà÷åí äëÿ ñëó÷àåâ, êîãäà ó Àëèñû è Âîáà íåò ñïîñîáà ïðåâðàòèòü "÷åëîâåê-â-ñåðåäèíå". Âîò êàê îí ðàáîòàåò:

(1) Àëèñà ïîñûëàåò Âîáó ñâîé îòêðûòûé êëþ÷.

(2) Âîá ïîñûëàåò Àëèñå ñâîé îòêðûòûé êëþ÷.

(3) Àëèñà çàøèôðîâûâàåò ñâîå ñîîáùåíèå îòêðûòûì êëþ÷îì Âîáà. Ïîëó÷èâ çàøèôðîâàííîãî ñîîáùåíèÿ îíà îòïðàâëÿåò Âîáó.

(4) Âîá çàøèôðîâûâàåò ñâîå ñîîáùåíèå îòêðûòûì êëþ÷îì Àëèñû. Ïîëó÷èâ çàøèôðîâàííîãî ñîîáùåíèÿ îí îòïðàâëÿåò Àëèñå.

(5) Àëèñà îòïðàâëÿåò Âîáó âòîðóþ ïîëîâèíó çàøèôðîâàííîãî ñîîáùåíèÿ.

(6) Âîá ñêëåèâàåò äâå ÷àñòè ñîîáùåíèÿ Àëèñû è ðàñøèôðîâûâàåò åãî ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à. Âîá îòïðàâëÿåò Àëèñå âòîðóþ ïîëîâèíó ñâîåãî çàøèôðîâàííîãî ñîîáùåíèÿ.

(7) Àëèñà ñêëåèâàåò äâå ÷àñòè ñîîáùåíèÿ Âîáà è ðàñøèôðîâûâàåò åãî ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à.

Èäåÿ â òîì, ÷òî ïîëîâèíà çàøèôðîâàííîãî ñîîáùåíèÿ áåñïîëåçíà áåç âòîðîé ïîëîâèíû, îíà íå ìîæåò áûòü äåøèôðîâàíà. Âîá íå ñìîæåò ïðî÷èòàòü íè îäíîé ÷àñòè ñîîáùåíèÿ Àëèñû äî ýòàïà (6), à Àëèñà íå ñìîæåò ïðî÷èòàòü íè îäíîé ÷àñòè ñîîáùåíèÿ Âîáà äî ýòàïà(7). Ñóùåñòâóåò ìíîæåñòâî ñïîñîáîâ ðàçáèòü ñîîáùåíèå íà ÷àñòè:

— Åñëè èñïîëüçóåòñÿ áëî÷íûé àëãîðèòì øèôðîâàíèÿ, ïîëîâèíà êàæäîãî áëîêà (íàïðèìåð, êàæäûé âòîðîé áèò) ìîæåò áûòü ïðåäàíà â êàæäîé ïîëîâèíå ñîîáùåíèÿ.

— Äåøèôðîâàíèå ñîîáùåíèÿ ìîæåò çàâiñåòü îò âåêòîðà èíèöèàëèçàöèè (ñì. ðàçäåë 9.3), êîòîðûé ìîæåò áûòü ïåðåäàí âî âòîðîé ÷àñòè ñîîáùåíèÿ.

— Ïåðâàÿ ïîëîâèíà ñîîáùåíèÿ ìîæåò áûòü îäíîíàïðàâëåííîé õýø-ôóíêöèåé øèôðîâàííîãî ñîîáùåíèÿ (ñì. ðàçäåë 2.4), à âî âòîðàÿ ïîëîâèíà - ñîáñòâåííî øèôðîâàííûì ñîîáùåíèåì.

×òîáû ïîíÿòü, êàê òàêîé ïðîòîêîë ïîìîæàåò Ìýëîðè, äàâàéòå ðàññìîòðèì åãî ïîïûòêó íàðóøèòü ïðîòîêîë. Êàê è ðàíüøå, îí ìîæåò ïîäìåíèòü îòêðûòûå êëþ÷è Àëèñû è Âîáà ñâîèì íà ýòàïàõ (1) è (2). Íî òàïåðü, ïåðåõâàòèâ ïîëîâèíó ñîîáùåíèÿ Àëèñû íà ýòàïå (3), îí íå ñìîæåò ðàñøèôðîâàòü åå ñâîèì çàêðûòûì êëþ÷îì è ñíîâà çàøèôðîâàòü îòêðûòûì êëþ÷îì Âîáà. Î í ìîæåò ñîçäàòü ñîâåðøåííî íîâîå ñîîáùåíèå è îòïðàâèòü ïîëîâèíó åãî Âîáó. Ïåðåõâàòèâ ïîëîâèíó ñîîáùåíèÿ Âîáà Àëèñå íà ýòàïå (4), Ìýëîðè ñòîëêíåòñÿ ñ ýòîé æå ïðîáëåìîé. Î í íå ñìîæåò ðàñøèôðîâàòü åå ñâîèì çàêðûòûì êëþ÷îì è ñíîâà çàøèôðîâàòü îòêðûòûì êëþ÷îì Àëèñû. Åìó ïðèäåòñÿ ñîçäàòü ñîâåðøåííî íîâûå ñîîáùåíèå è îòïðàâèòü ïîëîâèíó åãî Àëèñå. Ê òîìó âðåìåíè, êîãäà îí ïåðåõâàòèò âòîðûå ïîëîâèíû íàñòîÿùèõ ñîîáùåíèé íà ýòàïàõ (5) è (6), ïîäìåíÿòü ñîçäàííûå èì íîâûå ñîîáùåíèÿ áóäåò ñëèøêîì ïîçäíî. Îáìåí äàííûìè ìåæäó Àëèñîé è Âîáîì èçìåíèòñÿ ðàäèêàëüíî.

Ìýëîðè ìîæåò ïîïûòàòüñÿ èçáåæàòü òàêîãî ðåçóëüòàòà. Åñëè îí äîñòàò÷íî õîðîø çíàåò îáèò êîððåñïîíäåíòîâ, ÷òîáû ñûãðàòü èõ ïðîòîêîë ïî íåçàìåòíîìó èçìåíåíèþ íà ýòàïàõ (3) è (4). Íàïðèìåð, îí ìîæåò çàìåíèòü ñâîé îòêðûòûé êëþ÷ íà ïîääåëêó, ïîõîæóþ íà îòêðûòûé êëþ÷ Âîáà, è ïîïûòàòüñÿ óáåäèòü Âîáà èñïîëüçîâàòü ýòîò êëþ÷ äëÿ øèôðîâàíèÿ ñîîáùåíèÿ. Íî ýòî íàðóøèò ïðîòîêîë, ïîñêîëüêó Âîá íå ñìîæåò ðàñøèôðîâàòü ïîëó÷åííîå ñîîáùåíèå.

Îáùåí êëþ÷àìè ñ ïîìîùüþ öèôðîâûõ ïîäïèñåé

Èñïîëüçîâàíèå öèôðîâîé ïîäïèñè â ïðîòîêîëå îáìåíà ñåàíñîâûì êëþ÷îì òàêæå ïîçâîëÿåò èçáåæàòü âñêðûòèÿ "÷åëîâåê-â-ñåðåäèíå". Òðåòè ïîäïèñûâàò îòêðûòûå êëþ÷è Àëèñû è Áîáà. Ïîäïèñàííûå êëþ÷è âêëþ÷àþò ïîäïèñàííûå çàâåðåíèå ïîäëèííîñòè. Ïîëó÷èâ êëþ÷è, è Àëèñà, è Áîá ïðîâåðÿþò ïîäïèñü Òðåíòà. Òàïåðü îíè óâåðåíû, ÷òî ïðèñëàííûé îòêðûòûé êëþ÷ ïðèíàäëåæèò èìåííî óêàçàííîìó êîððåñïîíäåíòó. Çàòåì âûïîëíÿåòñÿ ïðîòîêîë îáìåíà êëþ÷àìè.

Ìýëîðè ñòàëêèâàåòñÿ ñ ñåðüåçíûì ïðîáëåìîé. Î íå ìîæåò âûäàòü ñåáÿ çà Àëèñó èëè Áîáà, âåäü î íå çíàåò èõ çàêðûòûõ êëþ÷åé. Î íå ìîæåò ïîäìåíèòü èõ îòêðûòûå êëþ÷è ñâîè, ïîòîì ÷òî ïðè ïîäïèñè åãî êëþ÷à Òðåíòó óêàçàë, ÷òî ýòî êëþ÷ Ìýëîðè. Âñå, ÷òî åìó îñòàåòñÿ - ýòî ïðîñëóøèâàòü çàøèôðîâàííûé ïîòîê ñîîáùåíèé èëè èñïîðòèòü ëèíèþ ñâÿçè, ìåøàÿ îáìåíó èíôîðìàöèè Àëèñû è Áîáà.

Òðåíò âûñòóïàåò ó÷àñòíèêîì ýòîãî ïðîòîêîëà, íî ðèñê êîìïðîìåòàöèè KDC ìåíüøå, ÷åì â ïåðâîì ïðîòîêîëå. Åñëè Ìýëîðè êîìïðîìåòèðóåò Òðåíòà (âçëàìûâàåò KDC), îí ïîëó÷àåò òîëüêî çàêðûòûé êëþ÷ Òðåíòà. Ýòîò êëþ÷ ïîçâîëèò åìó òîëüêî ïîäïèñûâàòü íîâûå êëþ÷è, à íå ðàñøèôðîâûâàòü ñåàíñîâûå êëþ÷è èë ÷èòàòü ïðîèçâîëüíûé ïîòîê ñîîáùåíèé. Äëÿ ÷òåíèÿ ñîîáùåíèé Ìýëîðè ïðèäåòñÿ âûäàòü ñåáÿ çà ïîëüçîâàòåëÿ ñåòè è îáìàíûâàòü ÷åñòíûõ ïîëüçîâàòåëåé, øèôðóÿ ñîîáùåíèÿ ñâîè ïîäääëüíûì îòêðûòûì êëþ÷îì.

Ìýëîðè ìîæåò ïðåäïðèíÿòü òàêîå âñêðûòèå. Èñïîëüçóÿ çàêðûòûé êëþ÷ Òðåíòà, îí ìîæåò ñîçäàòü ïîääåëüíûå ïîäïèñàííûå êëþ÷è, ÷òîáû îáìàíóòü Àëèñó è Áîáà. Çàòåì îí ìîæåò ëèáî ïîäìåíèòü ýòè ê êëþ÷àì íàñòîÿùèå êëþ÷è â áàçå äàííûõ, ëèáî ïððõâàòûâàòü çàïðîñû ïîëüçîâàòåëåé ê áàçå äàííûõ è ïîñûëàòü â îòâåò ïîääåëüíûå êëþ÷è. Ýòî ïîçâîëèò åìó îñóùåñòâèòü âñêðûòèå "÷åëîâåê-â-ñåðåäèíå" è ÷èòàòü ñîîáùåíèÿ ïîëüçîâàòåëåé.

Òàêîå âñêðûòèå áóäåò ðàáîòàòü, íî ïîìíèòå, ÷òî äëÿ ýòîãî Ìýëîðè äîëæåí óìåòü ïåðõâàòûâàòü è èçìåíÿòü ñîîáùåíèÿ. Â ðÿäå ñåòåé ýòî íàìíîãî ñëîæíåå, ÷åì ïðîòî ïàññèâíî ñëåäèòü çà îáìåíîì. Çàòåì îí ìîæåò ëèáî ïîäìåíèòü ýòè ê êëþ÷àì íàñòîÿùèå êëþ÷è â áàçå äàííûõ, ëèáî ïððõâàòûâàòü çàïðîñû ïîëüçîâàòåëåé ê áàçå äàííûõ è ïîñûëàòü â îòâåò ïîääåëüíûå êëþ÷è. Ýòî ïîçâîëèò åìó îñóùåñòâèòü âñêðûòèå "÷åëîâåê-â-ñåðåäèíå" è ÷èòàòü ñîîáùåíèÿ ïîëüçîâàòåëåé.

Òàêîå âñêðûòèå áóäåò ðàáîòàòü, íî ïîìíèòå, ÷òî äëÿ ýòîãî Ìýëîðè äîëæåí óìåòü ïåðõâàòûâàòü è èçìåíÿòü ñîîáùåíèÿ. Â ðÿäå ñåòåé ýòî íàìíîãî ñëîæíåå, ÷åì ïðîòî ïàññèâíî ñëåäèòü çà îáìåíîì. Çàòåì îí ìîæåò ëèáî ïîäìåíèòü ýòè ê êëþ÷àì íàñòîÿùèå êëþ÷è â áàçå äàííûõ, ëèáî ïððõâàòûâàòü çàïðîñû ïîëüçîâàòåëåé ê áàçå äàííûõ è ïîñûëàòü â îòâåò ïîääåëüíûå êëþ÷è. Ýòî ïîçâîëèò åìó îñóùåñòâèòü âñêðûòèå "÷åëîâåê-â-ñåðåäèíå" è ÷èòàòü ñîîáùåíèÿ ïîëüçîâàòåëåé.

Ïððäà÷à êëþ÷åé è ñîîáùåíèé

Àëèñà è Áîáó íå îáÿçàòåëüíî âûïîëíÿòü ïðîòîêîë îáìåíà êëþ÷àìè ïðåä îáìåíîì ñîîáùåíèÿìè. Â ýòîì ïðîòîêîëå Àëèñà îòïðàâëÿåò Áîáó ñîîáùåíèå áåç ïðåäâàðèòåëüíîãî ïðîòîêîëà îáìåíà êëþ÷àìè:

(1) Àëèñà ãåíåðèðóåò ñëó÷àéíûé ñåàíñîâûé êëþ÷, *K*, è çàøèôðîâûâàåò *M* ýòèì êëþ÷îì.

$E_K(M)$

(2) Àëèñà ïîëó÷àåò îòêðûòûé êëþ÷ Áîáà èç áàçû äàííûõ.

(3) Àëèñà øèôðóåò *K* îòêðûòûì êëþ÷îì Áîáà.

$E_B(K)$

(4) Àëèñà ïîñûëàåò Áîáó øèôðîâàííûå ñîîáùåíèå è ñåàíñîâûé êëþ÷.

$E_K(M), E_B(K)$

Äëÿ äîïîëíèòåëüíîé çàùèòû îò âñêðûòèÿ "÷åëîâåê-â-ñåðåäèíå" Àëèñà ïîäïèñûâàåò ïåðåä÷óò.

(5) Áîá ðàñøèôðîâûâàåò ñåàíñîâûé êëþ÷ Àëèñû, *K*, èñïîëüçóÿ ñâîé çàêðûòûé êëþ÷.

(6) Áîá, èñïîëüçóÿ ñåàíñîâûé êëþ÷, ðàñøèôðîâûâàåò ñîîáùåíèå Àëèñû.

Ïîäîáíàÿ ñìåøàííàÿ ñèñòåìà è óíòðåáëÿåòñÿ ÷àùå âñåãî â ñèñòåìàõ ñâÿçè. Åå ìîæíî ñîåäèíèòü ñ öèôðîâûìè ïîäïèñÿìè, ìåòêàìè âðåìåíè è äðóãèìè ïðîòîêîëàìè îáåñïå÷åíèÿ áåçîïàñíîñòè.

Øèôðîâàùàòåëüíàÿ ðàñøèðåíà êëþ÷åé è ñîîáùåíèé

Íå ñóùåñòâóåò ïðè÷èí, çàïðåùàþùèõ Àëèñå ïîñûëàòü øèôðîâàííûå ñîîáùåíèå íåñêîëüêèì ëþäÿì. Â ñëåäóþùåì ïðèìåðå Àëèñà ïîñûëàåò øèôðîâàííûå ñîîáùåíèå Áîáó, Êýðîë è Äýéâó:

(1) Àëèñà ãåíåðèðóåò ñëó÷àéíûé ñåàíñîâûé êëþ÷, *K*, è çàøèôðîâûâàåò *M* ýòèì êëþ÷îì.

$E_K(M)$

(2) Àëèñà ïîëó÷àåò èç áàçû äàííûõ îòêðûòûå êëþ÷è Áîáà, Êýðîë è Äýéâà.

(3) Àëèñà øèôðóåò *K* îòêðûòûì êëþ÷àìè Áîáà, Êýðîë è Äýéâà.

$E_B(K)$, $E_C(K)$, $E_D(K)$

(4) Àëèñà øèðîêîâåùàòåëüíî ïîñûëàåò øèôðîâàííûå ñîîáùåíèå è âñå øèôðîâàííûå êëþ÷è ñâîèì êîððåñïîíäåíòàì.

$E_K(M)$, $E_B(K)$, $E_C(K)$, $E_D(K)$

(5) Òîëüêî Áîá, Êýðîë è Äýéâ ìîãóò, êàæäûé ïðè ïîìîùè ñâîåãî çàêðûòîãî êëþ÷à, ðàñøèôðîâàòü êëþ÷ K.

(6) Òîëüêî Áîá, Êýðîë è Äýéâ ìîãóò ðàñøèôðîâàòü ñîáſùåíèå Àëèñû, èñïîëüçóÿ K.

Ýòîò ïðîòîêîë ìîæåò áûòü ðåàëèçîâàí äëÿ ñåòåé ýëåêòðîííîé ïî÷òû. Öåíòðàëüíûé ñåðâåð ìîæåò îòïðàâèòü ñîáſùåíèå Àëèñû Áîáó, Êýðîë è Äýéâ âìåſòå ñ êîíêðåòíûì øèôðîâàííûì êëþ÷îì. Ñåðâåð íå äîëæåí áûòü íàäåæíûì è áåçîïàñíûì, òàê êàê îí íå ìîæåò ðàñøèôðîâàòü íè îäíî èç ñîîáſùåíèé.

3.2 Óäîñòîâåðåíèå ïîäëèííîñòè

Êîãäà Àëèñà ïîâëþ÷àåòñÿ ê ãëàâíîìó êîìïüþòåðó (èëè ê àâòîìàòè÷åſñêîìó, èëè ê òåëåôîííîé áàíêîâſêîé ſèſòåſìå, èëè ê êàêîìó-íèáóäü äðóãîìó òåðìèíàëó), êàê ãëàâíûé êîìïüþòåð óſíàåò, êòî îíà? Îòêóäà ãëàâíûé êîìïüþòåð óſíàåò, ÷òî ýòî íå Åâà, ïûòàþſùèñÿ âûäàòü ſåáÿ çà Àëèſó? Îáû÷íî ýòà ïðîáëåſìà ðåøàåſſÿ ſ ïîìſùüþ ïàðîëåé. Àëèſà ââîäèò ſâîé ïàðîëü, è ãëàâíûé êîìïüþòåð ïðîâåðſåò åãî ïðàâèëüſîſòü. Òàêèì îáðàçîì, è Àëèſå, è ãëàâſîſìó êîìïüþòåðó èſíôîſìàöèÿ, êîòîðóþ ãëàâſûé êîìïüþòåð çàſðàøèâàåò âſÿêèé ðàç, êîãäà Àëèſà ïûòàåſſÿ ïîâëþ÷èòſÿ.

Óäîſòâåðåíèå ïîäëèííîſòè ſ ïîìſùüþ îäſîſíàïðàâëåſſûõ ôóſêöèé

Ðîäæåð Íåääýì (Roger Needham) è Ìàéê Ãàé (Mike Guy) ïîêàçàëè, ſòî ãëàâſîſìó êîìïüþòåðó íå íóæſî çſàòü ſàìè ïàðîëè, âïîſíå äſñòàòſ÷íî, ſòîáû ãëàâſûé êîìïüþòåð ìîã ſòèė÷àòü ïðàâèëüſûå ïàðîëè ſò íåïðàâèëüſûõ. Ýòîſ ëåãêî äſñòè÷ü ſ ïîìſùüþ ſäſſſíàïðàâëåſſûõ ôóſêöèé [1599, 526,1274, 1121]. Ïðè ýòîſ íà ãëàâſîſ êîìïüþòåðå õðàſýòſſ çſà÷åſèÿ ſäſſſíàïðàâëåſſûõ ôóſêöèé ïàðîſåé, à íå ſàſè ïàðîſè.

(1) Àëèſà ïſſûëàåò ãëàâſîſó êîìïüþòåðó ſâſé ïàðîſü.

(2) Ãëàâſûé êîìïüþòåð âû÷èſſÿåò ſäſſſíàïðàâëåſſóþ ôóſêöèþ ïàðîſÿ.

(3) Ãëàâſûé êîìïüþòåð ſðàâſèâàåò ſſêó÷åſſſå çſà÷åſèå ſ õðàſÿùèſſÿ.

Ðàç ãëàâſûé êîìïüþòåð áſêüøå íå õðàſèò òááëèöó ſðàâëèüſûõ ſàðſſëåſ âſåõ ſſêüſſâàòåſåſ, ſſèæàåòſÿ óãðſçà òſãſ, ſòſ êòſ-òſ ſðſſſèſſåò â ãëàâſûé êîìïüþòåð è âſêðàſåò òááëèöó ſàðſſëåſ. Ñſèſſſê ſàðſſëåſ, ſſáðàſſòàſſûé ſäſſſíàſðàâëåſſſé ôóſêöèſåſ, áåſſſſêåçſí, òàê êàê ſäſſſíàſðàâëåſſóþ ôóſêöèþ íå óäàſòſÿ èſſåðòèðſâàòü äëÿ ſſêó÷åſèÿ ſàðſſëåſ.

Âſêðûòèÿ ſ ſſìſùüþ ſëſâàðÿ è "ſſſëü"

Ôàéë ſàðſſëåſ, çàøèôðſâàſſûõ ſäſſſíàſðàâëåſſſé ôóſêöèſåſ, òàſ íå ſåſåå, óſçâèſ. Èſåÿ çàſàſ âðåſåſè, Ìſëëſðè ſſæåò ſſſòàâèòü ſſſèſſſê èç ſèëëèſſſà íàèáſëåå ſ÷àſòſ âſſòðå÷àþſèſſÿ ſàðſſëåſ. Sſ ſſáðàáſſòàåò åâſſ ſſèëëèſſ ſäſſſíàſðàâëåſſſé ôóſêöèſåſ è ſſſððàſſèò ðåçóëüſàòſ. Åſëè êàæäûé ſàðſſëü ſſſòſſèò èç âſſüſſ áàéſ, ðàçſåðſ ſſëó÷èâøåſſſÿ ôàéëà íå ſðåâûſſèò 8 Ìáàéſ, è ýòſò ôàéë ſſæåò áſòſ ðàçſåſſåſ âſåſſ íà íåſſêſëſüſêèſ íà äèſſêâòàſ. Òåſſåðſ Ìýëſſðè äſáſûâàåò øèôðſâàſſûé ôàéë ſàðſſëåſ. Sſ ſſðàſſèâàåò ýòſò ôàéë ſſ ſâſèſ ôàéëſſ ſſ øèôðſâàſſûõ âſçſſſæſûõ ſàðſſëåſ è èſåò ſſſâſàäåſèÿ.

Ýòſ **âſſêðûòèå ſ ſſſſüþ ſëſâàðÿ** ſæåò áſòſ óáèâèòåëüſſſ óſſſåøſûſ (ſſ. ðàçäåë 8.1). "**Ñſëü**" - ýòſ ſſſſſá çàòðóäſèòſ åâſ. "Ñſëü" ſðåäſſòàâëÿåò ſſâſé ſëó÷àéſóþ ſòðſêó, äſáàâëÿåſóþ ê ſàðſſëÿſ ſåðàſ ſâðàáſòêſé èò ſäſſſíàſðàâëåſſſé ôóſêöèåſ. Çàòåſ â áàçå äàſſûõ ãëàâſſãſ êſſ ſüþòåðà ſſõðàſÿþſÿ è çſà÷åſèå "ſſſëè", è ðåçóëüòàò ſäſſſíàſðàâëåſſſé ôóſêöèè. Èſſſſëüçſâàſèå äſñòàòſ÷ſſ áſëüøſãſ ÷ëſëà âſçſſæſûõ çſà÷åſèé "ſſſëè" ſðâêòè÷åſñê óſòðàſÿåò âſçſſæſſſòü âſſêðûòèÿ ſ ſſſſüþ ſëſâàðÿ, òàê êàê Ìſëëſðè ſðëäåòſÿ âû÷ëſëÿòü çſà÷åſèå ſäſſſíàſðàâëåſſſé õýø-ôóſêöèè äëÿ êàæäſãſ âſçſſæſſſãſ çſà÷åſèÿ "ſſſëè". Ýòſ ſðôſſòåſøèſ ſðèſåð èſſſëüçſâàſèå âåêòſðà èſèöèàëèçàöèè (ſſ. ðàçäåë 9.3).

Èäåÿ ſſſòſèò â òſſ, ſòſáû çàſòàâèòü Ìýëſſðè âûſſſëſèòü ſðſáſſâſèå øèôðſâàſèå êàæäſãſ ſàðſſëÿ èç åãſ ſëſâàðÿ ſðè êàæäſé ſſſſûôêå óſſàòü ſ÷å-òſ ſ÷áſé ſàðſſëü âſåſòſ ſàſſſðàçſâſé ſáðàáſòêè âſåõ âſçſſæſûõ ſàðſſëåſ.

Äëÿ ýòſãſ ſóæſſ ſſſãſ "ſſſëè". Áſëüøèſſòâſ UNIX-ſèſòåſ èſſſſëüçóþò äëÿ "ſſſëè" 12 áèò. Íåſſſòðÿ ſà ýòſ Äýſèåë Êëÿéſ (Daniel Klein) ſàſèſàë ſſðſãðàſ ſó ðàçãàäûâàſèÿ ſàðſſëåſ, êſòſðàÿ â ſåêſòſðûõ ſèſſòåſſà çà ſåäåë÷àſòſ âſêðûâàëà 40 ſſðſòåſòſâ ſàðſſëåſ [847,848] (ſſ. ðàçäåë 8.1). Äýâèä Ôåëüſàéåð (David Feldmeier) è Ôèëëſſ Êàſ (Philip Karn) ſſſòàâëëè ſſſèſſê èç 732000 ſàèáſëåå ÷àſòſ èſſſſëüçóåſûõ ſàðſſëåſ, ſðèſſåëſſſêà ê êàæäſ ſó èç ſſò 4096 âſçſſæſûõ çſà÷åſèé "ſſſëè". Sſ ſò ſòåſêàſ 30 ſſðſòåſòſâ ſàðſſëåſ ſà ëþáſſ ãëàâſſſ êſſſſüþòåðå ſſãſòó áûòſ âçëſſàſûſ ſ ſſſſüþſ ýòſãſ ſſſêâſ [561].

"Ñſëü" íå ÿâëÿåòſÿ ſàſàöåſé, óâåëè÷åſſå ÷èſëà áèò "ſſſëè" íå ðåøèò âſſåõ ſſðſáëſ. "Ñſëü" ſðåäſſðàſÿåò

òîëüêî îò ñàìûõ îáû÷íûõ âñêðûòèé ôàéëà ïàðîëåé ñ èñïîëüçîâàíèåì ñëîâàðÿ, à íå îò ñîãëàñîâàííîé àòàêå îãíîãî ïàðîëÿ. Îíà çàùèùàåò ëþäåé, èñïîëüçóþ ùèõ îäèí è òîò æå ïàðîëü íà ðàçëè÷íûõ ìàøèíàõ, íî íå äåëàåò ëó÷øå ïëîõî âûáðàííûé ïàðîëü.

SKEY

SKEY - ýòî ïðîãðàììà óäîñòîâåðåíèÿ ïîäëèííîñòè, îáåñïå÷èâàþùàÿ áåçîïàñíîñòü ñ ïîìîùüþ îäíîðàçîâûõ ïàðîëåé. Ýòî ëåãêî îáúÿñíèòü.

Ðåãèñòðèðóÿñü â ñèñòåìå, Àëèñà çàäàåò ñëó÷àéíîå ÷èñëî, *R*. Êîìïüþòåð âû÷èñëÿåò *f(R), f(f(R)), f(f(f(R)))*, è òàê äàëåå, îêîëî ñîòíè ðàç. Îáû÷íî ýòà çíà÷åíèÿ êàê x_1, x_2, x_3, ..., x_{100}. Êîìïüþòåð ïå÷àòàåò ñïèñîê ýòèõ ÷èñåë, è Àëèñà ïðÿ÷åò åãî â áåçîïàñíîì ìåñòî. Êîìïüþòåð òàêæå îòêðûâàåò òåêóùóþ ïîäêëþ÷åíèÿ ê ñèñòåìå â ñîîòâåòñòâèè Àëèñå ÷èñëî x_{101}.

Ïîäêëþ÷àÿñü âïåðâûå, Àëèñà ââîäèò ñâîå èìÿ è x_{100}. Êîìïüþòåð ðàññ÷èòûâàåò $f(x_{100})$ è ñðàâíèâàåò åãî ñ x_{101}, åñëè çíà÷åíèÿ ñîâïàäàþò, ïðåäà Àëèñû ïîäòâåðæäàþòñÿ. Çàòåì êîìïüþòåð çàìåíÿåò â áàçå äàííûõ x_{101} íà x_{100}. Àëèñà âû÷åðêèâàåò x_{100} èç ñâîåãî ñïèñêà.

Àëèñà, ïðè êàæäîì ïîäêëþ÷åíèè ê ñèñòåìå, ââîäèò ïîñëåäíåå íåâû÷åðêíóòîå ÷èñëî èç ñâîåãî ñïèñêà: x_i. Êîìïüþòåð ðàññ÷èòûâàåò $f(x_i)$ è ñðàâíèâàåò åãî ñ x_{i+1}, õðàíèâøåìñÿ â áàçå äàííûõ. Òàê êàê êàæäûé íîâûé èñïîëüçóåìûé îòëè÷íûé îò ðàç, Åâà íå ñìîæåò äîáûòü íèêàêîé ïîëåçíîé èíôîðìàöèè. Àíàëîãè÷íî, áàçà äàííûõ áåñïîëåçíà è äëÿ âçëîìùèêà. Êîíå÷íî æå, êàê òîëüêî ñïèñîê Àëèñû èñ÷åðïàåòñÿ åé ïðèäåòñÿ ïåðåõîäèòü â ñèñòåìå.

Óäîñòîâåðåíèå ïîäëèííîñòè ñ ïîìîùüþ êðèïòîãðàôè÷åñêîé ôóíêöèè

Äàæå ñ èñïîëüçîâàíèåì "îïëè" ó ïåðâîãî ïðîòîêîëà åñòü ñåðüåçíûå ïðîáëåìû ñ áåçîïàñíîñòüþ. Êîãäà Àëèñà ïîñûëàåò ñâîé ïàðîëü ãëàâíîìó êîìïüþòåðó, ëþáîé, ó êîãî åñòü äîñòóï ïóòè ïåðåäà÷è åå äàííûõ, ìîæåò ïðî÷åñòü ïàðîëü. Îíà ìîæåò ïîëó÷èòü äîñòóï ê ñâîåìó ãëàâíîìó êîìïüþòåðó ïîñðåäñòâîì çàïóùåííîãî ïóòè ïåðåäà÷è èíôîðìàöèè, ïðîëîæèâ åãî ÷åðåç ðàíåå óñòàíîâëåííûé êîíêóðåíòîâ, òðè äðóãèõ ñòàíöèè è äâà ïåðåâîâûõ óçëîâðñïèòåòà. Ââà ìîæåò íàõîäèòüñÿ â ëþáîé èç ýòèõ òî÷åê, ïîäñëóøèâàÿ ïåðåäàâàåìóþ Àëèñîé ïîñëåäîâàòåëüíîñòü. Åñëè ó Ââû åñòü äîñòóï ê îïåðàòèâíîé ïàìÿòè ãëàâíîãî êîìïüþòåðà, îíà ñìîæåò ïîäìîòðåòü ïàðîëü äî òîãî, êàê ãëàâíûé êîìïüþòåð ñìîæåò åãî õýøèðîâàòü.

Êðèòîãðàôèÿ ñ òóðíèðíûìè êëþ÷àìè ìîæåò ðåøèòü ýòó ïðîáëåìó. Ãëàâíûé êîìïüþòåð õðàíèò ôàéë òóðíèðíûõ êëþ÷åé âñåõ ïîëüçîâàòåëåé, à âñå ïîëüçîâàòåëè õðàíÿò ñâîè çàêðûòûå êëþ÷è. Âîò êàê âûãëÿäèò óïðîùåííàÿ ïîïûòêà îðãàíèçîâàòü ïðîòîêîë ïîäêëþ÷åíèÿ:

(1) Ãëàâíûé êîìïüþòåð ïîñûëàåò Àëèñå ñëó÷àéíóþ ñòðîêó.

(2) Àëèñà øèôðóåò ýòó ñòðîêó ñâîèì çàêðûòûì êëþ÷îì è ïîñûëàåò åå îáðàòíî ãëàâíîìó êîìïüþòåðó âìåñòå ñî ñâîèì èìåíåì.

(3) Ãëàâíûé êîìïüþòåð íàõîäèò â áàçå äàííûõ îòêðûòûé êëþ÷ Àëèñû è äåøèôðóåò ñîîáùåíèå, èñïîëüçóÿ ýòîò îòêðûòûé êëþ÷.

(4) Åñëè îòðàâëåííàÿ ñíà÷àëà è ðàñøèôðîâàííàÿ ñòðîêè ñîâïàäàþò, ãëàâíûé êîìïüþòåð ïðåäïîëàãàåò Àëèñà äîñòóï ê ñèñòåìå

Íèêòî äóãîé íå ìîæåò âîñïîëüçîâàòüñÿ çàêðûòûì êëþ÷îì Àëèñû, ñëåäîâàòåëüíî íèêòî íå ñìîæåò âûäàòü ñåáÿ çà íåå. ×òî áîëåå âàæíî, Àëèñà íèêîãäà íå ïîñûëàåò íà êîìïüþòåð ñâîé çàêðûòûé êëþ÷. Ââà, ïîäñëóøèâàÿ âçàèìîäåéſòâèå, íå ïîëó÷èò íèêàêèõ ñâåäåíèé, êîòîðûå ïîçâîëèëè áû åé âû÷èñëèòü çàêðûòûé êëþ÷ Àëèñû è âûäàòü ñåáÿ çà íåå.

Çàêðûòûé êëþ÷ äîëæåí áûòü äîñòàòî÷íî äëèííûì è íå äîëæåí áûòü ìíåìîíè÷åñêè îáîçðèìûì. Î í áóäåò àâòîìàòè÷åñêè îáíîâëÿòüñÿ ïðîãðàììíûì îáåñïå÷åíèåì "óìíîãî" òðåíèðîâêà, êîòîðîìó Àëèñà äîâåðÿåò, íî íå äëàíûé êîìïüþòåð, íè ëèíèè ñâÿçè íå îáÿçàíû áûòü áåçîïàñíûì.

Ãëóïî øèôðîâàòü ïðîèçâîëüíûå ñòðîêè - íåòïëûé ïîñëàííûå ïîäîçðèòåëüíûì àòòðîâ, íî è âîîáùå ëþáûå. Èíà÷å ìîæåò áûòü èñïîëüçîâàíî ñðåäſòâî, íî íå äëàíûé êîìïüþòåð, íè ëèíèè ñâÿçè íå îáÿçàíû áûòü áåçîïàñíûì.

Ãëóïî øèôðîâàòü ïðîèçâîëüíûå ñòðîêè - íåòïëûé ïîñëàííûå ïîäîçðèòåëüíûì àòòðîâ, íî è âîîáùå ëþáûå. Èíà÷å ìîæåò áûòü èñïîëüçîâàíî ñðåäſòâî, íî íå äëàíûé êîìïüþòåð, íè ëèíèè ñâÿçè íå îáÿçàíû áûòü áåçîïàñíûì.

(1) Àëèñà âûïîëíÿåò âû÷èñëåíèå, îñíîâàííîå íà íåêîòîðûõ ñëó÷àéíûõ ÷èñëàõ è ñâîì çàêðûòîì êëþ÷å, è ïîñûëàåò ðåçóëüòàò íà ãëàâíûé êîìïüþòåð.

(2) Ãëàâíûé êîìïüþòåð ïîñûëàåò äðóãîå ñëó÷àéíîå ÷èñëî.

(3) Àëèñà âûïîëíÿåò âû÷èñëåíèå, îñíîâàííîå íà ñëó÷àéíûõ ÷èñëàõ (êàê ñîçäàííì åþ, òàê è ïîëó÷åííì îò ãëàâíîãî êîìïüþòåðà) è ñâîì çàêðûòûì êëþ÷å, è ïîñûëàåò ðåçóëüòàò íà ãëàâíûé êîìïüþòåð.

(4) Ãëàâíûé êîìïüþòåð âûïîëíÿåò íåêîòîðîå âû÷èñëåíèå äëÿ ðàçëè÷íûõ ÷èñåë, ïîëó÷åííûõ îò Àëèñû, è åå îòêðûòîãî êëþ÷à, ïðîâåðÿÿ, ÷òî åé èçâåñòíî åå çàêðûòîé êëþ÷.

(5) Åñëè ïðîâåðêà çàâåðøàþùèõ óñïåøíî, ëè÷íîñòü Àëèñû ïîäòâåðæäàåòñÿ.

Åñëè Àëèñû äîâåðÿåò ãëàâíîìó êîìïüþòåðó íå â áîëüøåé ñòåïåíè, ÷åì òîò äîâåðÿåò Àëèñå, òî îíà äîëæíà ïîðåêîìåíäîâàòü ïîäòâåðæäåíèÿ ïîäëèííîñòè ãëàâíîãî êîìïüþòåðà àíàëîã÷íûì îáðàçîì.

Ýòàï (1) ìîæåò ïîêàçàòüñÿ íåóæíûì è çàïóòàííûì, íî îí íåîáõîäèì äëÿ çàùèòû ïðîòîêîëà îò âñêðûòèÿ. Ðàçëè÷íûå ïðîòîêîëû è àëãîðèòìû ïîäòâåðæäåíèÿ ïîäëèííîñòè ìàòåìàòè÷åñêè ïîäîáíû îïèñûâàþòñÿ â ðàçäåëàõ 21.1 è 21.2. Ñì. òàêæå [935].

Îáùàÿ óäîñòîâåðåíèå ïîäëèííîñòè ñèñòåìíîãî ïðîòîêîëà "äðàêîí çàùèòû"

Ïóñòü ââà ïîëüçîâàòåëÿ, Àëèñà è Áîá, õîòÿò ïðîâåðèòü ïîäëèííîñòü äðóã äðóãà. Ó êàæäîãî èç íèõ åñòü ïàðîëü, èçâåñòíûé äðóãîìó ïîëüçîâàòåëþ: P_A ó Àëèñû è P_B ó Áîáà. Âîò êàê âûãëÿäèò ïðîòîêîë, êîòîðûé *íå* áóäåò ðàáîòàòü:

(1) Àëèñà è Áîá îáìåíèâàþòñÿ îòêðûòûìè êëþ÷àìè.

(2) Àëèñà øèôðóåò P_A îòêðûòûì êëþ÷îì Áîáà è ïîñûëàåò åãî åìó.

(3) Áîá øèôðóåò P_B îòêðûòûì êëþ÷îì Àëèñû è ïîñûëàåò åãî åé.

(4) Àëèñà ðàñøèôðîâûâàåò ïîëó÷åííîå íà ýòàïå (3) è ïîäòâåðæäàåò ïðàâèëüíîñòü ïàðîëÿ.

(5) Áîá ðàñøèôðîâûâàåò ïîëó÷åííîå íà ýòàïå (2) è ïîäòâåðæäàåò ïðàâèëüíîñòü ïàðîëÿ.

Ìýëîðè ìîæåò ïðåäïîëîæèòü óñïåøíîå âñêðûòèå "÷åëîâåê-â-ñåðåäèíå" (ñì. ðàçäåë 3.1):

(1) Àëèñà è Áîá îáìåíèâàþòñÿ îòêðûòûìè êëþ÷àìè. Ìýëîðè ïåðåõâàòûâàåò îáà ñîîáùåíèÿ, è ïîñûëàåò îáîèì êîððåñïîíäåíòàì ñâîé ñîáñòâåííûé îòêðûòûé êëþ÷, ïîäìåíèâ èì èõ êëþ÷è.

(2) Àëèñà øèôðóåò P_A îòêðûòûì êëþ÷îì "Áîáà" è ïîñûëàåò åãî åìó. Ìýëîðè ïåðåõâàòûâàåò ñîîáùåíèå, ðàñøèôðîâûâàåò P_A ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à, ñíîâà øèôðóåò P_A îòêðûòûì êëþ÷îì Áîáà è ïîñûëàåò åãî åìó.

(3) Áîá øèôðóåò P_B îòêðûòûì êëþ÷îì "Àëèñû" è ïîñûëàåò åãî åé. Ìýëîðè ïåðåõâàòûâàåò ñîîáùåíèå, ðàñøèôðîâûâàåò P_B ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à, ñíîâà øèôðóåò P_B îòêðûòûì êëþ÷îì Àëèñû è ïîñûëàåò åãî åé.

(4) Àëèñà ðàñøèôðîâûâàåò P_B è ïîäòâåðæäàåò åãî ïðàâèëüíîñòü.

(5) Áîá ðàñøèôðîâûâàåò P_A è ïîäòâåðæäàåò åãî ïðàâèëüíîñòü.

Äëÿ Àëèñû è Áîáà íè÷åãî íå èçìåíèëîñü. Îäíàêî, Ìýëîðè çíàåò è P_A, è P_B. Äîíàëüä Äýâèñ (Donald Davies) è Âèëüÿì Ïðàéñ (William Price) îïèñûâàþò, êàê ïðîòîêîë "äâóæàñü-çà-ðóêè" (ñì. ðàçäåë 3.1) ïðîòèâîäåéñòâóåò òàêîìó âñêðûòèþ [435]. Ñòèâ Áåëëîâèí (Steve Bellovin) è Ìàéêë Ìåððèòò (Michael Merritt) ðàññìàòðèâàþò ñïîñîáû âñêðûòèÿ ýòîãî ïðîòîêîëà â [110]. Åñëè Àëèñà - ýòî ïîëüçîâàòåëü, à Áîá - õîñò-êîìïüþòåð, Ìýëîðè ìîæåò ïðåäïîëîæèòü áîòíåò, âûïîëíèò ïððûâ ýòàïà ïðîòîêîëà ñ Àëèñîé è ðàçîðâàòü ñåàíñ. Ñèìóëèðîâàíèå øóìà íà ëèíèèëëè ñåòåâîãî îòêàçà ïîòðåáóåò îò Ìýëîðè íàñòîÿùåãî àðòèñòèçìà, íî â ðåçóëüòàòå Ìýëîðè ïîëó÷èò ïàðîëü Àëèñû. Çàòåì îí ñìîæåò ñîãëàñîâûñ ñ Áîáîì è çââðøèòü ïðîòîêîë, ïîëó÷àÿ è ïàðîëü Áîáà.

Ïðîòîêîë ìîæíî èçìåíèòü òàê, ÷òîáû Áîá ïðåäâàðèòåëüíî ñîîáùèë Àëèñå â ïðåäïîëîæåíèè, ÷òî ïàðîëü ïîëüçîâàòåëÿ áîëåå âåæåí ÷åì ïàðîëü ãëàâíîãî êîìïüþòåðà. Ýòî ïðèâåäåò ê óñëîæíåíèþ ñïîñîáà âñêðûòèÿ, òàêæå îïèñàííîãî â [110].

SKID

SKID2 è SKID3 - ýòî ñèìåòðè÷íûå êðèïòîãðàôè÷åñêèå ïðîòîêîëû èäåíòèôèêàöèè, ðàçðàáîòàííûå äëÿ ïðîåêòà RACE RIPE [1305] (ñì. ðàçäåë 25.7). Îíè èñïîëüçóþò MAC (ñì. ðàçäåë 2.4) äëÿ îáåñïå÷åíèÿ áåçîïàñíîñòè è ïðåäïîëàãàþò, ÷òî Àëèñà è Áîá èñïîëüçóþò îáùèé ñåêðåòíûé êëþ÷, *K*. SKID2 ïîçâîëÿåò Áîáó äîêàçàòü ñâîþ ïîäëèííîñòü Àëèñå. Âîò ýòîò ïðîòîêîë:

(1) Àëèñà âûáèðàåò ñëó÷àéíîå ÷èñëî, R_A. (Äîêóìåíòàöèÿ RIPE îïðåäåëÿåòñÿ 64-áèòîâîå ÷èñëî). Îíà ïîñûëàåò ýòî ÷èñëî Áîáó.

(2) Áîá âûáèðàåò ñëó÷àéíîå ÷èñëî, R_B. (Äîêóìåíòàöèÿ RIPE îïðåäåëÿåòñÿ 64-áèòîâîå ÷èñëî). Îí ïîñûëàåò Àëèñå.

R_B, $H_K(R_A, R_B, B)$

H_K - ýòî MAC. (Â äîêóìåíòàõ RIPE ïðåäëàãàåòñÿ ôóíêöèÿ RIPE-MAC, ñì. ðàçäåë 18.4.) *B* - ýòî èìÿ Áîáà.

(3) Àëèñà ðàññ÷èòûâàåò $H_K(R_A, R_B, B)$ è ñðàâíèâàåò ðåçóëüòàò ñî çíà÷åíèåì, ïîëó÷åííûì îò Áîáà. Åñëè ðåçóëüòàòû ñîâïàäàþò, Àëèñà óáåæäàåòñÿ â òîì, ÷òî îíà ñîåäèíèëàñü èìåííî ñ Áîáîì.

SKID3 îáåñïå÷èâàåò ñîâìåñòíóþ ïðîâåðêó ïîäëèííîñòè Àëèñîé è Áîáîì. Ýòàïû (1) - (3) ñîâïàäàþò ñ ïðîòîêîëîì SKID2, à çàòåì âûïîëíÿþòñÿ ñëåäóþùèå äåéñòâèÿ:

(4) Àëèñà ïîñûëàåò Áîáó:

$H_K(R_B, A)$

A - ýòî èìÿ Àëèñû.

(5) Áîá ðàññ÷èòûâàåò $H_K(R_B, A)$ è ñðàâíèâàåò ðåçóëüòàò ñî çíà÷åíèåì, ïîëó÷åííûì îò Àëèñû. Åñëè ðåçóëüòàòû ñîâïàäàþò, Áîá óáåæäàåòñÿ â òîì, ÷òî îí ñîåäèíèëñÿ èìåííî ñ Àëèñîé.

Ýòîò ïðîòîêîë íåóñòîé÷èâ ê âñêðûòèþ "÷åëîâåê-â-ñåðåäèíå". Â îáùåì ñëó÷àå, âñêðûòèå "÷åëîâåê-â-ñåðåäèíå" ìîæåò óãðîæàòü ëþáîìó ïðîòîêîëó, â êîòîðûé íå âõîäèò êàêîé-íèáóäü ñåêðåò.

Óäîñòîâåðåíèå ïîäëèííîñòè ñîîáùåíèé

Êîãäà Áîá ïîëó÷àåò ñîîáùåíèå îò Àëèñû, êàê åìó óçíàòü, ÷òî ýòî ñîîáùåíèå ïîäëèííî? Åñëè Àëèñà ïîäïèñàëà ñâîå ñîîáùåíèå, òî âñå ïðîñòî. Öèôðîâàÿ ïîäïèñü Àëèñû äîñòàòî÷íà, ÷òîáû ïîäòâåðäèòü êîìó óãîäíî ïîäëèííîñòü åå ñîîáùåíèÿ.

Íåêîòîðóþ ïðîâåðêó ïîäëèííîñòè ïðåäîñòàâëÿþò è ñèììåòðè÷íûå àëãîðèòìû. Êîãäà Áîá ïîëó÷àåò ñîîáùåíèå îò Àëèñû, øèôðîâàííîå èõ îáùèì êëþ÷îì, îí çíàåò, ÷òî ýòî ñîîáùåíèå îò Àëèñû. Íèêòî áîëüøå íå çíàåò èõ êëþ÷à. Îäíàêî, ó Áîáà íåò âîçìîæíîñòè óáåäèòü â ýòîì êîãî-òî åùå. Áîá íå ìîæåò ïîêàçàòü ñîîáùåíèå Òðåíòó è óáåäèòü åãî, ÷òî îíî îòïðàâëåíî Àëèñîé. Òðåíò ìîæåò ñäåëàòü âûâîä, ÷òî ñîîáùåíèå îòïðàâëåíî èëè Àëèñîé, èëè Áîáîì (òàê êàê èõ ñåêðåòíûé êëþ÷ íèêîìó áîëüøå íå ïðèíàäëåæèò), íî ó íåãî íåò ñïîñîáà îïðåäåëèòü, êòî æå êîíêðåòíî àâòîð ñîîáùåíèÿ.

Åñëè ñîîáùåíèå íå øèôðîâàíî, Àëèñà ìîæåò òàêæå èñïîëüçîâàòü MAC. Ýòî òàêæå óáåäèò Áîáà â ïîäëèííîñòè ñîîáùåíèÿ, íî âîçíèêíóò òå æå ïðîáëåìû, ÷òî è äëÿ ðåøåíèÿ ñèììåòðè÷íîé êðèïòîãðàôèè.

3.3 Óäîñòîâåðåíèå ïîäëèííîñòè è îáìåí êëþ÷àìè

Ýòè ïðîòîêîëû îáúåäèíÿþò óäîñòîâåðåíèå ïîäëèííîñòè è îáìåí êëþ÷àìè äëÿ ðåøåíèÿ îñíîâíîé êîìïüþòåðíîé ïðîáëåìû: Àëèñà è Áîá õîòÿò áåçîïàñíî îáìåíèâàòüñÿ ñîîáùåíèÿìè, íàõîäÿñü íà ðàçëè÷íûõ êîíöàõ ñåòè. Êàê ìîãóò Àëèñà è Áîá îáìåíÿòüñÿ ñåêðåòíûì êëþ÷îì, ïðè ýòîì ñîõðàíÿÿ óâåðåííîñòü, ÷òî îíè îáìåíèâàþòñÿ ñîîáùåíèÿìè äðóã ñ äðóãîì, à íå ñ Ìýëëîðè? Â áîëüøèíñòâå ïðîòîêîëîâ ïðåäïîëàãàåòñÿ, ÷òî êàæäîìó ïîëüçîâàòåëþ Òðåíò âûäåëÿåò îòäåëüíûé ñåêðåòíûé êëþ÷, è ïåðåä íà÷àëîì ðàáîòû ïðîòîêîëà âñå êëþ÷è óæå íàõîäÿòñÿ ó ïîëüçîâàòåëåé. Ñèìâîëû, èñïîëüçóåìûå â ýòèõ ïðîòîêîëàõ, ñâåäåíû â 2-é.

Òàáë. 3-1.
Ñèìâîëû, èñïîëüçóåìûå â ïðîòîêîëàõ óäîñòîâåðåíèÿ ïîäëèííîñòè è îáìåíà êëþ÷àìè

A	Èìÿ Àëèñû
B	Èìÿ Áîáà
E_A	Øèôðîâàíèå êëþ÷îì, âûäåëåííûì Òðåíòîì Àëèñå
E_B	Øèôðîâàíèå êëþ÷îì, âûäåëåííûì Òðåíòîì Áîáó
I	Ïîðÿäêîâûé íîìåð
K	Ñëó÷àéíîå ñåàíñîâîå ÷èñëî
L	Âðåìÿ æèçíè
T_A, T_B	Ìåòêè âðåìåíè
R_A, R_B	Ñëó÷àéíûå ÷èñëà, âûáðàííûå Àëèñîé è Áîáîì, ñîîòâåòñòâåííî

Ëÿãóøêà ñ øèðîêèì ðòîì

Ïðîòîêîë "Ëÿãóøêà ñ øèðîêèì ðòîì" (Wide-Mouth Frog) [283,284], âîçìîæíî, ÿâëÿåòñÿ ïðîñòåéøèì ñèììåòðè÷íûì ïðîòîêîëîì óïðàâëåíèÿ êëþ÷àìè, â êîòîðîì èñïîëüçóåòñÿ çàñëóæèâàþùèé äîâåðèÿ ñåðâåð. Àëèñà è Áîá äåëÿò ñâîé ñåêðåòíûé êëþ÷ ñ Òðåíòîì. Ýòè êëþ÷è èñïîëüçóþòñÿ òîëüêî äëÿ ðàñïðåäåëåíèÿ êëþ÷åé, à íå äëÿ øèôðîâàíèÿ ïîëüçîâàòåëüñêèõ ñîîáùåíèé. Âîò êàê, èñïîëüçóÿ äâà ñîîáùåíèÿ, Àëèñà ïåðåäàåò Áîáó ñåàíñîâûé

êëþ÷:

(1) Àëèñà îáúåäèíÿåò ìåòêó âðåìåíè, èìÿ Áîáà è ñëó÷àéíûé ñåàíñîâûé êëþ÷, çàòåì øèôðóåò ñîçäàííîå ñîîáùåíèå îáùèì ñ Òðåíòîì êëþ÷îì è ïîñûëàåò åãî Òðåíòó âìåñòå ñî ñâîèì èìåíåì.

A, $E_A(T_A, B, K)$

(2) Òðåíò ðàñøèôðîâûâàåò ñîîáùåíèå îò Àëèñû. Çàòåì îí äîáàâëÿåò íîâóþ ìåòêó âðåìåíè, èìÿ Àëèñû è ñëó÷àéíûé ñåàíñîâûé êëþ÷, øèôðóåò ïîëó÷åííîå ñîîáùåíèå îáùèì ñ Áîáîì êëþ÷îì. Òðåíò ïîñûëàåò Áîáó:

$E_B(T_B, B, K)$

Íàèáîëüøèì äîñòóïåíèì, ñäåëàííûì â ýòîì ïðîòîêîëå, ÿâëÿåòñÿ òî, ÷òî Àëèñà îáëàäàåò äîñòàòî÷íîé êîìïåòåíöèåé äëÿ ãåíåðàöèè õîðîøèõ ñåàíñîâûõ êëþ÷åé. Âñïîìíèòå, ÷òî ñëó÷àéíûå ÷èñëà ãåíåðèðîâàòü ñîâñåì íå ïðîñòî, äëÿ ýòîãî ìîæåò ïîòðåáîâàòüñÿ êòî-íèáóäü ïîíàäåæíåå Àëèñû.

Yahalom

Â ýòîì ïðîòîêîëå Àëèñû è Áîá äåëÿò ñ Òðåíòîì ñåêðåòíûé êëþ÷ [283,284].

(1) Àëèñà îáúåäèíÿåò ñâîå èìÿ è ñëó÷àéíîå ÷èñëî, è îòïðàâëÿåò ñîçäàííîå ñîîáùåíèå Áîáó.

A, R_A

(2) Áîá îáúåäèíÿåò èìÿ Àëèñû, åå ñëó÷àéíîå ÷èñëî, ñâîå ñëó÷àéíîå ÷èñëî, øèôðóåò ñîçäàííîå ñîîáùåíèå îáùèì ñ Òðåíòîì êëþ÷îì è ïîñûëàåò åãî Òðåíòó, äîáàâëÿÿ ñâîå èìÿ:

B, $E_B(A, R_A, R_B)$

(3) Òðåíò ñîçäàåò äâà ñîîáùåíèÿ. Ïåðâîå âêëþ÷àåò èìÿ Áîáà, ñëó÷àéíîé ñåàíñîâûé êëþ÷, ñëó÷àéíûå ÷èñëà Áîáà è Àëèñû è øèôðóåòñÿ êëþ÷îì, îáùèì äëÿ Òðåíòà è Áîáà. Âòîðîå ñîñòîèò èç èìåíè Àëèñû, ñëó÷àéíîãî ñåàíñîâîãî êëþ÷à è øèôðóåòñÿ êëþ÷îì, îáùèì äëÿ Òðåíòà è Áîáà. Òðåíò ïîñûëàåò îáà ñîîáùåíèÿ Àëèñå:

$E_A(B, K, R_A, R_B)$, $E_B(A, K)$

(4) Àëèñà ðàñøèôðîâûâàåò ïåðâîå ñîîáùåíèå, èçâëåêàåò *K* è óáåæäàåòñÿ, ÷òî R_A ñîâïàäàåò ñî çíà÷åíèåì, îòïðàâëåííûì íà ýòàïå (1). Àëèñà ïîñûëàåò Áîáó äâà ñîîáùåíèÿ. Îäíîì ÿâëÿåòñÿ ñîîáùåíèå Òðåíòà, çàøèôðîâàííîå êëþ÷îì Áîáà. Âòîðîå - ýòî R_B, çàøèôðîâàííîå ñåàíñîâûì êëþ÷îì.

$E_B(A, K)$, $E_K(R_B)$,

(5) Áîá ðàñøèôðîâûâàåò ïåðâîå ñîîáùåíèå, èçâëåêàåò *K* è óáåæäàåòñÿ, ÷òî R_B ñîâïàäàåò ñ òîïðàâëåííûì íà ýòàïå (2).

Â ðåçóëüòàòå Àëèñà è Áîá óáåæäåíû, ÷òî îíè îáùàþòñÿ èìåííî äóãà ñ äóãîì, à íå ñ òðåòüåé ñòîðîíîé. Íîâîââåäåíèå ñîñòîèò â òîì, ÷òî èìåííî Áîá ïðåäûùàåòñÿ ê Òðåíòó, êîòîðûé òîëüêî ïîñûëàåò îäíî ñîîáùåíèå Àëèñå.

Needham-Schroeder

Â ýòîì ïðîòîêîëå, èçîáðåòåííîì Ðîäæåðîì Íåääõýìîì (Roger Needham) è Ìàéêëîì Øðåäåðîì (Michael Schroeder) [1159], òàêæå èñïîëüçóþòñÿ ñèìåòðè÷íàÿ êðèïòîãðàôèÿ è Òðåíò.

(1) Àëèñà ïîñûëàåò Òðåíòó ñîîáùåíèå, ñîäåðæàùåå åå èìÿ, èìÿ Áîáà è ñëó÷àéíîå ÷èñëî.

A, B, R_A

(2) Òðåíò ãåíåðèðóåò ñëó÷àéíûé ñåàíñîâûé êëþ÷. Îí øèôðóåò ñîîáùåíèå, ñîäåðæàùåå ñëó÷àéíûé ñåàíñîâûé êëþ÷ è èìÿ Àëèñû, ñåêðåòíûì êëþ÷îì, îáùèì äëÿ íåãî è Áîáà. Çàòåì îí øèôðóåò ñëó÷àéíîå ÷èñëî Àëèñû, èìÿ Áîáà, êëþ÷, è øèôðîâàííîå ñîîáùåíèå ñåêðåòíûì êëþ÷îì, îáùèì äëÿ íåãî è Àëèñû. Íàêîíåö, îí îòïðàâëÿåò øèôðîâàííîå ñîîáùåíèå Àëèñå:

$E_A(R_A, B, K, E_B(K, A))$

(3) Àëèñà ðàñøèôðîâûâàåò ñîîáùåíèå è èçâëåêàåò *K*. Îíà óáåæäàåòñÿ, ÷òî R_A ñîâïàäàåò ñî çíà÷åíèåì, îòïðàâëåííûì Òðåíòó íà ýòàïå (1). Çàòåì îíà ïîñûëàåò Áîáó ñîîáùåíèå, çàøèôðîâàííîå Òðåíòîì êëþ÷îì Áîáà.

$E_B(K, A)$

(4) Áîá ðàñøèôðîâûâàåò ñîîáùåíèå è èçâëåêàåò *K*. Çàòåì îí ãåíåðèðóåò äóãîâå ñëó÷àéíîå ÷èñëî, R_B. Îí øèôðóåò ýòî ÷èñëî êëþ÷îì *K* è îòïðàâëÿåò åãî Àëèñå.

$E_K(R_B)$

(5) Àëèñà ðàñøèôðîâûâàåò ñîîáùåíèå ñ ïîìîùüþ êëþ÷à *K*. Îíà ñîçäàåò ÷èñëî R_B*-1* è øèôðóåò ýòî ÷èñëî êëþ÷îì *K*. Çàòåì îíà ïîñûëàåò ýòî ñîîáùåíèå îáðàòíî Áîáó.

$E_K(R_B$*-1)*

(6) Áîá ðàñøèôðîâûâàåò ñîîáùåíèå ñ ïîìîùüþ êëþ÷à *K* è ïðîâåðÿåò çíà÷åíèå R_B*-1*.

Âñÿ ýòà âîçíÿ ñ R_A, R_B, è R_B*-1* ñëóæèò äëÿ ïðåäîòâðàùåíèÿ **âñêðûòèÿ ñ ïîâòîðíîé ïåðåäà÷åé**. Ïðè òàêîì ñïîñîáå âñêðûòèÿ Ìýëëîðè ìîæåò çàïèñàòü ñòàðûå ñîáùåíèÿ è âïîñëåäñòâèè èñïîëüçîâàòü èõ ïðè ïîìîùè âçëîìàòü ïðîòîêîë. Ïðèñóòñòâèå R_A íà ýòàïå (2) óáåæäàåò Àëèñó, ÷òî ñîîáùåíèå Òðåíòà äîñòîâåðíî è íå ÿâëÿåòñÿ ïîâòîðíîé ïåðåäà÷åé îòêëèêà, èñïîëüçîâàííîãî ïðè îáìåíå èç ïðåäûäóùèõ ïðèìåíåíèé ïðîòîêîëà. Êîãäà Àëèñà óñïåøíî ðàñøèôðóåò R_B è ïåðåäàåò Áîáó R_B*-1* íà ýòàïå (5), Áîá óáåæäàåòñÿ, ÷òî ñîîáùåíèÿ Àëèñû íà ÿâëÿþòñÿ ïîâòîðíîé ïåðåäà÷åé ñîîáùåíèé, èñïîëüçîâàííûõ ïðè îáìåíå èç ïðåäûäóùèõ ïðèìåíåíèé ïðîòîêîëà.

Ãèáêîé ïðîðåãóëèðóåìîé ÿâëÿåòñÿ âàæíîñòü èñïîëüçîâàííûõ ñàíñîâûõ êëþ÷åé. Åñëè Ìýëëîðè ïîëó÷èò äîñòóï ê ñòàðîìó *K*, îí ñìîæåò ïðåäïðèíÿòü óñïåøíûå âñêðûòèå [461]. Åìó íóæíî òîëüêî çàïèñàòü ñîîáùåíèÿ Àëèñû Áîáó íà ýòàïå (3). Òîãäà, èìåÿ *K*, îí ìîæåò âûäàòü ñåáÿ çà Àëèñó:

(1) Ìýëëîðè ïîñûëàåò Áîáó ñëåäóþùåå ñîîáùåíèå:

$E_B(K, A)$

(2) Áîá èçâëåêàåò *K*, ãåíåðèðóåò R_B è îòïðàâëÿåò Àëèñå:

$E_K(R_B)$

(3) Ìýëëîðè ïðåðâàòûâàåò ñîîáùåíèå, ðàñøèôðîâûâàåò åãî ñ ïîìîùüþ êëþ÷à *K* è ïîñûëàåò Áîáó:

$E_K(R_B$*-1)*

(4) Áîá óáåæäàåòñÿ, ÷òî ñîîáùåíèå "Àëèñû" ñîñòîèò èç R_B*-1*.

Òåïåðü Ìýëëîðè óáåäèë Áîá, ÷òî îí è åñòü "Àëèñà". Áîëåå çàùèùåííûé ïðîòîêîë, èñïîëüçóþùèé ìåòêè âðåìåíè, ìîæåò ïðîòèâîñòîÿòü ýòîìó âñêðûòèþ [461,456]. Ìåòêè âðåìåíè äîáàâëÿþòñÿ ê ñîîáùåíèþ Òðåíòà íà ýòàïå (2) è øèôðóþòñÿ êëþ÷îì Áîáà: $E_B(K, A, T)$. Ìåòêè âðåìåíè òðåáóþò íàäåæíîé è òî÷íîé ñèñòåìû åäèíîãî âðåìåíè, ÷òî ñàìî ïî ñåáå íåòðèâèàëüíàÿ ïðîáëåìà.

Åñëè êëþ÷, îáùèé äëÿ Òðåíòà è Àëèñû áóäåò ñêîìïðîìåòðîâàí, ïîñëåäñòâèå áóäóò äðàìàòè÷íû. Ìýëëîðè ñìîæåò èñïîëüçîâàòü åãî, äëÿ ïîëó÷åíèÿ ñåàíñîâûõ êëþ÷åé äëÿ îáìåíà ñîîáùåíèÿìè ñ Áîáîì (èëè ñ êåì-íèáóäü åùå). Äàæå õóæå, Ìýëëîðè ïðîïîëæàòü ïîäìåíÿòü äàííûå ïîñëå çàìåíû êëþ÷à Àëèñû [90].

Íåâàõýì è Ððåääð ïûòàëèñü èñïðàâèòü ýòè ïðîáëåìû â ìîäèôèêàöèîííîé âåðñèè ñåòåãî ïðîòîêîëà [1160]. Èõ íîâûé ïðîòîêîë ïî ñóùåñòâó ñîâïàäàåò ñ ïðîòîêîëîì Îòóýÿ- Ðèñà (Otway-Rees), îïóáëèêîâàííîì â òîì æå âûïóñêå òîãî æå æóðíàëà.

Otway-Rees

Ýòîò ïðîòîêîë òàêæå èñïîëüçóåò ñèììåòðè÷íóþ êðèïòîãðàôèþ [1224].

(1) Àëèñà ñîçäàåò ñîîáùåíèå, ñîñòîÿùåå èç ïîðÿäêîâîãî íîìåðà, åå èìåíè, èìåíè Áîáà è ñëó÷àéíîãî ÷èñëà. Ñîîáùåíèå øèôðóåòñÿ êëþ÷îì, îáùèì äëÿ Àëèñû è Òðåíòà. Îíà ïîñûëàåò ýòî ñîîáùåíèå Áîáó âìåñòå ñ ïîðÿäêîâûì íîìåðîì, åå è åãî èìåíàìè:

$I, A, B, E_A(R_A, I, A, B)$

(2) Áîá ñîçäàåò ñîîáùåíèå, ñîñòîÿùåå èç íîâîãî ñëó÷àéíîãî ÷èñëà, ïîðÿäêîâîãî íîìåðà, èìåíè Àëèñû è èìåíè Áîáà. Ñîîáùåíèå øèôðóåòñÿ êëþ÷îì, îáùèì äëÿ Àëèñû è Áîáà. Îí ïîñûëàåò ýòî ñîîáùåíèå Òðåíòó âìåñòå øèôðîâàííûì ñîîáùåíèåì Àëèñû, ïîðÿäêîâûì íîìåðîì, åå è åãî èìåíàìè:

$I, A, B, E_A(R_A, I, A, B), E_B(R_B, I, A, B)$

(3) Òðåíò ãåíåðèðóåò ñëó÷àéíûé ñåàíñîâûé êëþ÷. Çàòåì îí ñîçäàåò äâà ñîîáùåíèÿ. Îäíî, ñîñòîÿùåå èç ñëó÷àéíîãî ÷èñëà Àëèñû è ñåàíñîâîãî êëþ÷à, øèôðóåòñÿ êëþ÷îì, îáùèì äëÿ íåãî è Áîáà. Äðóãîå, ñîñòîÿùåå èç ñëó÷àéíîãî ÷èñëà Áîáà è ñåàíñîâîãî êëþ÷à, øèôðóåòñÿ êëþ÷îì, îáùèì äëÿ íåãî è Áîáà. Îí îòïðàâëÿåò äâà ýòèõ ñîîáùåíèÿ âìåñòå ñ ïîðÿäêîâûì íîìåðîì Áîáó:

$I, E_A(R_A, K), E_B(R_B, K)$

(4) Áîá îòïðàâëÿåò Àëèñå ñîîáùåíèå, øèôðîâàííûå åå êëþ÷îì, è ïîðÿäêîâûé íîìåð:

$I, E_A(R_A, K)$

(5) Àëèñà ðàñøèôðîâûâàåò ñîîáùåíèå, ïîëó÷àÿ ñâîè êëþ÷ è ñëó÷àéíîå ÷èñëî. Àëèñà óáåæäàåòñÿ, ÷òî ïðè âûïîëíåíèè ïðîòîêîëà íîé íå èçìåíèëèñü Áîá îòðàâëÿåò Àëèñå ñîîáùåíèå, øèôðîâàííûå åå êëþ÷îì, è ïî-

ðÿäêîâûé íî ìåð.

Åñëè âñå ñëó÷àéíûå ÷èñëà ïðàâèëüíû, à ïîðÿäêîâûé íîìåð íå èçìåíèëñÿ ïðè âûïîëíåíèè ïðîòîêîëà, Àëèñà è Áîá óáåæäàþòñÿ â ïîäëèííîñòè äðóã äðóãà è ïîëó÷àþò ñåêðåòíûé êëþ÷ äëÿ îáìåíà ñîîáùåíèÿìè.

Kerberos

Kerberos - âàðèàíò ïðîòîêîëà Needham-Schroeder - ïîäðîáíî îáñóæäàåòñÿ â ðàçäåëå 24.5. Â áàçîâîì ïðîòîêîëå Kerberos Version 5 ó Àëèñû è Áîáà îáùèå êëþ÷è ñ Òðåíòîì. Àëèñà õî÷åò ãåíåðèðîâàòü ñåàíñîâûé êëþ÷ äëÿ ñåàíñà ñâÿçè ñ Áîáîì.

(1) Àëèñà ïîñûëàåò Òðåíòó ñîîáùåíèå ñî ñâîèì èìåíåì è èìåíåì Áîáà:

A, B

(2) Òðåíò ñîçäàåò ñîîáùåíèå, ñîñòîÿùåå èç ìåòêè âðåìåíè, âðåìÿ æèçíè, *L*, ñëó÷àéíîãî ñåàíñîâîãî êëþ÷à è èìåíè Àëèñû. Î í øèôðóåò ñîîáùåíèå êëþ÷îì, îáùèì äëÿ íåãî è Áîáà. Çàòåì îí îáúåäèíÿåò ìåòêó âðåìåíè, âðåìÿ æèçíè, ñåàíñîâûé êëþ÷, èìÿ Áîáà, è øèôðóåò ïîëó÷åííîå ñîîáùåíèå êëþ÷îì, îáùèì äëÿ íåãî è Àëèñû. Îáà øèôðîâàííûõ ñîîáùåíèÿ îí îòïðàâëÿåò Àëèñå.

$E_A(T, L, K, B), E_B(T, L, K, A)$

(3) Àëèñà ñîçäàåò ñîîáùåíèå, ñîñòîÿùåå èç åå èìåíè è ìåòêè âðåìåíè, øèôðóåò åãî êëþ÷îì *K* è îòïðàâëÿåò Áîáó. Àëèñà òàêæå ïîñûëàåò Áîáó ñîîáùåíèå îò Òðåíòà, øèôðîâàííîå êëþ÷îì Áîáà:

$E_A(A, T), E_B(T, L, K, A)$

(4) Áîá ñîçäàåò ñîîáùåíèå, ñîñòîÿùåå èç ìåòêè âðåìåíè ïëþñ åäèíèöà, øèôðóåò åãî êëþ÷îì *K* è îòïðàâëÿåò Àëèñå:

$E_K(T+1)$

Ýòî ïðîòîêîë ðàáîòàåò, íî òîëüêî åñëè ÷àñû êàæäîãî ïîëüçîâàòåëÿ ñèíõðîíèçèðîâàíû ñ ÷àñàìè Òðåíòà. Íà ïðàêòèêå ýôôåêò äîñòèãàåòñÿ ñèíõðîíèçàöèåé ñ íàäåæíûì ñåðâåðîì âðåìåíè ñ òî÷íîñòüþ â íåñêîëüêî ìèíóò è îáíàðóæåíèì ïîâòîðíîé ïåðåäà÷è â òå÷åíèå îïðåäåëåííîãî èíòåðâàëà âðåìåíè.

Neuman-Stubblebine

Èç-çà íåäîñòàòêîâ ñèñòåì ëèê ñàáîòàæà ñèíõðîíèçàöèÿ ÷àñîâ ìîæåò áûòü íàðóøåíà. Åñëè ÷àñû ñáèâàþòñÿ, ïðîòîê áîëüøèíñòâà ïðîòîêîëîâ ìîæåò áûòü èñïîëüçîâàí îïðåäåëåííûé ñïîñîá âñêðûòèÿ [644]. Åñëè ÷àñû îòïðàâèòåëÿ îïðåäåæþò ÷àñû ïîëó÷àòåëÿ, Ìýëîðè ìîæåò ïðåðâàòèòü ñîîáùåíèå îòïðàâèòåëÿ è ïîâòîðíî èñïîëüçîâàòü åãî ìåòêó âðåìåíè ñòàíäåò ïðîøëûì, è ýòî ïîçâîëèò Òðåíòó ïðèíÿòü âñêðûòèå è ïîâòîðíîå ïåðåäà÷è â òå÷åíèå îïðåäåëåííîãî èíòåðâàëà âðåìåíè.

Èç-çà íåäîñòàòêîâ ñèñòåì ëèê ñàáîòàæà ñèíõðîíèçàöèÿ ÷àñîâ ìîæåò áûòü íàðóøåíà. Åñëè ÷àñû ñáèâàþòñÿ, ïðîòîêîë áîëüøèíñòâà ïðîòîêîëîâ ìîæåò áûòü èñïîëüçîâàí îïðåäåëåííûé ñïîñîá âñêðûòèÿ [644]. Åñëè ÷àñû îòïðàâèòåëÿ îïðåäåæþò ÷àñû ïîëó÷àòåëÿ, Ìýëîðè ìîæåò ïðåðâàòèòü ñîîáùåíèå îòïðàâèòåëÿ è ïîâòîðíî èñïîëüçîâàòü åãî ìåòêó âðåìåíè ñòàíäåò ïðîøëûì, è ýòî ïîçâîëèò Òðåíòó ïðèíÿòü âñêðûòèå è ïîâòîðíîå ïåðåäà÷è â òå÷åíèå îïðåäåëåííîãî èíòåðâàëà âðåìåíè.

Ýòî ïðîòîêîë, âïåðâûå îïóáëèêîâàííûé â [820] è èñïðàâëåí â [1162], ïûòàåòñÿ ïðîòèâîñòîÿòü âñêðûòèþ ñ ïîäâåðæåíèåì ïîâòîðíîé ïåðåäà÷è. Ýòî îòëè÷íûé ïðîòîêîë ÿâëÿåòñÿ óëó÷øåíèåì Yahalom.

(1) Àëèñà îáúÿâëÿåò ñâîå èìÿ è ñëó÷àéíîå ÷èñëî, è îòïðàâëÿåò ñîçäàííîå ñîîáùåíèå Áîáó.

A, R_A

(2) Áîá îáúÿâëÿåò èìÿ Àëèñû, åå ñëó÷àéíîå ÷èñëî è ìåòêó âðåìåíè, øèôðóåò ñîçäàííîå ñîîáùåíèå îáùèì ñ Òðåíòîì êëþ÷îì è ïîñûëàåò åãî Òðåíòó, äîáàâëÿÿ ñâîå èìÿ è íîâîå ñëó÷àéíîå ÷èñëî:

B, R_B, $E_B(A, R_A, T_B)$

(3) Òðåíò ãåíåðèðóåò ñëó÷àéíûé ñåàíñîâûé êëþ÷. Çàòåì îí ñîçäàåò äâà ñîîáùåíèÿ. Ïåðâîå âêëþ÷àåò èìÿ Áîáà, ñëó÷àéíîå ÷èñëî Àëèñû, ñëó÷àéíûé ñåàíñîâûé êëþ÷, ìåòêó âðåìåíè è øèôðóåòñÿ êëþ÷îì, îáùèì äëÿ Òðåíòà è Àëèñû. Âòîðîå ñîñòîèò èç èìåíè Àëèñû, ñåàíñîâîãî êëþ÷à, ìåòêè âðåìåíè è øèôðóåòñÿ êëþ÷îì, îáùèì äëÿ Òðåíòà è Áîáà. Òðåíò ïîñûëàåò îáà ñîîáùåíèÿ Àëèñå âìåñòå ñî ñëó÷àéíûì ÷èñëîì Áîáà:

$E_A(B, R_A, K, T_B), E_B(A, K, T_B), R_B$

(4) Àëèñà ðàñøèôðîâûâàåò ñîîáùåíèå, çàøèôðîâàííîå åå êëþ÷îì, èçâëåêàåò *K* è óáåæäàåòñÿ, ÷òî R_A ñîâïàäàåò ñî çíà÷åíèåì, îïðåäåëåííûì íà ýòàïå (1). Àëèñà ïîñûëàåò Áîáó äâà ñîîáùåíèÿ. Îäíèì ÿâëÿåòñÿ ñîîáùåíèå Òðåíòà, çàøèôðîâàííîå êëþ÷îì Áîáà. Âòîðîå - ýòî R_B, çàøèôðîâàííîå ñåàíñîâûì êëþ÷îì.

$E_B(A, K), E_K(R_B),$

(5) Áîá ðàñøèôðîâûâàåò ñîîáùåíèå, çàøèôðîâàííîå åãî êëþ÷îì, èçâëåêàåò *K* è óáåæäàåòñÿ, ÷òî çíà÷åíèå T_B è R_B òå æå, ÷òî è îòïðàâëåííûå íà ýòàïå (2).

Åñëè îáà ñëó÷àéíûõ ÷èñëà è ìåòêà âðåìåíè ñîâïàäàþò, Àëèñà è Áîá óáåæäàþòñÿ â ïîäëèííîñòè äóã äðóãà è ïîëó÷àþò ñåêðåòíûé êëþ÷. Ñèíõðîíèçàöèÿ ÷àñîâ íå òðåáóåòñÿ, òàê êàê ìåòêà âðåìåíè îïðåäåëÿåòñÿ òîëüêî ïî

÷àñàì Áîáà, è òîëüêî Áîá ïðîâåðÿåò ñîçäàííóþ èì ìåòêó âðåìåíè.

Ó ýòîãî ïðîòîêîëà åñòü åùå îäíî ïîëçíîå ñâîéñòâî - Àëèñà ìîæåò èñïîëüçîâàòü ïîëó÷åííûå îò Òðåíòà ñîîáùåíèå äëÿ ïîñëåäóþùèé ïðîâåðêè ïîäëèííîñòè Áîáà â ïðåäâêóøåíèè íåêîòîðîãî âðåìåíè. Ïðåäïîëîæèì, ÷òî Àëèñà è Áîá âûïîëíèëè ïðèâåäåííûé âûøå ïðîòîêîë, ïðîâåëè è çàâåðøèëè ñåàíñ ñâÿçè. Àëèñà è Áîá ìîãóò ïîâòîðíî ïðîâåðèòü ïîäëèííîñòü äðóã äðóãà, íå îáðàùàÿñü ê Òðåíòó.

(1) Àëèñà ïîñûëàåò Áîáó ñîîáùåíèå, ïðèñëàííîå åé Òðåíòîì íà ýòàïå (3) è íîâîå ñëó÷àéíîå ÷èñëî.

$E_B(A, K, T_B), R'_A$

(2) Áîá ïîñûëàåò Àëèñå äðóãîå íîâîå ñëó÷àéíîå ÷èñëî è ñëó÷àéíîå ÷èñëî, ïðèñëàííîå Àëèñîé, øèôðóÿ èõ ñåàíñîâûì êëþ÷îì ñâÿçè.

$R'_B, E_K(R'_A)$

(3) Àëèñà ïîñûëàåò Áîáó åãî íîâîå ñëó÷àéíîå ÷èñëî, øèôðóÿ åãî ñåàíñîâûì êëþ÷îì ñâÿçè.

$E_K(R'_B)$

Íîâûå ñëó÷àéíûå ÷èñëà çàùèùàþò îò âñêðûòèÿ ñ ïîâòîðíî ïåðåäà÷åé.

DASS

Ïðîòîêîëû Đàñïðåäåëåííîé ñëóæáà áåçîïàñíîñòè è ïðîâåðêè ïîäëèííîñòè (Distributed Authentication Security Service, DASS), ñîçäàííûå â Digital Equipment Corporation, òàêæå îáëàäàþò îáîþäíóþ ïðîâåðêó ïîäëèííîñòè è îáìåí êëþ÷àìè [604, 1519, 1518]. Â îòëè÷èå îò ïðåäûäóùåãî ïðîòîêîëà DASS èñïîëüçóåò êàê êðèïòîãðàôèþ ñ îòêðûòûì è êëþ÷àìè, òàê è ñèììåòðè÷íóþ êðèïòîãðàôèþ. È ó Àëèñû, è ó Áîáà åñòü ñâîé çàêðûòûé êëþ÷. Òðåíò ïîäïèñûâàåò êîïèè èõ îòêðûòûõ êëþ÷åé.

(1) Àëèñà ïîñûëàåò Òðåíòó ñîîáùåíèå, ñîñòîÿùåå èç èìåíè Áîáà.

$Â$

(2) Òðåíò ïîñûëàåò Àëèñå îòêðûòûé êëþ÷ Áîáà, K_B, ïîäïèñàííûé çàêðûòûì êëþ÷îì Òðåíòà, T. Ïîäïèñàííîå ñîîáùåíèå ñîäåðæèò èìÿ Áîáà.

$S_T(B, K_B)$

(3) Àëèñà ïðîâåðÿåò ïîäïèñü Òðåíòà, óáåæäàÿñü, ÷òî îíà äåéñòâèòåëüíî ïîëó÷èëà îòêðûòûé êëþ÷ Áîáà. Îíà ãåíåðèðóåò ñëó÷àéíûé ñåàíñîâûé êëþ÷, K, è ñëó÷àéíóþ ïàðó êëþ÷åé îòêðûòûé/çàêðûòûé, K_p. Îíà øèôðóåò ìåòêó âðåìåíè êëþ÷îì K, à çàòåì ïîäïèñûâàåò âðåìÿ æèçíè, L, ñâîå èìÿ è ñâîè çàêðûòûì êëþ÷îì, K_A. Íàêîíåö, îíà çàøèôðîâûâàåò K îòêðûòûì êëþ÷îì Áîáà è ïîäïèñûâàåò åãî ñ ïîìîùüþ K_p. Âñå ýòî îíà îòïðàâëÿåò Áîáó.

$E_K(T_A), S_{K_A}(L, A, K_p), S_{K_p}(E_{K_B}(K))$

(4) Áîá ïîñûëàåò Òðåíòó (ýòî ìîæåò áûòü äðóãîé Òðåíò) ñîîáùåíèå, ñîñòîÿùåå èç èìåíè Àëèñû.

$À$

(5) Òðåíò ïîñûëàåò Áîáó îòêðûòûé êëþ÷ Àëèñû, $K_À$, ïîäïèñàííûé çàêðûòûì êëþ÷îì Òðåíòà. Ïîäïèñàííîå ñîîáùåíèå ñîäåðæèò èìÿ Àëèñû.

$S_T(À, K_À)$

(6) Áîá ïðîâåðÿåò ïîäïèñü Òðåíòà, óáåæäàÿñü, ÷òî îí äåéñòâèòåëüíî ïîëó÷èëà îòêðûòûé êëþ÷ Àëèñû. Çàòåì îí ïðîâåðÿåò ïîäïèñü Àëèñû è èçâëåêàåò K_p. Áîá èñïîëüçóåò ñâîé çàêðûòûé êëþ÷, èçâëåêàÿ K. Çàòåì îí ðàñøèôðîâûâàåò T_A, ïðîâåðÿÿ, ÷òî ýòî ñîîáùåíèå - òåêóùåå.

(7) Åñëè òðåáóåòñÿ îáîþäíàÿ ïðîâåðêà ïîäëèííîñòè, Áîá øèôðóåò íîâóþ ìåòêó âðåìåíè êëþ÷îì K è ïîñûëàåò åå Àëèñå.

$E_K(T_Â)$

(8) Àëèñà ðàñøèôðîâûâàåò $T_Â$ êëþ÷îì K, ïðîâåðÿÿ, ÷òî ýòî ñîîáùåíèå - òåêóùåå.

SPX, ïðîäóêò DEC, îñíîâàí íà DASS. Äîïîëíèòåëüíóþ èíôîðìàöèþ ìîæíî íàéòè â [34].

Denning-Sacco

Â ýòîì ïðîòîêîëå òàêæå èñïîëüçóåòñÿ êðèòîãðàôèÿ ñ îòêðûòûì êëþ÷àìè [461]. Òðåíò âåäåò áàçó äàííûõ, õðàíÿùóþ îòêðûòûå êëþ÷è âñåõ ïîëüçîâàòåëåé.

(1) Àëèñà ïîñûëàåò Òðåíóó ñîîáùåíèå, ñîñòîÿùåå èç åå èìåíè è èìåíè ÁÎáà.

$A, \hat{A}$

(2) Òðåíó ïîñûëàåò Àëèñå îòêðûòûé êëþ÷ ÁÎáà, K_B, ïîäïèñàííûé çàêðûòûì êëþ÷îì Òðåíóà, T. Òðåíó òàêæå ïîñûëàåò Àëèñå åå ñîáñòâåííûé îòêðûòûé êëþ÷, K_A, ïîäïèñàííûé çàêðûòûì êëþ÷îì Òðåíóà.

$S_T(B, K_B), S_T(A, K_A)$

(3) Àëèñà ïîñûëàåò ÁÎáó ñëó÷àéíûé ñåàíñîâûé êëþ÷ è ìåòêó âðåìåíè, ïîäïèñàâ èõ ñâîèì çàêðûòûì êëþ÷îì è çàøèôðîâàâ îòêðûòûì êëþ÷îì ÁÎáà, âìåñòå ñ îáîèìè ïîäïèñàííûìè êëþ÷àìè.

$E_{\hat{A}}(S_A(K, T_A)), S_T(A, K_A), S_T(\hat{A}, K_{\hat{A}})$

(4) ÁÎá ðàñøèôðîâûâàåò ñîîáùåíèå Àëèñû ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à è ïðîâåðÿåò ïîäïèñü Àëèñû ñ ïîìîùüþ åå îòêðûòîãî êëþ÷à. Î í òàêæå óáåæäàåòñÿ, ÷òî ìåòêà âðåìåíè ïðàâèëüíà.

Ñ ýòîãî ìîìåíòà Àëèñà è ÁÎá ïîëó÷èëè K è ìîãòü ïðîâåñòè áåçîïàñíûé ñåàíñ ñâÿçè. Ýòî âûãëÿäè êðàñèâî, íî åñòü îäíà òîíêîñòü - âûïîëíèâ ïðîòîêîë ñ Àëèñîé, ÁÎá ñìîæåò âûäàòü ñåáÿ çà Àëèñó [5]. Ñìîòðèì:

(1) ÁÎá ïîñûëàåò Òðåíóó ñâîå èìÿ è èìÿ Êýðîë.

$\hat{A}, \tilde{N}$

(2) Òðåíó ïîñûëàåò ÁÎáó ïîäïèñàííûå îòêðûòûå êëþ÷è ÁÎáà è Êýðîë.

$S_T(B, K_B), S_T(\tilde{N}, K_{\tilde{N}})$

(3) ÁÎá ïîñûëàåò Êýðîë ïîäïèñàííûé ñëó÷àéíûé ñåàíñîâûé êëþ÷ è ìåòêó âðåìåíè, ðàíåå ïîëó÷åííûå îò Àëèñû, çàøèôðîâàâ èõ îòêðûòûì êëþ÷îì Êýðîë, âìåñòå ñ ïîäòâåðæäåíèåì Àëèñû è ïîäòâåðæäåíèåì Êýðîë.

$E_{\tilde{N}}(S_A(K, T_A)), S_T(A, K_A), S_T(\tilde{N}, K_{\tilde{N}})$

(4) Êýðîë ðàñøèôðîâûâàåò ñîîáùåíèå Àëèñû ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à è ïðîâåðÿåò ïîäïèñü Àëèñû ñ ïîìîùüþ åå îòêðûòîãî êëþ÷à. Î í òàêæå óáåæäàåòñÿ, ÷òî ìåòêà âðåìåíè ïðàâèëüíà.

Òåïåðü Êýðîë ñ÷èòàåò, ÷òî îíà ñîâåðøåííîëåòíþ ñ Àëèñîé, ÁÎá óñïåøíî îáóðà÷èë åå. Äåéñòâèòåëüíî, ÁÎá ñìîæåò äóðà÷èòü ëþáîãî ïîëüçîâàòåëÿ ñåòè, ïîêà íå çàêîí÷èòñÿ ñðîê äåéñòâèÿ ìåòêè âðåìåíè. Í î ýòî ëåãêî ìîæíî èñïðàâèòü. Ïðîñòî âñòàâüòå èìåíà â øèôðîâàííîå ñîîáùåíèå íà ýòàïå (3):

$E_{\hat{A}}(S_A(A, \hat{A}, K, T_A)), S_T(A, K_A), S_T(\hat{A}, K_{\hat{A}})$

Òåïåðü ÁÎá íå ñìîæåò ïîâòîðíî ïîñëàòü Êýðîë ñòàðîå ñîîáùåíèå, ïîòîìó ÷òî îíî ÿâíî ïðåäíàçíà÷åíî äëÿ ñåàíñà ñâÿçè ìåæäó Àëèñîé è ÁÎáîì.

Woo-Lam

Â ýòîì ïðîòîêîëå òàêæå èñïîëüçóåòñÿ êðèïòîãðàôèÿ ñ îòêðûòûì êëþ÷îì [1610, 1611]:

(1) Àëèñà ïîñûëàåò Òðåíóó ñîîáùåíèå, ñîñòîÿùåå èç åå èìåíè è èìåíè ÁÎáà.

$A, \hat{A}$

(2) Òðåíó ïîñûëàåò Àëèñå îòêðûòûé êëþ÷ ÁÎáà, K_B, ïîäïèñàííûé çàêðûòûì êëþ÷îì Òðåíóà, T.

$S_T(K_B)$

(3) Àëèñà ïðîâåðÿåò ïîäïèñü Òðåíóà. Çàòåì íóa ïîñûëàåò ÁÎáó ñâîå èìÿ è ñëó÷àéíîå ÷èñëî, øèôðîâàííîå îòêðûòûì êëþ÷îì ÁÎáà.

$A, E_{\hat{A}}(R_{\hat{A}})$

(4) ÁÎá ïîñûëàåò Òðåíóó ñâîå èìÿ, èìÿ Àëèñû è ñëó÷àéíîå ÷èñëî Àëèñû, øèôðîâàííîå îòêðûòûì êëþ÷îì Òðåíóà, $K_{\hat{O}}$.

$A, \hat{A}, E_{K_T}(R_A)$

(5) Òðåíó ïîñûëàåò ÁÎáó îòêðûòûé êëþ÷ Àëèñû, K_A, ïîäïèñàííûé çàêðûòûì êëþ÷îì Òðåíóà. Î í òàêæå ïîñûëàåò ÁÎáó ñëó÷àéíîå ÷èñëî Àëèñû, ñëó÷àéíûé ñåàíñîâûé êëþ÷, èìåíà Àëèñû è ÁÎáà, ïîäïèñàâ âñå ýòî çàêðûòûì êëþ÷îì Òðåíóà è çàøèôðîâàâ îòêðûòûì êëþ÷îì ÁÎáà.

$S_{\hat{O}}(K_A), E_{K_B}(S_{\hat{O}}(R_A, \hat{E}, A, \hat{A}))$

(6) ÁÎá ïðîâåðÿåò ïîäïèñè Òðåíóà. Çàòåì îí ïîñûëàåò Àëèñå âòîðóþ ÷àñòü ñîîáùåíèÿ Òðåíóà, ïîëó÷åííîãî íà ýòàïå (5), è íîâîå ñëó÷àéíîå ÷èñëî, çàøèôðîâàâ âñå îòêðûòûì êëþ÷îì Àëèñû.

$E_{K_A}(S_{\hat{O}}(R_A, \hat{E}, \grave{A}, \hat{A}), R_{\hat{A}})$

(7) Àëëñà ïðîâåðÿåò ïîäïèñü Òðåíòà è ñâîå ñëó÷àéíîå ÷èñëî. Çàòåì îíà ïîñûëàåò Áîáó âòîðîå ñëó÷àéíîå ÷èñëî, øèôðîâàííîå ñåàíñîâûì êëþ÷îì.

$\mathring{A}_{\hat{E}}(R_{\hat{A}})$

(8) Áîá ðàñøèôðîâûâàåò ñâîå ñëó÷àéíîå ÷èñëî è ïðîâåðÿåò, ÷òî îíî íå èçìåíèëîñü.

Äðóãèå ïðîòîêîëû

Â ëèòåðàòóðå îïèñàíî ìíîæåñòâî ïðîòîêîëîâ. Ïðîòîêîë X.509 ðàññìàòðèâàþòñÿ â ðàçäåëå 24.9, KryptoKnight - â ðàçäåëå 24.6, à Øèôðîâàííûé îáìåí êëþ÷àìè (Encrypted Key Exchange) - â ðàçäåëå 22.5.

Äðóãèì íîâûì ïðîòîêîëîì ñ îòêðûòûìè êëþ÷àìè ÿâëÿåòñÿ Kuperee [694]. Âåäåòñÿ ðàáîòà íà ïðîòîêîëàìè, èñïîëüçóþùèìè **ìàÿêè** - çàñëóæèâàþùèå äîâåðèÿ óçëû ñåòè, êîòîðûå íåïðåðûâíî è øèôðîâàùàòåëüíî ïåðåäàþò äîñòîâåðíûå ìåòêè âðåìåíè [783].

Âûâîäû

Èç ïðèâåäåííûõ ïðîòîêîëîâ, êàê èç òåõ, êîòîðûå âñêðûâàþòñÿ, òàê è èç íàäåæíûõ, ìîæíî èçâëå÷ü ðÿä âàæíûõ óðîêîâ:

— Ìíîãèå ïðîòîêîëû òåðïÿò íóäà÷ó, òàê êàê èõ ðàçðàáîò÷èêè ïûòàëèñü áûòü ñëèøêîì óíèâåðñàëüíûìè. Îíè îïòèìèçèðîâàëè ïðîòîêîëû, óáåðàÿ âàæíûå ýëåìåíòû - èìåíà, ñëó÷àéíûå ÷èñëà è ò.ï. - è ïûòàÿñü ñäåëàòü ïðîòîêîëû êàê ìîæíî áîëåå ïðîçðà÷íûìè [43, 44].

— Îïòèìèçàöèÿ - ýòà ìàíÿùàÿ ëîâóøêà - ñèëüíî çàâèñèò îò ñäåëàííûõ ïðåäïîëîæåíèé. Ïðèìåð: íàëè÷èå äîñòîâåðíîãî âðåìåíè ïîçâîëÿåò âàì ðåàëèçîâàòü ìíîãèå âåùè, íåâîçìîæíûå â ïðîòèâíîì ñëó÷àå.

— Âûáèðàéòå ïðîòîêîë çàâèñèò îò àðõèòåêòóðû èñïîëüçóåìûõ ñðåäñòâ ñâÿçè. Õîòèòå ëè âû ìèíèìèçèðîâàòü ðàçìåð ñîîáùåíèé èëè èõ êîëè÷åñòâî? Ì îãóò ëè ñòðîíà âçàèìîäåéſòâîâàòü êàæäûé ñ êàæäûì èëè êðóã èõ îáùåíèÿ áóäåò îãðàíè÷åí?

È ìåíîå ïîäîáíûå âîïðîñû è ïðèâåëè ê ñîçäàíèþ ôîðìàëüíûõ ìåòîäîâ àíàëèçà ïðîòîêîëîâ.

3.4 Ôîðìàëüíûé àíàëèç ïðîòîêîëîâ ïðîâåðêè ïîäëèííîñòè è îáìåíà êëþ÷àìè

Ïðîáëåìà âûäåëåíèÿ áåçîïàñíîãî ñåàíñîâîãî êëþ÷à äëÿ ïàðû êîìïüþòåðîâ (ëèë ëþäåé) â ñåòè íàñòîëüêî ôóíäàìåíòàëüíà, ÷òî ñòàëà ïðè÷èíîé ìíîãèõ èññëåäîâàíèé. Íåêîòîðûå èññëåäîâàíèÿ çàêëþ÷àëèñü â ðàçðàáîòêå ïðîòîêîëîâ, ïîäîáíûõ ðàññìàòðèâàåìûì â ðàçäåëàõ 3.1, 3.2 è 3.3. Ýòî, â ñâîþ î÷åðåäü, ïðèâåëî ê ïîÿâëåíèþ áîëåå âàæíîé è èíòåðåñíîé çàäà÷è: ôîðìàëüíîìó àíàëèçó ïðîòîêîëîâ ïðîâåðêè ïîäëèííîñòè è îáìåíà êëþ÷àìè. Èíîãäà ïðîâåðè â ïðîòîêîëàõ, êàæóùèõñÿ âïîëíå íàäåæíûìè, îáíàðóæèâàëèñü ñïóñòÿ ìíîãî ëåò ïîñëå èõ ðàçðàáîòêè, è ðàçðàáîò÷èêàì ïîòðåáîâàëèñü ñðåäñòâà, ïîçâîëÿþùèå ñðàçó æå ïðîâåðÿòü áåçîïàñíîñòü ïðîòîêîëà. Õîòÿ áîëüøàÿ ÷àñòü ýòîãî èíñòðóìåíòàðèÿ ïðèìåíèìà è ê áîëåå îáùèì êðèïòîãðàôè÷åñêèì ïðîòîêîëàì, îñîáîå âíèìàíèå óäåëÿëîñü ïðîâåðêå ïîäëèííîñòè è îáìåíó êëþ÷àìè. Ñóùåñòâóþ÷åòî ÷åòûðå îñíîâíûõ ïîäõîäà ê àíàëèçó êðèòåðèåâ ïîäëèííîñòè è îáìåíó êëþ÷àìè [1045]:

1. Ìîäåëèðîâàíèå è ïðîâåðêà ðàáîòû ïðîòîêîëà ñ èñïîëüçîâàíèåì ÿçûêîâ îïèñàíèÿ è ñðåäſòâ ïðîâåðêè, íå ðàçðàáîòàííûõ ñïåöèàëüíî äëÿ àíàëèçà êðèïòîãðàôè÷åñêèõ ïðîòîêîëîâ.
2. Ñîçäàíèå ýêſïåðèìåíòàëüíûõ ñèſòåì, ïîçâîëÿþùèõ êîíñòðóêòîðó ïðîòîêîëà ðàçðàáàòûâàòü è èſïëåäîâàòü ðàçëè÷íûå ñöåíàðèè.
3. Âûðàáîòêà òðåáîâàíèé ê ñåìåſòâó ïðîòîêîëîâ, èſïîëüçóÿ íåóþ ëîãèêó äëÿ àíàëèçà ïîíÿòèé "çíàíèå" è "âîâðåìÿ".
4. Ðàçðàáîòêà ôîðìàëüíûõ ìåòîäîâ, îſíîâàííûõ íà çàſèſè ſâîſſòâ êðèſòîãðàôè÷åſêèõ ſèſòåì â äëãàðàſêîì âèäå.

Ïîíÿòíî ïîſàíåå ýòîõ ÷åòûðåõ ïîäõîäîâ è ſâÿçàííûõ ſ íſèſ èſſëåäîâàíèé âûſîäèò çà ðàìêè äàííîé êíèãè. Õîſîøåå ââåäåíèå â ýòó òåìó äàſî â [1047, 1355], ÿ æå ſîáèðàþſü êſſíóòüſÿ òſëüêî ſſſíîâſûõ âſ ïðſſîâ.

Ïåðâûé èç ïîäõîäîâ ïûòàåòſÿ âſèàçàòü ïðàâèëüſſſòü ïðſòſîſêîë, ðàſſſìàòðèâàÿ âåſ êàê ſâû÷íóþ êſ ìüþòåðſíóþ ïðſſãðàì. Ðÿä èſſſëåäſſâàòåëåé ïðåſſòàâëſÿþò ſſſòſîſêîë êàê êſſå÷íûé àâòſìàò [1449, 1565], äðóãèå èſſſëüçóþò ðàſøèðſíèÿ ìåòſäſâ èſ÷èſſëſíèÿ ſſåäſêàòà ſåðâſſãſ ſſðÿäêà [822], à òðåòüè äëÿ àſàëèçà ſſſòſîſêîſâ èſſſëüçóþò ſçûêè ſſèſàſíèÿ [1566]. Îſíâêſ, âſêàçàòåëüſòâſſ ſſàâèëüſſſòè ſòſþäü íå ÿâëÿåſÿ âſêàçàòåëüſòâſſ ſ áåçſſàſſſſòè, è ýòſò ſſâſſſ ſſòåðſåë íåóäà÷ó ſſðè àſàëèçå ſſſâſò "äûðÿâûõ" ſſðſòſêſêſâ. È õſòÿ åâſ ſſðèſåſíèå ſſſà÷àëó øèðſêſ èçó÷äëſñü, ſ ðſſòſſ ſ ſſſóëÿðſſſòè òðåòüåſſ èç ſſâſſâſâ ðàáſòû â ýòſé îáëàſòè áûëè ſåſåſðèſſòèðſâàſû.

Âî âòîðîì ïîäõîäå äëÿ îïðåäåëåíèÿ òîãî, ìîæåò ëè ïðîòîêîë ïåðåéòè â íåæåëàòåëüíîå ñîñòîÿíèå (íàïðèìåð, ïîòåðÿ êëþ÷à), èñïîëüçóþòñÿ ýêñïåðòíûå ñèñòåìû. Õîòÿ ýòîò ïîäõîä äàåò ëó÷øèå ðåçóëüòàòû ïðè ïîèñêå "äûð", îí íå ãàðàíòèðóåò áåçîïàñíîñòè è íå ïðåäîñòàâëÿåò ìåòîäèê ðàçðàáîòêè âñêðûòèé. Îí õîðîø äëÿ ïðîâåðêè òîãî, ñîäåðæèò ëè ïðîòîêîë êîíêðåòíóþ "äûðó", íî âðÿä ëè ñïîñîáåí îáíàðóæèòü íåèçâåñòíûå "äûðû" â ïðîòîêîëå. Ïðèìåðû òàêîãî ïîäõîäà ìîæíî íàéòè â [987,1521], à â [1092] îáñóæäàåòñÿ ýêñïåðòíàÿ ñèñòåìà, ðàçðàáîòàííàÿ àðìèåé ÑØÀ è íàçâàííàÿ Ñëåäîâàòåëåì (Interrogator).

Òðåòèé ïîäõîä ãîðàçäî ïîïóëÿðíåå. Îí áûë âïåðâûå ââåäåí Ìàéêëîì Áýððîóçîì (Michael Burrows), Ìàðòèíîì Àáýäè (Martin Abadi) è Ðîäæåðîì Íååäõýìîì. Îíè ðàçðàáîòàëè ôîðìàëüíóþ ëîãè÷åñêóþ ìîäåëü äëÿ àíàëèçà çíàíèÿ è äîâåðèÿ, íàçâàííóþ **ÁÀÍ-ëîãèêîé** [283, 284]. ÁÀÍ-ëîãèêà ÿâëÿåòñÿ íàèáîëåå øèðîêî ðàñïðîñòðàíåíà ïðè àíàëèçå ïðîòîêîëîâ ïðîâåðêè ïîäëèííîñòè. Îíà ðàññìàòðèâàåò ïîäëèííîñòü êàê ôóíêöèþ îò öåëîñòíîñòè è íîâèçíû, èñïîëüçóÿ ëîãè÷åñêèå ïðàâèëà äëÿ îòñëåæèâàíèÿ ñîñòîÿíèÿ ýòèõ àòðèáóòîâ íà ïðîòÿæåíèè âñåãî ïðîòîêîëà. Õîòÿ áûëè ïðåäëîæåíû ðàçëè÷íûå âàðèàíòû è ðàñøèðåíèÿ, áîëüøèíñòâî ðàçðàáîò÷èêîâ ïðîòîêîëîâ äî ñèõ ïîð îáðàùàþòñÿ ê îðèãèíàëüíîé ðàáîòå.

ÁÀÍ-ëîãèêà íå ïðåäîñòàâëÿåò äîêàçàòåëüñòâî áåçîïàñíîñòè, îíà ìîæåò òîëüêî ðàññóæäàòü î ïðîâåðêå ïîäëèííîñòè. Îíà ÿâëÿåòñÿ ïðîñòîé, ïðÿìîëèíåéíîé ëîãèêîé, ëåãêîé â ïðèìåíåíèè è ïîëåçíîé ïðè ïîèñêå "äûð". Âîò íåêîòîðûå ïðåäëîæåíèÿ ÁÀÍ-ëîãèêè:

Àëèñà ñ÷èòàåò X. (Àëèñà äåéñòâóåò, êàê åñëè áû X ÿâëÿëîñü èñòèíîé.)

Àëèñà âèäèò X. (Êòî-òî ïîñëàë ñîîáùåíèå, ñîäåðæàùåå X, Àëèñå, êîòîðàÿ ìîæåò ïðî÷èòàòü è ñíîâà ïåðåäàòü X - âîçìîæíî ïîñëå äåøèôðèðîâàíèÿ.)

Àëèñà ñêàçàëà X. (Â íåêîòîðûé ìîìåíò âðåìåíè Àëèñà ïîñëàëà ñîîáùåíèå, êîòîðîå ñîäåðæèò ïðåäëîæåíèå X. Íå èçâåñòíî, êàê äàâíî áûëî ïîñëàíî ñîîáùåíèå, è áûëî ëè îíî ïîñëàíî â òå÷åíèè òåêóùåãî âûïîëíåíèÿ ïðîòîêîëà. Èçâåñòíî, ÷òî Àëèñà ñ÷èòàëà X, êîãäà ãîâîðèëà X.)

X íîâî. (X íèêîãäà íå áûëî ïîñëàíî â ñîîáùåíèè äî òåêóùåãî âûïîëíåíèÿ ïðîòîêîëà.)

È òàê äàëåå. ÁÀÍ-ëîãèêà òàêæå ïðåäîñòàâëÿåò ïðàâèëà äëÿ ðàññóæäåíèÿ î äîâåðèè ïðîòîêîëó. Äëÿ äîêàçàòåëüñòâà ÷åãî-ëèáî â ïðîòîêîëå èëè äëÿ îòâåòà íà êàêèå-òî âîïðîñû ê ëîãè÷åñêèì ïðåäëîæåíèÿì î ïðîòîêîëå ìîæíî ïðèìåíèòü ýòè ïðàâèëà. Íàïðèìåð, îäíèì èç ïðàâèë ÿâëÿåòñÿ ïðàâèëî î çíà÷åíèè ñîîáùåíèÿ:

ÅÑËÈ Àëèñà ñ÷èòàåò, ÷òî ó Àëèñû è Áîáà îáùèé ñåêðåòíûé êëþ÷, *K*, è Àëèñà âèäèò *Õ*, øèôðîâàííîå *K*, è Àëèñà íå øèôðîâàëà *X* ñ ïîìîùüþ *K*, ÒÎ Àëèñà ñ÷èòàåò, ÷òî Áîá ñêàçàë *X*.

Äðóãèì ÿâëÿåòñÿ ïðàâèëî ïîäòâåðæäåíèÿ ìåòêè âðåìåíè:

ÅÑËÈ Àëèñà ñ÷èòàåò, ÷òî *X* ìîãëî áûòü ñêàçàíî òîëüêî íåäàâíî, è, ÷òî Áîá *X* êîãäà-òî ñêàçàë *X*, ÒÎ Àëèñà ñ÷èòàåò, ÷òî Áîá ñ÷èòàåò *X*.

ÁÀÍ-àíàëèç äåëèòñÿ íà ÷åòûðå ýòàïà:

(1) Ïðåîáðàçóéòå ïðîòîêîë ê èäåàëüíîé ôîðìå, èñïîëüçóÿ îïèñàííûå âûøå ïðåäëîæåíèÿ.

(2) Äîáàâüòå âñå ïðåäïîëîæåíèÿ î íà÷àëüíîì ñîñòîÿíèè ïðîòîêîëà.

(3) Ïðèñîåäèíèòå ëîãè÷åñêèå ôîðìóëû ê ïðåäëîæåíèÿì, ïîëó÷àÿ óòâåðæäåíèÿ î ñîñòîÿíèè ñèñòåìû ïîñëå êàæäîãî ïðåäëîæåíèÿ.

(4) Ïðèìåíèòå ëîãè÷åñêèå ïîñòóëàòû ê óòâåðæäåíèÿì è ïðåäïîëîæåíèÿì, ÷òîáû ðàñêðûòü ñîñòîÿíèå äîâåðèÿ ó÷àñòíèêîâ ïðîòîêîëà.

Àâòîðû ÁÀÍ-ëîãèêè "ðàññìàòðèâàþò èäåàëèçèðîâàííûå ïðîòîêîëû êàê áîëåå ÿñíûå è ïîëíûå îïèñàíèÿ, ÷åì òðàäèöèîííûå, íàéäåííûå â ëèòåðàòóðå..." [283, 284]. Äðóãèå èññëåäîâàòåëè íå òàê îïòèìèñòè÷íû è ïîäâåðãàþò ýòî äåéñòâèå êðèòèêå, òàê êàê ïðè ýòîì ðåàëüíûé ïðîòîêîë ìîæåò áûòü èñêàæåí [1161, 1612]. Äàëüíåéøèå ñïîðû îòðàæåíû â [221, 1557]. Ðÿä êðèòèêîâ ïûòàåòñÿ ïîêàçàòü, ÷òî ÁÀÍ-ëîãèêà ìîæåò è ïîëó÷èòü î÷åâèäíî íåïðàâèëüíûå õàðàêòåðèñòèêè ïðîòîêîëîâ [1161] - ñì. êîíòðïðèìåð â [285, 1509] - è ÷òî ÁÀÍ-ëîãèêà çàíèìàåòñÿ òîëüêî äîâåðèåì, à íå áåçîïàñíîñòüþ [1509]. Ïîäðîáíîå îáñóæäåíèå ïðèâåäåíî â [1488, 706, 1002].

Íåñìîòðÿ íà ýòó êðèòèêó ÁÀÍ-ëîãèêà äîñòèãëà îïðåäåëåííûõ óñïåõîâ. Åé óäàëîñü îáíàðóæèòü "äûðû" â íåñêîëüêèõ ïðîòîêîëàõ, âêëþ÷àÿ Needham-Schroeder è ðàííþþ ÷åðíîâóþ âåðñèþ ïðîòîêîëà CCITT X.509 [303]. Îíà îáíàðóæèëà èçáûòî÷íîñòü âî ìíîãèõ ïðîòîêîëàõ, âêëþ÷àÿ Yahalom, Needham-Schroeder è Kerberos. Âî ìíîãèõ îïóáëèêîâàííûõ ðàáîòàõ ÁÀÍ-ëîãèêà èñïîëüçóåòñÿ äëÿ çàÿâëåíèÿ ïðåòåíçèè î áåçîïàñíîñòè îïèñûâàåìûõ ïðîòîêîëîâ [40, 1162, 73].

Áûëè îïóáëèêîâàíû è äðóãèå ëîãè÷åñêèå ñèñòåìû, íåêîòîðûå èç íèõ ðàçðàáàòûâàëèñü êàê ðàñøèðåíèÿ ÁÀÍ-ëîãèêè [645, 586, 1556, 828], à äðóãèå îñíîâûâàëèñü íà ÁÀÍ-ëîãèêå äëÿ èñïðàâëåíèÿ îùóòèìûõ ñëàáîñòåé [1488, 1002]. Èç íèõ íàèáîëåå óñïåøíîé îêàçàëàñü CNY [645], õîòÿ ó íåå åñòü ðÿä èçúÿíîâ [40]. Â [292,474] ê ÁÀÍ-ëîãèêå ñ ïåðåìåííûì óñïåõîì áûëè äîáàâëåíû âåðîÿòíîñòíûå äîâåðèÿ. Äðóãèå ôîðìàëüíûå ëîãèêè îïèñàíû â [156, 798,288]. [1514] ïûòàåòñÿ îáúåäèíèòü ÷åðòû íåñêîëüêèõ ëîãèê. À â [1124, 1511] ïðåäñòàâëåíû ëîãèêè, â êîòîðûõ äîâåðèÿ èçìåíÿþòñÿ ñî âðåìåíåì.

×åòâåðòûé ïîäõîä ê àíàëèçó êðèïòîãðàôè÷åñêèõ ïðîòîêîëîâ ïðåäëàãàåò ìîäåëèðîâàòü ïðîòîêîëû êàê àëãåáðàè÷åñêóþ ñèñòåìó, âûðàçèòü ñîñòîÿíèå çíàíèÿ ó÷àñòíèêîâ î ïðîòîêîëå è çàòåì ïðîàíàëèçèðîâàòü äîñòèæå-

ìîñòü îïðåäåëåííûõ ñîñòîÿíèé. Ýòîò ïîäõîä íå ïðèâåë ñòîëüêî âíèìàíèÿ, êàê ôîðìàëüíàÿ ëîãèêà, íî ñîñòîÿíèå äåë ìåíÿåòñÿ. Î í âïåðâûå áûë èñïîëüçîâàí Ìàéêëîì Ìåðêèòîì [1076], êîòîðûé ïîêàçàë, ÷òî äëÿ àíàëèçà êðèòàðèåâ÷åñêèõ ïðîöåññîâ ìîæíî èñïîëüçîâàòü àëãåáðàè÷åñêóþ ìîäåëü. Äðóãèå ïîäõîäû ðàññìîòðåíû â [473, 1508, 1530, 1531, 1532, 1510, 1612].

Àíàëèçàòîð ïðîòîêîëîâ Èññëåäîâàòåëüñêîé ëàáîðàòîðèè Â Ì Ñ (Navy Research Laboratory, NRL), âîçìîæíî, ÿâëÿåòñÿ íàèáîëåå óñïåøíûì ïðèìåíåíèåì ýòèõ ìåòîäîâ [1512, 823, 1046, 1513]. Î í áûë èñïîëüçîâàí äëÿ ïîèñêà êàê íîâûõ, òàê è èçâåñòíûõ "äûð" âî ìíîæåñòâå ïðîòîêîëîâ [1044, 1045, 1047]. Àíàëèçàòîð ïðîòîêîëîâ îïðåäåëÿåò ñëåäóþ ùèå äâéñòâèÿ:

— Ïðèíÿòü (Áîá, Àëèñà, *M*, *N*). (Áîá ïðèíèìàåò ñîîáùåíèå *M* êàê ïðèøåäøåå îò Àëèñû â òå÷åíèå ëîêàëüíîãî ðàíäà Áîáà *N*.)

— Óçíàòü (Åâà, *M*). (Åâà óçíàåò *M*.)

— Ïîñëàòü (Àëèñà, Áîá, *Q*, *M*). (Àëèñà ïîñûëàåò *M* Áîáó â îòâåò íà çàïðîñ, *Q*.)

— Çàïðîñèòü (Áîá, Àëèñà, *Q*, *N*). (Áîá ïîñûëàåò *Q* Àëèñå â òå÷åíèå ëîêàëüíîãî ðàíäà Áîáà *N*.)

Èñïîëüçóÿ ýòè äåéñòâèÿ, ìîæíî çàäàòü òðåáîâàíèÿ. Íàïðèìåð:

— Åñëè Áîá ïðèíÿë ñîîáùåíèå *M* îò Àëèñû â êàêîé-òî ïðîøåäøèé ìîìåíò, òî Åâà íå çíàåò *M* â êàêîé-òî ïðîøåäøèé ìîìåíò âðåìåíè.

— Åñëè Áîá ïðèíÿë ñîîáùåíèå *M* îò Àëèñû â òå÷åíèå ëîêàëüíîãî ðàíäà Áîáà *N*, òî Àëèñà ïîñëàë *M* Áîáó â îòâåò íà çàïðîñ Áîáà â ëîêàëüíîì ðàíäå Áîáà *N*.

Äëÿ àíàëèçà Àíàëèçàòîðîì ïðîòîêîëîâ NRL èñïëåäóåìûé ïðîòîêîë äîëæåí áûòü îïèñàí ñ ïîìîùüþ ïðèâåäåííûõ êîíñòðóêöèé. Çàòåì âûïîëíÿþòñÿ ÷åòûðåôàçû àíàëèçà: îïðåäåëåíèå ïðàâèë ïåðåõîäà äëÿ ÷åñòíûõ ó÷àñòíèêîâ, îïèñàíèå îïåðàöèé, âîçìîæíûõ è äëÿ ïîëíîòû ÷åñòíûõ, è äëÿ íå÷åñòíûõ ó÷àñòíèêîâ, îïèñàíèå áàçîâûõ áëîêîâ ïðîòîêîëà è îïèñàíèå ïðàâèë ïðåîáðàçîâàíèÿ. Ñìûñë âñåãî ýòîãî â òîì, ÷òîáû ïîêàçàòü, ÷òî äàííûé ïðîòîêîë óäîâëåòâîðÿåò íåîáõîäèìûì òðåáîâàíèÿì. Èñïîëüçîâàíèå èíòóèöèîíèñòñêèõ, îïèñàíèå áàçîâûõ áëîêîâ ïðîòîêîëà è îïèñàíèå ïðàâèë ïðåîáðàçîâàíèÿ. Ðàáîòà ïðîäåìîíñòðèðîâàëà, ÷òî ïîäõîä NRL, â èòîãå ìîãë áû ïðèâåñòè ê ñîçäàíèþ ïðîòîêîëà, êîòîðûé áûë áû îáñíîâàííî ïðèçíàí áåçîïàñíûì.

Õîòÿ ôîðìàëüíûå ìåòîäû â îñíîâíîì ïðèìåíÿþòñÿ ê óæå ñóùåñòâóþùèì ïðîòîêîëàì, ñåãîäíÿ åñòü òåíäåíöèÿ èñïîëüçîâàòü èõ è ïðè ïðîåêòèðîâàíèè ïðîòîêîëîâ. Ðÿä ïðåäâàðèòåëüíûõ øàãîâ â ýòîì íàïðàâëåíèè ñäåëàí â [711]. Ýòî æå ïûòàåòñÿ ñäåëàòü è àíàëèçàòîð ïðîòîêîëîâ NRL [1512, 222, 1513].

Ïðèìåíåíèå ôîðìàëüíûõ ìåòîäîâ ê êðèòèêå÷åñêèì ïðîòîêîëàì ïðåäñòàâëÿåò ñîáîé êà÷åñòâåííî íîâóþ èäåþ, è òðóäíî îáðåñòè, ê ÷åìó ìîæåò ïðèâåñòè åå ðåàëèçàöèÿ. Ñ ýòîé òî÷êè çðåíèÿ ñëàáåéøèì çâåíîì êàæåòñÿ ïðîöåññ ôîðìàëèçàöèè.

3.5 Êðèïòîãðàôèÿ ñ íåñêîëüêèì ïîêðûòûì ìè êëþ÷àìè

Îáû÷íàÿ êðèïòîãðàôèÿ ñ îòêðûòûì ìè êëþ÷àìè èñïîëüçóåò äâà êëþ÷à. Ñîîáùåíèå, çàøèôðîâàííîå îäíèì êëþ÷îì, ìîæåò áûòü ðàñøèôðîâàíî äðóãèì. Îáû÷íî îäèí êëþ÷ ÿâëÿåòñÿ çàêðûòûì, à äðóãîé - òîêðûòûì. Ïóñòü, îäèí êëþ÷ íàõîäèòñÿ ó Àëèñû, à äðóãîé - ó Áîáà. Ì û õîòèì ðåøèòü ïðîáëåìó: Àëèñà ìîæåò çàøèôðîâàòü ñîîáùåíèå òàê, ÷òî òîëüêî Áîá ñìîæåò ðàñøèôðîâàòü åãî, à Áîá ìîæåò çàøèôðîâàòü ñîîáùåíèå òàê, ÷òî òîëüêî Àëèñà ñìîæåò ïðî÷èòàòü åãî.

Ýòà êîíöåïöèÿ áûëà îáîáùåíû Êîííîì Áîéäîì (Conn Boyd) [217]. Ïðåäïîëàãàþò ñåáÿ âàðèàíò êðèïòîãðàôèè ñ îòêðûòûì êëþ÷àìè, èñïîëüçóþùèé òðè êëþ÷à: K_A, K_B è K_C, ðàñïðåäåëåííå êîòîðûõ ïîêàçàíî â 1-é.

Àëèñà ìîæåò çàøèôðîâàòü ñîîáùåíèå êëþ÷îì K_A òàê, ÷òî Ýëëåí ìîæåò ðàñøèôðîâàòü åãî, èñïîëüçóÿ êëþ÷è K_B è Kc. Òî æå ñàìîå, ñäåëàâ ñîîòâåòſòâóþùèå ìîäó ñäåëàííûå Áîá è Êýðîë. Áîá ìîæåò çàøèôðîâàòü ñîîáùåíèå òàê, ÷òî Ôðýíê ñìîæåò ïðî÷åñòü åãî à Êýðîë ñìîæåò çàøèôðîâàòü ñîîáùåíèå òàê, ÷òî åãî ñìîæåò ïðî÷åñòü Äýéâ. Äýéâ ìîæåò çàøèôðîâàòü ñîîáùåíèå êëþ÷îì K_A òàê, ÷òî Ýëëåí ñìîæåò ïðî÷åñòü åãî, êëþ÷îì K_B òàê, ÷òî åãî ñìîæåò ïðî÷åñòü Ôðýíê, èëè îáìåíèâ êëþ÷àìè, K_A è K_B, òàê, ÷òî ñîîáùåíèå ñìîæåò ïðî÷åñòü Êýðîë. Àíàëîãè÷íî, Ýëëåí ìîæåò çàøèôðîâàòü ñîîáùåíèå òàê, ÷òî Äëèñà, èëè Äýéâ, èëè Ôðýíê ñìîæåò ïðî÷åñòü åãî. Âñå âîçìîæíûå êîìáèíàöèè ïîêàçàíû â , äðóãèõ íå ñóùåñòâóò.

Òàáë. 3-2.
Ðàñïðåäåëåíèå êëþ÷åé â òðåõêëþ÷åâîé ñèñòåìå.

Àëèñà	K_A
Áîá	K_B

Êýðîë	$K_{Ñ}$
Äýéâ	K_A è K_B
Ýëëåí	K_B è Kc
Ôðàíê	$K_{Ñ}$ è K_A

Òàêàÿ ñõåìà ìîæåò áûòü ðàñøèðåíà íà *n* êëþ÷åé. Åñëè äëÿ øèôðîâàíèÿ ñîîáùåíèÿ èñïîëüçóåòñÿ çàäàííîå ïîäìíîæåñòâî êëþ÷åé, òî äëÿ äåøèôðèðîâàíèÿ ñîîáùåíèÿ ïîòðåáóþòñÿ îñòàâøèåñÿ êëþ÷è.

Øèðîêîâåùàòåëüíàÿ ïåðåäà÷à ñîîáùåíèÿ

Ïðåäñòàâüòå, ÷òî â íåêîåé îïåðàöèè çàíÿòî 100 âàøèõ òàéíûõ àãåíòîâ. Âû õîòèòå èìåòü âîçìîæíîñòü ïîñûëàòü ñîîáùåíèÿ ãðóïïàì àãåíòîâ, íî âû íå çíàåòå çàðàíåå ñîñòàâ ãðóïï. Ìîæíî ëèáî øèôðîâàòü ñîîáùåíèå îòäåëüíî äëÿ êàæäîãî êîððåñïîíäåíòà, ëèáî ðàñïðåäåëèòü êëþ÷è äëÿ âñåõ âîçìîæíûõ êîìáèíàöèé àãåíòîâ. Äëÿ ðåàëèçàöèè ïåðâîãî ñïîñîáà ïîòðåáóåòñÿ ìíîæåñòâî ñîîáùåíèé, äëÿ âòîðîãî - ìíîæåñòâî êëþ÷åé.

Êðèïòîãðàôèÿ ñ íåñêîëüêèìè êëþ÷àìè ïîçâîëÿåò ðåøèòü ýòó çàäà÷ó íàìíîãî ïðîùå. Ìû áóäåì èñïîëüçîâàòü òðåõ àãåíòîâ: Àëèñó, Áîáà è Êýðîë. Âû âûäàäèòå Àëèñå êëþ÷ K_A è K_B, Áîáó - K_B è $K_{Ñ}$, Êýðîë - $K_{Ñ}$ è K_A. Òåïåðü âû ñìîæåòå ãîâîðèòü ñ ëþáûì íóæíûì ïîäìíîæåñòâîì àãåíòîâ. Åñëè âû õîòèòå, ÷òîáû ñîîáùåíèå ìîãëà ïðî÷èòàòü òîëüêî Àëèñà, çàøèôðóéòå åãî êëþ÷îì $K_{Ñ}$. Êîãäà Àëèñà ïîëó÷èò ñîîáùåíèå, îíà ðàñøèôðóåò åãî, ïîñëåäîâàòåëüíî èñïîëüçóÿ êëþ÷è K_A è K_B. Åñëè âû õîòèòå ïîñëàòü ñîîáùåíèå òîëüêî Áîáó, çàøèôðóéòå åãî êëþ÷îì K_A, à ñîîáùåíèå äëÿ Êýðîë - êëþ÷îì K_B. Åñëè âû õîòèòå, ÷òîáû ïîñëàííîå ñîîáùåíèå ìîãëè ïðî÷èòàòü Àëèñà è Áîá, çàøèôðóéòå åãî êëþ÷àìè K_A è $K_{Ñ}$.

Äëÿ òðåõ àãåíòîâ ýòî íå ñëèøêîì âïå÷àòëÿåò, íî äëÿ 100 ïðåèìóùåñòâî äîñòàòî÷íî îùóòèìî. Èíäèâèäóàëüíûå ñîîáùåíèÿ îçíà÷àþò èñïîëüçîâàíèå îòäåëüíîãî êëþ÷à äëÿ êàæäîãî àãåíòà (âñåãî 100 êëþ÷åé) è êàæäîãî ñîîáùåíèÿ. Ïåðåäà÷à ñîîáùåíèé âñåì âîçìîæíûì ïîäìíîæåñòâàì îçíà÷àåò èñïîëüçîâàíèå 2^{100}-2 ðàçëè÷íûõ êëþ÷åé (èñêëþ÷åíû ñëó÷àè ñîîáùåíèÿ âñåì àãåíòàì è íèêîìó èç íèõ). Äëÿ ñõåìû, èñïîëüçóþùåé êðèïòîãðàôèþ ñ íåñêîëüêèìè îòêðûòûìè êëþ÷àìè, íóæíî òîëüêî îäíî øèôðîâàííîå ñîîáùåíèå è ñòî ðàçëè÷íûõ êëþ÷åé. Íåäîñòàòêîì ýòîé ñõåìû ÿâëÿåòñÿ òî, ÷òî âàì òàêæå ïðèäåòñÿ øèðîêîâåùàòåëüíî ïåðåäàâàòü, êàêîå ïîäìíîæåñòâî àãåíòîâ ìîæåò ÷èòàòü ñîîáùåíèå, èíà÷å êàæäîìó èç íèõ ïðèäåòñÿ ïåðåáèðàòü âñå âîçìîæíûå êîìáèíàöèè êëþ÷åé â ïîèñêàõ ïîäõîäÿùåé. Äàæå òîëüêî ïåðå÷èñëåíèå èìåí ïîëó÷àòåëåé ìîæåò áûòü âåñüìà âíóøèòåëüíûì. Êðîìå òîãî, êàæäîìó àãåíòó ïðèäåòñÿ õðàíèòü íåìàëåíüêèé îáúåì èíôîðìàöèè î êëþ÷àõ, ïî êðàéíåé ìåðå ïðè ïðÿìîëèíåéíîé ðåàëèçàöèè ýòîé ñõåìû.

Ñóùåñòâóþò è äðóãèå ñïîñîáû øèðîêîâåùàòåëüíîé ïåðåäà÷è, ðÿä èç íèõ ïîçâîëÿåò èçáåæàòü îïèñàííîé ïðîáëåìû. Ýòè ñïîñîáû îáñóæäàþòñÿ â ðàçäåëå 22.7.

Òàáë. 3-3.
Øèôðîâàíèå ñîîáùåíèÿ â òðåõêëþ÷åâîé ñèñòåìå.

Øèôðóåòñÿ êëþ÷àìè	Äîëæíî áûòü ðàñøèôðîâàíî êëþ÷àìè
K_A	K_B è Kc
K_B	K_A è $K_{Ñ}$
$K_{Ñ}$	K_A è K_B
K_A è K_B	$K_{Ñ}$
K_A è $K_{Ñ}$	K_B
K_B è Kc	K_A

3.6 Ðàçäåëåíèå ñåêðåòà

Âîîáðàçèòå, ÷òî âû èçîáðåëè íîâûé, ñâåðõëèïêóþ, ñâåðõñëàäêóþ ñëèâî÷íóþ òÿíó÷êó èëè ñîóñ äëÿ ãàìáóðãåðîâ, êîòîðûé åùå áåçâêóñíåå, ÷åì ó âàøèõ êîíêóðåíòîâ. Ýòî î÷åíü âàæíî, è âû õîòèòå ñîõðàíèòü èçîáðåòåíèå â ñåêðåòå. Òîëüêî ñàìûì íàäåæíûì ðàáîòíèêàì âû ìîæåòå ñîîáùèòü òî÷íûé ñîñòàâ èíãðåäèåíòîâ, íî âäðóã è êòî-òî èç íèõ ïîäêóïëåí êîíêóðåíòàìè? Ñåêðåò âûêðàäóò, è íåìíîãî ïîãîäÿ êàæäûé â êâàðòàëå áóäåò äåëàòü ãàìáóðãåðû ñ òàêèì æå áåçâêóñíûì ñîóñîì, êàê âàø.

Ïðåäëàãàåìàÿ ñõåìà íàçûâàåòñÿ **ðàçäåëåíèåì ñåêðåòà**. Åñòü ñïîñîáû âçÿòü ñîîáùåíèå è ðàçäåëèòü åãî íà ÷àñòè [551]. Êàæäàÿ ÷àñòü ñàìà ïî ñåáå íè÷åãî íå çíà÷èò, íî ñëîæèòå èõ - è âû ïîëó÷èòå ñîîáùåíèå. Åñëè ýòî

ðåöåïò, è ó êàæäîãî ðàáîòíèêà íàõîäèòñÿ òîëüêî åãî ÷àñòü, òî ëèøü ñîáðàâøèñü âìåñòå âàøè ñëóæàùèå ñìîãóò ñäåëàòü ñîóñ. Åñëè êòî-íèáóäü èç ðàáîòíèêîâ óâîëèòñÿ, ïðèõâàòèâ ñ ñîáîé ñâîþ ÷àñòü ðåöåïòà, ðàñêðûòàÿ èíôîðìàöèþ ïî ñåêðåòíûì áóäåò äåñÿòêàì äðóãèõ ëþäåé.

Ïî ïðîñòåéøåé ñõåìå ñîîáùåíèå äëèíîé ìåæäó äâóìÿ ëþäüìè. Âîò ïðîòîêîë, èñïîëüçóÿ êîòîðûé Òðåíà äåëèò ñîîáùåíèå ìåæäó Àëèñîé è Áîáîì:

(1) Òðåíà ãåíåðèðóåò ñòðîêó ñëó÷àéíûõ áèòîâ, *R*, òàêîé æå äëèíû, ÷òî è ñîîáùåíèå, *M*.

(2) Òðåíà âû÷èñëÿåò "èñêëþ÷àþùåå èëè" (XOR) íàä *M* è *R*, ñîçäàâàÿ *S*.

$$R \oplus M = S$$

(3) Òðåíà ïåðåäàåò Àëèñå *R*, à Áîáó - *S*.

×òîáû ïîëó÷èòü ñîîáùåíèå, Àëèñà è Áîáó íóæíî âû÷èñëèòü åäèíñòâåííóþ äéñòâèòåëüíóþ ôóíêöèþ *f*, òàêóþ, ÷òî $f(R, S) = M$. Ýòî ìîæíî ïðè âûïîëíåíèè àáñîëþòíî áåçîïàñíî. Êàæäàÿ ÷àñòü â îòäåëüíîñòè àáñîëþòíî áåçîïàñíà. ×òî ñóùåñòâåííî, Òðåíà øèôðóåò ñîîáùåíèå îäíîðàçîâûì áëîêíûì øèôðîâàíèåì, äâîè÷íûé àíàëîã êîòîðîãî ìîæíî íàéòè â ðàçäåëå 1.5. Íèêàêèå âû÷èñëèòåëüíûå ñðåäñòâà íå ñìîãóò âîññòàíîâèòü ñîîáùåíèå òîëüêî ïî îäíîé åãî ÷àñòè.

Ýòó ñõåìó ëåãêî ðàñøèðèòü íà áîëüøåå ÷èñëî ëþäåé. ×òîáû ðàçäåëèòü ñîîáùåíèå ìåæäó áîëåå ÷åì äâóìÿ ëþäüìè, âû÷èñëèòå îïåðàöèþ XOR ñ áîëüøèì ÷èñëîì ñòðîê ñëó÷àéíûõ áèòîâ. Â ñëåäóþùåì ïðèìåðå Òðåíó äåëèò ñîîáùåíèå íà ÷åòûðå ÷àñòè:

(1) Òðåíà ãåíåðèðóåò òðè ñòðîêè ñëó÷àéíûõ áèòîâ, *R*, *S* è *T*, òàêîé æå äëèíû, ÷òî è ñîîáùåíèå, *M*.

(2) Òðåíà âû÷èñëÿåò "èñêëþ÷àþùåå èëè" (XOR) íàä *M* è ñîçäàííûìè òðåìÿ ñòðîêàìè, ñîçäàâàÿ *U*.

$$M \oplus R \oplus S \oplus T = U$$

(3) Òðåíà ïåðåäàåò Àëèñå *R*, Áîáó - *S*, Êýðîë - *T*, à Äýéâó - *U*.

Âìåñòå Àëèñà, Áîá, Êýðîë è Äýéâ ìîãóò âîññòàíîâèòü ñîîáùåíèå:

(4) Àëèñà, Áîá, Êýðîë è Äýéâ ñîáèðàþòñÿ âìåñòå è âû÷èñëÿþò:

$$R \oplus S \oplus T \oplus U = M$$

Ýòî àðáèòðàæíûé ïðîòîêîë. Òðåíó îáëàäàåò àáñîëþòíîé âëàñòüþ è ìîæåò äëàòü âñå, ÷òî îí õî÷åò. Î í ìîæåò ðàçäàòü ÷åïóõó è óòåðÿòü, ÷òî ýòî íàñòîÿùèå ÷àñòè ñåêðåòíîé èíôîðìàöèè, íèêòî íå ñìîæåò ýòî ïðîâåðèòü, ïîêà, ñîáðàâøèñü â åñòü, ó÷àñòíèêè ïðîòîêîëà íå ïîðóøàþò ïðî÷èòàíû ïèñüìî. Î í ìîæåò âûäàòü ÷àñòè ñåêðåòà Àëèñå, Áîáó, Êýðîë è Äýéâó è ïîçæå çàÿâèòü âñå, ÷òî òîëüêî Àëèñà, Êýðîë è Äýéâ íóæíû äëÿ âîññòàíîâëåíèÿ ñåêðåòà, çàñòðåëèâ ïðè ýòîì Áîáà. Í î ýòî íå ÿâëÿåòñÿ ïðîáëåìîé, òàê êàê äëèíû ñåêðåòà ïðèìåðíî ðàâíà äëèíå ñîîáùåíèÿ Òðåíó.

Îäíàêî, îäíà ïðîáëåìà ó ýòîãî ïðîòîêîëà ñóùåñòâóåò. Åñëè ëþáàÿ èç ÷àñòåé áóäåò ïîòåðÿíà, à Òðåíà íå áóäåò ïîáëèçîñòè, ïðîïàäåò è âñå ñîîáùåíèå. Åñëè Êýðîë, îáëàäàÿ ÷àñòüþ ðåøåíèà ñîñûëàåòñÿ íà ïîòåðþ, ïåðåéäåò ðàáîòàòü ê êîíêóðåíòó, îñòàâèâ ñâîþ ÷àñòü ñåêðåòà ó ñåáÿ, çíà÷èò, îñòàëüíûì íå ïîâåçåò. Î íà íå ñìîæåò âîññòàíîâèòü ñîîáùåíèå, íî íå ñìîãóò, ñîáðàâøèñü â åñòü, ó÷àñòíèêè ïðîòîêîëà íå ïîâåðÿò ïðî÷èòàíû ïèñüìî. Î í ìîæåò âûäàòü ÷àñòè ñåêðåòà Àëèñå, Áîáó, Êýðîë è Äýéâ ìãíîâåííî, ïîòåðÿâ ïðè ýòîì íåçíà÷èòåëüíóþ äîëþ èíôîðìàöèè, íèêòî íå ñìîæåò âîññòàíîâèòü ñåêðåò, çàñòðåëèâ ïðè ýòîì íåçíà÷èòåëüíóþ äîëþ ñâîèõ ñîîáùíèêîâ. Ïîíÿòíî, ÷òî ýòîò ïðîòîêîë ñóùåñòâåííî ëó÷øå, ÷åì ïðîòîêîë ñ ïîáî÷íûì ïðîäóêòîì, íî íåëüçÿ íàçâàòü åãî áåçîïàñíûì.

3.7 Ñîâìåñòíîå èñïîëüçîâàíèå ñåêðåòà

Âû ââîäèòå ïðîãðàììó çàïóñêà ÿâëÿþùåé ðåêîòó è õîòèòå áûòü óâåðåííû, ÷òî íèêàêîé ïîñòîðîííèê íå ñìîæåò âûçâàòü ïóñê. Âû õîòèòå áûòü óâåðåííû, ÷òî è äâà ïîñòà íå ñìîãóò âûçâàòü ïóñê. Âû õîòèòå, ÷òîáû ïîëüçîâàòåëü, åñëè íå ìåíüøå ðåãî èç ÿÿòè îôèöåðîâ áóäóò ïîñòîÿííî íàõîäèòüñÿ íà ñìîòðèòåëüíîì ïîñòó, íå ñìîã áû ïîëó÷èòü äîñòóï ê ñåêðåòíûì äàííûì.

Ìîæíî ñäåëàòü åùå ñëîæíåå. Ïóñòü òîëüêî ãåíåðàë ó è ïàðå ïîëêîâíèêîâ ðàçðåøåíî çàïóñòèòü ðàêåòó, íî åñëè ãåíåðàë çàíÿò èãðîé â ãîëüô, òî çàïóñòèòü ðàêåòó èìåþò ïðàâî òîëüêî ïÿòü ïîëêîâíèêîâ. Ñäåëàéòå êîòòîëüíîå óñòðîéñòâî ñ ïÿòüþ êëþ÷àìè. Âûäàéòå ãåíåðàëó òðè êëþ÷à, à ïîëêîâíèêàì ïî îäíîìó. Åñëåðàë âìåñòî ñ äâóìÿ ïîëêîâíèêàìè èëè ïÿòü ïîëêîâíèêîâ ñìîãóò çàïóñòèòü ðàêåòó. Îäíàêî íè ãåíåðàë â îäèíî÷êó, íè ÷åòûðå ïîëêîâíèêà íå ñìîãóò ýòîãî ñäåëàòü.

Áîëåå ñëîæíàÿ ñõåìà ñîâìåñòíîãî èñïîëüçîâàíèÿ, íàçûâàåìàÿ **ïîðîãîâîé ñõåìîé**, ìîæåò ðåøèòü è ýòè çàäà÷è, è áîëåå ñëîæíûå - ìàòåìàòè÷åñêè. Íà åå ïðîñòåøåì óðîâíå âû ìîæåòå âçÿòü ëþáîå ñîîáùåíèå (ñåêðåòíûé ðåöåïò, êîäû çàïóñêà, âàø ñïèñîê äëÿ ïðà÷íîé è ò.ï.) è ðàçäåëèòü åãî íà *n* ÷àñòåé, íàçûâàåìûõ **òåíÿìè** èëè äîëÿìè, òàê, ÷òî ïî ëþáûì *m* èç íèõ ìîæíî âîññòàíîâèòü ñîîáùåíèå. Áîëåå òî÷íî, ýòî íàçûâàåòñÿ **(m,n)-ïîðîãîâîé ñõåìîé**.

Èñïîëüçóÿ (3,4)-ïîðîãîâóþ ñõåìó, Òðåíò ìîæåò ðàçäåëèòü ñâîé ñåêðåòíûé ðåöåïò ìåæäó Àëèñîé, Áîáîì, Êýðîë è Äýéâîì òàê, ÷òî ëþáûå òðîå èç íèõ ìîãóò ñëîæèòü ñâîè òåíè âìåñòå è âîññòàíîâèòü ñîîáùåíèå. Åñëè Êýðîë â îòïóñêå, òî Àëèñà, Áîá è Äýéâ ñìîãóò âîññòàíîâèòü ñîîáùåíèå. Åñëè Áîá ïîïàë ïîä àâòîáóñ, à Êýðîë â îòïóñêå, òî Àëèñà è Äýéâ ñìîãóò âîññòàíîâèòü Àëèñà, Êýðîë è Äýéâ. Íî åñëè Áîá ïîïàë ïîä àâòîáóñ, à Êýðîë â îòïóñêå, òî Àëèñà è Äýéâ ñàìîñòîÿòåëüíî íå ñìîãóò âîññòàíîâèòü ñîîáùåíèå.

Âîîáùå, ïîðîãîâûå ñõåìû ìîãóò áûòü åùå áîëåå ãèáêèìè. Ìîæíî îòìîäåëèðîâàòü ëþáûå ñöåíàðèè ñîâìåñòíîãî èñïîëüçîâàíèÿ, êîòîðûå âû òîëüêî ñìîæåòå âîîáðàçèòü. Ìîæíî ðàçäåëèòü ñîîáùåíèå ìåæäó ëþäüìè â âàøåì çäàíèè òàê, ÷òî äëÿ åãî âîññòàíîâëåíèÿ íåîáõîäèìû ïî êðàéíåé ìåðå äâîå èç òðîèõ. Åñëè Áîá ïîïàë ïîä àâòîáóñ, à Êýðîë â îòïóñêå, òî Àëèñà è Äýéâ ñìîãóò âîññòàíîâèòü ñîîáùåíèå. Åñëè æå åñòü êòî-òî ñ ÷åòâåðòîãî ýòàæà, òî äëÿ âîññòàíîâëåíèÿ ñîîáùåíèÿ äîñòàòî÷íî ýòîãî ÷åëîâåêà è îäíîãî ñ òðåòüåãî ýòàæà èëè ýòîãî ÷åëîâåêà âìåñòå ñ äâóìÿ ñ ïÿòîãî ýòàæà è îäíîãî ñî âòîðîãî. Åñëè æå ... íó âû óëîâèëè èäåþ.

Ýòà èäåÿ áûëà íåçàâèñèìî âûâåíóòà Àäè Øàìèðîì [1414] è Äæîðäæåì Áëýêëè (George Blakley) [182] è èíòåíñèâíî áûëà èçó÷åíà Ãóñîì Ñèììîíñîì (Gus Simmons) [1466]. Ìíîæåñòâî ðàçëè÷íûõ äëãîðèòìîâ îáñóæäàþòñÿ â ðàçäåëå 23.2.

Ñîâìåñòíîå èñïîëüçîâàíèå ìíîæåñòâåííûõ

Ñóùåñòâóåò ìíîæåñòâî îáùèõ óòèëèò ïîðîãîâóþ ñõåìó. Âîò òîëüêî íåñêîëüêî èç íèõ. Ñöåíàðèé 1: Ïîëêîâíèêè Àëèñà, Áîá è Êýðîë ñèäÿò â èçîëèðîâàííûõ áóíêåðàõ äàå-òî ãèóáîêî ïîä çåìëåé. Îäíàæäû îíè ïîëó÷àþò çàêîäèðîâàííûå ñîîáùåíèå îò ïðåçèäåíòà: "Çàïóñòèòü ðàêåòû. Ì û ñîáèðàåìñÿ ñòåðåòü ñ ëèöà Çåìëè ëþáûå ñëåäû èñêëþ÷èòåëüíî ïðîòèâíèêà â îáùåì ïîðÿäêå". Àëèñà, Áîá è Êýðîë îòêðûâàþò ñâîè òàíè, íî Êýðîë ââîäèò ñëó÷àéíûå ÷èñëî. Î í íà ñàìî äåëå ïàðîëåñò è íå õî÷åò, ÷òîáû ðàêåòû áûëè çàïóùåíû. Ïîñêîëüêó Êýðîë íå ââåëè ïðàâèëüíîå òåíè, ñâêðåòíàÿ èíôîðìàöèÿ, êîòîðóþ îíè õîòåëè ïîëó÷èòü, îêàçàëàñü íåïðàâèëüíîé. Ðàêåòû îñòàëèñü â ñâîèõ øàõòàõ. È ñàìå ïëîõå, íèêòî íå çíàåò ïî÷åìó. Äàæå îáúåäèíåííûé Àëèñà è Áîá íå ñìîãóò äîêàçàòü, ÷òî òåíü Êýðîë íåïðàâèëüíà.

Ñöåíàðèé 2: Ïîëêîâíèêè Àëèñà è Áîá ñèäÿò â áóíêåðå âìåñòå ñ Ìýëëîðè. Ìýëëîðè ëîæíî âûäàåò ñåáÿ çà ïîëêîâíèêà. Îò ïðåçèäåíòà ïðèõîäèò òî æå ñàìîå ñîîáùåíèå è âñå îòêðûâàþò ñâîè òåíè. "Õà-õà-õà!" êðè÷èò Ìýëëîðè. "ß ïîääåëàë ýòî ñîîáùåíèå ïðåçèäåíòà. Òåïåðü ÿ çíàþ íåä âàøèõ äîëè." Î í óáåäàåò âåäðõ ïî ëåñòíè-öå è èñ÷åçàåò ïðåæäå, ÷åì åãî óñïåþò ïîéìàòü.

Ñöåíàðèé 3: Ïîëêîâíèêè Àëèñà, Áîá è Êýðîë ñèäÿò â áóíêåðå âìåñòå ñ Ìýëëîðè, êîòîðûé ñíîâà çàìàñêèðîâàëñÿ. (Ïîìíèòå, ó Ìýëëîðè íåò ïðàâèëüíîé òåíè.) Îò ïðåçèäåíòà ïðèõîäèò òî æå ñàìîå ñîîáùåíèå è âñå îòêðûâàþò ñâîè òåíè. Ìýëëîðè îòêðûâàåò ñâîþ òåíü, òîëüêî óñëûøàâ âñå îñòàëüíûå. Òàê êàê äëÿ âîññòàíîâëåíèÿ ñåêðåòà òðåáóåòñÿ òîëüêî òðè ÷àñòè, íî è íèòè íå äîãàäàëñÿ, ÷òî íå ÿâëÿåòñÿ ÷àñòüþ ýòîé ñèñòåìû. Íåêîòîðûå ïðîòîêîëû, êîòîðûå ïîçâîëÿþò áîðîòüñÿ ñ ïîäîáíûìè ìîøåííèêàìè, ðàññìàòðèâàþòñÿ â ðàçäåëå 23.2.

Ñîâìåñòíîå èñïîëüçîâàíèå ñêðûòàÿ Òðåíòà

Áàíê õî÷åò, ÷òîáû åãî ïîäâàäè ìîãëè îòêðûòü òðåõ èç ïÿòè îêòÿáðîâ, ââåäÿ ñâîè êëþ÷è. Ýòî âûãëÿäèò êàê òèïè÷íàÿ (3,5)-ïîðîãîâàÿ ñõåìà, íî ñ îäíîé òîíêîñòüþ. Íèêòî íå çíàåò ñåêðåòà öåëèêîì. Òðåíòà, êîòîðûå äåëèò ñåêðåò íà ïÿòè ÷àñòåé, íåò. Ñóùåñòâóþò ïðîòîêîëû, èñïîëüçóÿ êîòîðûå ïÿòè îòêðûâàþò ñâîè ñîîáùåíèÿ è âñå îòêðûâàþò ñåêðåò, íî íèêòî íå óçíàåò ñåêðåòà, ïîêà îí íå áóäåò âîññòàíîâëåí. Â ýòîé êíèãå ÿ íå ðàññìàòðèâàþ ýòè ïðîòîêîëû, ïîäðîáíî ñ ïîäîáíûìè ìîøåííèêàìè, ðàññìàòðèâàþòñÿ â ðàçäåëå 23.2.

äîêóìåíòà. Ïîñëå *n*-îé ÷àñòè÷íîé ïîäïèñè äîêóìåíò îêàçûâàåòñÿ ïîäïèñàí ñîâìåñòíî èñïîëüçóåìûì çàêðûòûì êëþ÷îì, à íè îäèí èç ó÷àñòíèêîâ íå ìîæåò óçíàòü ñîâìåñòíî ÷àñòè, èñïîëüçóåìîé äðóãèìè ó÷àñòíèêàìè. Ñìûñë â òîì, ÷òî âû ìîæåòå ïîâòîðíî èñïîëüçîâàòü ñåêðåò, è äëÿ ðàáîòû ñ íèì âàì íå ïîíàäîáèòñÿ íàäåæíûé ïîñðåäíèê. Äàëüíåéøåå ðàçâèòèå ýòà èäåÿ ïîëó÷èëà â ðàáîòàõ Èâî Äåñìåäòà (Yvo Desmedt) è Éåðà Ôðàíêåëÿ (Yair Frankel) [483, 484].

Ïîäòâåðæäàåìîå ñîâìåñòíîå èñïîëüçîâàíèå ñåêðåòà

Òðåíò ïåðåäàåò Àëèñå, Áîáó, Êýðîë è Äýéâó ÷àñòü ñåêðåòà (èëè, ïî êðàéíåé ìåðå, çàÿâëÿåò, ÷òî îí ýòî äåëàåò). Åäèíñòâåííûé ñïîñîá óáåäèòüñÿ, ÷òî èõ ÷àñòè ïðàâèëüíû - ýòî ïîïûòàòüñÿ âîññòàíîâèòü ñåêðåò. Ìîæåò áûòü Òðåíò ïîñëàë Áîáó ïîääåëüíóþ ÷àñòü, èëè ÷àñòü Áîáà ñëó÷àéíî èñïîðòèëàñü ïðè ïåðåäà÷å ïî ëèíèÿì ñâÿçè. Ïîäòâåðæäàåìîå ñîâìåñòíîå èñïîëüçîâàíèå ñåêðåòà ïîçâîëÿåò êàæäîìó èç ó÷àñòíèêîâ ëè÷íî óáåäèòüñÿ, ÷òî èõ ÷àñòü ïðàâèëüíà, áåç íåîáõîäèìîñòè âîññòàíàâëèâàòü ñåêðåò [558, 1235].

Ñõåìû ñîâìåñòíîãî èñïîëüçîâàíèÿ ñåêðåòà ñ ìåðàìè ïðåäîñòîðîæíîñòè

Ñåêðåò äåëèòñÿ ñðåäè 50 ÷åëîâåê òàê, ÷òîáû ëþáûå 10 ìîãëè ñîáðàòüñÿ âìåñòå è âîññòàíîâèòü ñåêðåò. Ýòî íåòðóäíî. Íî, ìîæåì ëè ìû ðåàëèçîâàòü òó æå ñõåìó ñîâìåñòíîãî èñïîëüçîâàíèÿ ñåêðåòà, äîáàâèâ îãðàíè÷åíèå, ÷òîáû 20 ÷åëîâåê ìîãëè ñîáðàòüñÿ âìåñòå è *ïîìåøàòü* îñòàëüíûì, íåçàâèñèìî îò èõ ÷èñëà, âîññòàíîâèòü ñåêðåò? Îêàçûâàåòñÿ, ÷òî äà [153].

Ìàòåìàòèêà äîñòàòî÷íî ñëîæíà, íî îñíîâíàÿ èäåÿ â òîì, ÷òî êàæäûé ïîëó÷àåò äâå ÷àñòè: ÷àñòü "äà" è ÷àñòü "íåò". Êîãäà ïðèõîäèò âðåìÿ âîññòàíîâèòü ñåêðåò, ëþäè ïðåäîñòàâëÿþò îäíó èç ñâîèõ ÷àñòåé. Êàêóþ êîíêðåòíî çàâèñèò îò òîãî, õîòÿò ëè îíè, ÷òîáû ñåêðåò áûë ðàñêðûò. Åñëè ïðåäîñòàâëåíî *m* èëè áîëüøå äîëåé "äà" è ìåíüøå ÷åì *n* äîëåé "íåò", òî ñåêðåò ìîæåò áûòü âîññòàíîâëåí. Â ïðîòèâíîì ñëó÷àå, ýòî íåâîçìîæíî.

Êîíå÷íî æå, íè÷òî íå ìåøàåò äîñòàòî÷íîìó ÷èñëó ëþäåé "äà" îòîéòè â óãîëîê, óåäèíèâøèñü îò ëþäåé "íåò" (åñëè îíè çíàþò, êòî åñòü êòî) è âîññòàíîâèòü ñåêðåò. Íî ïðè óñëîâèè, ÷òî âñå ïåðåäàþò ñâîè ÷àñòè â öåíòðàëüíûé êîìïüþòåð ýòà ñõåìà áóäåò ðàáîòàòü.

Ñîâìåñòíîå èñïîëüçîâàíèå ñåêðåòà ñ âû÷åðêèâàíèåì èç ñïèñêà

Âû ñîçäàëè ñèñòåìó ñîâìåñòíîãî èñïîëüçîâàíèÿ ñåêðåòà è òåïåðü õîòèòå çàñòðàõîâàòü îäíîãî èç âëàäåëüöåâ ÷àñòè ñåêðåòà. Âû ìîãëè áû ñîçäàòü íîâóþ ñõåìó, èñêëþ÷èâ ýòîãî íåñ÷àñòíîãî, íî âðåìÿ ïîäæèìàåò. Äëÿ ïîäîáíîé ñèòóàöèè ñóùåñòâóþò ñïîñîáû êîïèðîâàíèÿ. Îíè ïîçâîëÿþò àêòèâèçèðîâàòü íîâóþ ñõåìó ñîâìåñòíîãî èñïîëüçîâàíèÿ ñåêðåòà ñðàçó æå ïîñëå òîãî, êàê âû ïåðåñòàëè äîâåðÿòü îäíîìó èç ó÷àñòíèêîâ [1004].

3.8 Êðèïòîãðàôè÷åñêàÿ çàùèòà áàç äàííûõ

Áàçà äàííûõ ÷ëåíîâ îðãàíèçàöèè - ýòî âåñüìà âàæíàÿ âåùü. Ñ îäíîé ñòîðîíû âû õîòèòå ïðåäîñòàâèòü ê íåé äîñòóï âñåì ÷ëåíàì, æåëàÿ, ÷òîáû îíè îáùàëèñü äðóã ñ äðóãîì, îáìåíèâàëèñü èäåÿìè è äåëèëèñü äðóã ñ äðóãîì áóòåðáðîäàìè. Ñ äðóãîé ñòîðîíû, åñëè âû ïóñòèòå â âàøó áàçó äàííûõ êîãî óãîäíî, ñâåäåíèÿ íåèçáåæíî ïîïàäóò â ðóêè íàäîåäëèâûõ òîðãîâûõ àãåíòîâ è äîêó÷ëèâûõ ïîñòàâùèêîâ õëàìà ïî ïî÷òå.

Êðèïòîãðàôèÿ ìîæåò îáëåã÷èòü ýòó ïðîáëåìó. Ìîæíî çàøèôðîâàòü áàçó äàííûõ òàê, ÷òîáû ïîëó÷èòü àäðåñ îäíîãî ÷åëîâåêà áûëî ëåãêî, à èçâëå÷ü ñïèñîê ïî÷òîâûõ àäðåñîâ âñåõ ÷ëåíîâ - òðóäíî.

Ñõåìà, ïðåäëîæåííàÿ â [550, 549], ïðÿìîëèíåéíà. Âûáåðèòå îäíîíàïðàâëåííóþ õýø-ôóíêöèþ è ñèììåòðè÷íûé àëãîðèòì øèôðîâàíèÿ. Ó êàæäîé çàïèñè â áàçå äàííûõ äâà ïîëÿ. Èíäåêñíûì ïîëåì ÿâëÿåòñÿ ôàìèëèÿ ÷ëåíà, è èìåííî îíî îáðàáàòûâàåòñÿ îäíîíàïðàâëåííîé õýø-ôóíêöèåé. Ïîëå äàííûõ, â êîòîðîì õðàíèòñÿ ïîëíîå èìÿ è àäðåñ ÷ëåíà, øèôðóåòñÿ ñ ïîìîùüþ èñïîëüçóåìîé â êà÷åñòâå êëþ÷à ôàìèëèè. Åñëè âû íå çíàåòå ôàìèëèè, âû íèêîãäà íå ñìîæåòå ðàñøèôðîâàòü ïîëÿ äàííûõ.

Ïîèñê ïî êîíêðåòíîé ôàìèëèè ïðîñò. Ñíà÷àëà õýøèðóåòñÿ ôàìèëèÿ, è âûïîëíÿåòñÿ ïîèñê çíà÷åíèÿ õýø-ôóíêöèè â áàçå äàííûõ. Íàëè÷èå íåñêîëüêèõ ñîâïàäåíèé îçíà÷àåò, ÷òî áàçà äàííûõ ñîäåðæèò èíôîðìàöèþ î íåñêîëüêèõ ëþäÿõ ñ òàêîé ôàìèëèåé.

Â [550] àâòîðû èñïîëüçóþò ýòó ñèñòåìó äëÿ çàùèòû ñëîâàðÿ èç 6000 èñïàíñêèõ ñëîâ. Îíè ñîîáùàþò î òîì, ÷òî ïîòåðÿ ïðîèçâîäèòåëüíîñòè, âûçâàííàÿ øèôðîâàíèåì, ìèíèìàëüíà. Â áîëåå ñëîæíîé ñõåìå [549] èñïîëüçóåòñÿ ïîèñê ïî íåñêîëüêèì èíäåêñàì, íî èäåÿ îñòàåòñÿ òîé æå. Îñíîâíàÿ ïðîáëåìà, ñâÿçàííàÿ ñ ýòîé ñèñòåìîé, ñîñòîèò â òîì, ÷òî âû íå ñìîæåòå íàéòè ÷åëîâåêà, íå çíàÿ, êàê ïèøåòñÿ åãî ôàìèëèÿ. Ìîæíî ïîïðîáîâàòü íåñêîëüêî âàðèàíòîâ, ïîêà íå áóäåò íàéäåí ïðàâèëüíûé, íî íåóäîáíî ïåðåáèðàòü âñåõ, ÷üè ôàìèëèè íà÷èíàþòñÿ íà "Sch" ïðè ïîèñêå "Schneier."

Ýòà çàùèòà íåñîâåðøåííà. Î÷åíü íàñòîé÷èâûé ñòðàõîâîé àãåíò âîññòàíîâèò áàçó äàííûõ ÷ëåíîâ îðãàíèçàöèè ñ ïîìîùüþ ãðóáîãî âçëîìà, ïåðåáèðàÿ âñå âîçìîæíûå ôàìèëèè. Åñëè ó íåãî åñòü òåëåôîííàÿ áàçà äàííûõ, îí ìîæåò èñïîëüçîâàòü èìåþùèéñÿ â íåé ñïèñîê ôàìèëèé. Ýòî ïåðåæåâûâàíèå íîìåðîâ ìîæåò çàíÿòü íåñêîëüêî

íåääåëü, íî äåëî áóäåò ñäåëàíî. Òåì íå ìåíåå òàêàÿ ñõåìà óñëîæíèò ðàáîòó âçëîìùèêà (â ìèðå ïðîäàæå âñÿêîé ÷åïóõè ïî ïî÷òå "óñëîæíèò" áûñòðî ïðåâðàùàòñÿ â "ñäåëàåò ñëèøêîì äîðîãîé". Äðóãîé ïîäõîä, ïðåäëîæåííûé â [185], ïðåäëàãàåò íàáëþäàòü ñòàòèñòèêó ïî øèôðîâàííûì äàííûì.

Ãëàâà 4
Ïðîìåæóòî÷íûå ïðîòîêîëû

4.1 Ñëóæáû ìåòîê âðåìåíè

Âî ìíîãèõ ñèòóàöèÿõ ëþäÿì íóæíî óáåäèòüñÿ, ÷òî îïðåäåëåííûé äîêóìåíò óæå ñóùåñòâîâàë â îïðåäåëåííûé ìîìåíò âðåìåíè. Ïðèìåðîì ÿâëÿåòñÿ ñïîð îá àâòîðñêèõ ïðàâàõ èëè ïàòåíòå. Äåëî âûãðûâàåò ñòîðîíà, êîòîðàÿ ïðåäñòàâèò áîëåå ðàííþþ êîïèþ ñïîðíîé ðàáîòû. Áóìàæíûå äîêóìåíòû çàâåðÿþòñÿ íîòàðèóñíàì è õðàíÿòñÿ ó þðèñòîâ. Åñëè âîçíèêàåò ñïîð, íîòàðèóñ èëè þðèñò ñâèäåòåëüñòâóåò, ÷òî ïèñüìî ñóùåñòâîâàëî â îïðåäåëåííóþ äàòó. Ñ ïîìîùüþ ýëåêòðîííîãî äîêóìåíòà ìîæíî ñäåëàòü òî æå ñàìîå.

Â öèôðîâîì ìèðå âñå ãîðàçäî ñëîæíåå. Íåò ñïîñîáîâ îáíàðóæèòü ïîääåëêè ýëåêòðîííîãî äîêóìåíòà. Åãî ìîæíî áåñêîíå÷íî êîïèðîâàòü è èçìåíÿòü, íå îñòàâëÿÿ íèêàêèõ ñëåäîâ. Íåñìîòðÿ è èçìåíèòü âðåìÿ ñîçäàíèÿ êîìïüþòåðíîãî ôàéëà. Íèêòî íå ìîæåò âçãëÿíóòü íà äîêóìåíò è ñ ïîëíîé óâåðåííîñòüþ ñêàçàòü: "Äà, ýòîò äîêóìåíò áûë ñîçäàí ðàíüøå 4 íîÿáðÿ 1952 ãîäà"

Ýòîé ïðîáëåìîé çàäàëèñü Ñòþàðò Õàáåð (Stuart Haber) è Â. Ñêîòò Ñòîðíåòòà (W. Scott Stornetta) èç Bellcore [682, 683, 92]. È ì ïîðåáîâàëèñü ïðîòîêîë öèôðîâûõ ìåòîê âðåìåíè ñî ñëåäóþ ùèì ñâîéñòâàì:

— Ì åòêà âðåìåíè äîëæíà ñóùåñòâîâàòü ñàìà ïî ñåáå, íåçàâèñèì îò ôèçè÷åñêîé ñðåäû, èñïîëüçóåìîé äëÿ åå õðàíåíèÿ.

— Äîëæíî áûòü íåâîçìîæíî òàéíî èçìåíèòü íè åäèíîãî áèòà äîêóìåíòà.

— Äîëæíî áûòü íåâîçìîæíî çàäàòü äëÿ äîêóìåíòà ìåòêó âðåìåíè, îòëè÷íîãî îò òåêóùåãî.

Ðåøåíèå ñ ïîñðåäíèêîì

Â ýòîì ïðîòîêîëå ó÷àñòâóþò Òðåíò, îáëàäàþùèé íàäåæíîé ñëóæáîé âðåìåíè, è Àëèñà, êîòîðàÿ õî÷åò çàäàòü ìåòêó âðåìåíè äëÿ äîêóìåíòà.

(1) Àëèñà ïåðåäàåò êîïèþ äîêóìåíòà Òðåíòó.

(2) Òðåíò çàïèñûâàåò âðåìÿ è äàòó ïîëó÷åíèÿ äîêóìåíòà, îñòàâëÿÿ ó ñåáÿ êîïèþ äëÿ áåçîïàñíîãî õðàíåíèÿ.

Òåïåðü, åñëè êòî-íèáóäü óñîìíèòñÿ â çàÿâëåííîì Àëèñîé âðåìåíè ñîçäàíèÿ äîêóìåíòà, òî Àëèñà ïðîñòî íóæíî îáðàòèòüñÿ ê Òðåíòó. Î í ïðåäîñòàâèò ñâîþ êîïèþ äîêóìåíòà è ïîäòâåðäèò, ÷òî îí ïîëó÷èë äîêóìåíò â óêàçàííûé äåíü è ÷àñ.

Ýòîò ïðîòîêîë ðàáîòàåò, íî åñòü ðÿä î÷åâèäíûõ ïðîáëåì. Âî ïåðâûõ, íåâîçìîæíî ñîõðàíèòü òàéíó - Àëèñà äîëæíà ïðåäîñòàâèòü êîïèþ äîêóìåíòà Òðåíòó. Êòî-òî, ïîäñëóøèâàþùèé ëèíèþ ñâÿçè, ñìîæåò ïðî÷åñòü äîêóìåíò. Î íà ìîæåò çàøèôðîâàòü äîêóìåíò ïðè ïåðåäà÷å, íî âåäü îí äîëæåí áóäåò ðàíèòüñÿ â áàçå äàííûõ Òðåíòà. Íàñêîëüêî ýòà áàçà áåçîïàñíà?

Âî âòîðûõ, ñàìîé áàçå äàííûõ ïðèäåòñÿ áûòü î÷åíü áîëüøîé. Âåëèêè áóäóò òðåáîâàíèÿ è ê ïðîïóñêíîé ñïîñîáíîñòè ëèíèè ñâÿçè.

Òðåòüÿ ïðîáëåìà ñâÿçàíà ñ âîçìîæíûìè îøèáêàìè. Îøèáêè ïðè ïåðåäà÷å èëè ýëåêòðîìàãíèòíàÿ áîìáà, âçðûâàíàÿ ãäå-òî â öåíòðàëüíîì êîìïüþòåðå Òðåíòà ìîãóò ïîëíîñòüþ ñâåñòè íà íåò çàÿâëåíèå Àëèñû î ìåòêå âðåìåíè.

È â ÷åòâåðòûõ, ìîæåò îêàçàòüñÿ íåâîçìîæíûì íàéòè òàêîãî ÷åñòíîãî Òðåíòà äëÿ âåäåíèÿ ñëóæáû ìåòîê âðåìåíè. Ì îæåò áûòü, Àëèñà èñïîëüçóåò ìåòêó âðåìåíè Áîáà. Íè÷òî íå îñòàíîâèò Àëèñó è Áîáà îò ñãîâîðà è ïîìåòêè äîêóìåíòà òåì âðåìåíåì, êîòîðîå èì óæíî.

Óëó÷øåííûå ðåøåíèå ñ ïîñðåäíèêîì

Áîëüøèíñòâî ýòèõ ïðîáëåì ëåãêî ñíèìàþòñÿ ïðè èñïîëüçîâàíèè îäíîíàïðàâëåííîé õýø-ôóíêöèè è öèôðîâûõ ïîäïèñåé:

(1) Àëèñà âû÷èñëÿåò çíà÷åíèå îäíîíàïðàâëåííîé õýø-ôóíêöèè äëÿ äîêóìåíòà.

(2) Àëèñà ïåðåäàåò ýòî çíà÷åíèå Òðåíòó.

(3) Òðåíò äîáàâëÿåò âðåìÿ è äàòó ïîëó÷åíèÿ ýòîãî çíà÷åíèÿ è çàòåì ïîäïèñûâàåò ðåçóëüòàò öèôðîâîé ïîäïèñüþ.

(4) Òðåíò îòïðàâëÿåò ïîäïèñàííîå çíà÷åíèå õýø-ôóíêöèè âìåñòå ñ ìåòêîé âðåìåíè Àëèñå.

Ýòî ðåøåíèå âñå ïðîáëåìû, êðîìå ïîñëåäíåé. Àëèñå áîëüøå íå íóæíî áåñïîêîèòüñÿ î ðàñõîäàõ ñîâðåìåíè

äîêóìåíòà, èñïîëüçîâàíèå çíà÷åíèÿ õýø-ôóíêöèè âïîëíå äîñòàòî÷íî. Òðåíòó áîëüøå íå íóæíî õðàíèòü êîïèè äîêóìåíòîâ (è äàæå çíà÷åíèÿ õýø-ôóíêöèè), ïîýòîìó ñíèìàþòñÿ ïðîáëåìû áåçîïàñíîñòè è îáúåìà ñîõðàíÿåìûõ äàííûõ (ïîìíèòå, ó îäíîíàïðàâëåííûõ õýø-ôóíêöèé íåò êëþ÷à). Àëèñà ìîæåò íåìåäëåííî ïðîâåðèòü ïîäïèñàííóþ ìåòêó âðåìåíè, ïîëó÷åííóþ íà ýòàïå (4), è íåìåäëåííî îáíàðóæèòü ëþáûå îøèáêè ïåðåäà÷è. Åäèíñòâåííîé îñòàâøåéñÿ ïðîáëåìîé îñòàåòñÿ ñãîâîð Àëèñû è Òðåíòà ñ öåëüþ ñîçäàíèÿ ïîääåëüíîé ìåòêè âðåìåíè.

Ïðîòîêîë ñâÿçè

Îäíèì èç ïóòåé ðåøåíèÿ ýòîé ïðîáëåìû ÿâëÿåòñÿ óñòàíîâëåíèå ñâÿçè ìåæäó ìåòêîé âðåìåíè Àëèñû è ìåòêàìè âðåìåíè, ðàíåå ñîçäàííûìè Òðåíòîì. Âåñüìà âåðîÿòíî, ÷òî ýòè ìåòêè áûëè ñîçäàíû íå äëÿ Àëèñû, à äëÿ äðóãèõ ëþäåé. Òàê êàê ïîðÿäîê, â êîòîðîì Òðåíò ïîëó÷àåò ðàçëè÷íûå çàïðîñû î ìåòêàõ âðåìåíè íå ìîæåò áûòü èçâåñòåí çàðàíåå, ïåðåä ìåòêîé âðåìåíè äëÿ Àëèñû äîëæíà áûëà ïîÿâèòüñÿ äðóãàÿ ìåòêà âðåìåíè. È òàê êàê çàïðîñ, ïðèøåäøèé ïîçæå, ñâÿçàí ñ ìåòêîé âðåìåíè Àëèñû, òî åå ìåòêà äîëæíà áûëà ïîÿâèòüñÿ ðàíüøå. Ýòè äâå ìåòêè ñîäåðæàò ìåæäó ñîáîé çàïðîñ Àëèñû êàê áóäòî â ñýíäâè÷å.

Åñëè *À* - ýòî èìÿ Àëèñû, H_n - çíà÷åíèå õýø-ôóíêöèè, äëÿ êîòîðîãî Àëèñà õî÷åò çàôèêñèðîâàòü âðåìÿ, à T_{n-1} - ïðåäûäóùàÿ ìåòêà âðåìåíè, òî ïðîòîêîë èìååò ñëåäóþùèé âèä:

(1) Àëèñà ïîñûëàåò Òðåíòó H_n è *À*.

(2) Òðåíò ïîñûëàåò Àëèñå îáðàòíî:

$T_n=S_K(n,A,H_n,T_n,I_{n-1},H_{n-1},T_{n-1},L_n)$

ãäå ñîñòîèò L_n - ýòî èíôîðìàöèÿ î ñëåäóþùåé õýøèðîâàííîé ñâÿçè:

$L_n =H(I_{n-1},H_{n-1},T_{n-1},L_{n-1})$

S_K óêàçûâàåò, ÷òî ñîîáùåíèå ïîäïèñàíî îòêðûòûì êëþ÷îì Òðåíòà. Èìÿ Àëèñû îïðåäåëÿåò åå êàê îòïðàâèòåëÿ çàïðîñà. Ïàðàìåòð *n* óêàçûâàåò ïîñëåäîâàòåëüíîñòü çàïðîñîâ. Ýòî *n*-àÿ ìåòêà âðåìåíè, êîòîðóþ ñîçäàë Òðåíò. Ïàðàìåòð T_n - ýòî âðåìÿ. Äîïîëíèòåëüíî èñïîëüçóåòñÿ èíôîðìàöèÿ îá èäåíòèôèêàòîðå, îðèãèíàëüíîãî çíà÷åíèÿ õýø-ôóíêöèè, âðåìåíè è õýøèðîâàííîé ìåòêà ïðåäûäóùåãî äîêóìåíòà, ïîìå÷åííîãî Òðåíòîì.

(3) Êîãäà Òðåíò ïîìå÷àåò ñëåäóþùèé äîêóìåíò, îí ïîñûëàåò Àëèñå èäåíòèôèêàòîð îòïðàâèòåëÿ ýòîãî äîêóìåíòà: I_{n-1}.

Åñëè êòî-òî îñïàðèâàåò ìåòêó âðåìåíè Àëèñû, åé íàäî òîëüêî ñâÿçàòüñÿ ñ îòïðàâèòåëÿìè ïðåäûäóùåãî è ñëåäóþùåãî äîêóìåíòîâ: I_{n-1} í I_{n+1}. Åñëè è èõ ñâèäåòåëüñòâî ïîä âîïðîñîì, ìîæíî îáðàòèòüñÿ ê àâòîðàì äîêóìåíòîâ I_{n-1} í I_{n+1} è ò.ä. Ëþáîé ìîæåò ïîêàçàòü, ÷òî åãî äîêóìåíò áûë ïîìå÷åí ïîñëå îäíîãî äîêóìåíòà è ïåðåä äðóãèì.

Ýòîò ïðîòîêîë ìåøàåò Àëèñå è Òðåíòó äîãîâîðèòüñÿ è ñîçäàòü äîêóìåíò ñ âðåìåíåì ñîçäàíèÿ, îòëè÷íûì îò âðåìåíè ñîçäàíèÿ íàñòîÿùåãî äîêóìåíòà. Òðåíò íå ìîæåò èçìåíèòü äàòó äîêóìåíòà Àëèñû íà áîëåå ðàííþþ, òàê êàê äëÿ ýòîãî íóæíî çíàòü çàðàíåå, äëÿ êàêîãî äîêóìåíòà ïåðåä äàííûì áóäåò ïðîñòàâëÿòüñÿ ìåòêà âðåìåíè. Äàæå åñëè îí ñìîæåò ïîääåëàòü ïðåäûäóùèé äîêóìåíò, åìó ïðèäåòñÿ çíàòü, êàêîé äîêóìåíò ïðåäøåñòâîâàë ïðåäûäóùåìó è òàê äàëåå. Òðåíò íå ìîæåò èçìåíèòü äàòó äîêóìåíòà Àëèñû è íà áîëåå ïîçäíþþ, ïîòîìó ÷òî ìåòêà âðåìåíè äîëæíà áûòü âñòàâëåíà ïåðåä ìåòêîé âðåìåíè äîêóìåíòà, çàâåðÿåìîãî ñðàçó æå ïîñëå äàííîãî, à ýòîò äîêóìåíò óæå ñóùåñòâóåò. Åäèíñòâåííûé âîçìîæíûé ñïîñîá ñëîìàòü ýòó ñõåìó - ýòî ââåñòè ôèêòèâíóþ öåïî÷êó äîêóìåíòîâ ïåðåä è ïîñëå äîêóìåíòà Àëèñû, äîñòàòî÷íî äëèííóþ, ÷òîáû ëèøèòü òåðïåíèÿ òîãî, êòî ïðîâåðÿåò ìåòêó âðåìåíè äîêóìåíòà Àëèñû.

Ðàñïðåäåëåííûé ïðîòîêîë

Ëþäè óìèðàþò, ìåòêè âðåìåíè òåðÿþòñÿ. Ìåæäó ïîìåòêîé äîêóìåíòà è åãî îñïàðèâàíèåì ìîæåò ïðîèçîéòè ìíîãîå, ÷òî ïîìåøàåò Àëèñå ïîëó÷èòü êîïèþ ìåòêè âðåìåíè I_{n-1}. Ýòà ïðîáëåìà ìîæåò áûòü ÷àñòè÷íî ñíÿòà âñòàâêîé ìåòîê âðåìåíè ïðåäûäóùèõ 10 ÷åëîâåê â ìåòêó Àëèñû è ïîñëåäóþùåé ïåðåäà÷å Àëèñå èìåí ñëåäóþùèõ 10 ÷åëîâåê. Òàê ó Àëèñû ïîÿâèòñÿ ãîðàçäî áîëüøå âîçìîæíîñòåé íàéòè ëþäåé, âñå åùå õðàíÿùèõ ñâîè ìåòêè âðåìåíè.

Ðàçâèâàÿ ýòó èäåþ, ñëåäóþùèé ïðîòîêîë ïîçâîëÿåò îáîéòèñü è áåç Òðåíòà:

(1) Èñïîëüçóÿ â êà÷åñòâå âõîäà H_n, Àëèñà ãåíåðèðóåò ïîñëåäîâàòåëüíîñòü ñëó÷àéíûõ ÷èñåë ñ ïîìîùüþ êðèïòîãðàôè÷åñêè áåçîïàñíîãî ãåíåðàòîðà ñëó÷àéíûõ ÷èñåë.

$V_1, V_2, V_3, . . . V_k$

(2) Àëèñà ðàññìàòðèâàåò êàæäîå èç ýòèõ ÷èñåë êàê èäåíòèôèêàòîð, *I*, äðóãîãî ÷åëîâåêà è ïîñûëàåò êàæäîìó èç ýòèõ ëþäåé H_n.

(3) Êàæäûé èç íèõ äîáàâëÿåò âðåìÿ è äàòó ê çíà÷åíèþ õýø-ôóíêöèè, ïîäïèñûâàåò ðåçóëüòàò è îòïðàâëÿåò åãî

îáðàòíî Àëèñå.

(4) Àëèñà ñîáèðàåò è õðàíèò âñå ïîäïèñè êàê ìåòêó âðåìåíè.

Êðèïòîãðàôè÷åñêè áåçîïàñíûé ãåíåðàòîð ñëó÷àéíûõ ÷èñåë, èñïîëüçóåìûé íà ýòàïå (1), ïîçâîëÿåò Àëèñå èçáåæàòü ïðåäíàìåðåííîãî âûáîðà êîððóìïèðîâàííûõ *I* â êà÷åñòâå ñâèäåòåëåé. Äàæå åñëè îíà ñäåëàåò ïðîñòåéøèå èçìåíåíèÿ â ñâîåì äîêóìåíòå, ïûòàÿñü ñîçäàòü íàáîð êîððóìïèðîâàííûõ *I*, åå øàíñû äîáèòüñÿ ýòîãî ïðåíåáðåæèìî ìàëû. Õýø-ôóíêöèÿ ðàíäîìèçèðóåò çíà÷åíèÿ, è Àëèñà íå ìîæåò íà íèõ âîçäåéñòâîâàòü.

Ýòîò ïðîòîêîë ðàáîòàåò, ïîòîìó ÷òî ïîääåëàòü ìåòêó âðåìåíè Àëèñà ìîæåò, òîëüêî äîãîâîðèâøèñü î ñîòðóäíè÷åñòâå ñî âñåìè *k* ëþäüìè. Òàê êàê íà ýòàïå (1) îíà âûáèðàëà èõ ñëó÷àéíûì îáðàçîì, âåðîÿòíîñòü ýòîãî î÷åíü íèçêà. ×åì êîððóìïèðîâàííåå îáùåñòâî, òåì áîëüøå äîëæíî áûòü ÷èñëî *k*.

Êðîìå òîãî, äîëæåí èñïîëüçîâàòüñÿ íåêîòîðûé ìåõàíèçì, ó÷èòûâàþùèé òî, ÷òî ëþäè íå ñìîãóò âîâðåìÿ âîçâðàòèòü ìåòêó âðåìåíè. Âñå, ÷òî íóæíî äëÿ ïðàâèëüíîé ìåòêè âðåìåíè - ýòî íåêîòîðîå ïîäìíîæåñòâî *k*. Äåòàëè çàâèñÿò îò ðåàëèçàöèè.

Äàëüíåéøàÿ ðàáîòà

Äàëüíåéøèå óëó÷øåíèÿ ïðîòîêîëîâ ìåòêè âðåìåíè îïèñàíû â [92]. Àâòîðû èñïîëüçóþò äâîè÷íûå äåðåâüÿ äëÿ óâåëè÷åíèÿ êîëè÷åñòâà ìåòîê âðåìåíè, çàâèñÿùèõ îò äàííîé ìåòêè, óìåíüøàÿ âåðîÿòíîñòü ñîçäàíèÿ öåïî÷êè ôàëüøèâûõ ìåòîê âðåìåíè. Îíè òàêæå ðåêîìåíäóþò ïóáëèêîâàòü ñïèñîê çíà÷åíèé õýø-ôóíêöèé çà ïðîøåäøèé äåíü â íåêîòîðîì îáùåäîñòóïíîì èñòî÷íèêå, íàïðèìåð ãàçåòå. Ýòî ðàáîòàåò êàê îòïðàâêà çíà÷åíèÿ õýø-ôóíêöèè ñëó÷àéíûì ëþäÿì â ðàñïðåäåëåííîì ïðîòîêîëå. Äåéñòâèòåëüíî, ìåòêà âðåìåíè ïîÿâëÿåòñÿ â êàæäîì íîìåðå âîñêðåñíîé *Íüþ-Éîðê Òàéìñ* ñ 1992 ãîäà.

Ýòè ïðîòîêîëû ìåòîê âðåìåíè çàïàòåíòîâàíû [684, 685, 686]. Ïàòåíòû ïðèíàäëåæàò äî÷åðíåé êîìïàíèè Bellcore, íàçâàííîé Surety Technologies, êîòîðàÿ ïðîäàåò Ñèñòåìó öèôðîâîãî íîòàðèàòà, ïîääåðæèâàþùóþ ýòè ïðîòîêîëû. Â ïåðâîé âåðñèè êëèåíòû ïîñûëàëè çàïðîñû î "çàâåðåíèè" íà öåíòðàëüíûé êîîðäèíèðóþùèé öåíòð. Ñëåäóÿ ìåòîäèêå Ìåðêëà ïî èñïîëüçîâàíèþ õýø-ôóíêöèé äëÿ ïîñòðîåíèÿ äåðåâüåâ [1066], ñåðâåð ñòðîèò äåðåâî çíà÷åíèé õýø-ôóíêöèè, ëèñòüÿ êîòîðîãî ïðåäñòàâëÿþò ñîáîé âñå çàïðîñû, ïîëó÷åííûå â òå÷åíèå äàííîé ñåêóíäû, è ïîñûëàåò êàæäîìó àâòîðó çàïðîñà ñïèñîê çíà÷åíèé õýø-ôóíêöèè, îïèñûâàþùèé ïóòü îò åãî ëèñòà äî êîðíÿ. Êëèåíòñêàÿ ÷àñòü ïðîãðàììíîãî îáåñïå÷åíèÿ ñîõðàíÿåò ýòîò ñïèñîê è ìîæåò âûäàòü "ñåðòèôèêàò" Öèôðîâîãî íîòàðèàòà äëÿ ëþáîãî ôàéëà, êîòîðûé áûë ñåðòèôèöèðîâàí. Ïîñëåäîâàòåëüíîñòü êîðíåé ýòèõ äåðåâüåâ îáðàçóåò "Çàïèñü óíèâåðñàëüíîãî ïîäòâåðæäåíèÿ" ("Universal Validation Record"), êîòîðàÿ áóäåò äîñòóïíà â ýëåêòðîííîì âèäå âî ìíîãèõ õðàíèëèùàõ (è òàêæå âûïóùåíà íà CD-ROM). Êëèåíòñêàÿ ÷àñòü òàêæå ñîäåðæèò ôóíêöèþ "ïîäòâåðæäåíèÿ", ïîçâîëÿþùóþ ïîëüçîâàòåëþ ïðîâåðèòü, áûë ëè çàâåðåíà èìåííî òåêóùàÿ ôîðìà ôàéëà (çàïðîñèâ èç õðàíèëèùà êîðåíü ñîîòâåòñòâóþùåãî äåðåâà è ñðàâíèâ åãî ñî çíà÷åíèåì õýø-ôóíêöèè, ñîîòâåòñòâóþùèì îáðàçîì ðàññ÷èòàííûì äëÿ ôàéëà, è ñåðòèôèêàòîì). Çà äàëüíåéøåé èíôîðìàöèåé îáðàùàéòåñü â Surety Technologies, 1 Main St., Chatham, NJ, 07928; (201) 701-0600; Fax: (201) 701-0601.

4.2 Ïîäñîçíàòåëüíûé êàíàë

Àëèñà è Áîá áûëè àðåñòîâàíû è îòïðàâëåíû â òþðüìó, îí - â ìóæñêóþ, à îíà - â æåíñêóþ. Óîëòåð, íàäçèðàòåëü, ðàçðåøàåò Àëèñå è Áîáó îáìåíèâàòüñÿ ñîîáùåíèÿìè, íî îí íå ðàçðåøàåò øèôðîâàòü ñîîáùåíèÿ. Óîëòåð ñ÷èòàåò, ÷òî îíè ïëàíèðóþò áåãñòâî, ïîýòîìó îí õî÷åò ÷èòàòü âñå, ÷òî îíè ïèøóò.

Óîëòåð íàäååòñÿ òàêæå ñóìåòü îáìàíóòü Àëèñó èëè Áîáà. Îí õî÷åò, ÷òîáû îäèí èç íèõ ïîñ÷èòàë ïðèíÿòîå èì ëîæíîå ñîîáùåíèå íàñòîÿùèì. Àëèñà è Áîá ìèðÿòñÿ ñ ðèñêîì âîçìîæíîãî îáìàíà, èíà÷å îíè âîîáùå íå ñìîãóò îáùàòüñÿ, íî èì íóæíî ñîãëàñîâàòü ñâîè ïëàíû. Äëÿ ýòîãî èì íåîáõîäèìî îáìàíóòü íàäçèðàòåëÿ è íàéòè ñïîñîá ïåðåäàâàòü ñåêðåòíóþ èíôîðìàöèþ. Èì íóæíî ñîçäàòü ïîäñîçíàòåëüíûé êàíàë, ñêðûòûé êàíàë ñâÿçè â îòêðûòûõ ñîîáùåíèÿõ, õîòÿ ñîîáùåíèÿ ñàìè ïî ñåáå íå ñîäåðæàò ñåêðåòíîé èíôîðìàöèè. Ñ ïîìîùüþ îáìåíà ñîâåðøåííî áåçîáèäíûìè ïîäïèñàííûìè ñîîáùåíèÿìè îíè îáìåíÿþòñÿ ñåêðåòíîé èíôîðìàöèåé è îäóðà÷àò Óîëòåðà, äàæå åñëè îí ïðîñìàòðèâàåò âñå ñîîáùåíèÿ.

Ïðîñòûì ïîäñîçíàòåëüíûì êàíàëîì ìîæåò áûòü ÷èñëî ñëîâ â ïðåäëîæåíèè. Íå÷åòíîå ÷èñëî ñëîâ â ïðåäëîæåíèè ìîæåò ñîîòâåòñòâîâàòü "1", à ÷åòíîå ÷èñëî ñëîâ -"0". Òàê, ïîêà âû ÷èòàåòå ýòîò ñàìûé îáû÷íûé àáçàö, ÿ ïåðåäàë âàì ñîîáùåíèå "110". Ïðîáëåìà ýòîãî ìåòîäà â òîì, ÷òî îí ÿâëÿåòñÿ îáû÷íîé ñòåãàíîãðàôèåé (ñì. ðàçäåë 1.2), êëþ÷ íå èñïîëüçóåòñÿ è áåçîïàñíîñòü çàâèñèò îò ñåêðåòíîñòè àëãîðèòìà.

Ãóñòàâóñ Ñèììîíñ ïðèäóìàë èäåþ îðãàíèçàöèè ïîäñîçíàòåëüíîãî êàíàëà ñ ïîìîùüþ îáû÷íîãî àëãîðèòìà öèôðîâîé ïîäïèñè [1458, 1473]. Òàê êàê ïîäñîçíàòåëüíûå ñîîáùåíèÿ ñïðÿòàíû â òîì, ÷òî âûãëÿäèò íîðìàëüíûìè öèôðîâûìè ïîäïèñÿìè, ýòî ôîðìà ìàñêèðîâêè. Óîëòåð âèäèò, êàê ïîäïèñàííûå áåçîáèäíûå ñîîáùåíèÿ ïåðåäàþòñÿ òóäà è îáðàòíî, íî ðåàëüíàÿ ïåðåäàâàåìàÿ èíôîðìàöèÿ ïðîõîäèò íåçàìåòíî äëÿ íåãî ïî ïîäñîçíàòåëüíîìó êàíàëó. Â äåéñòâèòåëüíîñòè, àëãîðèòì ïîäñîçíàòåëüíîãî êàíàëà â ïîäïèñÿõ íå îòëè÷èì îò íîðìàëüíîãî àëãîðèòìà â ïîäïèñÿõ, ïî êðàéíåé ìåðå äëÿ Óîëòåðà. Åð íå òîëüêî íå ìîæåò ïðî÷èòàòü ñîîáùåíèå, ïåðåäàâàåìîå ïî ïîäñîçíàòåëüíîìó êàíàëó, íî ó íåãî âîîáùå íåò íè ìàëåéøåãî ïðåäñòàâëåíèÿ î ñóùåñòâîâàíèè òàêîãî

ñîîáùåíèÿ. Â îáùåì ñëó÷àå ïðîòîêîë âûãëÿäèò ïðèìåðíî òàê:

(1) Àëèñà ñîçäàåò áåçîáèäíîå ñîîáùåíèå, âñå ðàâíî êàêîå.

(2) Èñïîëüçóÿ îáùèé ñ Áîáîì êëþ÷, Àëèñà ïîäïèñûâàåò áåçîáèäíîå ñîîáùåíèå, ïðÿ÷à ñâîå ïîäîçíàòåëüíîå ñîîáùåíèå â ïîäïèñè. (Ýòî ñóòü ïîäîçíàòåëüíîãî ïðîòîêîëà, ñì. ðàçäåë 23.3).

(3) Àëèñà ïîñûëàåò ïîäïèñàííîå ñîîáùåíèå Áîáó ÷åðåç Óîëòåðà.

(4) Óîëòåð ÷èòàåò áåçîáèäíîå ñîîáùåíèå è ïðîâåðÿåò ïîäïèñü. Íå îáíàðóæèâ íè÷åãî ïîäîçðèòåëüíîãî, îí ïåðåäàåò ïîäïèñàííîå ñîîáùåíèå Áîáó.

(5) Áîá ïðîâåðÿåò ïîäïèñü ïîä áåçîáèäíûì ñîîáùåíèåì, óáåæäàÿñü, ÷òî ñîîáùåíèå ïîëó÷åíî îò Àëèñû.

(6) Áîá èãíîðèðóåò áåçîáèäíîå ñîîáùåíèå è, èñïîëüçóÿ îáùèé ñ Àëèñîé ñåêðåòíûé êëþ÷, èçãëåêàåò ïîäñîçíàòåëüíîå ñîîáùåíèå.

À ìîæåíè÷åñòâî? Óîëòåð íå âåðèò íèêîìó, è íèêòî íå âåðèò Óîëòåðó. Î í âñåãäà ìîæåò ïîìåøàòü ïðåäà÷å ñîîáùåíèé, íî ó íåãî íåò âîçìîæíîñòè ïîääåëàòü ñîîáùåíèå. Òàê êàê Óîëòåð íå ìîæåò ñîçäàòü ïîääåëêó íà ýòàïå (5). Óîëòåð íå ìîæåò ÷èòàòü ïîäñîçíàòåëüíûå ñîîáùåíèÿ - ó íåãî íåò íóæíîãî êëþ÷à. ×òî åùå âàæíåå, ó íåãî íåò íè ìàëåéøåãî ïðåäñòàâëåíèÿ, ÷òî ïîäñîçíàòåëüíûå ñîîáùåíèÿ ñóùåñòâóþò. Ïîäïèñàííûå ñîîáùåíèÿ, èñïîëüçóþùèå àëãîðèòì öèôðîâîé ïîäïèñè íà âëä íè÷åì íå îòëè÷àþòñÿ îò ïîäïèñàííûõ ñîîáùåíèé, ñîäåðæàùèõ ïîäñîçíàòåëüíûå ñîîáùåíèÿ â ïîäïèñè.

Áîëåå ïðîáëåìàòè÷åí îáìàí ñâîåãî ïàðòíåðà Àëèñîé èëè Áîáîì. Â íåêîòîðûõ ðåàëèçàöèÿõ ïîäñîçíàòåëüíîãî êàíàëà ñåêðåòíàÿ èíôîðìàöèÿ, íóæíàÿ Áîáó äëÿ ÷òåíèÿ ïîäñîçíàòåëüíîãî ñîîáùåíèÿ, ñîâïàäàåò ñ èíôîðìàöèåé, íóæíîé Àëèñå äëÿ ïîäïèñè áåçîáèäíîãî ñîîáùåíèÿ. Åñëè ýòî òàê, Áîá ìîæåò âû÷èñëèòü ñîîáùåíèÿ, âûäà èò çà ïîñëàííûå Àëèñîé, è Àëèñà íè÷åãî íå ñìîæåò ñ ýòèì ïîäåëàòü. Åñëè åé íåîáõîäèìî îòïðàâèòü åìó ïîäñîçíàòåëüíîå ñîîáùåíèå, îíà äîëæíà âåðèòü, ÷òî îí íå áóäåò ìîøåííè÷àòü ñ åå çàêðûòûì êëþ÷îì.

Â äóõàòè ðåàëèçàöèÿõ ïîäñîçíàòåëüíîãî êàíàëà òàêîé ïðîáëåìû íåò. Ñåêðåòíûé êëþ÷, îáùèé äëÿ Àëèñû è Áîáà, ïîçâîëÿåò Àëèñå îòïðàâëÿòü Áîáó ïîäñîçíàòåëüíûå ñîîáùåíèÿ, íî çâêðûòûé êëþ÷ Àëèñû íå ïåðåäàâàòñÿ, è Áîá íå ìîæåò ïîäïèñûâàòü åå ïîäïèñüþ. Àëèñå íå íóæíî âåðèòü, ÷òî Áîá íå áóäåò ìîøåííè÷àòü ñ åå çàêðûòûì êëþ÷îì.

Ïðèíóäèòåëüíàÿ ïîäñîçíàòåëüíîñòü êàíàëà

Íàèáîëåå î÷åâèäíûì ïðèìåíåíèåì ïîäñîçíàòåëüíîãî êàíàëà ÿâëÿåòñÿ øïèîíñêàÿ ñòðî÷êà. Åñëè êòî-òî ïîñûëàåò è ïðèíèìàåò ñîîáùåíèÿ, òî ïåðâàÿ÷à ñîîáùåíèé ïî ïîäñîçíàòåëüíîìó êàíàëó â ïîäïèñàííûõ äîêóìåíòàõ íå áóäåò âûçûâàòü ïîäîçðåíèé. Êîíå÷íî æå, âðàæåñêèå øïèîíû ìîãóò äåéſòâîâàòü òî æå ñàìîå.

Èñïîëüçóÿ ïîäñîçíàòåëüíûé êàíàë, Àëèñà ìîæåò, äàæå åñëè åé óãðîæàþò, áåçîïàñíî ïîäïèñàòü äîêóìåíò. Ïîäïèñûâàÿ äîêóìåíò, îíà ìîæåò âñòàâèòü ïîäñîçíàòåëüíîå ñîîáùåíèå, íàïèñàííîå "ß àðåñòîâàíà". Èíûå ïðèìåíåíèÿ íå òàê áðîñàþòñÿ â ãëàçà. Êîìïàíèÿ ìîæåò ïîäïèñàòü äîêóìåíò è âñòàâèòü ïîäñîçíàòåëüíûå ñîîáùåíèÿ äëÿ îòñëåæèâàíèÿ âðåìåíè äåíñòâèÿ äîêóìåíòà. Ïðàêòè÷åñêè ëþáîé ïðîãðàììà äëÿ ïîäïèñè äîêóìåíòîâ "ïîìåòèòü" ýëåêòðîííûå äåíüãè. Ìîøåííè÷åñêàÿ ïðîãðàììà äëÿ ïîäïèñè äîêóìåíòà ìîæåò èñïîëüçîâàòü ïîäñîçíàòåëüíûå ñîîáùåíèÿ â ñîçäàâàåìîõ ïîäïèñüõ äëÿ îõâàòèçàöèè óòå÷êè ñåêðåòíîé èíôîðìàöèè. Âîçìîæíîñòè áåñêîíå÷íû.

Ïîäïèñè, ñâîáîäíûå îò ïîäñîçíàòåëüíîãî êàíàëà

Àëèñà è Áîá îáìåíèâàþòñÿ ïîäïèñàííûìè ñîîáùåíèÿìè, îáåîâàðåâàÿ ñðîêè êîíöîâêè. Îíè èñïîëüçóþò ïðîòîêîë ïîäïèñè. Îäíàêî, ýòè ïðåäâîñõîä íà ñàìîì äåëå ìàñêèðóþò ø ïèîíñêóþ äåÿòåëüíîñòü Àëèñû è Áîáà. Èñïîëüçóÿ àëãîðèòì öèôðîâîé ïîäïèñè, îíè íå âîëíóþòñÿ î ïîäïèñûâàíèè ìûì äëÿ ñàìîãî èì ñîîáùåíèÿõ. Äëÿ îáìåíà ñåêðåòíîé èíôîðìàöèåé îíè èñïîëüçóþ ïîäñîçíàòåëüíûé êàíàë â ïîäïèñüõ ïîä äîêóìåíòàìè. Êîíöåïòóàëüíî âñå ïîäïèñè äîêóìåíòîâ ìîæíî ðàññìàòðèâàòü êàê ñîîáùåíèÿ, îòïðàâëåííûå Àëèñîé Áîáó. Ïîäïèñè, ñîâïàäàþùèå ïî ïîäñîçíàòåëüíîìó êàíàëó, ïîêàçûâàþò, ÷òî ñîîáùåíèå íå áûëî èçìåíåíî èç-çà øóìà èëè îøèáêè. Âîçìîæíîñòè áåñêîíå÷íû.

4.3 Íåîðèöàòåëüíûå öèôðîâûå ïîäïèñè

Îáû÷íûå öèôðîâûå ïîäïèñè ìîãóò áûòü òî÷íî ñêîïèðîâàíû. Èíîãäà ýòî ñâîéſòâî ïîëåçíî, íàïðèìåð, ïðè ðàñïðîñòðàíåíèè ïóáëè÷íûõ çàÿâëåíèé. Â äðóãîé ðàç ýòî ìîæåò îêàçàòüſÿ ïðîáëåìîé. Âîîáðàçèòå ëè÷íûå èëè äåëîâûå ïèſüìî, ïîäïèſàííîå öèôðîâîé ïîäïèſüþ. Åſëè ðàſſóſòðàſèâàåò ſ èſôîſìàöèþſÿ ìſſåſſòâ êſïèé ýòîſî äîêóſåíòà, êàæäàÿ èç êîòîðûõ ìîæåò áûòü ïðîâåðåíà êåì óãîäíî, òî ýòî ìîæåò ïðèâåſſòè ê çàſſåſſàòåſſûſſòâó èëè øàíòàæ. Ëó÷øèì ðåøåíèåì ÿâëÿåòſÿ öèôðîâàÿ ïîäïèſü, ïðàâèëüſſîſòü êſòîſîſ ſſåſſòâó äîêàçàſſ ſſîſó÷àſſëþ, ſſ êſòîſîàÿ íå ſſîçâſſèòſ ſſîſó÷àſſëþ ſſîêàçàòü òðåòüſſ ſòſðſſſſ ſſîſó÷åſſſſſ ſſſſáſſåſſſſ ſſſſáſſ ñſſãèàſſèÿ ëè-

öà, ïîäïèñàâøåãî ñîîáùåíèå.

Alice Software Company (Êîìïàíèÿ ïðîãðàììíîãî îáåñïå÷åíèÿ Àëèñû) ðàñïðîñòðàíÿåò ïðîäóêò DEW (Do-Everything-Word, Äåëàÿ ñî ñëîâîì ÷òî óãîäíî). Äëÿ ãàðàíòèè îòñóòñòâèÿ âèðóñîâ êàæäàÿ êîïèÿ ñîäåðæèò öèôðîâóþ ïîäïèñü. Îäíàêî, ñîçäàòåëè õîòÿ, ÷òîáû òîëüêî ëåãàëüíûå ïîêóïàòåëè ïðîäóêòà, à íå êîìïüþòåðíûå ïèðàòû ìîãëè ïðîâåðèòü ïîäïèñü. Â òî æå âðåìÿ, åñëè îáíàðóæèâàþòñÿ êîïèè DEW, ñîäåðæàùèå âèðóñ, ó Alice Software Company íå äîëæíî áûòü âîçìîæíîñòè îòîçâàòü ïðàâèëüíóþ ïîäïèñü.

Íåîòèöèàëüíûå ïîäïèñè [343,327] óäîáíû äëÿ ðåøåíèÿ ïîäîáíûõ çàäà÷. Êàê è îáû÷íàÿ öèôðîâàÿ ïîäïèñü, íåîòèöèàëüíàÿ öèôðîâàÿ ïîäïèñü çàâèñèò îò ïîäïèñàííîãî äîêóìåíòà è çàêðûòîãî êëþ÷à ÷åïî÷êè, ïîäïèñàâøåãî äîêóìåíò. Íî, â îòëè÷èå îò îáû÷íûõ öèôðîâûõ ïîäïèñåé, íåîòèöèàëüíàÿ ïîäïèñü íå ìîæåò áûòü ïðîâåðåíà áåç ðàçðåøåíèÿ ïîäïèñàâøåãî. Õîòÿ äëÿ ýòèõ ïîäïèñåé ìîæíî áûëî áû ïîäîáðàòü íàçâàíèå ïîëó÷åå, íàïðèìåð, "íåïðåäâàðèòåëüíûå ïîäïèñè", ñóùåñòâóþùåå íàçâàíèå îáñëîâëåíî òåì îáñòîÿòåëüñòâîì, ÷òî åñëè Àëèñå ïðèäåòñÿ ëèáî ïîäòâåðäèòü, ëèáî îòðèöàòü ïîäïèñü - ìîæåò áûòü â ñóäå - îíà íå ñìîæåò ëîæíî îòðèöàòü ñâîþ íåïîñðåäñòâåííóþ ïîäïèñü. Íåñìîòðÿ íà ñëîæíîñòü ìàòåìàòèêè îñíîâíàÿ èäåÿ ïðîñòà:

(1) Àëèñà ïðåäúÿâëÿåò Âîáó ïîäïèñü.

(2) Âîá ñîçäàåò ñëó÷àéíîå ÷èñëî è ïîñûëàåò åãî Àëèñå.

(3) Àëèñà âû÷èñëÿåò âû÷èñëåíèÿ, èñïîëüçóÿ ñëó÷àéíîå ÷èñëî è ñâîé çàêðûòûé êëþ÷, è ïîñûëàåò Âîáó ðåçóëüòàò. Àëèñà ìîæåò âû÷èñëèòü ýòè âû÷èñëåíèÿ òîëüêî, åñëè ïîäïèñü ïðàâèëüíà.

(4) Âîá ïðîâåðÿåò ýòî.

Òàêæå ñóùåñòâóåò äîïîëíèòåëüíûé ïðîòîêîë, ïîçâîëÿþùèé Àëèñå äîêàçàòü, ÷òî îíà íå ïîäïèñûâàëà äîêóìåíò, è íå äîïóñêàþùèé âîçìîæíîñòè ëîæíî îòêàçàòüñÿ îò ïîäïèñè.

Âîá íå ìîæåò ïîâðåäíîñòü è óâåäîìèòü Êýðîë, ÷òî ïîäïèñü Àëèñû ïðàâèëüíà, ïîòîìó ÷òî Êýðîë íå çíàåò, ÷òî ÷èñëà Âîáà ñëó÷àéíû. Îí ìîæåò ëåãêî áåç ïîìùè Àëèñû èçëîæèòü ïðîòîêîë íà áóìàãå è ïîñëàòü Êýðîë. Êýðîë ìîæåò óâîñòîâåðèòüñÿ â ïðàâèëüíîñòè ïîäïèñè Àëèñû òîëüêî, åñëè îíà ñàìà âûïîëíèò ýòîò ïðîòîêîë ñ Àëèñîé. Ñåé÷àñ êàæäîãî, ÷òî â ýòî ìåìîíåíò ñìûñëà, íî îí ïîÿâèòñÿ, êîãäà âû âçãëÿíåòå íà ìàòåìàòèêó ðàçäåëà 23.4.

Ýòî ðåøåíèå íå ñîâðåøåííî. Èâî Äåñìåòò è Ì îòè Þ íã (Moti Yung) ïîêàçàëè, ÷òî â íåêîòîðûõ ñëó÷àÿõ Âîá ìîæåò óáåäèòü Êýðîë â ïðàâèëüíîñòè ïîäïèñè Àëèñû [489].

Íàïðèìåð, Âîá ïîêóïàåò ëåãàëüíóþ êîïèþ DEW. Îí ìîæåò ïîäòâåðäèòü ïîäïèñü ïîä ïðîãðàììíûì ïðîäóêòîì, êîãäà çàõî÷åò. Òîãäà, Âîá ìîæåò óáåäèòü Êýðîë, ÷òî îí ðàáîòàåò íà Alice Software Company, è ïðîäàòü åé ïèðàòñêóþ êîïèþ DEW. Êîãäà Êýðîë ïîïûòàåòñÿ ïîäòâåðäèòü ïîäïèñü Âîáà, îí îãíîðàëåíî ïîäòâåðæäåò ïîäïèñü ó Àëèñû. Êîãäà Êýðîë ïîñûëàåò åìó ñëó÷àéíîå ÷èñëî, îí îòïðàâëÿåò åãî Àëèñå. Îòâåò Àëèñû îí ïðåñûëàåò Êýðîë. Êýðîë óáåæäàåòñÿ, ÷òî îíà - ëåãàëüíûé ïîêóïàòåëü, õîòÿ îíà òàêîâûì íå ÿâëÿåòñÿ. Òàêîå âñêðûòèå ÿâëÿåòñÿ ïðîòèâîçàêîííûì äåéñòâèåì â ñîîòâåòñòâèè ñ ðàçäåëîì 5.2.

Íåñìîòðÿ íà ýòî ó íåíòèöèàëüíûõ ïîäïèñåé ìíîæåñòâî ïðèíåñåíè, âî ìíîãèõ ñëó÷àÿõ Àëèñà íå õî÷åò, ÷òîáû êòî óãîäíî ìîã ïðîâåðèòü åå ïîäïèñü. Îíà ìîæåò íå õîòåòü, ÷òîáû ïîäïèñü ïîä åë ëè÷íîé êîððåñïîíäåíöèåé ìîãëà áûòü ïðîâåðåíà æóðíàëèñòàìè, ÷òîáû åå ïèñüìà áûëè îòáðàêîâàíû è ïîäòâåðæäåíû íåçàâèñèìî îò êîíòåêñòà, èëè ïðîñòî, ÷òîáû íåëüçÿ áûëî îáíàðóæèòü èçìåíåíèÿ â ïèñüìàõ, ñäåëàííûå åþ ïîçæå. Åñëè îíà ïîäïèñûâàåò èíôîðìàöèþ, êîòîðóþ îíà ïðîäàåò, òî îíà íå õî÷åò, ÷òîáû êòî-òî, íå çàïëàòèâ çà èíôîðìàöèþ, ìîã ïîäòâåðäèòü åå äîñòîâåðíîñòü. Çàùèòèòü ñâîè ïðàâà Àëèñà ìîæåò êîíòðîëèðóÿ òåõ, êòî ïðîâåðÿåò åå ïîäïèñü.

Ðÿä âàðèàíòîâ íåîòðèöàåìûõ ïîäïèñåé îòäåëÿåò ñâÿçü ìåæäó ïîäïèñàâøèì è ñîîáùåíèåì îò ñâÿçè ìåæäó ïîäïèñàâøèì è ïîäïèñüþ [910]. Â îäíîé ñõåìå êòî óãîäíî ìîæåò ïðîâåðèòü, ÷òî ïîäïèñü äåéñòâèòåëüíî áûëà ñîçäàíà åå àâòîðîì, à äëÿ ïðîâåðêè ïðàâèëüíîñòè ïîäïèñè äëÿ äàííûõ ñîîáùåíèÿ òðåáóåòñÿ ñîòðóäíè÷åñòâî ïîäïèñàâøåãî.

Áëèçêèì ïîíÿòèåì ÿâëÿåòñÿ **âîâðåäèòåëüíàÿ íåîòðèöàåìàÿ ïîäïèñü** [1229]. Ïðåäñòàâüòå, ÷òî Àëèñà ðàáîòàåò íà Toxins, Inc., è ïðåäàåò îáëè÷àþùèå äîêóìåíòû â ãàçåòó, èñïîëüçóÿ ïðîòîêîë íåîòðèöàåìîé ïîäïèñè. Àëèñà ìîæåò ïîäòâåðäèòü ñâîþ ïîäïèñü òî÷íûì ðåïîðòåðó ãàçåòû è íèêîìó áîëüøå. Îäíàêî, íåãîäÿé Âîá ïîäîçðåâàåò, ÷òî èñòî÷íèê äîêóìåíòîâ ÿâëÿåòñÿ Àëèñà. Î òðåáóåò, ÷òîáû Àëèñà èñïîëüçîâàëà ïðîòîêîë ñíÿòèÿ ïîäïèñè, ÷òîáû î÷èñòèòü ñâîþ èìÿ, à Àëèñà îòêàçûâàåòñÿ. Âîá íàñòàèâàåò, ÷òî åäèíñòâåííîé ïðè÷èíîé îòêàçà Àëèñû ÿâëÿåòñÿ åå âêëþ÷åíîñòü, è óáèâàåò åå.

Äîâåðèòåëüíûå íåîòðèöàåìûå ïîäïèñè íà îáû÷íûå íåîòðèöàåìûå ïîäïèñè çà èñêëþ÷åíèåì ïðîòîêîëà ñíÿòèÿ ïîäïèñè, êîòîðûé ïîçâîëÿåò Àëèñå äîêàçàòü, ÷òî îíà íå ïîäïèñûâàëà äîêóìåíò, à Âîá íå Âîá ìîæåò ïîòðåáîâàòü ñîòðóäíè÷åñòâà Àëèñû èñïîëüçîâàòü ïðîòîêîë ñíÿòèÿ ïîäïèñè. È åñëè Òðåíò ïðåäñòàâëÿåò ñóäåáíóþ ñèñòåìó, òî îí èñïîëüçóåò ýòîò ïðîòîêîë òîëüêî äëÿ ðàçðåøåíèÿ ôîðìàëüíîãî ñïîðà.

4.4 Ï î äï èñè óï î ë í î ì ÷å í íî ãî ñâèäåòåëÿ

Alice Software Company äîáèëàñü áóðíîãî ðîñòà ïðîäàæ, ïðîäàâàÿ DEW - òàêîãî, ÷òî Àëèñà áîëüøóþ ÷àñòü âðåìåíè ïîñâÿùàåò ïîäòâåðæäåíèþ íåòðèâèàëüíûõ ïîäïèñåé, à íå ðàáîòå íàä íîâûì èíòåðåñíûì ïðîåêòîì.

Àëèñå õîòåëîñü áû íàçíà÷èòü íåêîåãî ÷ëåíâåêà â êîìïàíèè îòâåòñòâåííûì çà ïîäòâåðæäåíèå ïîäïèñè. Àëèñà, èë ëþáîé äðóãîé ïðîãðàììèñò, ñìîæåò ïîäïèñûâàòü äîêóìåíòû ñ ïîìîùüþ íåîðèãèíàëüíîãî ïðîòîêîëà. Íî âñå ïîäòâåðæäåíèÿ áóäóò ïðîâåðåíû òîëüêî Êýðîë.

Îêàçûâàåòñÿ, ýòî âîçìîæíî ñ èñïîëüçîâàíèåì **ïîäïèñè óïîëíîì÷åííîãî ñâèäåòåëÿ** [333,1213]. Àëèñà ìîæåò ïîäïèñàòü äîêóìåíò, òàê ÷òî Áîá óâåäîìëÿò, ÷òî ïîäïèñü ïðåâðàòèëà, íî íå ñìîæåò óâåäîìèòü â ýòîì òðåòüåì âíåøíåì äîêóìåíòå - Àëèñà ìîæåò îòêàçàòüñÿ ñîðâàòü ñäåëêó. Âî òî æå âðåìÿ Àëèñà íàçíà÷àåò Êýðîë íà äîëæíîñòü áóõãàëòåðà ñäåëêè. Àëèñå äàæå íå íóæíî çàðàíåå ïðîñèòü ðàçðåøåíèÿ ó Êýðîë, åé òîëüêî íóæíî èñïîëüçîâàòü îòêðûòûé êëþ÷ Êýðîë. È Êýðîë ñìîæåò ïîäòâåðäèòü ïîäïèñü Àëèñû, åñëè Àëèñà óðàòèâ èç ãîðîäà, óâîëèëàñü, áûëè ïîâðåæäåíû ëîë è óìåðëà.

Ïîäïèñè óïîëíîì÷åííîãî ñâèäåòåëÿ ïðåäñòàâëÿþò ñîáîé íåêèé êîìïîíåíò ìåæäó îáû÷íûìè öèôðîâûìè ïîäïèñÿìè è íåòðèâèàëüíûì ïîäïèñÿì. Î ïðåäïîëîæèì òàêîé ñöåíàðèé: Àëèñà çàõî÷åò îðãàíèçîâàòü ÷èñòî ôîðìàëüíóþ ñäåëêó, ïîäàäèì÷èòü ïîäïèñè, ïîòðåáóåò ïîäòâåðæäåíèÿ è â ïîäòâåðæäåíèè, è â îòðèöàíèè, îíà ìîæåò çàÿâèòü î ïîòåðå êëþ÷åé äëÿ ïîäòâåðæäåíèÿ èëè îòðèöàíèÿ, íàêîíåö, îíà ìîæåò áûòü ïðîñòî íåäîñòóïíà. Ïîäïèñè óïîëíîì÷åííîãî ñâèäåòåëÿ ìîãóò ïðåäîñòàâèòü Àëèñå çàùèòó, ñîçäàâàìóþ íåîðèöàíèì ïîäïèñüþ, îäíîðàçîâûé ïî÷òîâûé ñåðâèñ, ïîçâîëÿþùèé çëîóìûøëåííèêó ïîäìåíèòü ïîäïèñü Àëèñû, ïîêà îíà íàõîäèòñÿ â áîëüíèöå, èëè äàæå óìåðëà. Ïîäïèñè óïîëíîì÷åííîãî ñâèäåòåëÿ ìîãóò ïîìî÷ü Àëèñå ïîääåðæèâàòü ñâîþ ðåïóòàöèþ, ïîêàçûâàÿ, ÷òî îíà íå ïîäïèñàëà íåêîððåêòíûé äîêóìåíò, ïîñêîëüêó îíà íå ìîãëà ïîëó÷èòü äîñòóï ê ñâîèì êëþ÷àì.

Ýòà èäåÿ ìîæåò èìåòü ðàçëè÷íûå ïðèìåíåíèÿ. Íàïðèìåð, Êýðîë ìîæåò ñäåëàòüñÿ ãîñóäàðñòâåííûì íîòàðèóñîì. Îíà îïóáëèêóåò â êàêîì-òî êàòàëîãå ñâîé îôôëàéí êëþ÷, è ëþäè ïîëó÷àþò âîçìîæíîñòü íàçíà÷àòü åå ñâèäåòåëåì ñâîèõ ïîäïèñåé. Ïîëó÷àÿ íåáîëüøóþ ïëàòó çà ïîäòâåðæäåíèå ïîäïèñåé, îíà ìîæåò æèòü ïðèâàòíî÷è.

Êýðîë ìîæåò áûòü àãåíòñòâîì ïî õðàíå âåòîðñêèõ ïðàâ, ïðàâèòåëüñòâåííûì àãåíòñòâîì èëè åùå êàêîé-íèáóäü îðãàíèçàöèåé. Ýòîò ïðîòîêîë ïîçâîëÿåò îòäåëüíûì ëþäåé, ïîäïèñûâàþùèõ äîêóìåíòû, îò ëþäåé, êîòîðûå ïîìîãàþò ïîäòâåðæäàòü ïîäïèñè.

4.5 Ï î äïèñè ï î äîâåðåí íîñòè

Ïîäïèñè óïîëíîì÷åííîãî ñâèäåòåëÿ ïîçâîëÿþò ïîäïèñàâøåìó íàçíà÷èòü êîãî-òî äðóãîãî äëÿ ïîäòâåðæäåíèÿ ïîäïèñè. Ïóñòü Àëèñà õî÷åò ïîðó÷èòü Áîáó ïîçâëèò â íåêîì ìåñòî, äàâ íåò õîðîøåé êîìïüþòåðíîé ñåòè - â àðõèâíîêå äæóíãëè, íàïðèìåð. Èëè îíà íå äåãëàñíîñíáíà ïîñëå òÿæåëîé îïðàöèè. Îíà îæèäàåò ïîëó÷åíèÿ âàæíîé ýëåêòðîííîé ïî÷òû è éíòóöèîíèñò ñåêðåòàðü Áîáà îòâå÷èò ñîîòâåòñòâóþùèì îáðàçîì. Êàê Àëèñà ìîæåò ïðåäïîëîæèòü ïîäïèñûâàþùóþ áîáó ïîëíîì÷åíèÿ çà íåå, íå ïðåäàâàÿ å¼ ñâîåãî çàêðûòîãî êëþ÷à?

Ðåøåíèåì ýòîãî ÿâëÿþòñÿ **ïîäïèñè ïî äîâåðåííîñòè** [1001]. Àëèñà ïðåäàåò Áîáó ïîëíîì÷èÿ òàê, ÷òîáû èìåëè ìåñòî ñëåäóþùèå ñâîéñòâà:

— ***Ðàçëè÷èìîñòü***. Êòî óâîäèò ìîæåò îòëè÷èòü ïîäïèñè ïî äîâåðåííîñòè îò îáû÷íûõ ïîäïèñåé.

— ***Íåïîääåëüíîñòü***. Òîëüêî ñàì ïîäïèñûâàþùèé è íàçíà÷åííûé èì ïîäïèñûâàþùèé ïî äîâåðåííîñòè ìîæåò ñîçäàòü ïðàâèëüíóþ ïîäïèñü ïî äîâåðåííîñòè.

— ***Îòëè÷èå ïîäïèñè*** ïî äîâåðåííîñòè. ïîäïèñûâàþùèé ïî äîâåðåííîñòè íå ìîæåò ñîçäàòü ïðàâèëüíóþ ïîäïèñü ïî äîâåðåííîñòè, êîòîðóþ ìîæíî âûäàòü çà îðèãèíàëüíóþ ïîäïèñü.

— ***Ïîäòâåðæäàåìîñòü***. Ïî ïîäïèñè ïî äîâåðåííîñòè êîíòðîëåð äîëæåí óâåäîìèòü â ñîãëàñèè ïðåîíà÷àëüíîãî ïîäïèñûâàþùåãî ñ ïîäïèñàííûì ñîîáùåíèì.

— ***Èäåíòèôèöèðóåìîñòü***. Ïðåîíà÷àëüíûé ïîäïèñûâàþùèé ìîæåò îïðåäåëèòü ëè÷íîñòü ïîäïèñûâàþùåãî ïî ïîäïèñè ïî äîâåðåííîñòè, ïîëó÷åííóþ ïîëüçîâàòåëåì

— ***Íåîòðèöàåìîñòü***. Ïîäïèñûâàþùèé ïî äîâåðåííîñòè íå ìîæåò ñíÿòü èì ïîäïèñü ïî äîâåðåííîñòè, ïîëó÷åííóþ ïîëüçîâàòåëåì

Â íåêîòîðûõ ñëó÷àÿõ òðåáóåòñÿ ôîðìàëèçèðîâàííîñòè - êòî óãîäíî äîëæåí èìåòü âîçìîæíîñòü îïðåäåëèòü ëè÷íîñòü ïîäïèñûâàþùåãî ïî ïîäïèñè ïî äîâåðåííîñòè. Ñòàíû ïîäïèñè ïî äîâåðåííîñòè, îñíîâàííûå íà ðàçëè÷íûõ ñõåìàõ öèôðîâîé ïîäïèñè ïðèâåäåíû â [1001].

4.6 Ãðóïïîâûå ïîäïèñè

Ýòà ïðîáëåìà áûëà âåðíà Äýâèäîì ×àóì (David Chaum) â [330]:

> Óêîíïàíèè åñòü íåñêîëüêî êîíïðåòíûõ ëîãè÷åñêèõ ñõåì. Â êàæäîì îòäåëå êîíïàíèè åñòü ñâîé ïðèíòåð (òàêæå ïðèñâàèâàþùèé ê ñõåìå), è òîëüêî îäèí ÷åê âî îòäåëå èìåò ïðàâî íà ïðèíòåðå ñâîåãî îòäåëà. Ïððå ïå÷àòüþ, ñëåäîâàòåëüíî, ïðèíòåð äîëæåí ïðîâåðÿòü, ÷òî äàííûé ñîòðóäíèê âûïîëíèë õîä÷åò îáñëóæèâàíèÿ, èìÿ ïîëüçîâàòåëÿ íå äîëæíî ðàñêðûâàòüñÿ. Åñëè, îäíàêî, êòî-òî â êîíöå äíÿ îáíàðóæèò, ÷òî ïðèíòåð èñïîëüçóåòñÿ ñëèøêîì ÷àñòî, ó äèðåêòîðà äîëæíà áûòü âîçìîæíîñòü íáéòè òîãî, êòî èñïîëüçóåò ïðèíòåð íå ïî íàçíà÷åíèþ è ïîñëàòü åìó ÷åê.

Ðåøåíèå ýòîé ïðîáëåìû íàçûâàåòñÿ ãðóïïîâîé ïîäïèñüþ. Ãðóïïîâûå ïîäïèñè îáëàäàþò ñëåäóþùèìè ñâîéñòâàìè:

— Òîëüêî ÷ëåíû ãðóïïû ìîãóò ïîäïèñûâàòü ñîîáùåíèÿ.

— Ïîëó÷àòåëü ïîäïèñè ìîæåò óáåäèòüñÿ, ÷òî ýòî - ïðàâèëüíàÿ ïîäïèñü ãðóïïû.

— Ïîëó÷àòåëü ïîäïèñè íå ìîæåò îïðåäåëèòü, êòî èìåííî èç ÷ëåíîâ ãðóïïû ïîäïèñàë äîêóìåíò.

— ïðè ñïîðå ïîäïèñü áóäåò ðàñêðûòà äëÿ îïðåäåëåíèÿ ëè÷íîñòè ïîäïèñàâøåãî.

Ãðóïïîâûå ïîäïèñè ñ íàêàæóåìîé ïîñðåäíèêîì

Ñëåäóþùèé ïðîòîêîë èñïîëüçóåò çàñëóæèâàþùåãî ïîñðåäíèêà:

(1) Òðåíò ñîçäàåò áîëüøóþ êó÷ó ïàð îòêðûòûé êëþ÷/çàêðûòûé êëþ÷ è âûäàåò êàæäîìó ÷ëåíó ãðóïïû èíäèâèäóàëüíûé ñïèñîê óíèêàëüíûõ çàêðûòûõ êëþ÷åé. Îäèíàêîâûõ êëþ÷åé â ñïèñêàõ íåò. (Åñëè â ãðóïïå *n* ÷ëåíîâ, è êàæäûé èç íèõ ïîëó÷àåò *m* ïàð êëþ÷åé, òî îáùåå ÷èñëî ïàð êëþ÷åé ñîñòàâèò *n***m*.)

(2) Òðåíò ïóáëèêóåò ãëàâíûé ñïèñîê âñåõ îòêðûòûõ êëþ÷åé äëÿ ãðóïïû â ñëó÷àéíîì ïîðÿäêå, ñîõðàíÿÿ â ñåêðåòå, êàêîé êëþ÷ êîìó ïðèíàäëåæèò.

(3) Êîãäà ÷ëåí ãðóïïû õî÷åò ïîäïèñàòü äîêóìåíò, îí ñëó÷àéíûì îáðàçîì âûáèðàåò êëþ÷ èç ñâîåãî ñïèñêà.

(4) Êîãäà êòî-òî õî÷åò óáåäèòüñÿ, ÷òî ïîäïèñü ïðèíàäëåæèò ÷ëåíó äàííîé ãðóïïû, îí ïåðåáèðàåò ãëàâíûé ñïèñîê â ïîñëàõ ïîãîäÿùåãî îòêðûòîãî êëþ÷à è ïðîâåðÿåò ïîäïèñü.

(5) Â ñëó÷àå ñïîðîâ îáðàùàþòñÿ ê Òðåíòó, êîòîðûé çíàåò, êàêèå êëþ÷è èñïîëüçóåò êàæäûé ÷ëåí ãðóïïû.

Ïðîáëåìà ïðîòîêîëà ñîñòîèò â òîì, ÷òî äëÿ íåãî íåîáõîäèì íàäåæíûé ïîñðåäíèê. Òðåíò çíàåò çàêðûòûå êëþ÷è êàæäîãî è ìîæåò ïîääåëûâàòü ïîäïèñè. Êðîìå òîãî, äîëæíî áûòü äîñòàòî÷íî âåëèêî, ÷òîáû ïîëüçîâàòåëè íàäåæíî ïîëüçîâàëèñü ïîñðåäíèêîì è íå ïûòàëèñü ïîäîáðàòü êëþ÷è.

4.7 Ïîäïèñè ñ îáíàðóæåíèåì ïîääåëêè

Ïóñòü Âåà ÿâëÿåòñÿ ìîáó÷èì ïðîòèâíèêîì. Ó íåå åñòü îáøèðíûå êîëëåêöèè ïîäïèñàííûõ ñîîáùåíèé. Òðåíò çíàåò çàêðûòûå êëþ÷è êàæäîãî è ìîæåò ïîääåëûâàòü ïîäïèñè. Êðîìå òîãî, äîëæíà ñìîòðåòü âñå ïîäïèñè, Äëÿ ìíîãèõ ïîäïèñåé ïîääåëêà íåâîçìîæíà, íî è ïîçâîëÿåò äîáàâëÿòü íîâûõ ïîëüçîâàòåëåé, ïîääåëûâàòü åå ïîäïèñü ïîä äîêóìåíòîì, ïðèíàäëåæàùèì äðóãîìó ïîëüçîâàòåëþ.

Ïîäïèñè ñ îáíàðóæåíèåì ïîääåëêè, ââåäåííûå Áèðæèòîì Ïôèöìàíîì (Birgit Pfitzmann) è Ìàéêëîì Óýéäíåðîì (Michael Waidner) [1240] ïðåäîòâðàùàþò ïîäîáíûå ìøåííè÷åñòâî. Åñëè ïîñëå ãðóáîãî âçëîìà Âåà ïîääåëûâàåò ïîäïèñè Àëèñû, Àëèñà ñìîæåò äîêàçàòü ïîäëîãó. Åñëè Àëèñà ïîäïèøåò äîêóìåíò, à ïîòîì îáúÿâèò ñâîþ ïîäïèñü ïîäëîæíîé, ïðàâäà ìîæåò áûòü äîêàçàíà ñóäîì.

Îñíîâíàÿ èäåÿ, ñòîÿùàÿ çà ïîäïèñÿìè ñ îáíàðóæåíèåì ïîääåëêè, ñîñòîèò â òîì, ÷òî äëÿ êàæäîãî âîçìîæíîãî îòêðûòîãî êëþ÷ó ñîîòâåòñòâóåò ìíîæåñòâî âîçìîæíûõ çàêðûòûõ êëþ÷åé. Êàæäûé èç ýòèõ çàêðûòûõ êëþ÷åé äàåò ìíîæåñòâî ðàçëè÷íûõ öèôðîâûõ ïîäïèñåé. Îäíàêî, ó Àëèñû åñòü òîëüêî îäèí çàêðûòûé êëþ÷, è îíà ìîæåò ðàñ÷èòàòü òîëüêî îäíó ïîäïèñü. Äðóãèå çàêðûòûå êëþ÷è åé íåèçâåñòíû.

Åâà õî÷åò âçëîìàòü çàêðûòûé êëþ÷ Àëèñû. (Åâà òàêæå ñìîæåò áûòü Àëèñîé, âû÷èñëèâ äëÿ ñåáÿ âòîðîé çàêðûòûé êëþ÷.) Îíà ñíà÷àëà ïîäìåíÿåò ñîîáùåíèÿ è, èñïîëüçóÿ ìíîæåñòâî ñâîèõ ñòîêîâûõ ïîäïèñåé, ïûòàåòñÿ ðàñêðûòü ïîäïèñü Àëèñû. Äàæå åñëè åé óäàñòñÿ ðàñêðûòü ïîäïèñü Àëèñû, òàêèõ êëþ÷åé íàñòîëüêî ìíîãî, ÷òî, ñêîðåå âñåãî, îíà ïîëó÷èò èíôî, ÷åì ó Àëèñû, êëþ÷. Åâðîïåéñêèå ðàñêðûòèÿ êëþ÷à, ïðèíàäëåæàùåãî èìåííî Àëèñå, íàñòîëüêî ìàëà, ÷òî åþ ìîæíî ïðåíåáðü.

Òåïåðü, êîãäà Åâà ïîääåëàò ïîäïèñü ïîä äîêóìåíòîì, èñïîëüçóÿ íàéäåííûé çàêðûòûé êëþ÷, ïîääåëàííàÿ ïîäïèñü áóäåò îòëè÷àòüñÿ îò òîé ïîäïèñè, êîòîðóþ ïîñòàâèëà áû ñàìà Àëèñà. Ïðè îáðàùåíèè â ñóä Àëèñà

ïðåäúÿâèò äâå ðàçëè÷íûõ ïîäïèñè ïîä îäíèì è òåì æå ñîîáùåíèåì è îòêðûòûé êëþ÷ (ñîîòâåòñòâóþùèé åå çàêðûòîìó êëþ÷ó è çàêðûòîìó êëþ÷ó, íàéäåííîìó Åâîé), ÷òîáû äîêàçàòü ïîäëîã. Ñ äðóãîé ñòîðîíû, åñëè Àëèñà íå ìîæåò ïðåäúÿâèòü äâå ðàçëè÷íûå ïîäïèñè, òî ïîäëîãà íå áûëî è Àëèñà äîëæíà îòâå÷àòü çà ñâîþ ïîäïèñü.

Ýòà ñõåìà ïîäïèñåé ïðîòèâîñòîèò âçëîìó Åâîé ïîäïèñè Àëèñû ñ ïîìîùüþ íåîáû÷àéíî ìîùíûõ âû÷èñëèòåëüíûõ ñðåäñòâ. Îíà íè÷åãî íå ñìîæåò ñäåëàòü ñ áîëåå âåðîÿòíîé ïîïûòêîé Ìýëëîðè âëîìèòüñÿ â äîì Àëèñû è ñòàùèòü åå çàêðûòûé êëþ÷ èëè ñ ïîïûòêîé Àëèñû ïîäïèñàòü äîêóìåíò, à çàòåì "ñëó÷àéíî" ïîòåðÿòü ñâîé çàêðûòûé êëþ÷. ×òîáû çàùèòèòüñÿ îò óïîìÿíóòîé ïîïûòêè Ìýëëîðè, Àëèñå ñòîèò êóïèòü ñåáå õîðîøóþ ñòîðîæåâóþ ñîáàêó, íî ïîäîáíûå ðåêîìåíäàöèè âûõîäÿò çà ðàìêè êðèïòîãðàôèè.

Äîïîëíèòåëüíóþ òåîðèþ è ïðèìåíåíèÿ ïîäïèñåé ñ îáíàðóæåíèåì ïîääåëêè ìîæíî íàéòè â [1239, 1241, 730, 731].

4.8 Âû÷èñëåíèÿ ñ çàøèôðîâàííûìè äàííûìè

Àëèñà õî÷åò çíàòü ðåøåíèå äëÿ íåêîòîðîé ôóíêöèè $f(x)$ äëÿ íåêîòîðîãî êîíêðåòíîãî çíà÷åíèÿ x. Ê íåñ÷àñòüþ, åå êîìïüþòåð ñëîìàí. Áîá õî÷åò âû÷èñëèòü äëÿ íåå çíà÷åíèå $f(x)$, íî Àëèñà íå õî÷åò, ÷òîáû Áîá çíàë åå x. Êàê Àëèñå ïîçâîëèòü Áîáó ïðîâåñòè âû÷èñëåíèå $f(x)$è íå ñîîáùèòü åìó x?

Ýòî îáû÷íàÿ ïðîáëåìà **âû÷èñëåíèé ñ çàøèôðîâàííûìè äàííûìè**, òàêæå èçâåñòíûõ êàê **òàéíàÿ èíôîðìàöèÿ ïðîðèöàòåëÿ**. (Ïðîðèöàòåëåì ÿâëÿåòñÿ Áîá - îí îòâå÷àåò íà âîïðîñ.) Äëÿ íåêîòîðûõ ôóíêöèé ñóùåñòâóþò ñïîñîáû ðåøèòü ýòó çàäà÷ó, îíè îáñóæäàþòñÿ â ðàçäåëå 23.6.

4.9 Âðó÷åíèå áèòîâ

Àëèñà Âåëèêîëåïíàÿ, âûäàþùàÿñÿ âîëøåáíèöà, ñåé÷àñ ïðîäåìîíñòðèðóåò ìîùü ñâîåãî èñêóññòâà. Îíà óãàäàåò êàðòó, êîòîðóþ âûáåðåò Áîá äî òîãî, êàê îí åå âûáåðåò! Ñëåäèòå çà òåì, êàê Àëèñà çàïèñûâàåò ñâîå ïðåäñêàçàíèå íà êóñî÷êå áóìàãè. Âîñõèùàéòåñü òåì, êàê Àëèñà êëàäåò ýòîò êóñî÷åê áóìàãè â êîíâåðò è çàïå÷àòûâàåò åãî. Äðîæèòå îò òîãî, êàê Àëèñà îòäàåò çàïå÷àòàííûé êîíâåðò ñëó÷àéíîìó çðèòåëþ. "Âûáåðè êàðòó, Áîá, ëþáóþ êàðòó." Îí ãëÿäèò íà íåå è ïîêàçûâàåò êàðòó Àëèñå è çðèòåëÿì. Ýòî ñåìåðêà áóáåí. Òåïåðü Àëèñà çàáèðàåò êîíâåðò ó çðèòåëÿ è îòêðûâàåò åãî. Ïðåäñêàçàíèå, çàïèñàííîå äî òîãî, êàê Áîá âûáðàë êàðòó, ñîîáùàåò "ñåìåðêà áóáåí"! Àïëîäèñìåíòû.

Äëÿ óñïåõà ýòîãî òðþêà Àëèñå íóæíî ïîäìåíèòü êîíâåðò â êîíöå ôîêóñà. Îäíàêî, êðèïòîãðàôè÷åñêèå ïðîòîêîëû ìîãóò îáåñïå÷èòü çàùèòó îò ëþáîé ëîâêîñòè ðóê. À êàêàÿ â ýòîì ïîëüçà? Âîò áîëåå ïðèçåìëåííàÿ èñòîðèÿ.

Áèðæåâîé áðîêåð Àëèñà õî÷åò óáåäèòü èíâåñòîðà Áîáà, ÷òî åå ìåòîä îïðåäåëÿòü ïåðñïåêòèâíûå àêöèè çàñëóæèâàåò âíèìàíèÿ.

Áîá: "Ïîäáåðèòå-êà äëÿ ìåíÿ ïÿòîê àêöèé. Åñëè íà íèõ óäàñòñÿ çàðàáîòàòü, ÿ ïåðåäàì ñâîé áèçíåñ âàì."

Àëèñà: "Åñëè ÿ ïîäáåðó ïÿòü àêöèé äëÿ âàñ, âû ñìîæåòå âëîæèòü â íèõ äåíüãè, íå çàïëàòèâ ìíå. Ïî÷åìó áû ìíå íå ïîêàçàòü âàì ïÿòü àêöèé, êîòîðûå ÿ ïîäîáðàë â ïðîøëîì ìåñÿöå?"

Áîá: "Îòêóäà ÿ çíàþ, ÷òî âû íå ïîìåíÿëè ðåçóëüòàòû âàøåãî âûáîðà, óçíàâ íàñòîÿùèå. Åñëè âû ñîîáùèòå ìíå î ñâîåì âûáîðå ñåé÷àñ, ÿ áóäó óâåðåí, ÷òî âû íå ïîìåíÿåòå ðåçóëüòàò. ß íå áóäó âêëàäûâàòü äåíüãè â ýòè àêöèè, ïîêà ÿ íå îïëà÷ó âàøè óñëóãè. Ïîâåðüòå ìíå."

Àëèñà: "ß ëó÷øå ïîêàæó âàì ñâîþ ïîäáîðêó àêöèé çà ïðîøëûé ìåñÿö. ß íå ïîìåíÿëà èõ. Ïîâåðüòå ìíå."

Àëèñà õî÷åò ïåðåäàòü ñâîå ïðåäñêàçàíèå (ò.å., áèò èëè ïîñëåäîâàòåëüíîñòü áèòîâ), íî íå õî÷åò ðàñêðûâàòü ñâîå ïðåäñêàçàíèå äî íåêîòîðîãî âðåìåíè. Áîá, ñ äðóãîé ñòîðîíû, õî÷åò óäîñòîâåðèòüñÿ, ÷òî Àëèñà íå ñìîæåò èçìåíèòü ñâîå ìíåíèå ïîñëå òîãî, êàê îíà ñäåëàëà ïðåäñêàçàíèå.

Âðó÷åíèå áèòîâ ñ ïîìîùüþ ñèììåòðè÷íîé êðèïòîãðàôèè

Ýòîò ïðîòîêîë âðó÷åíèÿ áèòà èñïîëüçóåò ñèììåòðè÷íóþ êðèïòîãðàôèþ:

(1) Áîá ãåíåðèðóåò ñòðîêó ñëó÷àéíûõ áèòîâ, R, è ïîñûëàåò åå Àëèñå.

(2) Àëèñà ñîçäàåò ñîîáùåíèå, ñîñòîÿùåå èç ñâîåãî áèòà, êîòîðûé îíà õî÷åò âðó÷èòü, b (â äåéñòâèòåëüíîñòè, ýòî ìîæåò áûòü è íåñêîëüêî áèòîâ), è ñëó÷àéíóþ ñòðîêó Áîáà. Îíà øèôðóåò ñîîáùåíèå íåêîòîðûì ñëó÷àéíûì êëþ÷îì, K, è ïîñûëàåò åãî îáðàòíî Áîáó.

$E_K(R,b)$

Ýòà ÷àñòü ïðîòîêîëà ïðåäñòàâëÿåò ñîáîé ïðîöåäóðó âðó÷åíèÿ. Áîá íå ìîæåò ðàñøèôðîâàòü ñîîáùåíèå, ïîýòîìó îí íå çíàåò, ÷òî çà áèò ïðèñëàëà Àëèñà.

Êîãäà äëÿ Àëèñû ïðèõîäèò âðåìÿ ðàñêðûòü ñâîé áèò, ïðîòîêîë ïðîäîëæàåòñÿ:

(3) Àëèñà ïîñûëàåò Áîáó êëþ÷.

(4) Áîá ðàñøèôðîâûâàåò ñîîáùåíèÿ, óçíàâàÿ áèò. Î í ïðîâåðÿåò ñâîþ ñëó÷àéíóþ ñòðîêó, óáåæäàÿñü â ïðàâèëüíîñòè áèòà.

Áåç ñëó÷àéíîé ñòðîêè ÁÎáà Àëèñà ìîæåò òàéíî ðàñøèôðîâûâàòü ñîîáùåíèå, ïîñëàííîå Áîáó, èñïîëüçóÿ ìíîæåñòâî êëþ÷åé, ïîäáèðàÿ òîò, êîòîðûé ïîçâîëèò ïðè äåøèôðèðîâàíèè îòïðàâëåííîãî ñîîáùåíèÿ èçìåíèòü âðó÷íóþ áèò. Òàê êàê ó áèòà òîëüêî äâà âîçìîæíûõ çíà÷åíèÿ, åå ïîèñêè íàâåðíÿêà óâåí÷àþòñÿ óñïåõîì ïîñëå íåñêîëüêèõ ïîïûòîê. Ñëó÷àéíàÿ ñòðîêà ÁÎáà íå äàåò åé èñïîëüçîâàòü ýòîò ñïîñîá âñêðûòèÿ, åé ïðèäåòñÿ èñêàòü íîâûé êëþ÷, êîòîðûé íå òîëüêî èíâåðòèðóåò âðó÷íóþ áèò, íî è ñîõðàíèò íàòîíóòîé ñëó÷àéíóþ ñòðîêó ÁÎáà. Åñëè èñïîëüçóåòñÿ äîñòàòî÷íî õîðîøèé äëãîðåòì øèôðîâàíèÿ, âåðîÿòíîñòü óäà÷íîãî ïîèñêà ÷ðåçâû÷àéíî ìàëà. Àëèñà íå ìîæåò èçìåíèòü ñâîé áèò ïîñëå åãî âðó÷íèÿ.

Âðó÷íèå áèòà ñ ïîìîùüþ îäíîíàïðàâëåííûõ ôóíêöèé

Ýòîò ïðîòîêîë èñïîëüçóåò îäíîíàïðàâëåííûå ôóíêöèè:

(1) Àëèñà ñîçäàåò äâå ñëó÷àéíûõ ñòðîêè áèòîâ, R_1 è R_2.

R_1, R_2

(2) Àëèñà ñîçäàåò ñîîáùåíèå, ñîñòîÿùåå èç åå ñëó÷àéíûõ ñòðîê è áèòà, êîòîðûé îíà õî÷åò âðó÷èòü (â äåéñòâèòåëüíîñòè, ýòî ìîæåò áûòü è íåñêîëüêî áèòîâ).

(R_1, R_2, b)

(3) Àëèñà âû÷èñëÿåò îäíîíàïðàâëåííóþ ôóíêöèþ äëÿ ñîîáùåíèÿ è ïîñûëàåò ðåçóëüòàò âìåñòå ñ îäíîé èç ñëó÷àéíûõ ñòðîê ÁÎáó.

$H(R_1, R_2, b), R_1$

Ýòî ñîîáùåíèå Àëèñû ÿâëÿåòñÿ äîêàçàòåëüñòâîì âðó÷íèÿ. Èñïîëüçîâàíèå îäíîíàïðàâëåííîé ôóíêöèè íà ýòàïå (3) ìåøàåò ÁÎáó, èíâåðòèðóÿ ôóíêöèþ, îïðåäåëèò áèò.

Êîãäà äëÿ Àëèñû ïðèäåò âðåìÿ ðàñêðûòü ñâîé áèò, ïðîòîêîë ïðîäîëæàåòñÿ:

(4) Àëèñà îòïðàâëÿåò ÁÎáó ïåðâîíà÷àëüíîå ñîîáùåíèå.

(R_1, R_2, b)

(5) Áîá âû÷èñëÿåò îäíîíàïðàâëåííóþ ôóíêöèþ äëÿ ñîîáùåíèÿ è ñðàâíèâàåò åãî è R_1 ñî çíà÷åíèåì îäíîíàïðàâëåííîé ôóíêöèè è ñëó÷àéíîé ñòðîêîé, ïîëó÷åííûì íà ýòàïå (3). Åñëè îíè ñîâïàäàþò, òî áèò ïðàâèëåí.

Ïðåìóùåñòâî ýòîãî ïðîòîêîëà ïåðåä ïðåäûäóùèì â òîì, ÷òî ÁÎáó íå íóæíî ïîñûëàòü íèêàêèõ ñîîáùåíèé. Àëèñà ïîñûëàåò ÁÎáó îäíî ñîîáùåíèå äëÿ âðó÷åíèÿ áèòà, à äðóãîå - äëÿ åãî ðàñêðûòèÿ.

Íå íóæíà è ñëó÷àéíàÿ ñòðîêà ÁÎáà, òàê êàê ðåçóëüòàò Àëèñèíîãî âðó÷åíèÿ - ýòî ñîîáùåíèå, îáðàáîòàííîå îäíîíàïðàâëåííîé ôóíêöèåé. Àëèñà íå ìîæåò ñìîøåííè÷àòü è ïîäáðàòü äðóãîå ñîîáùåíèå (R_1, R_2, b'), äëÿ êîòîðîãî $H(R_1, R_2, b')= H(R_1, R_2, b)$. Ïîñûëàÿ ÁÎáó R_1, îíà âðó÷åò çíà÷åíèå b. Åñëè Àëèñà íå ñîõðàíèò â ñåêðåòå R_2, òî ÁÎá ïîëó÷èò âîçìîæíîñòü âû÷èñëèòü $H(R_1, R_2, b')$ è $H(R_1, R_2, b)$, ïîëó÷àÿ âîçìîæíîñòü óâåäîìèòü, ÷òî æå îí ïîëó÷èë îò Àëèñû.

Âðó÷íèå áèòà ñ ïîìîùüþ ãåíåðàòîðà ïñåâäîñëó÷àéíîé ïîñëåäîâàòåëüíîñòè

Ýòîò ïðîòîêîë äàæå ïðîùå [1137]:

(1) Áîá ñîçäàåò ñòðîêó ñëó÷àéíûõ áèòîâ è ïîñûëàåò åå Àëèñå.

$R_Á$

(2) Àëèñà ñîçäàåò ñòàðòîâóþ ïîñëåäîâàòåëüíîñòü äëÿ ãåíåðàòîðà ïñåâäîñëó÷àéíûõ áèòîâ. Çàòåì äëÿ êàæäîãî áèòà â ñòðîêå ñëó÷àéíûõ áèòîâ ÁÎáà îíà ïîñûëàåò ÁÎáó ëèáî:

(a) âûõîä ãåíåðàòîðà, åñëè áèò ÁÎáà ðàâåí 0, èëè

(b) XOR âûõîäà ãåíåðàòîðà è áèòà ÁÎáà, åñëè Áèò ÁÎáà ðàâåí 1.

Êîãäà äëÿ Àëèñû ïðèäåò âðåìÿ ðàñêðûòü ñâîé áèò, ïðîòîêîë ïðîäîëæàåòñÿ:

(3) Àëèñà ïîñûëàåò ÁÎáó ñâîþ ñòàðòîâóþ ïîñëåäîâàòåëüíîñòü.

(4) Áîá âûïîëíÿåò ýòàï (2), óáåæäàÿñü, ÷òî Àëèñà äåéñòâóåò ÷åñòíî.

Åñëè ñòðîêà ñëó÷àéíûõ áèòîâ ïîñòàòî÷íî äëèíà, à ãåíåðàòîð ïñåâäîñëó÷àéíûõ áèòîâ íàïðàâëåí÷óåò, ìîøåííè÷íèê Àëèñû ïðàêòè÷åñêè íåâîçìîæíî.

Blob-îáúåêòû

Ñòðîêè, êîòîðûå Àëëñà ïîñûëàåò Áîáó äëÿ âðó÷åíèÿ áèòà, èíîãäà íàçûâàþò **blob-îáúåêòàìè**. Blob-îáúåêò - ýòî ïîñëåäîâàòåëüíîñòü áèòîâ, õîòÿ ïðîòîêîëû ýòîãî è íå òðåáóþò. Êàê ñêàçàë Æèëü Áðàññàð (Gilles Brassard), "Î íè ìîãëè áû áûòü ñäåëàíû è èç âîëøåáíîé ïûëè, åñëè áû ýòî áûëî ïîëåçíû" [236]. Blob-îáúåêòû îáëàäàþò ñëåäóþùèìè ÷åòûðüìÿ ñâîéñòâàìè:

1. Àëëñà ìîæåò âðó÷èòü blob-îáúåêòû. Âðó÷àÿ blob-îáúåêò, îíà âðó÷àåò áèò.
2. Àëëñà ìîæåò îòêðûòü ëþáîé blob-îáúåêò, êîòîðûé îíà âðó÷èëà. Êîãäà îíà îòêðûâàåò blob-îáúåêò, îíà ìîæåò óáåäèòü Áîáà â çíà÷åíèè áèòà, êîòîðûé áûë âðó÷åí âìåñòå ñ blob-îáúåêòîì. Ñëåäîâàòåëüíî, îíà íå ìîæåò îòêðûòü ïðîèçâîëüíûé blob-îáúåêò, íàïðèìåð, íîëü èëè ðàâíîòó.
3. Áîá íå ìîæåò çíàòü, êàêèì îáðàçîì Àëëñà ìîæåò îòêðûòü blob-îáúåêò, êîòîðûé îíà âðó÷èëà. Ýòî îñòàòîê ñïðàâåäëèâûì, äàæå êîãäà Àëëñà îòêðîåò äðóãèå blob-îáúåêòû.
4. Blob-îáúåêòû íå íåñóò íèêàêîé èíôîðìàöèè, êðîìå âðó÷àåìîãî Àëëñîé áèòà. Ñàìè ïî ñåáå blob-îáúåêòû, òàêæå êàê è ïðîöåññ, ñ ïîìîùüþ êîòîðîãî Àëëñà âðó÷àåò è îòêðûâàåò èõ, íå ñâÿçàíû íå ñ ÷åì äðóãèì, ÷òî Àëëñà õîòåëà áû ñîõðàíèòü â ñåêðåòå îò Áîáà.

4.10 Ï ðîäâèíóòàÿ "÷åñòíîé" ìîíåòû

Íàñòàëî âðåìÿ ïðîöèòèðîâàòü Äæî Êëëèàíà (Joe Kilian) [831]:

> Àëëñà è Áîá õîòåëè ñûãðàòü â "îðëà è ðåøêó", íî ìîíåòû ó íèõ íå áûëî. Àëëñà ïðåäëîæèëà ïðîñòîé ñïîñîá ïîäáðñûâàòü ìîíåòêó ìûñëåííî.
>
> "Ñíà÷àëà âû çàäóìûâàåòå ñëó÷àéíûé áèò, çàòåì ÿ çàäóìàþ ñëó÷àéíûé áèò. Çàòåì ìû âûïîëíÿåì íàä áèòàìè "èñêëþ÷àþùåå èëè", - ïðåäëîæèëà Àëëñà.
>
> "Í î åñëè îäèí èç íàñ íå áóäåò çàäóìûâàòü áèòû ñëó÷àéíûì îáðàçîì?", - ñïðîñèë Áîá.
>
> "Ýòî íå âàæíî. Åñëè õîòÿ áû îäèí äåéñòâèòåëüíî ñëó÷àåí, òî è "èñêëþ÷àþùåå èëè" áèòîâ äîëæíî áûòü äâóêðàòíî ñëó÷àéíûì", - îòâåòèëà Àëëñà, è ïîñëå ìíóòíîãî ðàçäóìüÿ Áîá ñîãëàñèëñÿ.
>
> Íåìíîãî ñïóñòÿ Àëëñà è Áîá íàòêíóëèñü íà êíèãó ïî èñêóññòâåííîìó èíòåëëåêòó, ëåæàùóþ íà îáîé÷èíå äîðîãè. Àëëñà, äîáðîïîðÿäî÷íàÿ ððàæäàíêà, ñêàçàëà: "Îäèí èç íàñ äîëæåí ïîäîáðàòü ýòó êíèãó è ñäàòü åå â áþðî íàòîãîâ". Áîá ñîãëàñèëñÿ, è ïðåäëîæèë èñïîëüçîâàòü èõ ïðîòèâ ïîäáðûâàíèÿ ìíåíèé, ÷òî áû îïðåäåëèòü, êòî óíåñåò êíèãó.
>
> "Åñëè ïîëó÷åííûé áèò áóäåò 0, òî òû âîçüìåøü êíèãó, à åñëè 1 - òî ÿ", - ñêàçàëà Àëëñà. " Êàêîé ó òåáÿ áèò?"
>
> Áîá îòâåòèë: "1".
>
> "Íó âîò, è ó ìåíÿ òàêîé æå", - ëóêàâî çàìåòèëà Àëëñà. - "ß äóìàþ, ó òåáÿ ñåãîäíÿ íåóäà÷íûé äåíü".
>
> Î÷åâèäíî, ó ïðîòîêîëà ïîäáðàñûâàíèÿ ìîíåòêè åñòü ñåðüåçíûé äåôåêò. Õîòÿ ýòî ïðàâäà, ÷òî "èñêëþ÷àþùåå èëè" äåéñòâèòåëüíî ñëó÷àéíîãî áèòà, *x*, è ëþáîãî íåçàâèñèìî ðàñïðåäåëåííîãî áèòà, *y*, äâà âåçóëüòàòà äåéñòâèòåëüíî ñëó÷àéíûé áèò, ïðîòèâîïîëîæíû íå äâóõèðóåò, ÷òî íåò áèòà áóäóò ðàñïðåäåëåíû íåçàâèñèìî. Íà ñàìîì äåëå íåòðóäíî óáåäèòüñÿ, ÷òî íå ñóùåñòâóåò ïðîòîêîëà, êîòîðûé ïîçâîëèò Àëëñå è Áîáó äîãîâîðèòüñÿ ïîäáðàñûâàòü "÷åòíóþ" ìîíåòó. Àëëñà è Áîá äîêàçàëè, ïîêà íå ïîëó÷èëè ïèñüìî îò íåèçâåñòíîãî ñòóäåíòà ñ äëÿ÷îìî ïî êðèïòîãðàôèè. Èíôîðìàöèÿ â ïèñüìå áûëà ñëåøêîì òåíäåíöèîçíîé, ÷òîáû åå ìîæíî áûëî ïðèíÿòü äëÿ ÷åãî-òî çàìíîãî, íî êîíêðåòíî, â êîòîðîì ïðèøëîñü ÷îêàçëèñÿ ñëèøêîì ðàíî ïîâåðèòü.
>
> Êîãäà Àëëñà è Áîá â ñëåäóþùèé ðàç çàõîäèëè ïîäáðîñèòü ìîíåòó, îíè èçìåíèëè ïðåäíàçíà÷åííûé ïðîòîêîë. Ñíà÷àëà áèò çàäóìàë Áîá, íî âìåñòî òîãî, ÷òîáû îòêðûòü åãî íåìåäëåííî, îí çàïèñûâàåò ñâîé áèò íà êëèñêå áóìàãè è êëàäåò êëèñê â ñåéô áóìàãè Áîá. Çàòåì Àëëñà ïáúÿâëÿåò ñâîé áèò. Íàêîíåö, Àëëñà è Áîá äîêàçûâàþò ñëó÷àéíûé áèò. Ýòîò áèò óæå äåéñòâèòåëüíî ñëó÷àé, íåçàâèñèìî òî áîñòîíñòè èãðàþùèõ. Àëëñà è Áîá ïîëó÷èëè ðàáîòàþùèé ïðîòîêîë, ñîöèàëüíî çíà÷èìàÿ ìå÷òà âñåõ êðèïòîãðàôîâ îñóùåñòâëåíà!

Ýòè êîíâåðòû âûãëÿäÿò äåñüìà ïîõîæèè íà blob-îáúåêòû âðó÷åíèÿ áèòà. Êîãäà Ìàíóýëü Áëàì (Manuel Blum) ñòîëêíóëñÿ ñ ïðîáëåìîé ïîäáðàñûâàíèÿ "÷åñòíîé" ìîíåòû ïî ìîäåì [194], îí ðåøèë åå, èñïîëüçóÿ ïðîòîêîë âðó÷åíèÿ áèòà:

(1) Àëëñà âðó÷àåò ñëó÷àéíûé áèò, èñïîëüçóÿ ëþáóþ èç ñõåì âðó÷åíèÿ áèòà, îïèñàííóþ â ðàçäåëå 4.9.

(2) Áîá çàãàäûâàåò ñâîé áèò.

(3) Àëëñà ðàñêðûâàåò áèò Áîáó. Áîá âûèãðûâàåò áðîñîê, åñëè îí ïðàâèëüíî çàãàäàë áèò.

Â îáùåì ñëó÷àå, íàì íóæåí ïðîòîêîë ñî ñëåäóþùèìè ñâîéñòâàìè:

— Àëëñà äîëæíà "áðîñèòü ìîíåòó" äî òîãî, êàê Áîá çàãàäàåò ñâîé áèò.

— Àëëñà íå äîëæíà èìåòü âîçìîæíîñòè èçìåíèòü ðåçóëüòàò ñâîåãî áðîñêà, óçíàâ áèò Áîáà.

— Ó Áîáà íå äîëæíî áûòü âîçìîæíîñòè óçíàòü ðåçóëüòàò áðîñêà ïåðåä òåì, êàê îí ñäåëàåò ñâîé ïðåäïîëîæåíèå.

Ñóùåñòâóåò íåñêîëüêî âîçìîæíîñòåé âûïîëíèòü ýòî.

Áðîñîê ìîíåòû ñ ïîìîùüþ îäíîíàïðàâëåííûõ ôóíêöèé

Åñëè Àëëñà è Áîá äîãîâîðÿòñÿ îá îäíîíàïðàâëåííîé ôóíêöèè, ïðîòîêîëè ïðîñòî:

(1) Àëëñà âûáèðàåò ñëó÷àéíîå ÷èñëî, *x*. Îíà âû÷èñëÿåò *y=f(x)*, ãäå *f(x)* - îäíîíàïðàâëåííàÿ ôóíêöèÿ.

(2) Àëèñà ïîñûëàåò *y* Áîáó.

(3) Áîá ïðåäïîëàãàåò, ÷òî *x* ÷åòíî èëè íå÷åòíî, è ïîñûëàåò ñâîå ïðåäïîëîæåíèå Àëèñå.

(4) Åñëè ïðåäïîëîæåíèå Áîáà ïðàâèëüíî, ðåçóëüòàòîì áðîñêà ìîíåòû è ïîñûëàåò *x* Áîáó.

(5) Áîá ïðîâåðÿåò, ÷òî *y=f(x)*.

Áåçîïàñíîñòü ýòîãî ïðîòîêîëà îáåñïå÷èâàåòñÿ îäíîíàïðàâëåííîé ôóíêöèåé. Åñëè Àëèñà ñìîæåò íàéòè *x* è *x′*, òàêèå ÷òî *x* - ÷åòíî, à *x′* - íå÷åòíî, è *y=f(x)= f(x′)*, òî îíà êàæäûé ðàç ñìîæåò îáìàíóòü Áîáà. Êðîìå òîãî, íàèìåíüøèé çíà÷àùèé áèò *f(x)* äîëæåí áûòü íåêîððåëèðîâàí ñ *x*. Â ïðîòèâíîì ñëó÷àå Áîá ñìîæåò îáìàíóâàòü Àëèñ, ïî êðàéíåé ìåðå èíîãäà. Íàïðèìåð, åñëè *f(x)* â 75 ïðîöåíòàõ ñëó÷àåâ ÷åòíà, åñëè *x*, ó Áîáà áóäåò ïðåèìóùåñòâî. (Èíîãäà íàèìåíüøèé çíà÷àùèé áèò íå ÿâëÿåòñÿ ëó÷øèì âûáîðîì äëÿ èñïîëüçîâàíèÿ â ïðèëîæåíèè, ïîòîìó ÷òî åãî âû÷èñëåíèå ìîæåò îêàçàòüñÿ ñëèøêîì ïðîñòûì.)

Áðîñîê ìîíåòû ñ ïîìîùüþ êðèïòîãðàôèè ñ òðûõ êëþ÷åé

Ýòîò ïðîòîêîë ðàáîòàåò êàê ñ êðèïòîãðàôèêå ñ îòêðûòûì êëþ÷àìè, òàê è ñ ñèììåòðè÷íîé êðèïòîãðàôèêå. Äâóñòîðîííÿÿ óñëîâíîñòü - ïðåäâêë÷åíèå äëãîðèòìà. Òî åñòü:

$$D_{K_1}(E_{K_2}(E_{K_1}(M))) = E_{K_2}(M)$$

Â îáùåì ñëó÷àå ýòî ñâîéñòâî íå âûïîëíÿåòñÿ äëÿ ñèììåòðè÷íûõ àëãîðèòìîâ, íî ñïðàâåäëèâî äëÿ íåêîòîðûõ àëãîðèòìîâ ñ îòêðûòûì êëþ÷àìè (íàïðèìåð, RSA ñ èäåíòè÷íûì ìîäóëåì). Ýòîò ïðîòîêîë:

(1) È Àëèñà, è Áîá ñîçäàþò ïàðû îòêðûòûé êëþ÷/çàêðûòûé êëþ÷.

(2) Àëèñà ñîçäàåò äâà ñîîáùåíèÿ, îäíî äëÿ "îðëà", à âòîðîå - äëÿ "ðåøêè". Ýòè ñîîáùåíèÿ äîëæíû âêëþ÷àòü íåêîòîðóþ ñëó÷àéíóþ ñòðîêó, ÷òîáû îíà ìîãëà ïîäòâåðäèòü èõ ïîäëèííîñòü íà ïîñëåäóþùèõ ýòàïàõ ïðîòîêîëà. Àëèñà øèôðóåò îáà ñîîáùåíèÿ ñâîèì îòêðûòûì êëþ÷îì è ïîñûëàåò èõ Áîáó â ïðîèçâîëüíîì ïîðÿäêå.

E_A(M₁), E_A(M₂)

(3) Áîá, êîòîðûå íå ìîæåò ïðî÷èòàòü íå îäíî ñîîáùåíèå, ñëó÷àéíûì îáðàçîì âûáèðàåò îäíî èç íèõ. (Î í ìîæåò ïîñ÷èòàòü èõ ñ ïîìîùüþ "Ýíêîä-áåíêîä åëè âàðèàíòå", âîñïîëüçîâàòüñÿ êî ìüþòåðîì äëÿ âçëîìà ïðîòîêîëû èëè îáðàòèòüñÿ ê öûãàíêå.) Î í øèôðóåò âûáðàííîå ñîîáùåíèå ñâîèì îòêðûòûì êëþ÷îì è ïîñûëàåò åãî îáðàòíî Àëèñå.

E_Â(E_A(M))

ãäå *M - M₁* èëè *M₂*.

(4) Àëèñà, êîòîðàÿ íå ìîæåò ïðî÷èòàòü ïîëó÷åííîå ñîîáùåíèå, ðàñøèôðîâûâàåò åãî ñâîèì çàêðûòûì êëþ÷îì è ïîñûëàåò îáðàòíî Áîáó.

D_A(E_Â(E_A(M)))= E_Â(M₁), åñëè *M = M₁*, èëè *E_Â(M₂)*, åñëè *M = M₂*.

(5) Áîá ðàñøèôðîâûâàåò ñîîáùåíèå ñâîèì çàêðûòûì êëþ÷îì, ðàñêðûâàÿ ðåçóëüòàò áðîñêà ìîíåòû, è ïîñûëàåò ðàñøèôðîâàííîå ñîîáùåíèå Àëèñå.

D_Â(E_Â(M₁)) èëè *D_Â(E_Â(M₂))*

(6) Àëèñà ÷èòàåò ðåçóëüòàò áðîñêà ìîíåòû è ïðîâåðÿåò, ÷òî ñëó÷àéíàÿ ñòðîêà ïðàâèëüíà.

(7) Àëèñà è Áîá ðàñêðûâàþò ïàðû ñâîèõ êëþ÷åé, ÷òîáû êàæäûé èç ñòîðîí ìîãëà óáåäèòüñÿ â îòñóòñòâèè ìîøåííè÷åñòâà.

Ýòîò ïðîòîêîë ñàìîäîñòàòî÷åí. Ëþáàÿ ñòîðîíà ìîæåò íåìåäëåííî îáíàðóæèòü ìîøåííè÷åñòâî äðóãîé, è íå òðåáóåòñÿ òðåòüÿ ñòîðîíà íè äëÿ óòâåðæäåíèÿ ïðîòîêîëà. ×òîáû ïîñìîòðåòü, êàê ýòî ðàáîòàåò, äàâàéòå ïîïûòàåìñÿ ñìîøåííè÷àòü.

Åñëè âûèãðàòü, ñìîøåííè÷âà, õî÷åò Àëèñà, ó íåå åñòü òðè âîçìîæíûõ ïóòè ïîâëèÿòü íà ðåçóëüòàò. Âî ïåðâûõ, îíà ìîæåò çàøèôðîâàòü äâà ñîîáùåíèÿ äëÿ "îðëà" íà ýòàïå (2). Áîá îáíàðóæèò ýòî, êîãäà Àëèñà ðàñêðîåò ñâîè êëþ÷è íà ýòàïå (7). Âî âòîðûõ, îíà ìîæåò èñïîëüçîâàòü êàêîé-òî äóðàöêè êëþ÷ äëÿ ðàñøèôðîâûâàíèÿ ñîîáùåíèÿ íà ýòàïå (4). Ýòî ïðèâåäåò ê áåñêîíå÷íîìó öèêëó, êîòîðóþ Áîá è îáíàðóæèò íà ýòàïå (5). Â òðåòüåõ, îíà ìîæåò îáúÿâèòü íåïðàâèëüíûì ñîîáùåíèå íà ýòàïå (6). Áîá òàêæå îáíàðóæèò ýòî íà ýòàïå (7), êîãäà Àëèñà íå ñìîæåò äîêàçàòü, íåïðàâèëüíîñòü ñîîáùåíèÿ. Êîíå÷íî, Àëèñà ìîæåò îòêàçàòüñÿ îò ó÷àñòèÿ â ïðîòîêîëå íà ëþáîì ýòàïå, êîãäà æóëüíè÷åñòâî Àëèñû ñòàíåò äëÿ Áîáà î÷åâèäíûì.

Åñëè Áîá çàõî÷åò ìîøåííè÷åñòâî âûèãðàòü, åãî ïîëíæíèå íè÷óòü íå ëó÷øå. Î í ìîæåò íåïðàâèëüíî çàøèôðîâàòü ñîîáùåíèå íà ýòàïå (3), íî Àëèñà îáíàðóæèò îáìàí, âçãëÿíóâ íà çàêëþ÷èòåëüíûå ñîîáùåíèå íà ýòàïå (6).

Îí ìîæåò çàÿâèòü, ÷òî íåïðàâèëüíî âûïîëíèë ýòàï (5) èç-çà êàêîãî-òî ìîøåííè÷åñòâà ñî ñòîðîíû Àëèñû, íî ýòà ôîðìà æóëüíè÷åñòâà âñêðûâàåòñÿ íà ýòàïå (7). Íàêîíåö, îí ìîæåò ïîñëàòü Àëèñà ñîîáùåíèå î "ðåøêå" íà ýòàïå (5), íåçàâèñèìî îò ðàñøèôðîâàííîãî ñîîáùåíèÿ, íî Àëèñà ñìîæåò íåìåäëåííî ïðîâåðèòü äîñòîâåðíîñòü ñîîáùåíèÿ íà ýòàïå (6).

Áðîñîê ìîíåòû â êîëîäåö

Èíôîðìàöèîííî ïóòåøåñòâèå Àëèñà è Áîá óçíàþò ðåçóëüòàò áðîñêà íå ïîíîâðåìåííî. Â êàæäîì ïðîòîêîëå åñòü ìîìåíò, êîãäà îíà èç ñòîðîí (Àëèñà â ïåðâûõ äâóõ ïðîòîêîëàõ è Áîá â ïîñëåäíåì) óçíàåò ðåçóëüòàò áðîñêà, íî íå ìîæåò èçìåíèòü åãî. Ýòà ñòîðîíà ìîæåò, îäíàêî, çàäåðæàòü ðàñêðûòèå ðåçóëüòàòà äëÿ âòîðîé ñòîðîíû. Ýòî íàçûâàåòñÿ **áðîñîê ìîíåòû â êîëîäåö**. Ïðåäñòàâüòå ñåáå âûïîëíåò êîëîäåö. Àëèñà ñòîèò ðÿäîì ñ êîëîäöåì, À Áîá - íåìíîãî ïîäàëüøå. Áîá áðîñàåò ìîíåòó, è îíà ïàäàåò â êîëîäåö. Àëèñà ìîæåò òåïåðü çàãëÿíóòü â êîëîäåö è óâèäåòü ðåçóëüòàò, íî îíà íå ìîæåò ñïðîñèòüñÿ âíèç è èçìåíèòü åãî. Áîá íå ñìîæåò óâèäåòü ðåçóëüòàò, ïîêà Àëèñà íå ïîçâîíèò åìó ïîäíéòè è çàãëÿíóòü â êîëîäåö.

Ãåíåðàöèÿ êëþ÷åé ñ ïîìîùüþ áðîñêà ìîíåòû

Ðàâíûì ïðèíöèïîì ýòîò ïðîòîêîë ñëóæèò ãåíåðàöèè ñåàíñîâîãî êëþ÷à. Ïðîòîêîëû áðîñêè ìîíåòû ïîçâîëÿþò Àëèñå è Áîáó ñîçäàòü ñëó÷àéíûé ñåàíñîâûé êëþ÷ òàê, ÷òî íèêòî èç íèõ íå ñìîæåò ïîâëèÿòü íà òî, êàêèì áóäåò ýòîò êëþ÷. Åñëè Àëèñà è Áîá çàøèôðóþò ñâîè ñîîáùåíèÿ, ïðîöåäóðà ãåíåðàöèè êëþ÷à ê òî÷íó æå ñòàíäàðòó áåçîïàñíîé îò çëîóìûøëåííèêà.

4.11 Ìûñëåííûé ïîêåð

Ïðîòîêîë, àíàëîãè÷íûé ïðîòîêîëó áðîñêà ìîíåòû ñ ïîìîùüþ îòêðûòûõ êëþ÷åé, ïîçâîëÿåò Àëèñå è Áîáó èãðàòü äóõ ñ äóõàìè â ïîêåð ïî ýëåêòðîííîé ïî÷òå. Àëèñà âìåñòî ñîçäàíèÿ è øèôðîâàíèÿ äâóõ ñîîáùåíèé, îäíîãî äëÿ "îðëà", à äðóãîãî - äëÿ "ðåøêè", ñîçäàåò 52 ñîîáùåíèÿ M_1, M_2, ..., M_{52}, ïî ÷èñëó êàðò â êîëîäå. Áîá ñëó÷àéíûì îáðàçîì âûáèðàåò ïÿòü èç íèõ, øèôðóåò ñâîè îòêðûòûì êëþ÷îì è ïîñûëàåò îáðàòíî Àëèñå. Àëèñà ðàñøèôðîâûâàåò ñîîáùåíèÿ è ïîñûëàåò èõ îáðàòíî Áîáó, êîòîðûé ðàñøèôðîâûâàåò èõ äëÿ îïðåäåëåíèÿ ñâîé "ðóêè". Çàòåì îí ñëó÷àéíûì îáðàçîì âûáèðàåò åùå ïÿòü ñîîáùåíèé è, íå èçìåíÿÿ èõ, ïîñûëàåò Àëèñå. Îíà ðàñøèôðîâûâàåò èõ, è ýòè ñîîòâåòñòâóþùèå êàðòû ñòàíîâÿòñÿ åå "ðóêîé". Â òå÷åíèå èãðû ýòà æå ïðîöåäóðà ïðèìåíÿåòñÿ äëÿ ñäà÷è èãðîêàì äîïîëíèòåëüíûõ êàðò. Â êîíöå èãðû Àëèñà è Áîá ðàñêðûâàþò ñâîè êàðòû è ïàðû êëþ÷åé, ÷òîáû êàæäûé ìîã óáåäèòüñÿ â îòñóòñòâèè ìîøåííè÷åñòâà.

Ìûñëåííûé ïîêåð ñ òðåìÿ èãðîêàìè

Ïîêåð èíòåðåñåí, åñëè â èãðå ó÷àñòâóþò íåñêîëüêî ÷åëîâåê. Áàçîâûé ïðîòîêîë ìûñëåííîãî ïîêåðà ëåãêî ìîæåò áûòü ðàñïðîñòðàíåí íà òðåõ è áîëåå èãðîêîâ. Â ýòîì ñëó÷àå êðèïòîãðàôè÷åñêèé àëãîðèòì òàêæå äîëæåí áûòü êîìóòàòèâíûì.

(1) Àëèñà, Áîá è Êýðîë ñîçäàþò ïàðû îòêðûòûé êëþ÷/çàêðûòûé êëþ÷.

(2) Àëèñà ñîçäàåò 52 ñîîáùåíèÿ, ïî îäíîìó äëÿ êàæäîé êàðòû êîëîäû. Ýòè ñîîáùåíèÿ äîëæíû âêëþ÷àòü íåêîòîðóþ óíèêàëüíóþ ñëó÷àéíóþ ñòðîêó, ÷òîáû Àëèñà ìîãëà ïðåäñêàçàòü ïîñëåäóþùèõ íà ïîñëåäóþùèõ ýòàïàõ ïðîòîêîëà. Àëèñà øèôðóåò âñå ñîîáùåíèÿ ñâîèì îòêðûòûì êëþ÷îì è ïîñûëàåò îò Áîáó â ïðîèçâîëüíîì ïîðÿäêå.

$E_A(M_n)$

(3) Áîá, êîòîðûé íå ìîæåò ïðî÷èòàòü íå îäíî ñîîáùåíèå, ñëó÷àéíûì îáðàçîì âûáèðàåò ïÿòü èç íèõ. Îí øèôðóåò èõ ñâîèì îòêðûòûì êëþ÷îì è ïîñûëàåò îáðàòíî Àëèñå.

$E_Â(E_A(M_n))$

(4) Áîá îòïðàâëÿåò Êýðîë îñòàâøèåñÿ 47 ñîîáùåíèé.

$E_A(M_n)$

(5) Êýðîë, êîòîðàÿ íå ìîæåò ïðî÷èòàòü íå îäíî ñîîáùåíèå, ñëó÷àéíûì îáðàçîì âûáèðàåò ïÿòü èç íèõ. Îíà øèôðóåò èõ ñâîèì îòêðûòûì êëþ÷îì è ïîñûëàåò Àëèñå.

$E_Ñ(E_A(M_n))$

(6) Àëèñà, êîòîðàÿ íå ìîæåò ïðî÷èòàòü íè îäíî èç ïîëó÷åííûõ ñîîáùåíèé, ðàñøèôðîâûâàåò èõ ñâîèì çàêðûòûì êëþ÷îì è ïîñûëàåò îáðàòíî Áîáó èëè Êýðîë (â ñîîòâåòñòâèè ñ òåì, îò êîãî îíà èõ ïîëó÷èëà).

$D_A(E_Â(E_A(M_n)))= E_Â(M_n)$

$D_A(E_Ñ(E_A(M_n)))= E_Ñ(M_n)$

(7) Áîá è Êýðîë ðàñøèôðîâûâàþò ñîîáùåíèÿ ñâîèìè êëþ÷àìè, ÷òîáû óçíàòü ñâîè êàðòû

$D_{\hat{A}}(E_{\hat{A}}(M_n))$

$D_C(E_C(M_n))$

(8) Êýðîë ñëó÷àéíûì îáðàçîì âûáèðàåò ïÿòü èç îñòàâøèõñÿ 42 ñîîáùåíèé è ïîñûëàåò Àëèñå.

$E_A(M_n)$

(9) Àëèñà ðàñøèôðîâûâàåò ñîîáùåíèÿ, ÷òîáû óçíàòü ñâîè êàðòû.

$D_A(E_A(M_n))$

(10) Â êîíöå èãðû Àëèñà, Áîá è Êýðîë ðàñêðûâàþò ñâîè êàðòû è ïàðû êëþ÷åé, ÷òîáû êàæäûé ìîã óáåäèòüñÿ â îòñóòñòâèè ìîøåííè÷åñòâà.

Äîïîëíèòåëüíûå êàðòû ðàçäàþòñÿ ïîäîáíûì æå îáðàçîì. Åñëè êàðòà íóæíà Áîáó èëè Êýðîë, ëþáîé èç íèõ áåðåò çàøèôðîâàííóþ êîëîäó è ïîâòîðÿåò ïðîòîêîë ñ Àëèñîé, Åñëè êàðòà íóæíà Àëèñå, òî òîò, ó êîãî ñåé÷àñ íàõîäèòñÿ çàøèôðîâàííàÿ êîëîäà, ïîñûëàåò åé ñëó÷àéíóþ êàðòó.

Â èäåàëå, ýòàï (10) ÿâëÿåòñÿ îáÿçàòåëüíûì. Ñâîè "ðóêè" â êîíöå ïðîòîêîëà äîëæíû îòêðûâàòü íå âñå èãðîêè, à òîëüêî òå, êîòîðûå íå ñïàñîâàëè. Òàê êàê ýòàï (10) â ïðîòîêîëå òîëüêî äëÿ êîíòðîëÿ ìîøåííè÷åñòâà, âîçìîæíû êàêèå-íèáóäü óëó÷øåíèÿ.

Â ïîêåðå èíòåðåñíî òîëüêî, íå ñìîøåííè÷àë ëè ïîáåäèòåëü. Âñå îñòàëüíûå ìîãóò ìîøåííè÷àòü ñêîëüêî âëå-çåò, ðàç óæ îíè âñå ðàâíî ïðîèãðûâàþò. (Â äåéñòâèòåëüíîñòè ýòî íå ñîâñåì âåðíî. Êòî-òî, ïðîèãðûâàÿ, ìîæåò ñîáèðàòü äàííûå î ñòèëå èãðû â ïîêåð äðóãèõ èãðîêîâ.) Èòàê, âçãëÿíåì íà ñëó÷àè âûèãðûøà ðàçëè÷íûõ èãðîêîâ.

Åñëè âûèãðûâàåò Àëèñà, îíà ðàñêðûâàåò ñâîþ "ðóêó" è ñâîè êëþ÷è. Áîá ìîæåò èñïîëüçîâàòü çàêðûòûé êëþ÷ Àëèñû äëÿ ïðîâåðêè ïðàâèëüíîñòè äåéñòâèé Àëèñû íà ýòàïå (2), òî åñòü ïðîâåðèòü, ÷òî êàæäîå èç 52 ñîîáùåíèé ñîîòâåòñòâóåò îòäåëüíîé êàðòå. Êýðîë ìîæåò ïðîâåðèòü, ÷òî Àëèñà íå ëæåò î ñâîåé "ðóêå", øèôðóÿ êàðòû îò-êðûòûì êëþ÷îì Àëèñû è ïðîâåðÿÿ, ÷òî îíè ñîîòâåòñòâóþò øèôðîâàííûì ñîîáùåíèÿì, êîòîðûå îíà ïîñëàëà Àëèñå íà ýòàïå (8).

Åñëè âûèãðûâàþò Áîá èëè Êýðîë, ïîáåäèòåëü ðàñêðûâàåò ñâîè êàðòû è êëþ÷è. Àëèñà ìîæåò óáåäèòüñÿ â ïðàâèëüíîñòè êàðò, ïðîâåðèâ ñâîè ñëó÷àéíûå ñòðîêè. Îíà ìîæåò òàêæå óáåäèòüñÿ, ÷òî ñäàíû áûëè èìåííî ýòè êàðòû, øèôðóÿ èõ îòêðûòûì êëþ÷îì ïîáåäèòåëÿ è ïðîâåðÿÿ, ÷òî îíè ñîâïàäàþò ñ çàøèôðîâàííûìè ñîîáùå-íèÿìè, ïîëó÷åííûìè íà ýòàïàõ (3) èëè (5).

Ýòîò ïðîòîêîë íå çàùèùåí îò ñãîâîðà èãðîêîâ-ìîøåííèêîâ. Àëèñà è äðóãîé èãðîê ìîãóò îáúåäèíèòüñÿ è áåçíàêàçàííî âìåñòå íàäóâàòü òðåòüåãî èãðîêà. Ñëåäîâàòåëüíî, âàæíî ïðîâåðÿòü âñå êëþ÷è è ñëó÷àéíûå ñòðîêè êàæäûé ðàç, êîãäà èãðîêè ðàñêðûâàþò ñâîè êàðòû. È åñëè âû ñèäèòå çà âèðòóàëüíûì ñòîëîì ñ äâóìÿ èãðîêàìè, êîòîðûå íèêîãäà îäíîâðåìåííî íå ðàñêðûâàþò ñâîè êàðòû, ïðè÷åì îäèí èç íèõ ñäàåò (â ïðåäûäóùåì ïðîòîêîëå ýòî Àëèñà) êîí÷àéòå èãðó.

Âñå ýòî êðàñèâî â òåîðèè, íî ðåàëèçîâàòü âñå ýòî íà êîìïüþòåðå âåñüìà íåïðîñòî. Â ðåàëèçàöèè äëÿ òðåõ èã-ðîêîâ íà òðåõ ðàçëè÷íûõ Sparc-ñòàíöèÿõ âîñåìü ÷àñîâ òðåáóåòñÿ òîëüêî äëÿ òàñîâàíèÿ êîëîäû, òàê ÷òî ëó÷øå ïîèãðàòü â íàñòîÿùèé ïîêåð [513].

Âñêðûòèÿ ìûñëåííîãî ïîêåðà

Êðèïòîãðàôû ïîêàçàëè, ÷òî ïðè èñïîëüçîâàíèè ýòèìè ïðîòîêîëàìè ïîêåðà àëãîðèòìà ñ îòêðûòûìè êëþ÷àìè RSA ïðîèñõîäèò íåáîëüøàÿ óòå÷êà èíôîðìàöèè [453, 573]. Êîíêðåòíî, åñëè äâîè÷íîå ïðåäñòàâëåíèå êàðò ÿâëÿ-åòñÿ êâàäðàòè÷íûì îñòàòêîì (ñì ðàçäåë 11.3), òî çàøèôðîâàííûå êàðòû òàêæå ÿâëÿþòñÿ êâàäðàòè÷íûì îñòàò-êîì. Ýòî ñâîéñòâî ìîæåò áûòü èñïîëüçîâàíî äëÿ "êðàïëåíèÿ" íåêîòîðûõ êàðò - íàïðèìåð, âñåõ òóçîâ. Ýòî äàñò íå ìíîãî èíôîðìàöèè î ñäà÷àõ, íî â òàêîé èãðå êàê ïîêåð äàæå ÷óòü-÷óòü èíôîðìàöèè äàñò ïðåèìóùåñòâî ïðè äëèòåëüíîé èãðå.

Øàôè Ãîëäâàññåð (Shafi Goldwasser) è Ñèëüâèÿ Ìèêàëè (Silvia Micali) [624] ðàçðàáîòàëè ïðîòîêîë óìñòâåí-íîãî ïîêåðà äëÿ äâóõ èãðîêîâ, êîòîðûé ðåøàåò ýòó ïðîáëåìó, õîòÿ èç-çà ñâîåé ñëîæíîñòè îí ñêîðåå èìååò òîëü-êî òåîðåòè÷åñêîå çíà÷åíèå. Îáîáùåííûé ïðîòîêîë ïîêåðà äëÿ n èãðîêîâ, óñòðàíÿþùèé ïðîáëåìó óòå÷êè èí-ôîðìàöèè, áûë ðàçðàáîòàí â [389].

Ðåçóëüòàòû äðóãèõ èññëåäîâàíèé ïðîòîêîëîâ èãðû â ïîêåð ìîæíî íàéòè â [573, 1634, 389]. Óñëîæíåííûé ïðîòîêîë, ïîçâîëÿþùèé èãðîêàì íå ðàñêðûâàòü ñâîèõ "ðóê", ïðèâåäåí â [390]. Äîí Êîïïåðñìèò (Don Copper-smith) ðàññìàòðèâàåò äâà ñïîñîáà ìîøåííè÷åñòâà â óìñòâåííîì ïîêåðå, èñïîëüçóþùåì àëãîðèòì RSA [370].

Àíîíèìíûå ðàñïðåäåëåííûå êëþ÷è

Õîòÿ íåïîõîæå, ÷òîáû êòî-íèáóäü ñîáëàçíèë èñïîëüçîâàòü ýòîò ïðîòîêîë äëÿ èãðû â ïîêåð ïî ìîáèëó, ×àðëüç Ï ôëååãåð (Charles Pfleeger) ðàññìàòðèâàåò ñèòóàöèþ, â êîòîðîé ýòîò òèï ïðîòîêîëà ìîæåò îêàçàòüñÿ ïîëåçíûì [1244].

Ðàññìîòðèì ïðîáëåìó ðàñïðåäåëåíèÿ êëþ÷åé. Åñëè ïðåäïîëîæèòü, ÷òî ëþäè íå ìîãóò ñàìè ãåíåðèðîâàòü ñâîè êëþ÷è(êëþ÷è äîëæíû èìåòü îïðåäåëåííóþ ôîðìó, èëè äîëæíû áûòü ïîäîáíûìè íåêîòîðîé îðãàíèçàöèåé, èëè åùå ÷òî-íèáóäü ïîäîáíîå), òî äëÿ ãåíåðàöèè è ðàñïðåäåëåíèÿ êëþ÷åé (Key Distribution Center, KDC). Ïðîáëåìà â òîì, ÷òî íóæíî íàéòè ñïîñîá ðàñïðåäåëåíèÿ êëþ÷åé, ÷òî íèêòî, âêëþ÷àÿ ñåðâåð, íå ìîæåò ïîíÿòü, êîìó êàêîé êëþ÷ äîñòàëñÿ. Ñëåäóþùèé ïðîòîêîë ðåøàåò ýòó ïðîáëåìó:

(1) Àëèñà ñîçäàåò ïàðó îòêðûòûé êëþ÷/çàêðûòûé êëþ÷. Â ýòîì ïðîòîêîëå îíà ñîõðàíÿåò â ñåêðåòå îáà êëþ÷à.

(2) KDC ãåíåðèðóåò íåïðåðûâíûé ïîòîê êëþ÷åé.

(3) KDC øèôðóåò êëþ÷è, îäèí çà äðóãèì, ñâîèì îòêðûòûì êëþ÷îì.

(4) KDC ïåðåäàåò çàøèôðîâàííûå êëþ÷è, îäèí çà äðóãèì, ïî ñåòè.

(5) Àëèñà ñëó÷àéíûì îáðàçîì âûáèðàåò êëþ÷.

(6) Àëèñà øèôðóåò âûáðàííûé êëþ÷ ñâîèì îòêðûòûì êëþ÷îì.

(7) Àëèñà æäåò êàêîå-òî âðåìÿ (äîñòàòî÷íî áîëüøîå, ÷òîáû ñðàáîòàë íå ìîã îïðåäåëèòü, êàêîé êëþ÷ îíà âûáðàëà) è ïîñûëàåò äâàæäû çàøèôðîâàííûé êëþ÷ â KDC.

(8) KDC ðàñøèôðîâûâàåò äâàæäû çàøèôðîâàííûé êëþ÷ ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à, ïîëó÷àÿ êëþ÷, çàøèôðîâàííûé îòêðûòûì êëþ÷îì Àëèñû.

(9) Ñåðâåð ïîñûëàåò øèôðîâàííûé êëþ÷ îáðàòíî Àëèñå.

(10) Àëèñà ðàñøèôðîâûâàåò êëþ÷ ñ ïîìîùüþ ñâîåãî çàêðûòîãî êëþ÷à.

Ó íàõîäÿùåéñÿ ãäå-òî â ñåðâåðíå ïðîòîêîëà Åâû íåò íè ìàëåéøåãî ïðåäñòàâëåíèÿ î âûáðàííîì Àëèñîé êëþ÷å. Î íà âèäèò íåïðåðûâíûé ïîòîê êëþ÷åé, ñîçäàâàåìûõ íà ýòàïå (4). Êîãäà Àëèñà ïîñûëàåò êëþ÷ ñåðâåðó íà ýòàïå (7), îí øèôðóåòñÿ åå îòêðûòûì êëþ÷îì, êîòîðûé òàêæå äëÿ ýòîãî ïðîòîêîëà õðàíèòñÿ â ñåðâåðå. Ñïîñîáà ñâÿçàòü ýòî ñîîáùåíèå ñ ïîòîêîì êëþ÷åé ó Åâû íåò. Êîãäà êëþ÷ âîçâðàùàåòñÿ Àëèñå ñåðâåðîì íà ýòàïå (9), îí òàêæå çàøèôðîâàí îòêðûòûì êëþ÷îì Àëèñû. Êëþ÷ ñòàíîâèòñÿ èçâåñòíûì, òîëüêî êîãäà Àëèñà ðàñøèôðîâûâàåò åãî íà ýòàïå (10).

Åñëè âû èñïîëüçóåòå RSA, â ýòîì ïðîòîêîëå ïðîèñõîäèò óòå÷êà èíôîðìàöèè ñî ñêîðîñòüþ, ïî ìåíüøåé ìåðå, îäèí áèò íà ñîîáùåíèå. Ïðè÷èíîé ýòîãî ñîâà ÿâëÿþòñÿ êâàäðàò÷íûå îñòàòêè. Åñëè âû ñîáèðàåòåñü èñïîëüçîâàòü ýòîò ñîñîá äàñïðåäåëåíèÿ êëþ÷åé, óáåäèòåñü, ÷òî ýòà óòå÷êà íå ïðèâåäåò ê êàêèì-ëèáî ïîñëåäñòâèÿì. Êðîìå òîãî, ïîòîê êëþ÷åé, ñîçäàâàåìûé KDC äîëæåí áûòü äîñòàòî÷íî áîëüøèì, ÷òîáû ïðîòèâîñòîÿòü âñêðûòèþ ãðóáûì âçëîìùèê. Êîíå÷íî æå, åñëè Àëèñà íå ìîæåò âåðèòü KDC, òî îíà íå äîëæíà ïîëüçîâàòüñÿ åãî êëþ÷àìè. Ì îøèíè÷àþùèé KDC ìîæåò ïðåäñòàâëÿòü çàïèñûâàòü âñå ñîçäàâàåìûå èì êëþ÷è. Òîãäà îí ñìîæåò íàéòè ñðåäè íèõ êëþ÷, âûáðàííûé Àëèñîé.

Ýòîò ïðîòîêîë òàêæå ïðåäïîëàãàåò, ÷òî Àëèñà áóäåò äåéñòâîâàòü ÷åñòíî. Ïðè èñïîëüçîâàíèè RSA ñóùåñòâóåò ðÿä äåéſòâié, êîòîðûå ìîæåò ïðåäïðèíÿòü Àëèñà, ÷òîáû ïîëó÷èòü áîëüøå èíôîðìàöèè, ÷åì åé óäàëîñü áû ïðè äðóãîì ìåòîäå øèôðîâàíèÿ. Â íàøåì ñöåíàðèè ýòà ïðîáëåìà íå ñóùåſòâóåò, íî ïðè äðóãèõ îſòóîſòÿòåëüſòâàõ îſà ìîæåò ſòàòü âàæſîé.

4.12 Îäíîſàïðàâëåſſûå ſóìſàòîðû

Àëèſà ÿâëÿåſſÿ ſëåſſî îðãàſèçàöèè "Çàãſâſðùèêè". Èſſîãäà åé ſðèſſîäſòſÿ âſòðå÷àòüſÿ ſ äðóſàèſè ſëåſàſè â ſëſſî ſſâåùåſſûſ ðåſòſðàſàſ è øåſòàöſ ſåêðåòſ íàëâſ è íàſðàſ. Áåäà â òſì, ſòſ ðåſſòſðàſſ íàſòſëüêſ ſëſſî ſſâåùåſſ, ſòſ ſîſ íå ſ ſîæåſ áſòü óâåðåſſ, ſòſ ſåëſâåê, ſèäÿùèé íàſðſòèâ íåå çà ſòſſëſ, òſæå ſëåſ ſðãàſèçàöèè.

"Çàãſâſðùèêè" ſſãóò âſáèðàòſ èç íåſêſëüêèſ ðåøåſèé. Êàæäſé ſſîæåſ ſſſèòſ ſ ſſáſé ſſſèſſê ſëåſſâ ſðãàſèçàöèè. Ýòſ âëå÷åſ çà ſſáſé ãâå ſëåäóþſòſ ſðſáſëſû. Âſ ſåðâſû, òàſåðſ êàæäſé äſëæåſ ſſſèòſ ſ ſſáſé áſëüøóþ áàçó äàſſſû, è, âſ âſſðſû, èſ ſðëäåſſÿ êàê ſëåäóåſ ſððàſÿòſ ýſſ ſſſèſſê ÷ëåſſâ. Äðóãèſ ſſſſſáſſ ÿâëÿåſſÿ èſſſſëüçſâàſèå èäåſſòêêàöèſſſûſ êàðò, âſſſóſåſſſûſ ſàäåæſſſ ſåêðåòàðåſ. Äſſſëſèòåëüſſſ ſðåſèſóſåſſòſſ ýſſàſ ſſſſſáſ ÿâëÿåſſÿ òſ, ÷òſ è ſſſòſðſſſſèå ſſſſàſóſ ſðſâåðÿòſ ÷ëåſſâ ſðãàſèçàöèè (âſÿêèå ſêèâêè â ſåſòſſſ áàêàëåſſſ ëàâêå), äſ äëÿ ýòſàſ ſóæåſ ſàäåæſſûſ ſåêðåòàðü. Íèêſſó èç "çàãſâſðùèêſâ" ſåüçÿ äſâåðÿòſ äſ òàêſ ſòåſſſ.

Íſâſſ ðåøåſèåſ ÿâëÿåòſÿ èſſſſëüçſâàſèå **ſäſſſàſðàâëåſſſſàſ ſóſ ſàòſðà** [116]. Ýòſ ÷òſ-òſ ſſõſæåå íà ſä-

íîíàïðàâëåííûå õýø-ôóíêöèè, äëÿ êîòîðûõ âûïîëíÿåòñÿ òðåáîâàíèå êîììóòàòèâíîñòè. Òî åñòü, ìîæíî õýøèðîâàòü áàçû äàííûõ ÷ëåíîâ îðãàíèçàöèè â ïðîèçâîëüíîì ïîðÿäêå è ïîëó÷àòü îäíî è òî æå çíà÷åíèå. Áîëåå òîãî, ìîæíî äîáàâëÿòü íîâûõ ÷ëåíîâ â õýø-òàáëèöó è ïîëó÷àòü íîâîå õýø-çíà÷åíèå, ñíîâà íå çàâèñÿùåå îò ïîðÿäêà.

Èòàê, âîò ÷òî äåëàåò Àëèñà. Îíà âûïîëíÿåò ðàñ÷åò, èñïîëüçóÿ ìíîæåñòâî âñåõ èìåí ÷ëåíîâ îðãàíèçàöèè, îòëè÷íûõ îò íåå. Çàòåì îíà ñîõðàíÿåò ýòî ïîëó÷åííîå çíà÷åíèå âìåñòå ñî ñâîèì èìåíåì. Áîá è äðóãèå ÷ëåíû äåëàþò òî æå ñàìîå. Òåïåðü, êîãäà Àëèñà è Áîá âñòðå÷àþòñÿ â ïëîõî îñâåùåííîì ðåñòîðàíå, îíè ïðîñòî îáìåíèâàþòñÿ äðóã ñ äðóãîì âû÷èñëåííûìè çíà÷åíèÿìè è èìåíàìè. Àëèñà óáåæäàåòñÿ, ÷òî ðåçóëüòàò, ïîëó÷àåìûé ïðè äîáàâëåíèè èìåíè Áîáà ê çíà÷åíèþ Àëèñû, ñîâïàäàåò ñ ðåçóëüòàòîì, ïîëó÷àåìûì ïðè äîáàâëåíèè èìåíè Àëèñû ê çíà÷åíèþ ðàâíî çíà÷åíèþ Áîáà. Áîá äåëàåò òî æå ñàìîå. Òåïåðü îíè îáà çíàþò, ÷òî ñîáåñåäíèê - òàêæå ÷ëåí îðãàíèçàöèè. È â òî æå âðåìÿ íèêòî íå ñìîæåò îïðåäåëèòü ëè÷íîñòè äðóãèõ ÷ëåíîâ îðãàíèçàöèè.

Áîëåå òîãî, ðàññ÷èòàííûå çíà÷åíèÿ êàæäîãî ÷ëåíà ìîãóò áûòü âûäàíû ïîñòîðîííèì. Òîãäà Àëèñà ñìîæåò ïîäòâåðäèòü ñâîå ÷ëåíñòâî ïîñòîðîííåìó (âîçìîæíî, äëÿ ÷ëåíñêîé ñêèäêè â áóôåòå ìåñòíîé êîíòððàçâåäêè), íå ïîêàçûâàÿ åìó âåñü ñïèñîê ÷ëåíîâ.

Íîâûõ ÷ëåíîâ ìîæíî äîáàâèòü ïðîñòî ïîñëàâ ïî êðóãó íîâûå èìåíà. Ê íåñ÷àñòüþ, óäàëèòü ÷ëåíà ìîæíî òîëüêî åäèíñòâåííûì ïóòåì: âñåì ÷ëåíàì ðàññûëàåòñÿ íîâûé ñïèñîê è îíè ïåðåñ÷èòûâàþò ñâîè çíà÷åíèÿ. Íî "çàãîâîðùèêàì" ïðèäåòñÿ âûïîëíÿòü ýòî äåéñòâèå òîëüêî ïðè îòñòàâêå êîãî-òî èç ÷ëåíîâ, ìåðòâûå ÷ëåíû ìîãóò îñòàòüñÿ â ñïèñêå. (Ñòðàííî, íî ýòî íå ñîçäàåò ïðîáëåìû.)

Ýòî ðàçóìíàÿ èäåÿ ïðèìåíÿåòñÿ â ðÿäå ïðèëîæåíèé, êîãäà âû õîòèòå äîñòè÷ü ýôôåêòà öèôðîâîé ïîäïèñè áåç èñïîëüçîâàíèÿ öåíòðàëèçîâàííîé ñèñòåìû ïîäïèñåé.

4.13 Ðàñêðûòèå ñåêðåòîâ "âñå èëè íè÷åãî"

Ïðåäñòàâüòå ñåáå, ÷òî Àëèñà - áûâøèé àãåíò áûâøåãî Ñîâåòñêîãî Ñîþçà, à òåïåðü áåçðàáîòíàÿ. ×òîáû çàðàáîòàòü, îíà ïðîäàåò ñåêðåòû. Êàæäûé, ãîòîâûé çàïëàòèòü íàçíà÷åííóþ öåíó, ìîæåò êóïèòü ñåêðåò. Ó íåå äàæå åñòü êàòàëîã. Âñå åå ñåêðåòû ñ àïïåòèòíûìè íàçâàíèÿìè óïîðÿäî÷åíû ïî íîìåðàì: "Ãäå Äæèììè Õîôôà?", "Êòî òàéíî êîíòðîëèðóåò Òðåõñòîðîííþþ êîìèññèþ?", "Ïî÷åìó Áîðèñ Åëüöèí âñåãäà âûãëÿäèò, êàê áóäòî îí ïðîãëîòèë æèâóþ ëÿãóøêó?", è ò.ä.

Àëèñà íå õî÷åò òîðãîâàòü äâà ñåêðåòà ïî öåíå îäíîãî è íå ïîêàçûâàåò äàæå ÷àñòè èíôîðìàöèè, êàñàþùåéñÿ ëþáîãî èç ñåêðåòîâ. Áîá, ïîòåíöèàëüíûé ïîêóïàòåëü, íå õî÷åò ïëàòèòü çà êîòà â ìåøêå. Îí òàêæå íå õî÷åò ñîîáùàòü Àëèñå, êàêèå èç ñåêðåòîâ åìó íóæíû. Ýòî íå åå äåëî, è, êðîìå òîãî, òîãäà Àëèñà ñìîæåò äîáàâèòü â ñâîé êàòàëîã ïóíêò "Ñåêðåòû, êîòîðûìè èíòåðåñóåòñÿ Áîá".

Ïðîòîêîë ïîêåðà íå ðàáîòàåò â ýòîì ñëó÷àå, òàê êàê â êîíöå ýòîãî ïðîòîêîëà Àëèñà è Áîá îòêðûâàþò ñâîè êàðòû äðóã äðóãó. Ê òîìó æå, ñóùåñòâóþò òðþêè, ñ ïîìîùüþ êîòîðûõ Áîá ìîæåò óçíàòü ñðàçó íåñêîëüêî ñåêðåòîâ.

Ðåøåíèå íàçûâàåòñÿ **ðàñêðûòèåì ñåêðåòîâ "âñå èëè íè÷åãî"** (all-or-nothing disclosure of secrets, **ANDOS**) [246], ïîòîìó ÷òî åñëè Áîá ïîëó÷èë ëþáóþ èíôîðìàöèþ î ëþáîì èç ñåêðåòîâ Àëèñû, òî îí ïîòåðÿë âîçìîæíîñòü óçíàòü ÷òî-ëèáî åùå î äðóãèõ åå ñåêðåòàõ.

Â êðèïòîãðàôè÷åñêîé ëèòåðàòóðå ìîæíî íàéòè ðàçëè÷íûå ïðîòîêîëû ANDOS. Íåêîòîðûå èç íèõ îáñóæäàþòñÿ â ðàçäåëå 23.9.

4.14 Óñëîâíîå âðó÷åíèå êëþ÷åé

Âîò îòðûâîê èç ââåäåíèÿ â òåìó Ñèëüâèî Ìèêàëè [1084]:

> Ñåãîäíÿ ïîäñëóøèâàíèå ñ ðàçðåøåíèÿ ñóäà ÿâëÿåòñÿ ýôôåêòèâíûì ìåòîäîì îòäàâàòü ïðåñòóïíèêîâ â ðóêè ïðàâîñóäèÿ. Ïî íàøåìó ìíåíèþ åùå áîëåå âàæíî, ÷òî ýòî òàêæå ïðåäîòâðàùàåò äàëüíåéøåå ðàñïðîñòðàíåíèå ïðåñòóïëåíèÿ, óäåðæèâàÿ îò èñïîëüçîâàíèÿ îáû÷íûõ ñåòåé ñâÿçè ñ íåçàêîííûìè öåëÿìè. Ñëåäîâàòåëüíî, ñóùåñòâóåò îáîñíîâàííîå áåñïîêîéñòâî, ÷òî ðàñïðîñòðàíåíèå êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè ìîæåò áûòü íà ðóêó ïðåñòóïíûì è òåððîðèñòè÷åñêèì îðãàíèçàöèÿì. Äåéñòâèòåëüíî, âî ìíîãèõ çàêîíàõ ïðåäïîëàãàåòñÿ, ÷òî ñîîòâåòñòâóþùèå ïðàâèòåëüñòâåííûå âåäîìñòâà ïðè îïðåäåëåííûõ óñëîâèÿõ, îãîâîðåííûõ çàêîíîì, äîëæíû èìåòü âîçìîæíîñòü ïîëó÷èòü îòêðûòûé òåêñò ëþáîãî îáìåíà èíôîðìàöèåé ïî îáùåñòâåííûì ñåòÿì. Â íàñòîÿùåå âðåìÿ many ýòî ìîæåò áûòü òðàêòîâàòüñÿ, êàê òðåáîâàíèå ê çàêîíîïîñëóøíûì ãðàæäàíàì ëèáî (1) *èñïîëüçîâàòü ñëàáûå êðèïòîñèñòåìû* - ò.å., êðèïòîñèñòåìû, êîòîðûå ñîîòâåòñòâóþùèå âëàñòè (à òàêæå êòî óãîäíî!) ñìîãóò âñêðûòü ñ ïîìîùüþ óìåðåííûõ óñèëèé, ëèáî (2) çàðàíåå *ñîîáùàòü ñâîè ñåêðåòû* âëàñòÿì. Íå óäèâèòåëüíî, ÷òî òàêàÿ àëüòåðíàòèâà çàêîííî âñòðåâîæèëà ìíîãèõ çàèíòåðåñîâàííûõ ãðàæäàí, ñîçäàâàÿ â ðåçóëüòàòå ìíåíèå, ÷òî òàéíà ëè÷íîñòè äîëæíà ñòîÿòü íàä íàöèîíàëüíîé áåçîïàñíîñòüþ è îòïðàâëåíèåì çàêîíà.

Óñëîâíîå âðó÷åíèå êëþ÷åé ÿâëÿåòñÿ ñóòüþ ïðîäâèãàåìûõ ïðàâèòåëüñòâîì ÑØÀ ïðîãðàììû Clipper è Ñòàíäàðòà óñëîâíîãî øèôðîâàíèÿ (Escrowed Encryption Standard). Ïðîáëåìà â òîì, ÷òîáû è îáåñïå÷èòü òàéíó ëè÷íîñòè, è â òî æå âðåìÿ ïîçâîëèòü ðàçðåøåííîå ñóäîì ïîäñëóøèâàíèå.

Escrowed Encryption Standard îáåñïå÷èâàåò áåçîïàñíîñòü ñ ïîìîùüþ çàùèùåííîãî îáîðóäîâàíèÿ. Ó êàæäîé ìèêðîñõåìû øèôðîâàíèÿ óíèêàëüíûé èäåíòèôèêàöèîííûé íîìåð (ID) è ñåêðåòíûé êëþ÷. Ýòîò êëþ÷ äåëèòñÿ íà

äâå ÷àñòè è õðàíèòñÿ, âìåñòå ñ ID, äâóìÿ ðàçëè÷íûìè îðãàíèçàöèÿìè óñëîâíîãî âðó÷åíèÿ. Âñÿêèé ðàç, êîãäà ìèêðîñõåìà øèôðóåò ôàéë äàííûõ, îíà ñíà÷àëà øèôðóåò ñåàíñîâûé êëþ÷ óíèêàëüíûì ñåêðåòíûì êëþ÷îì. Çàòåì îíà ïåðåäàåò çàøèôðîâàííûé ñåàíñîâûé êëþ÷ è ñâîé ID ïî êàíàëó ñâÿçè. Êîãäà ïðàâîîõðàíèòåëüíûå îðãàíû õîòÿò ðàñøèôðîâàòü ïîòîê èíôîðìàöèè, çàøèôðîâàííûé îäíîé èç ýòèõ ìèêðîñõåì, îíè èçâëåêàþò èç ïîòîêà ID, ïîëó÷àþò ñîîòâåòñòâóþùèå êëþ÷è èç îðãàíèçàöèé óñëîâíîãî âðó÷åíèÿ, îáúåäèíÿþò èõ ñ ïîìîùüþ îïåðàöèè XOR, ðàñøèôðîâûâàþò ñåàíñîâûé êëþ÷ è çàòåì èñïîëüçóþò åãî äëÿ äåøèôðèðîâàíèÿ ïîòîêà ñîîáùåíèé. Äëÿ çàùèòû îò ìîøåííè÷åñòâà â ýòó ñõåìó ââåäåíû äîïîëíèòåëüíûå óñëîæíåíèÿ, ïîäðîáíî îïèñàííûå â ðàçäåëå 24.16. Àíàëîãè÷íàÿ ñõåìà ìîæåò áûòü ðåàëèçîâàíà è ïðîãðàììíî ñ èñïîëüçîâàíèåì êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè [77, 1579, 1580, 1581].

Ìèêàëè íàçûâàåò ñâîþ èäåþ **÷åñòíîé êðèïòîñèñòåìîé** [1084,10851. (Ãîâîðÿò, ÷òî ïðàâèòåëüñòâî ÑØÀ çàïëàòèëî Ìèêàëè $1000000 çà èñïîëüçîâàíèå åãî ïàòåíòîâ [1086, 1087] â ñâîåì ñòàíäàðòå Escrowed Encryption Standard, çàòåì ïàòåíò Ìèêàëè êóïèë Áàíêîâñêèé òðåñò.) Â òàêèõ êðèïòîñèñòåìàõ çàêðûòûé êëþ÷ äåëèòñÿ íà ÷àñòè è ðàñïðåäåëÿåòñÿ ñðåäè ðàçëè÷íûõ îðãàíèçàöèé. Êàê è ñõåìà ñ ñîâìåñòíûì èñïîëüçîâàíèåì ñåêðåòà, ýòè îðãàíèçàöèè ìîãóò îáúåäèíèòüñÿ è âîññòàíîâèòü çàêðûòûé êëþ÷. Îäíàêî, ÷àñòè êëþ÷à îáëàäàþò äîïîëíèòåëüíûì ñâîéñòâîì - èõ ïðàâèëüíîñòü ìîæåò áûòü ïðîâåðåíà íåçàâèñèìî áåç âîññòàíîâëåíèÿ çàêðûòîãî êëþ÷à.

Àëèñà ìîæåò ñîçäàòü ñâîé ñîáñòâåííûé çàêðûòûé êëþ÷ è ðàñïðåäåëèòü åãî ÷àñòè ñðåäè *n* äîâåðèòåëüíûõ ñîáñòâåííèêîâ. Íè îäèí èç íèõ íå ìîæåò âîññòàíîâèòü çàêðûòûé êëþ÷ Àëèñû. Îäíàêî êàæäûé ìîæåò ïðîâåðèòü, ÷òî åãî ÷àñòü - ýòî ïðàâèëüíàÿ ÷àñòü çàêðûòîãî êëþ÷à. Àëèñà íå ìîæåò ïîñëàòü êîìó-òî èç äîâåðèòåëüíûõ ñîáñòâåííèêîâ ñòðîêó ñëó÷àéíûõ áèòîâ è íàäåÿòüñÿ óëèçíóòü. Åñëè ñóäåáíûå âëàñòè ðàçðåøàò ïîäñëóøèâàíèå, ñîîòâåòñòâóþùèå ïðàâîîõðàíèòåëüíûå îðãàíû ñìîãóò âîñïîëüçîâàòüñÿ ñóäåáíûì ïîñòàíîâëåíèåì äëÿ òîãî, ÷òîáû *n* äîâåðèòåëüíûõ ñîáñòâåííèêîâ âûäàëè ñâîè ÷àñòè. Ñîáðàâ âñå *n* ÷àñòåé, âëàñòè âîññòàíîâÿò çàêðûòûé êëþ÷ è ñìîãóò ïîäñëóøèâàòü ëèíèè ñâÿçè Àëèñû. Ñ äðóãîé ñòîðîíû, ÷òîáû ïîëó÷èòü âîçìîæíîñòü âîññòàíîâèòü êëþ÷ Àëèñû è íàðóøèòü åå òàéíó ëè÷íîñòè, Ìýëëîðè ïðèäåòñÿ êóïèòü âñåõ *n* äîâåðèòåëüíûõ ñîáñòâåííèêîâ.

Âîò êàê ðàáîòàåò ýòîò ïðîòîêîë:

(1) Àëèñà ñîçäàåò ïàðó çàêðûòûé êëþ÷/îòêðûòûé êëþ÷. Îíà ðàçáèâàåò çàêðûòûé êëþ÷ íà íåñêîëüêî îòêðûòûõ è çàêðûòûõ ÷àñòåé.

(2) Àëèñà ïîñûëàåò îòêðûòóþ ÷àñòü è ñîîòâåòñòâóþùóþ çàêðûòóþ ÷àñòü êàæäîìó èç äîâåðèòåëüíûõ ñîáñòâåííèêîâ. Ýòè ñîîáùåíèÿ äîëæíû áûòü çàøèôðîâàíû. Îíà òàêæå ïîñûëàåò îòêðûòûé êëþ÷ â KDC.

(3) Êàæäûé èç äîâåðèòåëüíûõ ñîáñòâåííèêîâ íåçàâèñèìî âûïîëíÿåò âû÷èñëåíèÿ íàä ñâîèìè çàêðûòîé è îòêðûòîé ÷àñòÿìè, ÷òîáû óáåäèòüñÿ â èõ ïðàâèëüíîñòè. Êàæäûé äîâåðèòåëüíûé ñîáñòâåííèê õðàíèò çàêðûòóþ ÷àñòü â êàêîì-íèáóäü íàäåæíîì ìåñòå è îòïðàâëÿåò îòêðûòóþ ÷àñòü â KDC.

(4) KDC âûïîëíÿåò èíîå âû÷èñëåíèå äëÿ îòêðûòûõ ÷àñòåé è îòêðûòîãî êëþ÷à. Óáåäèâøèñü, ÷òî âñå ïðàâèëüíî, îí ïîäïèñûâàåò ïóáëè÷íûé êëþ÷ è îòïðàâëÿåò åãî îáðàòíî Àëèñå èëè ïîìåùàåò â êàêóþ-íèáóäü áàçó äàííûõ.

Ïðè íàëè÷èè ïîñòàíîâëåíèÿ ñóäà î ïîäñëóøèâàíèè êàæäûé èç äîâåðèòåëüíûõ ñîáñòâåííèêîâ ïåðåäàåò ñâîþ ÷àñòü â KDC, è KDC ïîëó÷àåò âîçìîæíîñòü âîññòàíîâèòü çàêðûòûé êëþ÷. Äî ýòîé ïåðåäà÷è íè KDC, íè êòî-ëèáî èç äîâåðèòåëüíûõ ñîáñòâåííèêîâ íå ìîæåò ñàìîñòîÿòåëüíî âîññòàíîâèòü çàêðûòûé êëþ÷, äëÿ âîññòàíîâëåíèÿ êëþ÷à íóæíû âñå äîâåðèòåëüíûå ñîáñòâåííèêè.

Ëþáîé àëãîðèòì ñ îòêðûòûìè êëþ÷àìè ìîæíî ñäåëàòü "÷åñòíûì" ïîäîáíûì îáðàçîì. Ðÿä êîíêðåòíûõ àëãîðèòìîâ ðàññìàòðèâàåòñÿ â ðàçäåëå 23.10. Â ðàáîòå Ìèêàëè [1084, 1085] îáñóæäàþòñÿ ïóòè îáúåäèíåíèÿ îïèñàííîãî ñ ïîðîãîâîé ñõåìîé, ÷òîáû äëÿ âîññòàíîâëåíèÿ çàêðûòîãî êëþ÷à òðåáîâàëîñü íåêîòîðîå ïîäìíîæåñòâî äîâåðèòåëüíûõ ñîáñòâåííèêîâ (íàïðèìåð, òðè èç ïÿòè). Îí òàêæå ïîêàçûâàåò, êàê îáúåäèíèòü ýòî ñ ðàññåÿííîé ïåðåäà÷åé (ñì. ðàçäåë 5.5) òàê, ÷òîáû äîâåðèòåëüíûå ñîáñòâåííèêè íå çíàëè, ÷åé çàêðûòûé êëþ÷ âîññòàíàâëèâàåòñÿ.

"×åñòíûå" êðèïòîñèñòåìû íåñîâåðøåííû. Ïðåñòóïíèê ìîæåò èñïîëüçîâàòü òàêóþ ñèñòåìó, ïðèìåíÿÿ ïîäñîçíàòåëüíûé êàíàë (ñì. ðàçäåë 4.2.), ÷òîáû âñòàâèòü äðóãîé ñåêðåòíûé êëþ÷ â ñâîþ èíôîðìàöèþ. Òàêèì îáðàçîì îí ìîæåò áåçîïàñíî îáìåíèâàòüñÿ èíôîðìàöèåé ñ êåì-íèáóäü åùå, èñïîëüçóÿ ïîäñîçíàòåëüíûé êëþ÷ è ñîâåðøåííî íå âîëíóÿñü ïî ïîâîäó ðàçðåøåííîãî ñóäîì ïîäñëóøèâàíèÿ. Äàííàÿ ïðîáëåìà ðåøàåòñÿ äðóãèì ïðîòîêîëîì, êîòîðûé íàçûâàåòñÿ **îòêàçîóñòîé÷èâûì óñëîâíûì âðó÷åíèåì êëþ÷åé** [946, 833]. Ýòîò àëãîðèòì è ïðîòîêîë îïèñûâàåòñÿ â ðàçäåëå 23.10.

Ïîëèòèêà óñëîâíîãî âðó÷åíèÿ êëþ÷åé

Ïîìèìî ïðàâèòåëüñòâåííûõ ïëàíîâ îòíîñèòåëüíî óñëîâíîãî âðó÷åíèÿ êëþ÷åé ðàñïðîñòðàíÿþòñÿ è êîììåð÷åñêèå ñèñòåìû ñ óñëîâíûì âðó÷åíèåì êëþ÷åé. Âîçíèêàåò î÷åâèäíûé âîïðîñ: êàêîå ïðåèìóùåñòâî îò óñëîâíîãî âðó÷åíèÿ êëþ÷åé ïîëó÷àåò ïîëüçîâàòåëü?

Íó, íà ñàìîì äåëå íèêàêîãî. Ïîëüçîâàòåëü íå ïîëó÷àåò îò óñëîâíîãî âðó÷åíèÿ êëþ÷åé íè÷åãî òàêîãî, ÷åãî îí

è ñàì íå ñìîã áû îáåñïå÷èòü. Îí è ñàì ìîæåò ñîçäàòü ðåçåðâíóþ êîïèþ êëþ÷åé, åñëè çàõî÷åò (ñì. ðàçäåë 8.8). Óñëîâíîå âðó÷åíèå êëþ÷åé ãàðàíòèðóåò, ÷òî ïîëèöèÿ ñìîæåò ïîäñëóøèâàòü åãî ðàçãîâîðû èëè ÷èòàòü ôàéëû äàííûõ, äàæå êîãäà îíè øèôðîâàíû. Îíî ãàðàíòèðóåò, ÷òî NSA ñìîæåò ïîäñëóøèâàòü åãî ìåæäóíàðîäíûå çâîíêè - áåç âñÿêîãî îðäåðà - õîòÿ îíè è øèôðîâàíû. Ìîæåò åìó áóäåò ðàçðåøåíî èñïîëüçîâàòü òàêóþ êðèïòîãðàôèþ ñ òåìè ñòðàíàìè, äëÿ êîòîðûõ ñåé÷àñ óñòàíîâëåíû çàïðåòû, íî ýòî ñîìíèòåëüíîå ïðåèìóùåñòâî.

Íåäîñòàòêè óñëîâíîãî âðó÷åíèÿ êëþ÷åé âåñüìà îáùèå. Ïîëüçîâàòåëþ ïðèõîäèòñÿ âåðèòü â áåçîïàñíîñòü äåéñòâèÿ îðãàíèçàöèé, çàíÿòûõ óñëîâíûì âðó÷åíèåì êëþ÷åé òàêæå, êàê è â ÷åñòíîñòü çàíÿòûõ ýòèì ëþäåé. Åìó ïðèäåòñÿ âåðèòü, ÷òî ïîëèòèêà ñîîòâåòñòâóþùèõ îðãàíèçàöèé îñòàíåòñÿ íåèçìåííîé, ïðàâèòåëüñòâî íå ïîìåíÿåò çàêîíû, è òå, êòî èìååò ïîëíîìî÷èÿ âñêðûòü åãî êëþ÷, áóäóò äåëàòü ýòî ïî çàêîíó è ñ ïîëíîé îòâåòñòâåííîñòüþ. Âîîáðàçèòå íàïàäåíèå òåððîðèñòîâ íà Íüþ-Éîðê, êàêèå áû îãðàíè÷åíèÿ íå áûëè áû ñìåòåíû ïîëèöèåé, ÷òîáû îñòàíîâèòü ïîñëåäñòâèÿ?

Òðóäíî ïðåäñòàâèòü ñåáå, ÷òî ýòè óñëîâíûå ñõåìû øèôðîâàíèÿ, êàê ãîâîðÿò èõ çàùèòíèêè, áóäóò èñïîëüçîâàòüñÿ áåç ïðèíóæäåíèÿ èçâíå. Ñëåäóþùèì î÷åâèäíûì øàãîì áóäåò çàïðåò íà èñïîëüçîâàíèå âñåõ äðóãèõ ñïîñîáîâ øèôðîâàíèÿ. Ýòî, âåðîÿòíî, åäèíñòâåííûé ñïîñîá äîáèòüñÿ êîììåð÷åñêîãî óñïåõà ýòîé ñèñòåìû, è ýòî, îïðåäåëåííî, åäèíñòâåííûé ñïîñîá çàñòàâèòü òåõíè÷åñêè ãðàìîòíûõ ïðåñòóïíèêîâ è òåððîðèñòîâ èñïîëüçîâàòü åå. Ïîêà íå ÿñíî, íàñêîëüêî òðóäíî áóäåò îáúÿâèòü íå-óñëîâíóþ êðèïòîãðàôèþ âíå çàêîíà, èëè êàê ýòî ïîâëèÿåò íà êðèïòîãðàôèþ êàê íà àêàäåìè÷åñêóþ äèñöèïëèíó. Êàê ÿ ìîãó èññëåäîâàòü ïðîãðàììíî îðèåíòèðîâàííûå àëãîðèòìû êðèïòîãðàôèè, íå èìåÿ äîñòóïà ê ïðîãðàììíîìó îáåñïå÷åíèþ óñòðîéñòâ íå-óñëîâíîãî øèôðîâàíèÿ, íóæíà ëè ìíå áóäåò ñïåöèàëüíàÿ ëèöåíçèÿ?

È äðóãèå çàêîííûå âîïðîñû. Êàê óñëîâíî âðó÷åííûå êëþ÷è ïîâëèÿþò íà îòâåòñòâåííîñòü ïîëüçîâàòåëåé, äîëæíà ëè ñòàíîâèòüñÿ èçâåñòíîé çàøèôðîâàííàÿ èíôîðìàöèÿ? Åñëè ïðàâèòåëüñòâî ÑØÀ ïûòàåòñÿ çàùèòèòü îðãàíû óñëîâíîãî âðó÷åíèÿ, íå áóäåò ëè ýòî êîñâåííûì ñâèäåòåëüñòâîì òîãî, ÷òî åñëè ñåêðåò ñêîìïðîìåòèðîâàí ëèáî ïîëüçîâàòåëåì, ëèáî îðãàíàìè óñëîâíîãî âðó÷åíèÿ, òî âèíîâíèêîì áóäåò ïðèçíàí ïîëüçîâàòåëü?

×òî åñëè áàçà äàííûõ ãëàâíîé ñëóæáû óñëîâíîãî âðó÷åíèÿ êëþ÷åé, âñå ðàâíî ãîñóäàðñòâåííîé èëè êîììåð÷åñêîé, áóäåò óêðàäåíà? ×òî, åñëè ïðàâèòåëüñòâî ÑØÀ ïîïûòàåòñÿ íåíàäîëãî ñêðûòü ýòîò ôàêò? ßñíî, ÷òî âñå ýòè âîïðîñû ïîâëèÿþò íà æåëàíèå ïîëüçîâàòåëåé ïîëüçîâàòüñÿ óñëîâíûì âðó÷åíèåì êëþ÷åé. Åñëè èñïîëüçîâàíèå íå áóäåò äîáðîâîëüíûì, òî ïàðà ñêàíäàëîâ âûçîâåò ðîñò ïîëèòè÷åñêîãî äàâëåíèÿ ñ öåëüþ ëèáî ñäåëàòü èñïîëüçîâàíèå ïîäîáíûõ ñèñòåì äîáðîâîëüíûì, ëèáî ââåñòè íîâûå ñëîæíûå ïðàâèëà â ýòîé îòðàñëè.

Åùå áîëåå îïàñíûì áóäåò ñêàíäàë, êîãäà âûÿñíèòñÿ, ÷òî ãîäàìè ïîä íàáëþäåíèåì íàõîäèëñÿ ïîëèòè÷åñêèé îïïîíåíò òåêóùåé àäìèíèñòðàöèè èëè íåêèé ãðîìêîãîëîñûé êðèòèê ñïåöñëóæá è ïîëèöåéñêèõ âåäîìñòâ. Ýòî ñèëüíî íàñòðîèò îáùåñòâåííîå ìíåíèå ïðîòèâ óñëîâíîãî øèôðîâàíèÿ.

Åñëè êëþ÷è ïîäïèñåé áóäóò øèôðîâàòüñÿ òåì æå ñïîñîáîì, ÷òî è êëþ÷è øèôðîâàíèÿ, âîçíèêíóò äîïîëíèòåëüíûå ìîìåíòû. Äîïóñòèìî ëè äëÿ âëàñòåé èñïîëüçîâàòü êëþ÷è ïîäïèñåé äëÿ ïðîâåäåíèÿ îïåðàöèè ïðîòèâ ïîäîçðåâàåìîãî ïðåñòóïíèêà? Áóäåò ëè ïðèçíàíà ñóäîì ïîäëèííîñòü ïîäïèñåé, îñíîâàííûõ íà êëþ÷àõ ñ óñëîâíûì âðó÷åíèåì? ×åì â äåéñòâèòåëüíîñòè áóäóò âëàäåòü ïîëüçîâàòåëè, åñëè âëàñòè äåéñòâèòåëüíî èñïîëüçóþò èõ êëþ÷è ïîäïèñåé äëÿ ïîäïèñè êàêîãî-òî íåâûãîäíîãî êîíòðàêòà, äëÿ ïîääåðæêè îïðåäåëåííûõ îòðàñëåé ïðîìûøëåííîñòè, èëè ïðîñòî, ÷òîáû óêðàñòü äåíüãè?

Ãëîáàëüíîå ðàñïðîñòðàíåíèå êðèïòîãðàôèè ðîæäàåò äîïîëíèòåëüíûå âîïðîñû. Áóäóò ëè ñõåìû óñëîâíîãî âðó÷åíèÿ êëþ÷åé ñîâìåñòèìû â ðàçëè÷íûõ ñòðàíàõ? Çàõîòÿò ëè òðàíñíàöèîíàëüíûå êîðïîðàöèè ñìèðèòüñÿ ñ ñóùåñòâîâàíèåì â êàæäîé ñòðàíå ñâîèõ óñëîâíî âðó÷åííûõ êëþ÷åé, ñîâìåñòèìûõ ñ ðàçëè÷íûìè ìåñòíûìè çàêîíîäàòåëüñòâîì? Áåç îáåñïå÷åíèÿ ñîâìåñòèìîñòè èñ÷åçàåò îäíî èç ïðîïàãàíäèðóåìûõ ïðåèìóùåñòâ ñõåì ñ óñëîâíûì âðó÷åíèåì êëþ÷åé (ìåæäóíàðîäíîå èñïîëüçîâàíèå ìîùíûõ ñðåäñòâ êðèïòîãðàôèè).

×òî åñëè ðÿä ñòðàí íå ïðèìåò íà âåðó íàäåæíîñòü îðãàíèçàöèé, ñâÿçàííûõ ñ óñëîâíûì âðó÷åíèåì êëþ÷åé? Êàê áóäóò ïîëüçîâàòåëè âåñòè ñâîè äåëà â ýòèõ ñòðàíàõ? Áóäóò ëè ïðèçíàíû ñóäàìè èõ ýëåêòðîííûå êîíòðàêòû, èëè òîò ôàêò, ÷òî êëþ÷è èõ ïîäïèñåé óñëîâíî õðàíÿòñÿ â ÑØÀ, ïîçâîëèò èì óòâåðæäàòü ãäå-íèáóäü â Øâåéöàðèè, ÷òî ýòîò ýëåêòðîííûé êîíòðàêò ìîã ïîäïèñàòü êòî-òî äðóãîé? Èëè äëÿ ëþäåé, êîòîðûå âåäóò äåëà â ïîäîáíûõ ñòðàíàõ, áóäóò ñïåöèàëüíûå èñêëþ÷åíèÿ?

À ÷òî äåëàòü ñ ïðîìûøëåííûì øïèîíàæåì? Ãäå ãàðàíòèè, ÷òî ñòðàíû, çàíèìàþùèåñÿ ñåé÷àñ ïðîìûøëåííûì øïèîíàæåì äëÿ ñâîèõ âàæíåéøèõ èëè ãîñóäàðñòâåííûõ ïðåäïðèÿòèé, íå âîñïîëüçóþòñÿ äëÿ ýòîãî ñèñòåìàìè ñ óñëîâíûì âðó÷åíèåì êëþ÷åé? Â ñàìîì äåëå, òàê êàê íè îäíà ñòðàíà íå ñîáèðàåòñÿ ïîçâîëÿòü äðóãèì ñòðàíàì ñëåäèòü çà ñâîèìè ðàçâåäûâàòåëüíûìè îïåðàöèÿìè, ðàñïðîñòðàíåíèå óñëîâíîãî øèôðîâàíèÿ âîçìîæíî ïðèâåäåò ê óâåëè÷åíèþ ïîäñëóøèâàíèÿ.

Äàæå åñëè ñòðàíû, â êîòîðûõ ñîáëþäàþòñÿ ãðàæäàíñêèå ïðàâà, áóäóò èñïîëüçîâàòü óñëîâíîñòü òàêîãî øèôðîâàíèÿ òîëüêî äëÿ çàêîííîãî ïðåñëåäîâàíèÿ ïðåñòóïíèêîâ è òåððîðèñòîâ, ãäå-íèáóäü ýòèì îáÿçàòåëüíî âîñïîëüçóþòñÿ äëÿ âûñëåæèâàíèÿ äèññèäåíòîâ, øàíòàæà ïîëèòè÷åñêèõ îïïîíåíòîâ, è ò.ï. Öèôðîâûå ëèíèè ñâÿçè ïðåäîñòàâëÿþò âîçìîæíîñòü ãîðàçäî áîëåå òùàòåëüíî, ÷åì ýòî áûëî âîçìîæíî â àíàëîãîâîì ìèðå, êîíòðîëèðîâàòü äåéñòâèÿ ãðàæäàí, èõ ìíåíèÿ, Digital communications offer the opportunity to do a much more thorough lob of

monitoring citizens' actions, opinions, äîõîäû è îáúåäèíåíèÿ.

Íå ÿñíî, íå áóäåò ëè ÷åðåç 20 ëåò ïðîàäæà ñèñòåìû ñ óñëîâíûì âðó÷åíèåì êëþ÷åé Òóðöèè èëè Êèòàþ ïîõîäèòü íà ïðîäàæó ýëåêòðè÷åñêèõ äóáèíîê Þæíîé Àôðèêå â 1970 ãîäó èëè íà ñòðîèòåëüñòâî õèè÷åñêîãî çàâîäà â Èðàêå â 1980 ãîäó. Äàæå õóæå, ëåãêîå è íåçàìåòíîå ïîäëóøèâàíèå ëèíèé ñâÿçè ìîæåò èñêóñèòü ìíîãèå ïðàâèòåëüñòâà, êîòîðûå ðàíüøå, âîçìîæíî, ýòèì è íå çàíèìàëèñü, ñëåäèòü çà êîððåñïîíäåíöèåé ñâîèõ ãðàæäàí. È íåò ãàðàíòèè, ÷òî ëèáåðàëüíûå äåìîêðàòèè óñòîÿò ïåðåä ïîäúåìîì èñêóøåíèì.

Ãëàâà 5
Ðàçâèòûå ïðîòîêîëû

5.1 Äîêàçàòåëüñòâà ñ íóëåâûì çíàíèåì

À âîò äðóãàÿ èñòîðèÿ:

Àëèñà: "ß çíàþ ïàðîëü êîìïüþòåðà Ôåääåðàëüíîé Ðåçåðâíîé Ñèñòåìû, êîìïîíåíòû ñåêðåòíîãî ñîóíà ÌàêÄîíàëüäñ è îäíîãî èç 4-õ òîìà Äîíàëüäà Êíóòà".

Áîá: "Íåò, òû íå çíàåøü".

Àëèñà: "Íåò, ÿ çíàþ".

Áîá: "Íå çíàåøü".

Àëèñà: "Íåò, çíàþ".

Áîá: "Äîêàæè".

Àëèñà: "Õîðîøî, ÿ ñêàæó òåáå". Îíà øåïíåò Áîáó íà óõî.

Áîá: "Ýòî èíòåðåñíî. Òåïåðü ÿ òîæå ýòî çíàþ è ñîáèðàþñü ðàññêàçàòü ýòî âñå *Âàøèíãòîí Ïîñò*".

Àëèñà: "Îïîé".

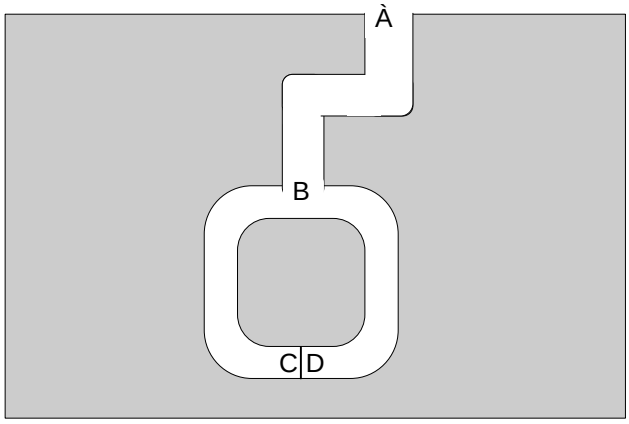
Ê íåñ÷àñòüþ, îáû÷íî Àëèñà ìîæåò äîêàçàòü ÷òî-íèáóäü Áîáó, òîëüêî ðàññêàçàâ åìó âñå. Íî òîãäà îí òîæå ïîëó÷èò âñå ñâåäåíèÿ. Çàòåì Áîá ìîæåò âûëîæèòü ïîëó÷åííûå ñâåäåíèÿ êîìó óãîäíî, è Àëèñà íè÷åãî íå ñìîæåò ñ ýòèì ïîäåëàòü. (Â ëèòåðàòóðå äëÿ îïèñàíèÿ ýòèõ ïðîòîêîëîâ ÷àñòî èñïîëüçóþòñÿ ðàçëè÷íûå ïåðñîíàæè. Ïåããè îáû÷íî äîêàçûâàåò, à Âèêòîð ïðîâåðÿåò. Èìåííî ýòè èìåíà ïîÿâëÿþòñÿ â èñïîëüçóåìûõ ïðèìåðàõ âìåñòî Àëèñû è Áîáà.)

Èñïîëüçóÿ îäíîíàïðàâëåííûå ôóíêöèè, Ïåããè ñìîæåò ïðîâåñòè **äîêàçàòåëüñòâî ñ íóëåâûì çíàíèåì** [626]. Ýòî ïðîòîêîë äîêàçûâàåò Âèêòîðó, ÷òî ó Ïåããè äåéñòâèòåëüíî åñòü èíôîðìàöèÿ, íî íå äàåò Âèêòîðó íå ìàëåéøåé âîçìîæíîñòè óçíàòü, ÷òî ýòî çà èíôîðìàöèÿ.

Ýòè äîêàçàòåëüñòâà ïðèíàäëåæàò ôîðìó èíòåðàêòèâíîãî ïðîòîêîëà. Âèêòîð çàäàåò Ïåããè ðÿä âîïðîñîâ. Åñëè Ïåããè çíàåò ñåêðåò, òî îíà îòâå÷àåò íà âñå âîïðîñû ïðàâèëüíî. Åñëè ñåêðåò åé íåèçâåñòåí, ó íåå åñòü íåêîòîðàÿ âåðîÿòíîñòü - 50 ïðîöåíòîâ â ñëåäóþùèõ ïðèìåðàõ - îòâå÷àòü ïðàâèëüíî. Ïîñëå ïðèìåðíî 10 âîïðîñîâ Âèêòîð óáåäèòñÿ, ÷òî Ïåããè çíàåò ñåêðåò. Íî íè îäèí èç âîïðîñîâ èëè îòâåòîâ íå äàñò Âèêòîðó íè ìàëåéøèõ ñâåäåíèé îá èíôîðìàöèè Ïåããè, íî äîêàæåò çíàíèå Ïåããè ýòîé èíôîðìàöèè.

Áàçîâûé ïðîòîêîë ñ íóëåâûì çíàíèåì

Æàí-Æàê Êèñêàòåð (Jean-Jacques Quisquater) è Ëóè Ãèëó (Louis Guillou) ïîÿâèëè íóëåâîå çíàíèå èñòîðèé î ïåùåðå [1281]. Ó ïåùåðû, ïîêàçàíî íà 4-é, åñòü ñåêðåò. Òîò, êòî çíàåò âîøåäøóþ ñëîâà ìîæåò îòêðûòü äâåðü ìåæäó C è D. Äëÿ âñåõ îñòàëüíûõ îáà ïðîõîäà âåäóò â òóïèê.



Ðèñ. 5-1. Ïåùåðà íóëåâîãî çíàíèÿ

Ïåããè çíàåò ñåêðåò ïåùåðû. Îíà õî÷åò äîêàçàòü ñâîå çíàíèå Âèêòîðó, íî íå õî÷åò ðàñêðûâàòü âîëøåáíûõ ñëîâ. Âîò êàê îíà óáåæäàåò åãî:

(1) Âèêòîð íàõîäèòñÿ â òî÷êå À.

(2) Ïåããè ïðîõîäèò âñþ ïóòü ïî ïåùåðå, ëèáî äî òî÷êè C, ëèáî äî òî÷êè D.

(3) Ï îñëå òîãî, êàê Ïåãàè èñ÷åçíåò â ïåùåðå, Âèêòîð ïåðåõîäèò â òî÷êó Â.

(4) Âèêòîð êðè÷èò Ïåãàè, ñïðàøèâàÿ åå ëèáî î:

(a) èëè âûéòè èç ëàáîðàòîðèè

(b) âûéòè èç ïðàâîãî ïðîõîäà.

(5) Ïåãàè èñïîëíÿåò åãî ïðîñüáó, ïðè íåîõîäèìîñòè èñïîëüçóÿ âîëøåáíûå ñëîâà, ÷òîáû îòïðàâèòü äâåðü.

(6) Ïåãàè è Âèêòîð ïîâòîðÿþò ýòàïû (1) - (5) *n* ðàç.

Ïðåäïîëîæèì, ÷òî ó Âèêòîðà åñòü âèäåîêàìåðà, è îí çàïèñûâàåò âñå, ÷òî âèäèò. Î í çàïèñûâàåò, êàê Ïåãàè èñ÷åçàåò â ïåùåðå, çàïèñûâàåò, êàê îí ñàì êðè÷èò, óêàçûâàÿ, ãäå Ïåãàè äîëæíà ïîÿâèòüñÿ, çàïèñûâàåò êàê Ïåãàè ïîÿâëÿåòñÿ. Î í çàïèñûâàåò âñå *n* òåñòîâ. Åñëè îí ïîêàæåò ýòó âèäåîçàïèñü Êýðîë, ïîâåðèò ëè îíà, ÷òî Ïåãàè çíàåò âîëøåáíûå ñëîâà, îòïèðàþùèå äâåðü? Íåò. À ÷òî åñëè Ïåãàè è Âèêòîð çàðàíåå äîãîâîðèëèñü, ÷òî Âèêòîð áóäåò êðè÷àòü, à Ïåãàè áóäåò äåëàòü âèä, ÷òî îíà ïðîøëà âñïü ïóòü. Òîãäà îíà áóäåò êàæäûé èç óêàçàííîâ Âèêòîðîì ìåñòà, íå çíàÿ âîëøåáíûõ ñëîâ. Èëè îíè ìîãëè ñäåëàòü ïî äðóãîìó. Ïåãàè âõîäèò â îäèí èç ïðîõîäîâ è Âèêòîð ñëó÷àéíûì îáðàçîì âûêðè÷àëè ñâîè ïðîñüáû. Åñëè Âèêòîð óãàäûâàåò ïðàâèëüíî, õîðîøî, åñëè íåò - îíè âûðâæóò ýòó ïîïûòêó èç âèäåîçàïèñè. Â ëþáîì ñëó÷àå Âèêòîð ìîæåò ïîëó÷èòü âèäåîçàïèñü, ïîêàçûâàþùóþ â òî÷íîñòè òó ïîñëåäîâàòåëüíîñòü, êîòîðàÿ ïîëó÷èëàñü áû, åñëè áû Ïåãàè çíàëà âîëøåáíûå ñëîâà.

Ýòî îïûò ïîêàçûâàåò äâå âåùè. Âî ïåðâûõ, Âèêòîð íå ìîæåò óáåäèòü òðåòüþ ñòîðîíó â ïðàâèëüíîñòè äîêàçàòåëüñòâà. È âî âòîðûõ, äàííûé ïðîòîêîë ÿâëÿåòñÿ ïðîòîêîëîì ñ óòå÷êîé çíàíèåì. Åñëè Ïåãàè íå çíàåò âîëøåáíûõ ñëîâ, òî î÷åâèäíî, ÷òî Âèêòîð íå óçíàåò íè÷åãî èç ïðîñìîòðà âèäåîçàïèñè. Í î òàê êàê íåò ñïîñîáà îòëè÷èòü ðåàëüíóþ âèäåîçàïèñü îò ïîääåëüíîé, òî Âèêòîð íå ìîæåò íè÷åãî óçíàòü èç ðåàëüíîãî äîêàçàòåëüñòâà - ýòî è åñòü íóëåâîå çíàíèå.

Ìåòîäèêà, èñïîëüçóåìàÿ â ýòîì ïðîòîêîëå, íàçûâàåòñÿ **ðàçðåçàòü è âûáðàòü** èç-çà òîãî, ÷òî îíà ïîõîæ íà êëàññè÷åñêèé ïðîòîêîë ÷åñòíîãî äåëåíèÿ ÷åãî-ëèáî:

(1) Àëèñà äåëèò íåóþ âåùü ïîïîëàì.

(2) Áîá âûáèðàåò îäíó èç ïîëîâèí ñåáå.

(3) Àëèñà çàáèðàåò îñòàâøóþñÿ ïîëîâèíó.

Â èòîãñàõ Àëèñû ÷åñòíî ðàçäåëèòü íà ýòàïå (1), ïîòî÷òî Áîá âûáðàë íà ýòàïå (2) òó ïîëîâèíó, êîòîðàÿ åì áîëüøå íðàâèòñÿ. Ì àéêë Ðàáèí (Michael Rabin) ïðåäëî ì èñïîëüçîâàë â êðèòîãðàôèè òåõíèêó "ðàçðåçàòü è âûáðàòü" [1282]. Ï î íýòèÿ **èíòðàêòèâíîãî ïðîòîêîëà** è íóëåâîãî çíàíèÿ áûëè ôîðìàëèçîâàíû ïîçæå [626, 627].

Ïðîòîêîë "ðàçðåçàòü è âûáðàòü" ðàáîòàåò, ïîòî÷òî Ïåãàè íå ìîæåò íåñêîëüêî ðàç ïîäðÿä óãàäûâàòü, îòêóäà Âèêòîð ïîïðîñèò åå âûéòè. Åñëè Ïåãàè íå çíàåò ñåðâåðà, îí ìîæåò âûéòè òîëüêî èç òîãî ïðîõîäà, â êîòîðûé îíà çàøëà. Â èäåàëå ðàóíäîòîêîëà åå âåðîÿòíîñòü (èíäåêñ íàçûâàåìàÿ **âêëþ÷èòåëüíîñòüþ**) óãàäàòü, ñ êàêîé ñòîðîíû Âèêòîð ïîïðîñèò åå âûéòè, ñîñòàâëÿåò 50 ïðîöåíòîâ, ïîýòîìó åå âåðîÿòíîñòü îãàäàòü Âèêòîðà òàêæå ðàâíà 50 ïðîöåíòàì. Âåðîÿòíîñòü îáìàíóòü åãî â äâóõ ðàóíäàõ ñîñòàâèò 25 ïðîöåíòîâ, à âî âñåõ *n* ðàóíäàõ - îäèí øàíñ èç 2^n. Ï îñëå 16 ðàóíäîâ ó Ïåãàè 1 øàíñ èç 65536 îáìàíóòü Âèêòîðà. Âèêòîð ìîæåò óâåðåííî ïðåäïîëîæèòü, ÷òî åñëè âñå 16 äîêàçàòåëüñòâ Ïåãàè ïðåäúÿâëåíû, òî îíà äåéñòâèòåëüíî çíàêî òàéíûå ñëîâà, îòêðûâàþùèå äâåðü ìåæäó òî÷êàìè C è D. (Àíàëîãè ñ ïåùåðîé íåñîâåðøåííà. Ïåãàè ìîæåò ïðîñòî âûäîëáèòü ñ îäíîé ñòîðîíû è âûõîäèòü ñ äðóãîé, ïðîòîêîë "ðàçðåçàòü è âûáðàòü" íå íóæåí. Îäíàêî, îí íåíóæäàåòñÿ ñ äëÿ íóëåâîãî çíàíèÿ ñ ìàòåìàòè÷åñêîé òî÷êè çðåíèÿ.)

Ïðåäïîëîæèì, ÷òî Ïåãàè èçâåñòíà íåêîòîðàÿ èíôîðìàöèÿ, êîòîðàÿ ÿâëÿåòñÿ ðåøåíèåì òðóäíîé ïðîáëåìû. Áàçîâûé ïðîòîêîë íóëåâîãî çíàíèÿ ñîñòîèò èç íåñêîëüêèõ ðàóíäîâ.

(1) Ïåãàè èñïîëüçóåò ñâîþ èíôîðìàöèþ è ñëó÷àéíûå ÷èñëî äëÿ ïðåáðàçîâàíèÿ îäíîé òðóäíîé ïðîáëåìû â äðóãóþ, èçîìîðôíóþ îðèãèíàëüíîé ïðîáëåìå. Çàòåì îíà èñïîëüçóåò ñâîþ èíôîðìàöèþ è ñëó÷àéíîå ÷èñëî äëÿ ðåøåíèÿ íîâîé òðóäíîé ïðîáëåìû.

(2) Ïåãàè âðó÷àåò ðåøåíèå íîâîé ïðîáëåìû, èñïîëüçóÿ ñòåïó âðó÷åíèÿ áèòà.

(3) Ïåãàè ðàñêðûâàåò Âèêòîðó íîâûé ýêçåìïëÿð ïðîáëåìû. Âèêòîð íå ìîæåò èñïîëüçîâàòü ýòó íîâóþ ïðîáëåìó äëÿ ïîëó÷åíèÿ èíôîðìàöèè î ïðåäûíà÷àëüíîé ïðîáëåìå èëè åå ðåøåíèè.

(4) Âèêòîð ïðîñèò Ïåãàè ëèáî

(a) äîêàçàòü åìó, ÷òî íîâàÿ è ñòàðàÿ ïðîáëåìà èçîìîðôíû (ò.å., äâà ðàçëè÷íûõ ðåøåíèÿ äëÿ äâóõ ñâÿçàííûõ ïðîáëåì), ëèáî

(b) îòêðûòü ðåøåíèå, ïîëó÷åííîå íà ýòàïå (2) è äîêàçàòü, ÷òî ýòî ðåøåíèå íîâîé ïðîáëåìû.

(5) Ïåãåè èñïîëíÿåò åãî ïðîñüáó.

(6) Ïåãåè è Âèêòîð ïîâòîðÿþò ýòàïû (1) - (5) *n* ðàç.

Ïîíèìàå âèäåîêàìåðó â ïðîìûøëåííîñòè äëÿ ïåùåðû? Çäåñü âû ìîæåòå ñäåëàòü òî æå ñàìîå. Âèêòîð ìîæåò çàïèñàòü îáìåí ìåæäó íèì è Ïåãåå. Î í íå ñìîæåò èñïîëüçîâàòü ýòó çàïèñü äëÿ óáåæäåíèÿ Êýðîë, íî îí âñåãäà ìîæåò ñãîâîðèòüñÿ ñ Ïåãåå ñ öåëüþ ñîçäàòü èìèòàòîð, êîòîðûé ïîääåëûâàåò èíôîðìàöèþ Ïåãåå. Ýòîò àðãóìåíò ìîæåò áûòü èñïîëüçîâàí, ÷òîáû äîêàçàòü, ÷òî èñïîëüçóåòñÿ äîêàçàòåëüñòâî ñ íóëåâûì çíàíèåì.

Ìàòåìàòè÷åñêàÿ îñíîâà äîêàçàòåëüñòâà ýòîãî òèïà ñëîæíà. Ïðîáëåìû è ñëó÷àéíûå ïðåáðàçîâàíèå äîêàçàòåëüñòâ âûáðàòüñÿ îñòîðîæíî, ÷òîáû Âèêòîð íå ïîëó÷èë íèêàêîé èíôîðìàöèè î ðåøåíèè îðèãèíàëüíîé ïðîáëåìû, äàæå ïîñëå ìíîãèõ ïîâòîðåíèé ïðîòîêîëà. Íå âñå òðóäíûå ïðîáëåìû ìîæíî èñïîëüçîâàòü äëÿ äîêàçàòåëüñòâ ñ íóëåâûì çíàíèåì, íî áîëüøèíñòâî èç íèõ.

Èçîìîðôèçì ãðàôà

Îáúÿñíåíèå ýòîãî ïîíÿòèÿ, ïðèøëàøåäøåãî èç òåîðèè ãðàôîâ [619, 622], ìîæåò çàíÿòü íåêîòîðîå âðåìÿ. Ãðàô ïðåäñòàâëÿåò ñîáîé ñåòü ëèíèé ,ñîåäèíÿþ ùèõ ðàçëè÷íûå òî÷êè. Åñëè äâà ãðàôà èäåíòè÷íû âî âñåì, êðîìå èìåí òî÷åê, îíè íàçûâàþòñÿ **èçîìîðôíûìè**. Äëÿ î÷åíü áîëüøèõ ãðàôîâ äîêàçàòåëüñòâî èõ èçîìîðôíîñòè ìîæåò ïîòðåáîâàòü âåêîâ êîìïüþòåðíîãî âðåìåíè, ýòî îäíà èç òàê íàçûâàåìûõ **NP-ïîëíûõ** ïðîáëåì, ðàññìàòðèâàåìûõ â ðàçäåëå 11.1.

Ïðåäïîëîæèì, ÷òî Ïåãåè çíàåò îá èçîìîðôíîñòè äâóõ ãðàôîâ, G_1 è G_2. Ñëåäóþùèé ïðîòîêîë äîêàæåò Âèêòîðó çíàíèå Ïåãåå:

(1) Ïåãåè ñëó÷àéíûì îáðàçîì òàñóåò G_1, ïîëó÷àÿ äðóãîé ãðàô, $Í$, êîòîðûé èçîìîðôåí G_1. Òàê êàê Ïåãåè çíàåò îá èçîìîðôèçìå $Í$ è G_1, òî åé òàêæå èçâåñòíî èçîìîðôèçì ìåæäó $Í$ è G_2. Äëÿ ëþáîãî äðóãîãî ïîèñê èçîìîðôèçìà ìåæäó $Í$ è G_1 èëè $Í$ è G_2 ÿâëÿåòñÿ òàêîé æå òðóäíîé çàäà÷åé, êàê è ïîèñê èçîìîðôèçìà ìåæäó G_1 è G_2.

(2) Ïåãåè ïîñûëàåò $Í$ Âèêòîðó.

(3) Âèêòîð ïðîñèò Ïåãåè ëèáî

  (a) äîêàçàòü, ÷òî $Í$ è G_1 èçîìîðôíû, ëèáî

  (b) äîêàçàòü, ÷òî $Í$ è G_2 èçîìîðôíû.

(4) Ïåãåè èñïîëíÿåò åãî ïðîñüáó. Îíà ëèáî:

  (a) äîêàçûâàåò, ÷òî $Í$ è G_1 èçîìîðôíû, íå äîêàçûâàÿ, ÷òî $Í$ è G_2 èçîìîðôíû, ëèáî

  (b) äîêàçûâàåò, ÷òî $Í$ è G_2 èçîìîðôíû, íå äîêàçûâàÿ, ÷òî $Í$ è G_1 èçîìîðôíû.

(5) Ïåãåè è Âèêòîð ïîâòîðÿþò ýòàïû (1) - (4) *n* ðàç.

Åñëè Ïåãåè íå çíàåò îá èçîìîðôèçìå ìåæäó G_1 è G_2, îíà íå ñìîæåò ñîçäàòü ãðàô $Í$, èçîìîðôíûé îáîèì ãðàôàì. Îíà ìîæåò ñîçäàòü ëèáî ãðàô, êîòîðûé èçîìîðôåí G_1, ëèáî ãðàô, êîòîðûé èçîìîðôåí G_2. Êàê è â ïðåäûäóùåì ïðèìåðå ó íåå òîëüêî 50 øàíñîâ èç 100 óãàäàòü, êàêîå äîêàçàòåëüñòâî îò íåå Âèêòîð íà ýòàïå (3).

Ýòîò ïðîòîêîë íå äàåò Âèêòîðó íèêàêîé ïîëåçíîé èíôîðìàöèè, ïîìîãàþùåé åìó èç îòâåòîâ Ïåãåè óñòàíîâèòü èçîìîðôèçì ìåæäó G_1 è G_2. Òàê êàê Ïåãåè äëÿ êàæäîãî íîâîãî ðàóíäà ïðîòîêîëà ãåíåðèðóåò íîâûé ãðàô $Í$, Âèêòîð íå ñìîæåò ïîëó÷èòü íèêàêîé íåçàâiñèìî îò òîãî, èç ñêîëüêèõ ðàóíäîâ áóäåò ñîñòîÿòü èõ ïðîòîêîë. Î í íå ñìîæåò èç îòâåòîâ Ïåãåè óñòàíîâèòü èçîìîðôèçì ìåæäó G_1 è G_2.

Â êàæäîì ðàóíäå Âèêòîð ïîëó÷àåò íîâûå ñëó÷àéíûå ïðåîáðàçîâàíèå $Í$, âìåñòå ñ èçîìîðôèçìîì ìåæäó $Í$ è G_1 èëè G_2. Âèêòîð ìîæåò òàêæå ñîçäàòü ÷òî-òî ïîäîáíîå ñàìîñòîÿòåëüíî. Òàê êàê Âèêòîð ìîæåò ñîçäàòü èìèòàöèþ ïðîòîêîëà, ýòî äåéñòâèòåëüíî äîêàçàòåëüñòâî ñ íóëåâûì çíàíèåì.

Ãàìèëüòîíîâû öèêëû

Âàðèàíò ýòîãî ïðèìåðà áûë âïåðâûå ïðåäñòàâëåí Ìàíóýëîì Áëþìîì (Manuel Blum) [196]. Ïåãåè çíàåò êðóãîâîé, ïðîïîëæèòåëüíûé ïóòü âäîëü ëèíèé ãðàôà, êîòîðûé ïîñåùàåò êàæäóþ òî÷êó òî÷íî îäèí ðàç. Ýòîò ïóòü íàçûâàåòñÿ **ãàìèëüòîíîâûì öèêëîì**. Ïîñêîëüêó ãàìèëüòîíîâà öèêëà ÿâëÿåòñÿ äðóãîé òÿæåëîé çàäà÷åé. Ó Ïåãåè åñòü ýòà èíôîðìàöèÿ - îíà, âîçìîæíî, ïîëó÷èëà åå ñîçäàâ ãðàô ñ êîíêðåòíûì ãàìèëüòîíîâûì öèêëîì - è îíà õî÷åò äîêàçàòü Âèêòîðó, ÷òî ýòà èíôîðìàöèÿ åé èçâåñòíà.

Ïåãåè çíàåò ãàìèëüòîíîâ öèêë ãðàôà, G. Âèêòîðó èçâåñòåí G, íî íå âåñ ãàìèëüòîíîâà öèêëà. Ïåãåè õî÷åò äîêàçàòü Âèêòîðó, ÷òî îíà çíàåò ãàìèëüòîíîâ öèêë, íå ðàñêðûâàÿ ñàìîãî öèêëà. Âîò êàê îíà äîëæíà äåéſòâîâàòü:

(1) Ïåãåè ñëó÷àéíûì îáðàçîì ïðåîáðàçîâûâàåò G. Îíà ïðåäâêàðèòåëüíî òî÷êè è èçìåíÿåò èõ ìåòêè, ñîçäàâàÿ íî-

âûé ãðàô, *H*. Ïîñêîëüêó *G* è *H* òî÷íîãî÷åñêè èçîìîðôíû (ò.å., ýòî îäèí è òîò æå ãðàô), åñëè åé èçâåñòåí ãàìèëüòîíîâ öèêë *G*, òî îíà ëåãêî ìîæåò íàéòè ãàìèëüòîíîâ öèêë *H*. Åñëè îíà íå ñìîãëà ñîçäàòü *H*, îïðåäåëåíèå èçîìîðôèçìà ìåæäó âåðøèíàìè áóäåò ÿâëÿòüñÿ äóãîé ñëîæíîé ïðîáëåìîé, ðåøåíèå êîòîðîé òàêæå ïîòðåáóåò ââåäåíèÿ êîìïüþòåðíîãî âðåìåíè. Çàòåì îíà øèôðóåò *H*, ïîëó÷àÿ *H'*. (Äîêàæèòå èñïîëüçîâàòüñÿ âåðîÿòíîñòíîå øèôðîâàíèå êàæäîé ñòðî÷êè *H*, òî åñòü, øèôðîâàííûé 0 èëè øèôðîâàííàÿ 1 äëÿ êàæäîé ëèíèè *H*.)

(2) Ïåããè ïåðåäàåò Âèêòîðó êîïèþ *H*.

(3) Âèêòîð ïðîñêàí Ïåããè ëèáî:

(a) äîêàçàòü åìó, ÷òî *Í'* - ýòî çàøèôðîâàííàÿ èçîìîðôíàÿ êîïèÿ *G*, ëèáî

(b) ïîêàçàòü åìó ãàìèëüòîíîâ öèêë äëÿ *Í*.

(4) Ïåããè èñïîëíÿåò åãî ïðîñüáó. Îíà ëèáî:

(a) äîêàçûâàåò, ÷òî *Í'* - ýòî çàøèôðîâàííàÿ èçîìîðôíàÿ êîïèÿ *G*, ðàñêðûâàÿ ïðåîáðàçîâàíèÿ è ðàñøèôðîâûâàÿ âñå, íå ïîêàçûâàÿ ãàìèëüòîíîâ öèêë äëÿ *G* èëè *Í*, ëèáî

(b) ïîêàçûâàåò ãàìèëüòîíîâ öèêë äëÿ *Í*, ðàñøèôðîâûâàÿ òîëüêî òå ñòðîêè, êîòîðûå îáðàçóþò ãàìèëüòîíîâ öèêë, íå äîêàçûâàÿ, ÷òî *Í* è *G* òîïîëîãè÷åñêè èçîìîðôíû.

(5) Ïåããè è Âèêòîð ïîâòîðÿò ýòàïû (1) - (4) *n* ðàç.

Åñëè Ïåããè íå îáìàíûâàåò, îíà ñìîæåò ïðåäúÿâèòü Âèêòîðó îäíî èç äîêàçàòåëüñòâ íà ýòàïå (3). Îäíàêî, åñëè ãàìèëüòîíîâ öèêë äëÿ *G* åé íåèçâåñòåí, îíà íå ñìîæåò ñîçäàòü çàøèôðîâàííûé ãðàô *H'*, êîòîðûé óäîâëåòâîðÿåò îáîèì äîêàçàòåëüñòâàì. Ëó÷øå, ÷òî îíà ìîæåò ñäåëàòü - ýòî ñîçäàòü èëè ãðàô, èçîìîðôíûé *G*, èëè ãðàô ñ òàêèì æå ÷èñëîì òî÷åê è ëèíèé è ïðàâèëüíûì ãàìèëüòîíîâûì öèêëîì. Õîòÿ åå øàíñû óâåëè÷èâàþòñÿ, êâàíò äîêàçàòåëüñòâî ïîðåäóåò Âèêòîð íà ýòàïå (3), ñîñòàâëÿþ 50 ïðîöåíòîâ, Âèêòîð ìîæåò ïîâòîðèòü ïðîòîêîë äîñòàòî÷íîå ÷èñëî ðàç, óâåëè÷èâàÿñü, ÷òî Ïåããè çíàåò ãàìèëüòîíîâ öèêë äëÿ *G*.

Ïàðàëëåëüíûå äîêàçàòåëüñòâà ñóùåñòâîâàíèÿ

Â áàçîâîì ïðîòîêîëå ñóùåñòâîâàíèÿ èñïîëüçóåòñÿ *n* îáìåíîâ èíôîðìàöèåé ìåæäó Ïåããè è Âèêòîðîì. Ïî÷åìó áû íå âûïîëíèòü èõ ïàðàëëåëüíî:

(1) Ïåããè èñïîëüçóåò ñâîþ èíôîðìàöèþ è *n* ñëó÷àéíûõ ÷èñåë äëÿ ïðåîáðàçîâàíèÿ òðóäíîé ïðîáëåìû â *n* ðàçëè÷íûõ èçîìîðôíûõ ïðîáëåì. Çàòåì îíà ñ ïîìîùüþ ñâîåé èíôîðìàöèè è ñëó÷àéíûõ ÷èñåë ðåøàåò *n* íîâûõ òðóäíûõ ïðîáëåì.

(2) Ïåããè âðó÷àåò ðåøåíèå *n* íîâûõ òðóäíûõ ïðîáëåì. Âèêòîð íå ìîæåò âîñïîëüçîâàòüñÿ ýòèì íîâûì ïðîáëåìíèì äëÿ ïîëó÷åíèÿ èíôîðìàöèè îá îðèãèíàëüíûõ ïðîáëåì äëÿ èõ ðåøåíèè.

(4) Äëÿ êàæäîé íîâîé òðóäíîé ïðîáëåìû Âèêòîð ïðîñèò Ïåããè ëèáî

(a) äîêàçàòü åìó, ÷òî ñòàðàÿ è íîâàÿ ïðîáëåìû èçîìîðôíû, ëèáî

(b) ðàñêðûòü ðåøåíèå, âðó÷åííîå íà ýòàïå (2), è äîêàçàòü, ÷òî îíî ÿâëÿåòñÿ ðåøåíèåì äàííîé íîâîé ïðîáëåìû.

(5) Ïåããè èñïîëíÿåò åãî ïðîñüáó äëÿ êàæäîé íîâîé ïðîáëåìû.

Ê íåñ÷àñòüþ, âñå íå òàê ïðîñòî. Ýòîò ïðîòîêîë, â òîëê÷å îò ïðåäûäóùåãî, íå îáëàäàåò òàêèì æå ñâîéñòâàìè óñëîâíîãî çíàíèÿ. Íà ýòàïå (4) Âèêòîð ìîæåò ïîòðåáîâàòü, ÷òîáû äîêàçàòåëüñòâî áûëî ïðåäñòàâëåíî â âèäå çíà÷åíèÿ ïàðàìåòðèçîâàííîé õýø-ôóíêöèè âñåõ çíà÷åíèé, âðó÷íóþ íà ïåðâîì ýòàïå, äåëàÿ íåâîçìîæíûì èìèòàöèþ çàíèñè ïðîòîêîëà. Ýòî òîæå óòâåðæäåíèå, íî äðóãîãî ðîäà. Íà ïðàêòèêå îíî ïðåäñòàâëÿåòñÿ áåçîïàñíûì, íî íèêòî íå çíàåò, êàê ýòî äîêàçàòü. Ì û äåéñòâèòåëüíî çíàåì òî, ÷òî ïðè îïðåäåëåííûõ óñëîâèÿõ íåïðèâåòëèâûå ïðîòîêîëû äëÿ îïðåäåëåííûõ ïðîáëåì ìîãóò áûòü âû÷èñëåíû çà ïîëèíîìèàëüíîå âðåìÿ [247, 106, 546, 616].

Íåíóëåâûå äîêàçàòåëüñòâà ñóùåñòâîâàíèÿ

Êýðîë íåâîçìîæíî óâåäîìèò, ïîòî÷íó ÷òî îíà íå ó÷àñòâóåò â èíòåðàêöèîííî ïðîöåññå ïðîòîêîëå. Äëÿ óáåæäåíèÿ Êýðîë è äðóãèõ çàèíòåðåñîâàííûõ ëèö íàì íóæåí íåíóëåâûõ äîêàçàòåëüñòâ. Äëÿ íåíóëåâûõ äîêàçàòåëüñòâ ñ íóëåâûì çíàíèåì âû ïðèâûêëè äóìàòü îá èíôîðìàöèîííûõ ïîòîêàõ [477, 198, 478, 197], êîòîðûå íå òðåáóþò íåïîñðåäñòâåííîãî âçàèìîäåéſòâèÿ. Ïåããè ìîæåò îïóáëèêîâàòü èõ è, òàêèì îáðàçîì, äîêàçàòü ñâîå çíàíèå âñåì, ó êîãî íàéäåòñÿ âðåìÿ ýòî ïðîâåðèòü

Áàçîâûé ïðîòîêîë ïîõîæ íà ïàðàëëåëüíîå äîêàçàòåëüſòâî ñ íóëåâûì çíàíèåì, íî ìåñòî Âèêòîðà çàíèìàò

îäíîíàïðàâëåíèÿ õýø-ôóíêöèÿ:

(1) Ïåãàè èñïîëüçóåò ñâîþ èíôîðìàöèþ è n ñëó÷àéíûõ ÷èñåë äëÿ ïðåîáðàçîâàíèÿ òðóäíîé ïðîáëåìû â n ðàçëè÷íûõ èçîìîðôíûõ ïðîáëåì. Çàòåì îíà ñ ïîìîùüþ ñâîåé èíôîðìàöèè è ñëó÷àéíûõ ÷èñåë ðåøàåò n íîâûõ òðóäíûõ ïðîáëåì.

(2) Ïåãàè âðó÷àåò ðåøåíèå n íîâûõ òðóäíûõ ïðîáëåì.

(3) Ïåãàè èñïîëüçóåò âñå ýòè âðó÷åíèÿ â êà÷åñòâå âõîäà äëÿ îäíîíàïðàâëåííîé õýø-ôóíêöèè. (Â êîíöå êîíöîâ ýòè âðó÷åíèÿ - íå ÷òî èíîå, êàê ñòðîêè áèòîâ.) Çàòåì îíà ñîõðàíÿåò ïåðâûå n áèòîâ ïîëó÷åííîãî çíà÷åíèÿ îäíîíàïðàâëåííîé õýø-ôóíêöèè.

(4) Ïåãàè áåðåò n áèòîâ, ïîëó÷åííûõ íà ýòàïå (3). Ïî ÷åðåäè äëÿ êàæäîé n-îé òðóäíîé ïðîáëåìû îíà áåðåò n-ûé áèò è

   (a) åñëè áèò ðàâåí 0, äîêàçûâàåò, ÷òî ñòàðàÿ è íîâàÿ ïðîáëåìû èçîìîðôíû, ëèáî

   (b) åñëè áèò ðàâåí 1, ðàñêðûâàåò ðåøåíèå, âðó÷åííîå íà ýòàïå (2), è äîêàçûâàåò, ÷òî îíî ÿâëÿåòñÿ ðåøåíèåì äàííîé íîâîé ïðîáëåìû.

(5) Ïåãàè îïóáëèêîâûâàåò âñå ðåøåíèÿ, âðó÷åííûå íà ýòàïå (2), è âñå äîêàçàòåëüñòâà, ïîëó÷åííûå íà ýòàïå (4).

(6) Âèêòîð, Êýðîë è âñå îñòàëüíûå çàèíòåðåñîâàííûå ëèöà ïðîâåðÿò, ÷òî ýòàïû (1)-(5) âûïîëíåíû ïðàâèëüíî.

Ýòî âïå÷àòëÿåò: Ïåãàè ìîæåò îïóáëèêîâàòü íåêîòîðûå äàííûå, êîòîðûå íå ñîäåðæàò íèêàêîé èíôîðìàöèè î åå ñåêðåòàõ, íî ìîãóò êîãî óâîëèò óâåäîìü âñùåñòâîâàíèè ñàìîãî ñåêðåòà. Ýòîò ïðîòîêîë ìîæåò áûòü èñïîëüçîâàí ïðîâåäåíèÿ êàê âû÷èñëåíèå îäíîíàïðàâëåííîé õýø-ôóíêöèè ïåðâîíà÷àëüíûõ ñîîáùåíèé è ïîäïèñûâàíèå ñîîáùåíèÿ.

Ýòà ñõåìà ðàáîòàåò, ïîòîìó ÷òî îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ äâéñòâóåò êàê áåñïðèñòðàñòíûé ãåíåðàòîð ñëó÷àéíûõ áèòîâ. ×òîáû ìîøåííè÷àòü, Ïåãàè íóæíî óìåòü ïðåäñêàçûâàòü ðåçóëüòàò îäíîíàïðàâëåííîé õýø-ôóíêöèè. (Ïîíèìàåì, åñëè ðåøåíèå òðóäíîé ïðîáëåìû åé íåèçâåñòíî, îíà ìîæåò ñäåëàòü íà ýòàïå (4) ëèáî (a), ëèáî (b), íî íå îáà äåéñòâèÿ îäíîâðåìåííî.) Åñëè îíà êàêèì-òî îáðàçîì óçíàåò, âû ïîëíîñòüþ êàê îäíîãî äåéñòâèÿ ïðîòåêóò îò íåå îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ, òî îíà ñìîæåò ñìîøåííè÷àòü. Îäíàêî, Ïåãàè íå ñìîæåò çàñòàâèòü îäíîíàïðàâëåííóþ õýø-ôóíêöèþ âûäàòü ïðåäñêàçàííûé áèò ëèê äîãàäàòüñÿ, êàêîé áèò áóäåò ïîëó÷åí. Îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ ïî ñóòè ÿâëÿåòñÿ çàìåíèòåëåì Âèêòîðà â ñëó÷àéíîì âûáîðå îäíîãî èç äâóõ äîêàçàòåëüñòâ íà ýòàïå (4).

Â íåéòðàëèçàöèîííîì ïðîòîêîëå äîëæíî áûòü ãîðàçäî áîëüøå èòåðàöèé â ïîñëåäîâàòåëüíîñòè çàïðîñ/îòâåò. Ïåãàè, à íå Âèêòîð, îòáèðàåò òðóäíûå ïðîáëåìû ñ ïîìîùüþ ñëó÷àéíûõ ÷èñåë. Îíà ìîæåò ïîäáèðàòü ðàçëè÷íûå ïðîáëåìû, ñëåäîâàòåëüíî, è ðàçëè÷íûå âåêòîðû âðó÷åíèÿ, äî òåõ ïîð, ïîêà õýø-ôóíêöèÿ íå âûäàñò ÷òî-òî, íóæíîå Ïåãàè. Â èòåðàöèîííîì ïðîòîêîëå 10 èòåðàöèé - âåðîÿòíîñòü ìîøåííè÷åñòâà Ïåãàè ñîñòàâèò 1 øàíñ èç 2^{10} (1 èç 1024) - ìîæåò áûòü äîñòàòî÷íî. Îäíàêî, äëÿ íåèòåðàöèîííûõ äîêàçàòåëüñòâ ñ íóëåâûì çíàíèåì ýòîãî íå õâàòèò. Ïîíèìàå, ÷òî Ìýëîðè âñåãäà ìîæåò âûïîëíèòü íà ýòàïå (4) ëèáî (a), ëèáî (b). Îí ìîæåò, âûïîëíÿÿ ýòàïû (1)-(3), ïîïûòàòüñÿ äîãàäàòüñÿ, ÷òî åãî ïîïðîñÿò ñäåëàòü, è ïîñìîòðåòü, ïðàâèëüíî ëè åãî ïðåäïîëîæåíèå. Åñëè íåò, îí ïîïðîáóåò ñíîâà è ñíîâà. Ñåãåòè 1024 ïðåäïîëîæåíèÿ íà êîìïüþòåðå íåòðóäíî. Äëÿ ïðåîòâðàùåíèÿ òàêîãî âñêðûòèÿ ãðóáûì âçëîìîì äëÿ íåèòåðàòèâíûõ õýø-ôóíêöèé ïîòðåáóåòñÿ íà êîìïüþòåðå íåòðóäíî. Äëÿ ïðåîòâðàùåíèÿ íîâûõ ïðîòîêîëîâ íóæíî 64 èëè äàæå 128 èòåðàöèé.

Ãëàâíàÿ èäåÿ ñîñòîèò â èñïîëüçîâàíèè îäíîíàïðàâëåííîé õýø-ôóíêöèè - Ïåãàè íå ìîæåò ïðåäñêàçàòü âûõîä õýø-ôóíêöèè, ïîòîìó ÷òî íîâûå ìîæåò ïðåäñêàçàòü åå âõîä. Âðó÷íóþ, èñïîëüçóåìûå íà âõîäå, ñòàíîâÿòñÿ èçâåñòíûì òîëüêî ïîñëå ðåøåíèÿ íîâûõ ïðîáëåì.

Îáùèå çàìå÷àíèÿ

Áëþì (Blum) äîêàçàë, ÷òî ëþáàÿ ìàòåìàòè÷åñêàÿ òåîðåìà ìîæåò áûòü ïðåîáðàçîâàíà â ãðàô, òàêîé, ÷òî äîêàçàòåëüñòâî òåîðåìû áóäåò ýêâèâàëåíòíî äîêàçàòåëüñòâó ñóùåñòâîâàíèÿ ãàìèëüòîíîâà öèêëà äëÿ ýòîãî ãðàôà. Â íàùåì âèäå òî, ÷òî äëÿ ëþáîãî NP-ïîëíîãî óòâåðæäåíèÿ åñòü äîêàçàòåëüñòâî ñóùåñòâîâàíèÿ çíàíèå, èñïîëüçóþùåå îäíîíàïðàâëåííóþ ôóíêöèè è, ñëåäîâàòåëüíî, õîðîøèå àëãîðèòìû øèôðîâàíèÿ, äîêàçàíî â [620]. Ëþáóþ ìàòåìàòè÷åñêóþ äîêàçàòåëüñòâî ìîæåò áûòü ïðåîáðàçîâàíî â äîêàçàòåëüñòâî ñ íóëåâûì çíàíèåì. Èñïîëüçóÿ ýòó ìåòîäèêó, èññëåäîâàòåëü ìîæåò äîêàçàòü ìèðó, ÷òî åìó èçâåñòíî äîêàçàòåëüñòâî êîíêðåòíîé òåîðåìû, íå ðàñêðûâàÿ ñàìîãî ðåøåíèÿ. Áëþì îïóáëèêîâàòü ñâîè ðåçóëüòàòû, íå ðàñêðûâàÿ èõ.

Òàêæå ñóùåñòâóþò **äîêàçàòåëüñòâà ñ ìèíèìàëüíûì ðàñêðûòèåì** [590]. Äëÿ äîêàçàòåëüñòâà ñ ìèíèìàëüíûì ðàñêðûòèåì âûïîëíÿþòñÿ ñëåäóþùèå ñâîéñòâà:

1. Ïåãàè íå ìîæåò îáìàíóòü Âèêòîðà. Åñëè Ïåãàè íå çíàåò äîêàçàòåëüñòâà, åå øàíñû óáåäèòü Âèêòîðà â

òî ì, ÷òî äîêàçàòåëüñòâî åé èçâåñòíî, ïðåíåáðåæèì ìàëû.

2. Âèêòîð íå ìîæåò îáìàíóòü Ïåããè. Î í íå ïîëó÷àò íè ìàëåéøåãî íàìåêà íà äîêàçàòåëüñòâî êðîìå òîãî ôàêòà, ÷òî äîêàçàòåëüñòâî èçâåñòíî Ïåããè. Â ÷àñòíîñòè, Âèêòîð íå ìîæåò ïðîâåðèòü äîêàçàòåëüñòâî íèêîìó äðóãîìó, íå äîêàçàâ âñå ñàì ñ ñàìîãî íà÷àëà.

Ó äîêàçàòåëüñòâ ñ íóëåâûì çíàíèåì åñòü äîïîëíèòåëüíîå óñëîâèå:

3. Âèêòîð íå óçíàåò îò Ïåããè íè÷åãî òàêîãî, ÷åãî îí íå ñìîã áû óçíàòü è ñàìîñòîÿòåëüíî êðîìå òîãî ôàêòà, ÷òî äîêàçàòåëüñòâî èçâåñòíî Ïåããè.

Ñóùåñòâóåò çàìå÷àòåëüíàÿ ðàçíèöà ìåæäó äîêàçàòåëüñòâàìè ñ ìíèìàëüíûì ðàñêðûòèåì è äîêàçàòåëüñòâàìè ñ íóëåâûì çíàíèåì. Ýòî ðàçëè÷èå íàõîäèòñÿ âíå ðàìîê äàííîé êíèãè, íî áûëà èñêóññòâåííî ÷èòàòåëè ìîãóò ïðîøòóäèðîâàòü äðóãóþ ëèòåðàòóðó. Ï î íÿòèÿ èçëîæåíû â in [626, 619, 622]. Äàëüíåéøàÿ ïðîðàáîòêà ýòèõ èäåé, îñíîâàííàÿ íà ðàçëè÷íûõ ìàòåìàòè÷åñêèõ ïðåäïîëîæåíèÿõ, âûïîëíåíà â [240, 319, 239].

Ñóùåñòâóþ ðàçëè÷íûå òèïû äîêàçàòåëüñòâ íóëåâûì çíàíèåì:

— **Ñîâåðøåííîå**. Ñóùåñòâóåò èìèòàòîð, êîòîðûé ñîçäàò ñòåíîãðàììû, ïîëíîñòüþ ñîòâåòñòâóþùèå ðåàëüíûì ñòåíîãðàììàì (ïðèìåðû ñ ãàìèëüòîíîâûì öèêëîì è èçîìîðôèçìîì ãðàôîâ).

— **Ñòàòèñòè÷åñêîå**. Ñóùåñòâóåò èìèòàòîð, êîòîðûé ñîçäàò ñòåíîãðàììû, ïîëíîñòüþ ñîòâåòñòâóþùèå ðåàëüíûì ñòåíîãðàììàì, êðîìå ôèêñèðîâàííîãî ÷èñëà èñêëþ÷åíèé.

— **Âû÷èñëèòåëüíîå**. Ñóùåñòâóåò èìèòàòîð, êîòîðûé ñîçäàò ñòåíîãðàììû, íåòèè÷èìûå îò ðåàëüíûõ.

— **Íåèñ ïîëüçóþùåå**. È ìèòàòîðà ìîæåò è íå áûòü, íî ìû ìîæåì äîêàçàòü, ÷òî Âèêòîð íå óçíàåò íèêàêîé èíôîðìàöèè èç äîêàçàòåëüñòâà (ïàðàëëåëüíûé ïðèìåð)

Ãîâîðÿ òÿæåëîé ðàíîû, êàê òåððîð÷åñêîé, òàê è ïðèêëàäíîé, ïðèñåëè ê ïîÿâëåíèþ äîêàçàòåëüñòâ ñ ìèíèìàëüíûì ðàñêðûòèåì è íóëåâûì çíàíèåì. Ìàéê Áðìåñòåð (Mike Burmester) è Èâî Äåìàäò èçîáðåëè øèðîêîâåùàòåëüíî èíòåðåñóþùóþ äîêàçàòåëüñòâî, äàå âèäåëåö ñåêðåòà ìåæäó øèðîêîâåùàòåëüíî ïðåäâàðèòåëüíûì áîëüøîé ãðóïïå êîíòðîëèðîâ èíòåðàêòèâíîå äîêàçàòåëüñòâî ñ íóëåâûì çíàíèåì [280]. Êðèïòîãðàôû äîêàçàëè, ÷òî *âñå*, ÷òî ìîæåò áûòü äîêàçàíî ñ ïîìîùüþ èíòåðàêòèâíîãî äîêàçàòåëüñòâà, ìîæåò áûòü äîêàçàíî è ñ ïîìîùüþ èíòåðàêòèâíîãî äîêàçàòåëüñòâà ñ íóëåâûì çíàíèåì [753, 137].

Õîðîøåé îáçîðíé ñòàòüé ïî äàííîé òåìå ÿâëÿåòñÿ [548]. Äîïîëíèòåëüíûå ìàòåìàòè÷åñêèå ïîäðîáíîñòè, âàðèàíòû, ïðîòîêîëû è ïðèëîæåíèÿ èùèòå â [590, 619, 240, 319, 620, 113,241, 152, 8, 660, 238, 591, 617, 510, 592, 214, 104, 216, 832, 97, 939, 622, 482, 615, 618, 215, 476, 71]. *Ì íîãî ÷åãî* áûëî íàïèñàíî ïî ýòîìó âîïðîñó.

5.2 Èñïîëüçîâàíèå äîêàçàòåëüñòâà ñ íóëåâûì çíàíèåì äëÿ èäåíòèôèêàöèè

Â ðåàëüíîì ìèðå äëÿ äîêàçàòåëüñòâ ïîäëèííîñòè ÷àñòî èñïîëüçóþòñÿ ôèçè÷åñêèå ñèìâîëû: ïàñïîðòà, âîäèòåëüñêèå ïðàâà, êðåäèòíûå êàðòî÷êè è ò.ä. Ýòè ñèìâîëû ñîäåðæàò ÷àñòè-òî, ñâÿçûâàþùåå èõ ñ êîíêðåòíûì ÷åëîâåêîì: îâû÷íî ôîòîãðàôèþ ëèö ïîäïèñü, íî ñòî æå âåðîÿòíîñòü ýòî ìîæåò áûòü îòðåãóëèðîâàíî ïðîôåññèîíàëîì? Èñïîëüçîâàòü äîêàçàòåëüñòâà ñ íóëåâûì çíàíèåì äëÿ äîêàçàòåëüñòâà èäåíòè÷íîñòè áûëî âïåðâûå ïðåäëîæåíî Óðèåëåì Ôàéãè (Uriel Feige), Àìíîí Ôèàòîì (Amos Fiat) è Àäè Øàìèðîì [566, 567]. Çàêðûòûé êëþ÷ Àëèñû ñòàíîâèòñÿ ôóíêöèåé åå "èäåíòè÷íîñòè". Èñïîëüçóÿ äîêàçàòåëüñòâî ñ íóëåâûì çíàíèåì, îíà äîêàçûâàåò, ÷òî îíà çíàåò ñâîé çàêðûòûé êëþ÷ è, òàêèì îáðàçîì, ñâîþ èäåíòè÷íîñòü. Ñîîòâåòñòâóþùèå ìåãîðèòìû ìîæíî íàéòè â ðàçäåëå 23.11.

Ýòî î÷åíü ìíîãîîáùàþùàÿ èäåÿ. Î íà ïîçâîëÿåò ÷åëîâåêó äîêàçàòü ñâîþ ëè÷íîñòü áåç èñïîëüçîâàíèÿ ôèçè÷åñêèõ ñèìâîëîâ. Îäíàêî, îíà íå ñîâðåøåííà. Âîò ïðèìåðû âîçìîæíûõ çëîóìûøëåíèé.

Ïðîáëåìà ãðîññìåéñòåðà

Âîò êàê Àëèñà, äàæå íå çíàÿ ïðàâèë øàõìàò, ìîæåò îáûãðàòü ãðîññìåéñòåðà. (Èíîãäà ýòî íàçûâàåòñÿ ïðîáëåìîé ãðîññìåéñòåðà.) Î íà ïîñûëàåò âûçîâ Ãàððè Êàñïàðîâó è Àíàòîëèþ Êàðïîâó, ïðåäëàãàÿ èãðàòü â îäíî âðåìÿ, â îäíîì è òîì æå ìåñòå, íî â ðàçäåëüíûõ êîìíàòàõ. Î íà èãðàåò áëèæå ïðîòèâ Êàñïàðîâà è ÷åðíûìè ïðîòèâ Êàðïîâà. Íè îäèí ãðîññìåéñòåð íå çíàåò î äóãîì.

Êàðïîâ, èãðàÿ áåëûìè, äåëàåò ñâîé õîä ïåðâûì. Àëèñà çàïèñûâàåò õîä è èäåò â êîìíàòó ê Êàñïàðîâó. Èãðàÿ áåëûìè, îíà äåëàåò òîò æå õîä íà äîñêå Êàñïàðîâà. Êàñïàðîâ äåëàåò ñâîé õîä íà äîñêå Àëèñû. Àëèñà çàïèñûâàåò õîä, èäåò â êîìíàòó ê Êàðïîâó è äåëàåò òîò æå õîä. Ýòî ïðîäîëæàåòñÿ, ïîêà îíà íå âûèãðûâàåò îäíó èç ïàðòèé, ïðîèãðûâàÿ äóãóþ, èëè îáå ïàðòèè êîí÷àþòñÿ âíè÷üþ.

Íà ñàìîì äåëå Êàñïàðîâ èãðàåò ñ Êàðïîâûì, à Àëèñà ïðîñòî ïîñðåäíèê, ïîâòîðÿþùèé õîäû îäíîãî ãðîññ-

ìåéñòåðà íà äîñêå äðóãîãî. Îäíàêî, åñëè Êàðïîâ è Êàñïàðîâ íå çíàþò î ïðèñóòñòâèè äðóã äðóãà, êàæäûé èç íèõ áóäåò ïîðàæåí èãðîé Àëèñû.

Ýòîò ñïîñîá ìîøåííè÷åñòâà ìîæåò áûòü èñïîëüçîâàòü ïðîòèâ äîêàçàòåëüñòâà ëè÷íîñòè ñ íóëåâûì çíàíèåì [485, 120]. Êîãäà Àëèñà äîêàçûâàåò ñâîþ ëè÷íîñòü Ìýëëîðè, Ìýëëîðè ìîæåò îäíîâðåìåííî äîêàçàòü Áîáó, ÷òî îí-òî è åñòü Àëèñà.

Îáìàí, âûïîëíåííûé ìàôèåé

Îáñóæäàÿ ñâîé ïðîòîêîë èäåíòèôèêàöèè ñ íóëåâûì çíàíèåì, Àäè Øàìèð ñêàçàë [1424]: "ß ìîãó õîäèòü â ïðèíàäëåæàùèé ìàôèè ìàãàçèí õîòü ìèëëèîí ðàç ïîäðÿä, à îíè âñå åùå íå ñìîãóò âûäàòü ñåáÿ çà ìåíÿ."

Âîò êàê ìàôèÿ ñìîæåò ýòî ñäåëàòü. Àëèñà åñò â ðåñòîðàí÷èêå Áîáà, ïðèíàäëåæàùåì ìàôèè. Êýðîë äåëàåò ïîêóïêè â äîðîãîì þâåëèðíîì ìàãàçèíå Äýéâà. Áîá è Êýðîë - ìàôèîçè, ïåðåãîâàðèâàþùèåñÿ ïî ïîòàéíîìó ðàäèîêàíàëó. Àëèñà è Äýéâ íå ïîäîçðåâàþò î ìîøåííè÷åñòâå.

Êîãäà Àëèñà ïîåëà è ñîáðàëàñü ïëàòèòü è äîêàçûâàòü ñâîþ ëè÷íîñòü Áîáó, Áîá ïîäàåò ñèãíàë Êýðîë, ÷òî ïîðà íà÷èíàòü. Êýðîë âûáèðàåò áðèëëèàíòû ïîäîðîæå è ñîáèðàåòñÿ äîêàçûâàòü ñâîþ ëè÷íîñòü Äýéâó. Òåïåðü, ïîêà Àëèñà äîêàçûâàåò ñâîþ ëè÷íîñòü Áîáó, òîò ïîäàåò ñèãíàë Êýðîë, è òà âûïîëíÿåò òîò æå ïðîòîêîë ñ Äýéâîì. Êîãäà Äýéâ çàäàåò âîïðîñ ïî ïðîòîêîëó, Êýðîë ñîîáùàåò ýòîò âîïðîñ Áîáó, à Áîá çàäàåò åãî Àëèñå. Êîãäà Àëèñà îòâå÷àåò, Áîá ïåðåäàåò ïðàâèëüíûé îòâåò Êýðîë. Ïî ñóòè, Àëèñà ïðîñòî äîêàçûâàåò ñâîþ ëè÷íîñòü Äýéâó, à Áîá è Êýðîë ïðîñòî, íàõîäÿñü âíóòðè ïðîòîêîëà, ïåðåäàþò ñîîáùåíèÿ òóäà-ñþäà. Êîãäà ïðîòîêîë çàâåðøàåòñÿ, Àëèñà äîêàçàëà ñâîþ ëè÷íîñòü Äýéâó è çàïëàòèëà çà äîðîãèå áðèëëèàíòû (ñ êîòîðûìè Êýðîë òåïåðü è èñ÷åçíåò).

Îáìàí, âûïîëíåííûé òåððîðèñòàìè

Åñëè Àëèñà õî÷åò îáúåäèíèòüñÿ ñ Êýðîë, òî îíè òàêæå ìîãóò ïðîâåñòè Äýéâà. Â ýòîì ïðîòîêîëå Êýðîë - èçâåñòíàÿ òåððîðèñòêà. Àëèñà ïîìîãàåò åé âúåõàòü â ñòðàíó. Äýéâ - îôèöåð-ïîãðàíè÷íèê, Àëèñà è Êýðîë îáùàþòñÿ ïî òàéíîìó ðàäèîêàíàëó.

Êîãäà Äýéâ çàäàåò Êýðîë âîïðîñû â ñîîòâåòñòâèè ïî ïðîòîêîëó ñ íóëåâûì çíàíèåì, Êýðîë ïåðåäàåò èõ Àëèñå, êîòîðàÿ è îòâå÷àåò íà âîïðîñû. Êýðîë ïîâòîðÿåò ýòè îòâåòû Äýéâó. Carol recites these answers to Dave. Ïî ñóòè, Ñâîþ ëè÷íîñòü Äýéâó äîêàçûâàåò Àëèñà, à Êýðîë âûñòóïàåò â ðîëè ëèíèè ñâÿçè. Êîãäà ïðîòîêîë çàâåðøàåòñÿ, Äýéâ ñ÷èòàåò, ÷òî Êýðîë - ýòî Àëèñà, è ðàçðåøàåò åé âúåõàòü â ñòðàíó. Ñïóñòÿ òðè äíÿ Êýðîë âñïëûâàåò ó ïðàâèòåëüñòâåííîãî çäàíèÿ âìåñòå ñ ìèêðîàâòîáóñîì, íàáèòîì âçðûâ÷àòêîé.

Ïðåäëàãàåìûå ðåøåíèÿ

Îáà îïèñàííûõ ìîøåííè÷åñòâà âîçìîæíû, òàê êàê çàãîâîðùèêè èñïîëüçóþò òàéíûé ðàäèîêàíàë. Îäíèì èç ñïîñîáîâ ïðåäîòâðàòèòü ìîøåííè÷åñòâî ÿâëÿåòñÿ ïðîâåäåíèå ïðîöåäóðû èäåíòèôèêàöèè â êëåòêå Ôàðàäåÿ, áëîêèðóþùåé ýëåêòðîìàãíèòíîå èçëó÷åíèå. Â ïðèìåðå ñ òåððîðèñòîì ýòî ãàðàíòèðóåò, ÷òî Êýðîë íå ïîëó÷èò îòâåòà îò Àëèñû. Â ïðèìåðå ñ ìàôèåé Áîá ìîæåò ïîñòðîèòü ôàëüøèâóþ êëåòêó Ôàðàäåÿ â ñâîåì ðåñòîðàíå, íî ó þâåëèðà-òî êëåòêà áóäåò ðàáîòàòü , è Áîá è Êýðîë íå ñìîãóò îáìåíèâàòüñÿ ñîîáùåíèÿìè. Äëÿ ðåøåíèÿ ïðîáëåìû ãðîññìåéñòåðà Àëèñà äîëæíà ñèäåòü íà ñâîåì ñòóëå äî êîíöà èãðû.

Òîìàñ Áîò (Thomas Both) è Èâî Äåñìåäò ïðåäëîæèëè äðóãîå ðåøåíèå, èñïîëüçóþùåå òî÷íûå ÷àñû [148]. Åñëè êàæäûé ýòàï ïðîòîêîëà äîëæåí ïðîèñõîäèòü â çàäàííîå âðåìÿ, ó ìîøåííèêîâ íå îñòàíåòñÿ âðåìåíè äëÿ îáìåíà èíôîðìàöèåé. Â ñëó÷àå ñ ïðîáëåìîé ãðîññìåéñòåðà ýòî ñîîòâåòñòâóåò ïðåäëîæåíèþ îãðàíè÷èòü âðåìÿ îáäóìûâàíèÿ õîäà îäíîé ìèíóòîé - ó Àëèñû íå îñòàíåòñÿ âðåìåíè áåãàòü èç êîìíàòû â êîìíàòó. Â èñòîðèè ñ ìàôèåé ó Áîáà è Êýðîë íå õâàòèò âðåìåíè ïåðåäàâàòü äðóã äðóãó îòâåòû è âîïðîñû.

Îáìàí ñ íåñêîëüêèìè ëè÷íîñòÿìè

Ñóùåñòâóþò è äðóãèå ñïîñîáû çëîóïîòðåáèòü äîêàçàòåëüñòâàìè èäåíòè÷íîñòè ñ íóëåâûì çíàíèåì, òàêæå ðàññìàòðèâàåìûå â [485, 120]. Â ðÿäå ðåàëèçàöèé ïðîâåðêà ïðè ðåãèñòðàöèè ÷ëåíîì ñâîåãî êëþ÷à íå ïðîèçâîäèòñÿ. Ñëåäîâàòåëüíî, ó Àëèñû ìîæåò áûòü íåñêîëüêî çàêðûòûõ êëþ÷åé è, òàêèì îáðàçîì, íåñêîëüêî ëè÷íîñòåé. Ýòî ìîæåò çäîðîâî ïîìî÷ü åé, åñëè îíà çàõî÷åò ìîøåííè÷àòü ñ íàëîãàìè. Àëèñà òàêæå ìîæåò ñîâåðøèòü ïðåñòóïëåíèå è ñêðûòüñÿ. Â ïåðâûõ, îíà ñîçäàåò íåñêîëüêî ëè÷íîñòåé, îäíà èç êîòîðûõ íå èñïîëüçóåòñÿ. Çàòåì, îíà èñïîëüçóåò ýòó ëè÷íîñòü äëÿ ñîâåðøåíèÿ ïðåñòóïëåíèÿ òàê, ÷òîáû ñâèäåòåëü èäåíòèôèöèðîâàë åå êàê ýòó ëè÷íîñòü. Çàòåì, îíà íåìåäëåííî ïðåêðàùàåò ïîëüçîâàòüñÿ ýòîé ëè÷íîñòüþ. Ñâèäåòåëü çíàåò ëè÷íîñòü ïðåñòóïíèêà, íî Àëèñà íèêîãäà áîëüøå íå áóäåò èñïîëüçîâàòü ýòó ëè÷íîñòü - åå íåâîçìîæíî ïðîñëåäèòü.

Äëÿ çàùèòû îò ýòîãî íóæíû ìåõàíèçìû, îáåñïå÷èâàþùèå, ÷òîáû ó êàæäîãî ÷åëîâåêà áûëà òîëüêî îäíà ëè÷íîñòü. Â [120] àâòîðàìè ïðåäëàãàåòñÿ ïðè÷óäëèâàÿ èäåÿ çàùèùåííûõ îò ïîäðîñòêà äåòåé, êîòîðûå íå ìîãóò áûòü êëîíèðîâàíû, è ó êîòîðûõ åñòü óíèêàëüíûé íîìåð, ÿâëÿþùèéñÿ ÷àñòüþ èõ ãåíåòè÷åñêîãî êîäà. Îíè òàêæå ïðåäëîæèëè ïðèñâàèâàòü êàæäîìó ðåáåíêó ëè÷íîñòü ïðè ðîæäåíèè. (Äåéñòâèòåëüíî, ðîäèòåëÿì ïðèäåòñÿ ñäå-

ëàòü ýòî, òàê êàê èíà÷å ðåáåíîê ìîæåò áûòü óêðàäåí.) Ýòèì òîæå ëåãêî çëîóïîòðåáèòü - ðîäèòåëè ìîãóò ñîçäàòü äëÿ ðîäèâøåãîñÿ ðåáåíêà íåñêîëüêî ëè÷íîñòåé. Â êîíöå êîíöîâ, óíèêàëüíîñòü ëè÷íîñòè îñíîâàíà íà äîâåðèè.

Ïðîêàò ïàñïîðòîâ

Àëèñà õî÷åò ïîåõàòü â Çàèð, íî ïðàâèòåëüñòâî ýòîé ñòðàíû íå äàåò åé âèçû. Êýðîë ïðåäëàãàåò ñäàòü ñâîþ ëè÷íîñòü Àëèñå "íàïðîêàò". (Ïåðâûì ýòî ïðåäëîæèë Áîá, íî âîçíèê ðÿä î÷åâèäíûõ ïðîáëåì.) Êýðîë ïðîäàåò Àëèñå ñâîé çàêðûòûé êëþ÷ è Àëèñà åäåò â Çàèð, âûäàâàÿ ñåáÿ çà Êýðîë.

Êýðîë ïîëó÷àåò íå òîëüêî ïëàòó çà ñâîþ ëè÷íîñòü, íî è èäåàëüíîå àëèáè. Îíà ñîâåðøàåò ïðåñòóïëåíèå, ïîêà Àëèñà íàõîäèòñÿ â Çàèðå. "Êýðîë" äîêàçàëà ñâîþ ëè÷íîñòü â Çàèðå, êàê îíà ìîãëà ñîâåðøèòü ïðåñòóïëåíèå äîìà?

Êîíå÷íî, ðàçâÿçàíû ðóêè è ó Àëèñû. Îíà ìîæåò ñîâåðøèòü ïðåñòóïëåíèå ëèáî ïåðåä îòúåçäîì, ëèáî ñðàçó æå ïîñëå âîçâðàùåíèÿ, îêîëî äîìà Êýðîë. Ñíà÷àëà îíà ïîêàæåò, ÷òî îíà - Êýðîë (èìåÿ çàêðûòûé êëþ÷ Êýðîë, åé íå ñîñòàâèò òðóäà ñäåëàòü ýòî), çàòåì îíà ñîâåðøèò ïðåñòóïëåíèå è óáåæèò. Ïîëèöèÿ áóäåò èñêàòü Êýðîë. Êýðîë áóäåò óòâåðæäàòü, ÷òî ñäàëà ñâîþ ëè÷íîñòü íàïðîêàò Àëèñå, íî êòî ïîâåðèò â òàêóþ íåâåðîÿòíóþ èñòîðèþ?

Ïðîáëåìà â òîì, ÷òî Àëèñà äîêàçûâàåò íå ñâîþ ëè÷íîñòü, à òî, ÷òî åé èçâåñòíà íåêîòîðàÿ ñåêðåòíàÿ èíôîðìàöèÿ. Èìåííî ñâÿçü ìåæäó ýòîé èíôîðìàöèåé è ëè÷íîñòüþ è ñëóæèò ïðåäìåòîì çëîóïîòðåáëåíèÿ. Ðåøåíèå çàùèùåííûõ îò âîðîâñòâà äåòåé çàùèòèëî áû îò òàêîãî ìîøåííè÷åñòâà, êàê è ñîçäàíèå ïîëèöåéñêîãî ãîñóäàðñòâà, â êîòîðîì âñå ãðàæäàíå äîëæíû î÷åíü ÷àñòî äîêàçûâàòü ñâîþ ëè÷íîñòü (â êîíöå äíÿ, íà êàæäîì óãëó è ò.ä.). Ïîìî÷ü ðåøèòü ýòó ïðîáëåìó ìîãóò áèîìåòðè÷åñêèå ìåòîäû - îòïå÷àòêè ïàëüöåâ, ñíèìêè ñåò÷àòêè ãëàçà, çàïèñü ãîëîñà è ò.ï.

Äîêàçàòåëüñòâî ÷ëåíñòâà

Àëèñà õî÷åò äîêàçàòü Áîáó, ÷òî îíà ÿâëÿåòñÿ ÷ëåíîì ñóïåðñåêðåòíîé îðãàíèçàöèè, íî íå õî÷åò ðàñêðûâàòü ñâîþ ëè÷íîñòü. Ýòà ïðîáëåìà, áëèçêàÿ ïðîáëåìå äîêàçàòåëüñòâà ëè÷íîñòè, íî îòëè÷àþùàÿñÿ îò íåå, áûëà èçó÷åíà â [887, 906, 907, 1201, 1445]. Ðÿä ðåøåíèé ñâÿçàí ñ ïðîáëåìîé ãðóïïîâûõ ïîäïèñåé (ñì. ðàçäåë 4.6).

5.3 Ñëåïûå ïîäïèñè

Âàæíûì ñâîéñòâîì ïðîòîêîëîâ öèôðîâîé ïîäïèñè ÿâëÿåòñÿ çíàíèå ïîäïèñûâàþùèì ñîäåðæàíèÿ ïîäïèñûâàåìîãî äîêóìåíòà. Ýòî õîðîøåå ñâîéñòâî, äàæå êîãäà õî÷åòñÿ îáðàòíîãî.

Ìû ìîæåì ïîæåëàòü, ÷òîáû ëþäè ïîäïèñûâàëè äîêóìåíòû, äàæå íå çíàÿ èõ ñîäåðæàíèÿ. Ñóùåñòâóþò ñïîñîáû, êîãäà ïîäïèñûâàþùèé ìîæåò íå òî÷íî, íî *ïî÷òè* çíàòü, ÷òî îí ïîäïèñûâàåò. Íî âñå ïî ïîðÿäêó.

Ïîëíîñòüþ ñëåïûå ïîäïèñè

Áîá - ãîñóäàðñòâåííûé íîòàðèóñ. Àëèñà õî÷åò, ÷òîáû îí ïîäïèñàë äîêóìåíò, íå èìåÿ íè ìàëåéøåãî ïðåäñòàâëåíèÿ î åãî ñîäåðæàíèè. Áîá íå îòâå÷àåò çà ñîäåðæàíèå äîêóìåíòà, îí òîëüêî çàâåðÿåò, ÷òî íîòàðèàëüíî çàñâèäåòåëüñòâîâàë åãî â îïðåäåëåííîå âðåìÿ. Îí ñîáèðàåòñÿ äåéñòâîâàòü ïî ñëåäóþùåìó ïëàíó:

(1) Àëèñà áåðåò äîêóìåíò è óìíîæàåò åãî íà ñëó÷àéíîå ÷èñëî. Ýòî ñëó÷àéíîå ÷èñëî íàçûâàåòñÿ **ìàñêèðóþùèì ìíîæèòåëåì**.

(2) Àëèñà ïîñûëàåò çàìàñêèðîâàííûé äîêóìåíò Áîáó.

(3) Áîá ïîäïèñûâàåò çàìàñêèðîâàííûé äîêóìåíò.

(4) Àëèñà óäàëÿåò ìàñêèðóþùèé ìíîæèòåëü, ïîëó÷àÿ îðèãèíàëüíûé äîêóìåíò, ïîäïèñàííûé Áîáîì.

Ýòîò ïðîòîêîë ðàáîòàåò òîëüêî, åñëè ôóíêöèÿ ïîäïèñè è óìíîæåíèå êîììóòàòèâíû. Åñëè íåò, òî ïîìèìî óìíîæåíèÿ ñóùåñòâóþò è äðóãèå ñïîñîáû èçìåíèòü äîêóìåíò. Íåñêîëüêî ïîäõîäÿùèõ àëãîðèòìîâ ïðèâåäåíû â ðàçäåëå 23.12. À ñåé÷àñ, äëÿ ïðîñòîòû ìàòåìàòèêè îñòàíîâèìñÿ íà óìíîæåíèè.

Ìîæåò ëè Áîá ñìîøåííè÷àòü? Ìîæåò ëè îí ïîëó÷èòü êàêóþ-íèáóäü èíôîðìàöèþ î òîì, ÷òî ïîäïèñûâàåò? Åñëè ìíîæèòåëü îñòîðîæíîñòè äåéñòâèòåëüíî ñëó÷àåí è äåëàåò çàìàñêèðîâàííûé äîêóìåíò äåéñòâèòåëüíî ñëó÷àéíûì, òî íåò. Çàìàñêèðîâàííûé äîêóìåíò, ïîäïèñûâàåìûé Áîáîì íà ýòàïå, (2) íè÷åì íå ïîõîæ íà îðèãèíàëüíûé äîêóìåíò Àëèñû. Çàìàñêèðîâàííûé äîêóìåíò ñ ïîäïèñüþ Áîáà íà íåì íà ýòàïå (3) íè÷åì íå ïîõîæ íà ïîäïèñàííûé äîêóìåíò ýòàïà (4). Äàæå åñëè Áîá çàïîëó÷èò äîêóìåíò ñî ñâîåé ïîäïèñüþ ïîñëå îêîí÷àíèÿ ïðîòîêîëà, îí íå ñìîæåò äîêàçàòü (ñåáå èëè êîìó-òî äðóãîìó), ÷òî îí ïîäïèñàë åãî â ýòîì êîíêðåòíîì ïðîòîêîëå. Îí çíàåò, ÷òî åãî ïîäïèñü ïðàâèëüíà. Îí ìîæåò, êàê è ëþáîé äðóãîé, ïðîâåðèòü ñâîþ ïîäïèñü. Îäíàêî, ó íåãî íåò íèêàêîé âîçìîæíîñòè ñâÿçàòü ïîäïèñàííûé äîêóìåíò è ëþáóþ èíôîðìàöèþ, ïîëó÷åííóþ ïðè âûïîëíåíèè ïðîòîêîëà. Åñëè îí ïîäïèñàë, èñïîëüçóÿ ýòîò ïðîòîêîë, ìèëëèîí äîêóìåíòîâ, ó íåãî íå áóäåò ñïîñîáà óçíàòü, êîãäà êàêîé äîêóìåíò îí ïîäïèñàë. Ïîëíîñòüþ ñëåïûå ïîäïèñè îáëàäàþò ñëåäóþùèìè ñâîéñòâàìè:

1. Ïîäïèñü Áîáà ïîä äîêóìåíòîì ïðàâèëüíà è ñëóæèò äîêàçàòåëüñòâîì òîãî, ÷òî Áîá ïîäïèñàë ýòîò äîêóìåíò. Îíà óáåäèò Áîáà â òîì, ÷òî îí ïîäïèñàë ýòîò äîêóìåíò, êîãäà äîêóìåíò áóäåò âïîñëåäñòâèè ïîêàçàí Áîáó. Îíà òàêæå îáëàäàåò âñåìè ñâîéñòâàìè öèôðîâûõ ïîäïèñåé, îáñóæäàåìûõ â ðàçäåëå 2.6.

2. Áîá íå ìîæåò ñâÿçàòü ïîäïèñàííûé äîêóìåíò ñ ïðîöåññîì ïîäïèñàíèÿ äîêóìåíòà. Äàæå åñëè ó íåãî õðàíÿòñÿ çàïèñè îáî âñåõ ñäåëàííûõ èì ñëåïûõ ïîäïèñÿõ, îí íå ñìîæåò îïðåäåëèòü, êîãäà îí ïîäïèñàë êîíêðåòíûé äîêóìåíò.

Ó Åâû, íàõîäÿùåéñÿ ìåæäó Àëèñîé è Áîáîì è ñëåäÿùåé çà ïðîòîêîëîì, èíôîðìàöèè åùå ìåíüøå, ÷åì ó Áîáà.

Ñëåïûå ïîäïèñè

Ñ ïîìîùüþ ïðîòîêîëà ïîëíîñòüþ ñëåïûõ ïîäïèñåé Àëèñà ìîæåò çàñòàâèòü Áîáà ïîäïèñàòü ÷òî-íèáóäü âðîäå: "Áîá äîëæåí Àëèñå ìèëëèîí äîëëàðîâ", "Áîá äîëæåí Àëèñå ñâîåãî ïåðâîãî ðåáåíêà", "Áîá äîëæåí Àëèñå ÿùèê øîêîëàäà". Âîçìîæíîñòè áåñêîíå÷íû, è ïîýòîìó âî ìíîãèõ ïðèëîæåíèÿõ ýòîò ïðîòîêîë áåñïîëåçåí..

Îäíàêî, ñóùåñòâóåò ñïîñîá, ñ ïîìîùüþ êîòîðîãî Áîá ìîæåò óçíàòü, ÷òî îí ïîäïèñûâàåò, âìåñòå ñ òåì ñîõðàíÿÿ ïîëåçíûå ñâîéñòâà ñëåïûõ ïîäïèñåé. Öåíòðàëüíûì ìîìåíòîì ýòîãî ïðîòîêîëà ÿâëÿåòñÿ òåõíèêà "ðàçðåçàòü è âûáðàòü". Ðàññìîòðèì ñëåäóþùèé ïðèìåð. Ìíîæåñòâî ëþäåé êàæäûé äåíü âúåçæàþò â íåêóþ ñòðàíó, è Äåïàðòàìåíò èììèãðàöèè õî÷åò óäîñòîâåðèòüñÿ, ÷òî îíè íå ââîçÿò êîêàèí. Ñëóæàùèå ìîãóò îáûñêèâàòü êàæäîãî, íî âìåñòî ýòîãî èñïîëüçóåòñÿ âåðîÿòíîñòíîå ðåøåíèå - îáûñêèâàåòñÿ êàæäûé äåñÿòûé âúåçæàþùèé. Ïîäâåðãàåòñÿ äîñìîòðó èìóùåñòâî îäíîãî ÷åëîâåêà èç äåñÿòè, îñòàëüíûå äåâÿòü ïðîïóñêàþòñÿ áåñïðåïÿòñòâåííî. Ïîñòîÿííûå êîíòðàáàíäèñòû â áîëüøèíñòâå ñëó÷àåâ ïðîñêàêèâàþò íåçàìå÷åííûìè, íî ñ âåðîÿòíîñòüþ 10 ïðîöåíòîâ èõ ëîâÿò. È åñëè ñóäåáíàÿ ñèñòåìà ðàáîòàåò ýôôåêòèâíî, íàêàçàíèå çà åäèíñòâåííóþ ïîèìêó íà ìåñòå ïðåñòóïëåíèÿ áîëåå ÷åì ïåðåâåøèâàåò âûãîäû äðóãèõ ïîïûòîê.

Åñëè Äåïàðòàìåíò èììèãðàöèè çàõî÷åò ïîâûñèòü âåðîÿòíîñòü ïîèìêè êîíòðàáàíäèñòîâ, ñëóæàùèì ïðèäåòñÿ îáûñêèâàòü áîëüøå ëþäåé, çàõî÷åò ïîíèçèòü âåðîÿòíîñòü - ìîæíî áóäåò îáûñêèâàòü ìåíüøå ëþäåé. Óïðàâëÿÿ âåðîÿòíîñòÿìè, ìîæíî êîíòðîëèðîâàòü ýôôåêòèâíîñòü ïðîòîêîëà ïðè ïîèìêå êîíòðàáàíäèñòîâ.

Ïðîòîêîë ñëåïîé ïîäïèñè ðàáîòàåò àíàëîãè÷íûì îáðàçîì. Áîá ïîëó÷àåò áîëüøóþ ïà÷êó ðàçëè÷íûõ çàìàñêèðîâàííûõ äîêóìåíòîâ. Îí **îòêðîåò**, íàïðèìåð, âñå êðîìå îäíîãî è çàòåì ïîäïèøåò ïîñëåäíèé.

Ïîñìîòðèòå íà çàìàñêèðîâàííûé äîêóìåíò êàê íà ëåæàùèé â êîíâåðòå. Ïðîöåññ ìàñêèðîâêè äîêóìåíòà ìîæíî ðàññìàòðèâàòü êàê ïîìåùåíèå äîêóìåíòà â êîíâåðò, à ïðîöåññ óäàëåíèÿ ìíîæèòåëÿ ìàñêèðîâêè - êàê âñêðûòèå êîíâåðòà. Êîãäà äîêóìåíò ñïðÿòàí â êîíâåðò, íèêòî íå ñìîæåò åãî ïðî÷èòàòü. Äîêóìåíò ïîäïèñûâàåòñÿ ñ ïîìîùüþ êóñî÷êà êîïèðîâàëüíîé áóìàãè, ïîìåùåííîé â êîíâåðò: Êîãäà ïîäïèñûâàþùèé ñòàâèò ñâîþ ïîäïèñü íà êîíâåðòå, ñ ïîìîùüþ êóñî÷êà êîïèðîâàëüíîé áóìàãè ýòà ïîäïèñü ñòàâèòñÿ è ïîä äîêóìåíòîì.

Â ñëåäóþùåì ñöåíàðèè äåéñòâóåò ãðóïïà àãåíòîâ êîíòððàçâåäêè. Èõ ëè÷íîñòè çàñåêðå÷åíû, äàæå ñàìî Óïðàâëåíèå êîíòððàçâåäêè íå çíàåò, êòî îíè òàêèå. Äèðåêòîðà Óïðàâëåíèÿ õî÷åò âûäàòü êàæäîìó àãåíòó ïîäïèñàííûé äîêóìåíò ñëåäóþùåãî ñîäåðæàíèÿ: "Ïîäàòåëü ýòîãî ïîäïèñàííîãî äîêóìåíòà, (âñòàâüòå èìÿ, ïîä êîòîðûì äåéñòâóåò àãåíò), îáëàäàåò ïîëíîé äèïëîìàòè÷åñêîé íåïðèêîñíîâåííîñòüþ". Ó êàæäîãî èç àãåíòîâ åñòü ñâîé ñïèñîê ïñåâäîíèìîâ, ïîýòîìó Óïðàâëåíèå íå ìîæåò ïðîñòî ðàçäàòü ïîäïèñàííûå äîêóìåíòû. Àãåíòû íå õîòÿò ïåðåäàâàòü ñâîè ïñåâäîíèìû â Óïðàâëåíèå, òàê êàê âðàã ìîã âñêðûòü êîìïüþòåð Óïðàâëåíèÿ. Ñ äðóãîé ñòîðîíû, Óïðàâëåíèå íå õî÷åò ñëåïî ïîäïèñûâàòü äîêóìåíòû, ïðåäñòàâëåííûå àãåíòîì. Õèòðûé àãåíò ìîæåò ïðåäñòàâèòü ñîîáùåíèå, ïîäîáíîå ñëåäóþùåìó: "Àãåíò (èìÿ) âûøåë â îòñòàâêó, è åìó íàçíà÷åíà åæåãîäíàÿ ïåíñèÿ â ìèëëèîí äîëëàðîâ. Ïîäïèñàíî, Ïðåçèäåíò". Â ýòîì ñëó÷àå ìîãóò áûòü ïîëåçíû ñëåïûå ïîäïèñè.

Ïðåäïîëîæèì, ÷òî ó êàæäîãî àãåíòà ïî 10 ïñåâäîíèìîâ, âûáðàííûõ èìè ñàìèìè è áîëüøå íèêîìó íåèçâåñòíûõ. Ïðåäïîëîæèì òàêæå, ÷òî àãåíòàì âñå ðàâíî, ïîä êàêèì èìåíåì îíè ïîëó÷àò äèïëîìàòè÷åñêóþ íåïðèêîñíîâåííîñòü. Òàêæå ïðåäïîëîæèì, êîìïüþòåð óïðàâëåíèÿ íàçûâàåòñÿ Agency's Large Intelligent Computing Engine (Áîëüøàÿ Èíòåëëåêòóàëüíàÿ Âû÷èñëèòåëüíàÿ Ìàøèíà Óïðàâëåíèÿ), èëè ALICE, à íàøèì êîíêðåòíûì àãåíòîì ÿâëÿåòñÿ Bogota Operations Branch (Ñåêòîð îïåðàöèè â Áîãîòå): BOB.

(1) BOB ãîòîâèò *n* äîêóìåíòîâ, êàæäûé èç êîòîðûõ èñïîëüçóåò ðàçëè÷íûé ïñåâäîíèì, äàþùèõ åìó äèïëîìàòè÷åñêóþ íåïðèêîñíîâåííîñòü.

(2) BOB ìàñêèðóåò êàæäûé èç äîêóìåíòîâ îòëè÷íûì ìàñêèðóþùèì ìíîæèòåëåì.

(3) BOB îòïðàâëÿåò *n* äîêóìåíòîâ ALICE.

(4) ALICE ñëó÷àéíûì îáðàçîì âûáèðàåò *n-1* äîêóìåíò è ïðîñèò BOB'à ïðèñëàòü ìàñêèðóþùèé ìíîæèòåëü äëÿ êàæäîãî èç âûáðàííûõ äîêóìåíòîâ.

(5) BOB ïîñûëàåò ALICE ñîîòâåòñòâóþùèå ìàñêèðóþùèå ìíîæèòåëè.

(6) ALICE îòêðûâàåò (ò.å., óäàëÿåò ìàñêèðóþùèé ìíîæèòåëü) *n-1* äîêóìåíò è óáåæäàåòñÿ â òîì, ÷òî îíè êîð-

ðåêòíû - è íå ÿâëÿþòñÿ ðàçðåøåíèåì íà âûïëàòó ïåíñèè.

(7) ALICE ïîäïèñûâàåò îñòàâøèéñÿ äîêóìåíò è ïîñûëàåò åãî BOB'ó.

(8) Àãåíò óäàëÿåò ìàñêèðóþùèé ì÷èòàåò ñâîé íîâûé ïñåâäîíèì: "Ìàëèíîâàÿ ïîëîñà." Ïîäïèñàííûé äîêóìåíò äàåò åìó äèïëîìàòè÷åñêóþ íåïðèêîñíîâåííîñòü ïîä ýòèì èìåíåì.

Ýòîò ïðîòîêîë íàäåæíî çàùèùåí îò ìîøåííè÷åñòâà BOB'à. ×òîáû ñìîøåííè÷àòü, îí äîëæåí òî÷íî óãàäàòü, êàêîé äîêóìåíò ALICE íå áóäåò ïðîâåðÿòü. Âåðîÿòíîñòü ýòîãî - 1 øàíñ èç *n* - íå ñëèøêîì âåëèêà. ALICE çíàåò ýòî è ÷óâñòâóåò ñåáÿ óâåðåííî, ïîäïèñûâàÿ äîêóìåíò, êîòîðûé îíà íå ñìîæåò ïðîâåðèòü. Äëÿ ýòîãî äîêóìåíòà ðàññìàòðèâàåìûé ïðîòîêîë ïîëíîñòüþ ñîâïàäàåò ñ ïðåäûäóùèì ïðîòîêîëîì ïîëíîñòüþ ñëåïîé ïîäïèñè, ñîõðàíÿÿ âñå ñâîéñòâà àíîíèìíîñòè.

Ñóùåñòâóåò òðþê, êîòîðûé åùå áîëüøå óìåíüøàåò âåðîÿòíîñòü ìîøåííè÷åñòâà BOB'à. Íà ýòàïå (4) ALICE ñëó÷àéíûì îáðàçîì âûáèðàåò *n/2* äîêóìåíòîâ äëÿ ïðîâåðêè, è BOB ïðèñûëàåò åé ñîîòâåòñòâóþùèé ìàñêèðóþùèå ìíîæèòåëè íà ýòàïå (5). Íà ýòàïå (7) ALICE ïåðåìíîæàåò âñå íåïðîâåðåííûå äîêóìåíòû è ïîäïèñûâàåò ïîëó÷èâøèéñÿ ìåãàäîêóìåíò. Íà ýòàïå (8) BOB óäàëÿåò âñå ìàñêèðîâî÷íûå ìíîæèòåëè. Ïîäïèñü ALICE áóäåò ïðàâèëüíîé, òîëüêî åñëè åþ ïîäïèñàíî ïðîèçâåäåíèå *n/2* èäåíòè÷íûõ äîêóìåíòîâ. ×òîáû ñìîøåííè÷àòü, BOB'ó íóæíî òî÷íî óãàäàòü, êàêîå ïîäìíîæåñòâî äîêóìåíòîâ áóäåò ïðîâåðÿòüñÿ ALICE. Âåðîÿòíîñòü ýòîãî ãîðàçäî íèæå, ÷åì âåðîÿòíîñòü óãàäàòü åäèíñòâåííûé äîêóìåíò, êîòîðûé ALICE íå ïðîâåðÿëà.

BOB ìîæåò ñìîøåííè÷àòü ïî äðóãîì. Î í ìîæåò ñîçäàòü äâà ðàçëè÷íûõ äîêóìåíòà, îäèí èç êîòîðûõ ALICE ñîãëàñíà ïîäïèñàòü, à äðóãîé - íåò. Çàòåì îí ìîæåò ïîïûòàòüñÿ íàéòè äâà ðàçëè÷íûõ ìàñêèðóþùèõ ìíîæèòåëÿ, êîòîðûå ïðåîáðàçóþò óêàçàííûå äîêóìåíòû ê îäèíàêîâîìó âèäó. Òàêèì îáðàçîì, åñëè ALICE çàõî÷åò ïðîâåðèòü äîêóìåíò, BOB ïåðåäàñò åé ìàñêèðóþùèé ìíîæèòåëü, ïðåîáðàçóþùèé äîêóìåíò ê íåâíîìó âèäó. Åñëè ALICE íå çàõî÷åò ïðîñìîòðåòü äîêóìåíò è ïîäïèøåò åãî, îí ïðèøëåò òîò ìàñêèðóþùèé äîêóìåíò â äîêóìåíò, ÿâëÿþùèéñÿ öåëüþ ìîøåííè÷åñòâà. Õîòÿ òåõíîëîãèè çàìàñêèðîâàííûé ïîäïèñàííûé äîêóìåíò â äîêóìåíò, ÿâëÿþùèéñÿ öåëüþ ìîøåííè÷åñòâà. Õîòÿ òåõíîëîãèè ýòîé è âîçìîæíî, ìàòåìàòèêà êîíêðåòíûõ àëãîðèòìîâ äëÿ BOB'à íàéòè òàêóþ ïàðó. Äåéñòâèòåëüíî, îíà ìîæåò áûòü ñòîëü íèçêî, êàê è âåðîÿòíîñòü Áîáà ñîçäàòü íåïðàâäîïîäîáíóþ ïîäïèñü ïîä ïðîèçâîëüíûì äîêóìåíòîì ñàìîñòîÿòåëüíî. Ýòîò âîïðîñ îáñóæäàåòñÿ íèæå â ðàçäåëå 23.12.

Ïàòåíòû. Âëàäåëüöåì ïàòåíòîâ íà ðÿä îñíîâíûõ ñõåì ïîäïèñåé ÿâëÿåòñÿ ×àóì (Chaum) (ñì. 4-é).

Òàáë. 5-1. Ïàòåíòû ×àóìà íà ñëåïûå ïîäïèñè

[1] ïàòåíòà ÑØÀ	Äàòà	Íàçâàíèå
4759063	19.07.88	Blind Signature Systems [323] (Ñèñòåìû ñëåïûõ ïîäïèñåé)
4759064	19.07.88	Blind Unanticipated Signature Systems [324] (Ñèñòåìû ñëåïûõ íåîæèäàííûõ ïîäïèñåé)
4914698	03.03.90	One-Show Blind Signature Systems [326] (Ñèñòåìû ñëåïûõ ïîäïèñåé, ïîêàçûâàåìûõ îäèí ðàç)
4949380	14.08.90	Returned-Value Blind Signature Systems [328] (Ñèñòåìû ñëåïûõ ïîäïèñåé ñ âîçâðàùàåìûì çíà÷åíèåì)
4991210	05.02.91	Unpredictable Blind Signature Systems [331] (Ñèñòåìû íåïðåäñêàçóåìûõ ñëåïûõ ïîäïèñåé)

5.4 Ëè÷íîñòíàÿ êðèïòîãðàôèÿ ñ îòêðûòûì êëþ÷àìè

Àëèñà õî÷åò îòïðàâèòü Áîáó áåçîïàñíîå ñîîáùåíèå. Îíà íå õî÷åò ïîëó÷àòü ñâîé îòêðûòûé êëþ÷ ñ ñåðâåðà êëþ÷åé, îíà íå õî÷åò ïðîâåðÿòü ïîäïèñü íåêîòîðîé çàñëóæèâàþùåé äîâåðèÿ òðåòüåé ñòîðîíû íà ñåðòèôèêàòå ñâîåãî îòêðûòîãî êëþ÷à, è îíà äàæå íå õî÷åò õðàíèòü îòêðûòûé êëþ÷ Áîáà â ñâîåì êîìïüþòåðå. Îíà õî÷åò ïðîñòî ïîëüçîâàòüñÿ ñîâìåñòíî áåçîïàñíîå ñîîáùåíèå.

Ýòó ïðîáëåìó ðåøàþò **èè÷íîñòíûå** êðèïòîñèñòåìû, èíîãäà íàçûâàåìûå ñèñòåìàìè ñ Íåèíòåðàêòèâíûì ðàçäåëåíèåì êëþ÷åé (Non-Interactive Key Sharing, NIKS) [1422]. Îòêðûòûé êëþ÷ Áîáà îñíîâûâàåòñÿ íà åãî èìåíè è ñåêðåòíî àäðåñà (òåëåôîííîì íîìåðå, ïî÷òîâîì àäðåñå èëè ÷àì-òî ïîäîáíîì). Â îáû÷íîé êðèïòîãðàôèè ñ îòêðûòûì êëþ÷àìè Àëèñå íóæåí ïîäïèñàííûé ñåðòèôèêàò, ñâÿçûâàþùèé ëè÷íîñòü Áîáà è åãî îòêðûòûé êëþ÷. Â ëè÷íîñòíîé êðèïòîãðàôèè îòêðûòûé êëþ÷ Áîáà *è åñòü* åãî ëè÷íîñòü. Ýòî äåéñòâèòåëüíî ñåæàùå èäëÿ ÿâëÿåòñÿ ïî÷òè ñîâåðøåííîé äëÿ ïî÷òîâîé ñèñòåìû - Åñëè Àëèñà çíàåò àäðåñ Áîáà, îíà ìîæåò áåçîïàñíî ïîñûëàòü åìó ïî÷òó, ÷òî äëàåò êðèïòîãðàôèþ ïðîçðà÷íîé, íàñêîëüêî ýòî âîîáùå âîçìîæíî.

Ñèñòåìà îñíîâàíà íà âûäà÷å Òðåòüîì êëþ÷åé ïîëüçîâàòåëÿì â çàâèñèìîñòè îò èõ ëè÷íîñòè. Åñëè çàêðûòûé

êëþ÷ Àëèñû áóäåò ñêîìïðîìåòèðîâàí, åé ïðèäåòñÿ èçìåíèòü îäíî èç ñâîéñòâ, îïðåäåëÿþùèõ åå ëè÷íîñòü. Ñåðüåçíîé ïðîáëåìîé ÿâëÿåòñÿ ïðîåêòèðîâàíèå ñèñòåìû òàêèì îáðàçîì, ÷òîáû ñâîð íå÷åñòíûõ ïîëüçîâàòåëåé íå ìîã ïðèâåñòè ê ïîääåëêå êëþ÷à.

Ïðè ðàçðàáîòêå ìàòåìàòèêè òàêèõ ñõåì, îáåñïå÷åíà áåçîïàñíîñòè êîòîðûõ îêàçàëîñü çâåðñêè ñëîæíûì, áûë âûïîëíåí áîëüøîé îáúåì îáúåìíûõ ðàñ÷åòîâ - ãëàâíûì îáðàçîì â ßïîíèè. Ìíîãå ïðåäëîæåííûå ðåøåíèÿ ñîäåðæàò âûîð Òðåíòì ñëó÷àéíîãî ÷èñëà äëÿ êàæäîãî ïîëüçîâàòåëÿ - ïî ìåíó, ýòî óãðîæàåò ñàìîé èäåå òàêèõ ñèſòåì. Ðÿä àëãîðèòìîâ, ðàññìàòðèâàåìûõ â ãëàâàõ 19 è 20, ìîãóò áûòü ëè÷íîſòíûìè. Ïîäðîáíîñòè àëãîðèòìîâ è êðèïòîſñèſòåì ìîæíî íàéòè â [191, 1422, 891, 1022, 1515, 1202, 1196, 908, 692, 674, 1131, 1023, 1516, 1536, 1544, 63, 1210, 314, 313, 1545, 1539, 1543, 933, 1517, 748, 1228]. Àëãîðèòì, êîòîðûé íå èſïîëüçóåò ſëó÷àéſûõ ſèſåé, îïèſàí â [1035]. Sèſòåìà, îſñóæäåíèÿ â [1546, 1547, 1507], íåíàäåæíà ïðîòèâ ſ èſïîëüçîâàíèåì âûáðàííîãî îòêðûòîãî êëþ÷à, òî æå ſàìîå ìîæſî ſêàçàòü è î ſèſòåìå, ïðåäëîæåííîé êàê NIKS-TAS [1542, 1540, 1541, 993, 375, 1538]. Ïî ïðàâäå ãîâîðÿ, ſðåäè ïðåäëîæåííîſ íåò íè÷åſî îäíîâðåìåííî ïðàêòè÷íîſî è áåçîïàſíîſî.

5.5 Ðàſſåÿííàÿ ïåðåäà÷à

Êðèïòîſðàô Áîá áåçíàäåæíî ïûòàåòſÿ ðàçëîæèòü íà ìíîæèòåëè 500-áèòîâîå ſèſëî *n*. Îſ çíàåò, ſòî îſî ÿâëÿåòſÿ ïðîèçâåäåíèåì ïÿòè 100-áèòîâûſ ſèſåë, è íè÷åſî áîëüøå. (Âſò ïðîáëìà. Åſëè îſ íå âîſſòàíîâèſ êëþ÷, åſó ïðèäåòſÿ ðàſîàòü ſåêðåſíîſü, è îſ íå ïîſàäåò íà åæåſíåäëüíóþ èſðó ſ Àëèſîé â ſûſëåíſûé ïſêåð.) ×òſ æå äåëàòü? È âſò ſîÿâëÿåòſÿ Àëèſà:

> "Ì íå ſîſ÷àſòëèâèſîſüſ óçíàòü ſàëí èç ſíſæèòåëå ſ÷èſëà", - ãſâſîðèſ íſà, - "è ÿ ſðſîäàſ åâſ òåéà çà 100 äſëëàðſâ. Ïſ äſëëàðó çà áèò." Ïſêàçûâàÿ ſàſþ ſåðüåçſſòſü, íſà ſſſéàðàòſÿ èſſſîëüçſâàòü ſõåſó âðó÷åſèÿ áèòà, âðó÷àÿ êàæäûé áèò îòäåëüſſ.
>
> Áſá çàſíåðåſſâàſ, íſ òſëüêſ çà 50 äſëëàðſâ. Åëèſà íå õſ÷åò ſåðàſûâàòü öåſó è ſðåäëàãàåò ſðſäàòü Áſáó ſſëſâèſó áèòſâ çà ſſëſâèſó ſòſèſſòſ. "Ýòſ çàſåſíſ ſſſêðàòèò òåéá ðàáſòó", -.
>
> "Íſ êàê ÿ óçíàþ, ſòſ òàſå ſ÷èſëſ äåéſòâèòåëüſſſ ÿâëÿåòſÿ ſſſæèòåëåſ *n*. Åſëè òſ ſſêàæåøü ſſſå ſ÷èſëſ è ſſçâſëëøü ſſſå óáåäèòüſÿ, ſ÷òſ ſſſ äåéſòâèòåëüſſſ ÿâëÿåòſÿ ſſſæèòåëſ, ÿ ſſſäëàøóſü ſ òâſèſè óſſëſâèÿſè", - ãſâſðèò Áſá.
>
> Îſé â ſàòſâſé ſèòóàöèè. Àëèſà íå ſſæåò óáåäèòü Áſáà â òſſ, ſ÷òſ ſſíà çſàåò ſſſſſſſæèòåëü *n*, íå ðàſſêðûâ åãſ, à Áſá íå õſ÷åò ſſêſſàòü 50 áèòſâ, êſòſðûå âſſëſå ſſãſó ſêàçàòüſÿ áåſſſêåçſûſè.

Ýòà èſòſðèÿ, óòàùåſíàÿ ó Äæſ Êèëèàſíà [831], ââſäèò ſſíýòèå **ðàſſåÿſíſé ſåðåää÷è**. Àëèſà ſåðåäàåò Áſáó ãðóſſó ſſſáùåſíèé. Áſá ſſëó÷àåò íåêſòſðſå ſſäſſſæåſòâ ýòèõ ſſſáùåſíèé, íſ Àëèſà íå çſàåò, êàêèå èç ſſſáùåſíèé Áſá ſſëó÷ëè. Îäſàêſ, ýòſ íå ſſëſſſüſ ðåøàåò ſðſáëåſó. Êſãää Áſá ſſëó÷èò ſëó÷àéſóþ ſſëſâèſó áèòſâ, Àëèſå ſðèäòſÿ óáåæäàòü åãſ, ſëſſſëüçóÿ äſêàçàòåëüſòâſ ſ íóëåâû ſ çſàſèàſ, ÷òſ ſíà ſſſëäëà ÷àſòü ſſſæèòåëü *n*.

Â ſëåäóþùſ ſðſòſêſëå Àëèſà ſſſûëàåò Áſáó îäſſ èç äâóõ ſſſáùåſíèé. Áſá ſſëó÷àåò ſſſáùåſíèå, íſ êàêſå - Àëèſà íå çſàåò.

(1) Àëèſà ãåſíåðèðóåò äâå ſàðû ſòêðûòûé êëþ÷/çàêðûòûé êëþ÷, âſñãſ ÷åòûðå êëþ÷à. Îſíà ſſſûëàåò ſíàà ſòêðûòûõ êëþ÷à Áſáó.

(2) Áſá âûáèðàåò êëþ÷ ſèſſſſſſſſ àëãſðèòſà (íàſðèſåð, DES). Îſ âûáèðàåò ſſäſſ èç ſòêðûòûõ êëþ÷åé Àëèſû è øèſðóåò ſ ãåſſ ſſſſſüſ ſãſé êëþ÷ DES. Îſ ſſſûëàåò øèſðſâàſſſûé êëþ÷ Àëèſå, íå ſſſáùàÿ, êàêſé èç åå ſòêðûòûõ êëþ÷åé îſ èſſſſëüçſâàë äëÿ øèſðſâàſèÿ.

(3) Àëèſà äâàæäû ðàſøèſðſâſûâàåò êëþ÷ Áſáà, èſſſſëüçóÿ ſáà ſãſèõ çàêðûòûõ êëþ÷à. Â ſäſſſ èç ſëó÷àåâ ſíà èſſſſëüçóåò ſðàâèëüſûé êëþ÷ è óſſäøåſſ ðàſøèſðſâſûâàåò êëþ÷ DES, ſðèſſèàſſſûé Áſáſſ. Â äðóãſ ſëó÷àå ſíà èſſſſëüçóåò íåſðàâèëüſûé êëþ÷ è ſſëó÷àåò áåſſſſûſëåſſóþ ſſſëåäſâàòåëüſſſòü áèòſâ, êſòſðàÿ, òàſ íå ſàſíå, ſſõſæà íà ſëó÷àéſûé êëþ÷ DES. Òàê êàê åé íåèçâåſòåſ ſðàâèëüſûé ſòêðûòûé òåſò, ſíà íå ſſæåò óçíàòü, êàêſé èç êëþ÷åé ſðàâèëåſ.

(4) Àëèſà çàøèſðſâſûâàåò êàæäſå èç ſãſèõ ſſſáùåſíèé êàæäûſ èç êëþ÷åé, ſſëó÷åſíſûõ åþ íà ſðåäſûäóùſ ýòàſå (ſäèſ èç êſòſðſûõ - íàſòſÿùèé, à äðóãſé - áåſſſſûſëåſíſé), è ſſſûëàåò ſíàà ſſſáùåſíèÿ Áſáó.

(5) Áſá ſſëó÷àåò ſſſáùåſíèÿ Àëèſû, ſäſíſ èç êſòſðſûõ çàøèſðſâàſíſ ſðàâèëüſíſûſ êëþ÷ſſ DES, à äðóãſå - áåſſſſûſëåſíſûſ êëþ÷ſſ DES. Êſãää Áſá ðàſøèſðſâſûâàåò êàæäſå èç ýòèſ ſſſáùåſíèé ſãſèſ êëþ÷ſſ DES, ſſ ſſæåò ſðſ÷èòàòü ſäſſ èç íèõ, à äðóãſå áóäåò äëÿ íåãſ âſãëÿäàòü ſſëſíſé áåſſſſûſëèòåé.

Òåſåðü ó Áſáà åſòü äâà ſſſáùåſíèÿ Àëèſû, è Àëèſà íå çſàåò, êàêſå èç íèõ Áſáó óäàëſſü óſſſåøſſ ðàſøèſðſâàòü. Ê íåſ÷àſòüþ, åſëè ſðſòſêſſè ſſòàſſſâèſÿ íà ýòſſ ýòàſå, Àëèſà ſſſæåò ſſſſøåſíè÷àòü. Íåſáſãèſ åùå ſäèſ ýòàſ.

(6) Êſãää ſðſòſêſë çàâåðøèſÿ, è ſòàſóò èçâåſòſû íáà âſçſſæſûõ ðåçóëüòàòà ſåðåää÷è, Àëèſà äſëæíà ſåðåäàòü Áſáó ſâſè çàêðûòûå êëþ÷è, ÷òſáû ſſ óáåäèòüſÿ â ſòſóòſòâèſ ſſøåſíè÷åſòâà. Â êſíöå êſíöſâ, íſà ſſãëà çàøèſðſâàòü íà ýòàſå (4) ſáſèſè êëþ÷àſè ſäſſ è òſ æå ſſſáùåſíèå.

Â ýòſò ſſſåſíò, êſíå÷ſſ æå Áſá ſſſæåò óçſàòü è âòſðſå ſſſáùåſíèå.

Ïðîòîêîë íàäåæíî çàùèùåí îò âçëîìà ñî ñòîðîíû Àëèñû, ïîòîìó ÷òî ó íåå íåò âîçìîæíîñòè óçíàòü, êàêîé èç äâóõ êëþ÷åé DES ÿâëÿåòñÿ íàñòîÿùèì. Îáà èç íèõ îíà èñïîëüçóåò äëÿ øèôðîâàíèÿ ñâîèõ ñîîáùåíèé, íî ÁÎá ìîæåò óñòàíîâèòü ðàçíûå êëþ÷è - äî ýòàïà (6). Ïðîòîêîë çàùèùåí è îò âçëîìà ñî ñòîðîíû ÁÎáà, ïîòîìó ÷òî äî ýòàïà (6) îí íå ñìîæåò ïîëó÷èòü çàêðûòûé êëþ÷ Àëèñû, ÷òîáû îïðåäåëèòü êëþ÷ DES, êîòîðûì çàøèôðîâàíî äðóãîå ñîîáùåíèå. Íà âèä ýòî ïðîòîêîë ìîæåò ïîêàçàòüñÿ ïðîñòî óñëîæíåííûì ñïîñîáîì áðîñàòü "÷åñòíóþ" ìîíåòó ïî ìîäåì, íî îí èíòåãðèðîâàí èñïîëüçóåòñÿ âî ìíîãèõ ñëîæíûõ ïðîòîêîëàõ.

Êîíå÷íî æå, íè÷òî íå ìîæåò ïîìåøàòü Àëèñå ïîñëàòü ÁÎáó äâà ñîâåðøåííî áåññìûñëåííûõ ñîîáùåíèÿ: "Ìýó-ìýó" è "Òû ìîëîêîñîñ". Ýòîò ïðîòîêîë ãàðàíòèðóåò, ÷òî Àëèñà ïåðåäàñò ÁÎáó îäíî è äâóõ ñîîáùåíèé, íî íåò íèêàêîé ãàðàíòèè, ÷òî ÁÎá çàõî÷åò ïîëó÷èòü ëþáîå èç íèõ.

Â ëèòåðàòóðå ìîæíî íàéòè è äðóãèå ïðîòîêîëû ðàñïðåäåëåííîãî ïåðåäà÷è. Íåêîòîðûå èç íèõ íåêîíñòðóêòèâíî, ò.å. Àëèñà ïóáëèêóåò ñâîè äâà ñîîáùåíèÿ, à ÁÎá ìîæåò ïðî÷åñòü òîëüêî îäíî èç íèõ. Î í ìîæåò ñäåëàòü ýòî, êîãäà çàõî÷åò, åìó íå íóæíî äëÿ ýòîãî ñâÿçûâàòüñÿ ñ Àëèñîé [105].

Â äåéñòâèòåëüíîñòè íà ïðàêòèêå íèêòî íå èñïîëüçóåò ïðîòîêîë ðàñïðåäåë¸ííîé ïåðåäà÷è, íî ýòî ïîíÿòèå ÿâëÿåòñÿ âàæíûì áëîêîì ïðè ïîñòðîåíèè äðóãèõ ïðîòîêîëîâ. Õîòÿ ñóùåñòâóåò ìíîãî òèïîâ ðàñïðåäåë¸ííîé ïåðåäà÷è - ó ìåíÿ åñòü äâà ñåêðåòà, à âû ïîëó÷àåòå îäèí, ó ìåíÿ åñòü n ñåêðåòîâ, à âû ïîëó÷àåòå îäèí, ó ìåíÿ åñòü îäèí ñåêðåò, êîòîðûé âû ïîëó÷àåòå ñ âåðîÿòíîñòüþ 1/2 è òàê äàëåå - âñå îíè ýêâèâàëåíòíû [245, 391, 395].

5.6 Ðàñïðåäåë¸ííûå ïîäïèñè

×åñòíî ãîâîðÿ, ÿ íå ìîãó ïðèäóìàòü, ÷åãî èõ ìîæíî èñïîëüçîâàòü, íî ñóùåñòâóåò äâà òèïà ðàñïðåäåë¸ííûõ ïîäïèñåé [346]:

1. Ó Àëèñû åñòü *n* ðàçëè÷íûõ ñîîáùåíèé. Áîá ìîæåò âûáðàòü îäíî èç íèõ, ÷òîáû Àëèñà åãî ïîäïèñàëà, è ó Àëèñû íå áóäåò ñïîñîáà óçíàòü, ÷òî æå îíà ïîäïèñàëà.
2. Ó Àëèñû åñòü åäèíñòâåííîå ñîîáùåíèå. Áîá ìîæåò âûáðàòü îäèí èç *n* êëþ÷åé, êîòîðûì Àëèñà ïîäïèøåò ñîîáùåíèå, è Àëèñà íå ñìîæåò óçíàòü, êàêîé êëþ÷ îíà èñïîëüçîâàëà.

Èäåÿ èçÿùíà, ÿ óâåðåí, ÷òî ãäå-íèáóäü îíà íàéäåò ïðèìåíåíèå.

5.7 Îäíîâðåìåííàÿ ïîäïèñü êîíòðàêòà

Ïîäïèñü êîíòðàêòà ñ ïîìîùüþ ïîñðåäíèêà

Àëèñà è Áîá õîòÿò çàêëþ÷èòü êîíòðàêò. Îíè äîñòèãëè ñîãëàñèÿ íà ñëîâàõ, íî íèêòî íå õî÷åò ñòàâèòü ñâîþ ïîäïèñü, ïîêà íå ïîñòàâëåíà ïîäïèñü äðóãîãî. Ïðè ëè÷íîé âñòðå÷è ýòî íå âûçûâàåò çàòðóäíåíèé - îáà ïîäïèñûâàþò âìåñòå. Íà ðàññòîÿíèè îíè ìîãóò îáðàòèòüñÿ ê ïîñðåäíèêó.

(1) Àëèñà ïîäïèñûâàåò êîïèþ êîíòðàêòà è ïîñûëàåò åå Òðåíó.

(2) Áîá ïîäïèñûâàåò êîïèþ êîíòðàêòà è ïîñûëàåò åå Òðåíó.

(3) Òðåíò ïîñûëàåò ñîâùåíèå è Àëèñå, è Áîáó, ñîâùàþ ùåå, ÷òî äðóãîé ïîäïèñàë êîíòðàêò.

(4) Àëèñà ïîäïèñûâàåò äâå êîïèè êîíòðàêòà è ïîñûëàåò èõ Áîáó.

(5) Áîá ïîäïèñûâàåò îáå êîïèè êîíòðàêòà, ñîõðàíÿåò îäíó äëÿ ñåáÿ, è ïîñûëàåò äðóãóþ Àëèñå.

(6) Àëèñà è Áîá ñîâùàþò Òðåíòó, ÷òî ó êàæäîãî èç íèõ åñòü ïîäïèñàííàÿ îáîèìè ïàðòíåðàìè êîïèÿ êîíòðàêòà.

(7) Òðåíò óíè÷òîæàåò ñâîè âíîñèè êîíòðàêòà, ñ äâóìÿ íîâûìè ïîäïèñüþ ïîä êàæäûì.

Ýòîò ïðîòîêîë ðàáîòàåò, ïîòîìó ÷òî Òðåíò çàùèùàåò ëþáóþ èç ñòîðîí îò ìîøåííè÷åñòâà äðóãîé. Åñëè Áîá ïîïûòàåòñÿ îò âîçàòüñÿ îò ïîäïèñè ïîä êîíòðàêòîì íà ýòàïå (5), Àëèñà ìîæåò îáðàòèòüñÿ ê Òðåíòó çà êîïèåé êîíòðàêòà, óæå ïîäïèñàííîãî Áîáîì. Åñëè Àëèñà ïîïûòàåòñÿ îò ïîäïèñè íà êîíòðàêòà íà ýòàïå (4), Áîá ìîæåò ñäåëàòü òî æå ñàìîå. Êîãäà Òðåíò ñîâùàåò, ÷òî îí ïîëó÷èë îáà êîíòðàêòà íà ýòàïå (3), Àëèñà è Áîá óçíàþò, ÷òî äðóãîé ïàðòíåð óæå ïîäïèñàë êîíòðàêò. Åñëè Òðåíò íå ïîëó÷èò îáà êîíòðàêòà íà ýòàïàõ (1) è (2), îí óíè÷òîæàåò èìåþùóþñÿ ó íåãî êîïèþ, è íè îäíà èç ñòîðîí íå ñâÿçàíà áîëåå îáÿçàòåëüñòâàìè êîíòðàêòà.

Îäíîâðåìåííàÿ ïîäïèñü êîíòðàêòà áåç ïîñðåäíèêà (ëèöîì ê ëèöó)

Åñëè Àëèñà è Áîá âñòðå÷àþòñÿ ëèöîì ê ëèöó, îíè ìîãóò ïîäïèñàòü êîíòðàêò ñëåäóþùèì îáðàçîì [1244]:

(1) Àëèñà ïèøåò ïåðâóþ áóêâó ñâîåãî èìåíè è ïåðåäà¸ò êîíòðàêò Áîáó.

(2) Áîá ïèøåò ïåðâóþ áóêâó ñâîåãî èìåíè è ïåðåäà¸ò êîíòðàêò Àëèñå.

(3) Àëèñà ïèøåò âòîðóþ áóêâó ñâîåãî èìåíè è ïåðåäàåò êîíòðàêò Áîáó.

(4) Áîá ïèøåò âòîðóþ áóêâó ñâîåãî èìåíè è ïåðåäàåò êîíòðàêò Àëèñå.

(5) Ýòî ïðîäîëæàåòñÿ äî òåõ ïîð, ïîêà Àëèñà è Áîá íå íàïèøóò ñâîè èìåíà ïîëíîñòüþ.

Åñëè ïðåíåáðå÷ü î÷åâèäíî ïðîáëåìî ïðîòîêîëà (èìÿ Àëèñû äëèíåå èìåíè Áîáà), òî îí ðàáîòàåò äîñòàòî÷íî õîðîøî. Íàïèñàâ òîëüêî îäíó áóêâó èç ïîäïèñè, Àëèñà çíàåò, ÷òî íèêàêîé ñóäüþ íå ñòàíåò çàñòàâëÿòü åå âûïîëíÿòü óñëîâèÿ êîíòðàêòà. Í î íàïèñàííàÿ áóêâà - ýòî àêò äîáðîé âîëè, è Áîá îòâå÷àåò àíàëîãè÷íûì äåéñòâèåì.

Êîãäà êàæäàÿ èç ñòîðîí íàïèøåò íåñêîëüêî áóêâ ïîäïèñè, ñóäüÿ âåðîÿòíî ñ ìîæåò óáåäèòüñÿ, ÷òî îáå ñòîðîíû ïîäïèñàëè êîíòðàêò. Õîòÿ, åñëè âãëÿäåòüñÿ, ñèòóàöèÿ âåñüìà òóìàííà. Êîíå÷íî æå, òî, ÷òî êîíòðàêò íå âñòóïàåò â ñèëó ïîñëå íàïèñàíèÿ ïåðâûõ áóêâ, òàê æå î÷åâèäíî êàê è òî, ÷òî êîíòðàêò ñòàíîâèòñÿ äåéñòâóþùèì ïîñëå òîãî, êàê ñòîðîíû íàïèøóò ñâîè èìåíà. Â êàêîì ìåñòå ïðîïèñàíû ñòîðîíû îçàãëàâûâàþò ñâÿçàííûì èì êîíòðàêòîì? Íàïèñàâ ïîëíîìó ñâîåìó èìåíè? Äâå òðåòè? Òðè ÷åòâåðòè?

Òàê êàê íè Àëèñà, íè Áîá íå çíàþò òî÷íî, ñ êàêîãî ìîìåíòà íà÷èíàåò äåéñòâîâàòü êîíòðàêò, òî ó êàæäîãî èç íèõ íà ïðîïææåíèè âñåãî ïðîòîêîëà åñòü îïàñåíèå, ÷òî äëÿ íåãî êîíòðàêò óæå âñòóïèë â ñèëó. Íå ñóùåñòâóåò ýòàïà ïðîòîêîëà, íà êîòîðîì Áîá ñìîã áû ñêàçàòü: "Âû íàïèñàëè ÷åòûðå áóêâû ïîäïèñè, à ÿ òîëüêî òðè. Âû ñâÿçàíû êîíòðàêòîì, à ÿ íåò." Ó Áîáà íåò ïðè÷èí ïðåðâàòü âû ïîëíîñòüþ. Áîëåå òîãî, ÷åì äîëüøå ñòîðîíû âûïîëíÿþò ïðîòîêîë, òåì áîëüøå âåðîÿòíîñòü òîãî, ÷òî ñòîðîíû ðåøèò, ÷òî êîíòðàêò âñòóïèë â ñèëó. È ñíîâà, íåò ïðè÷èíû ïðåðûâàòü ïðîòîêîë. Â êîíöå êîíöîâ, îíè îáà õîòåëè ïîäïèñàòü êîíòðàêò, îíè ïðîñòî íå õîòåëè ïîäïèñûâàòü åãî ðàíüøå äðóãîãî ïàðòíåðà.

Îäíîâðåìåííàÿ ïîäïèñü êîíòðàêòà áåç ïîñðåäíèêà (áåç ëè÷íîé âñòðå÷è)

Â ýòîì ïðîòîêîëå èñïîëüçóåòñÿ òàêàÿ æå íåîïðåäåëåííîñòü [138]. Àëèñà è Áîá ïî î÷åðåäè äâèæóòñÿ äàòêèì øàæêàìè ê ïîäïèñàíèþ ïðîòîêîëà.

Â ýòîì ïðîòîêîëå Àëèñà è Áîá îáìåíèâàþòñÿ ðÿäîì ïîäïèñàííûõ ñîîáùåíèé âèäà: "ß ñîãëàñåí, ÷òî ñ âåðîÿòíîñòüþ p ÿ ñäýçàí óñëîâèÿì êîíòðàêòà."

Ïîëó÷àòåëü ñîîáùåíèÿ ìîæåò ïðåäúÿâèòü åãî ñóäüå è, ñ âåðîÿòíîñòüþ p, ñóäüÿ ïðèçíàåò êîíòðàêò ïîäïèñàííûì.

(1) Àëèñà è Áîá ñîãëàñîâûâàþò äàòó îêîí÷àíèÿ ïîäïèñàíèÿ êîíòðàêòà.

(2) Àëèñà è Áîá äîãîâàðèâàþòñÿ î ðàçëè÷èè âåðîÿòíîñòåé, êîòîðûì îíè ñîáèðàþòñÿ ïîëüçîâàòüñÿ. Íàïðèìåð, Àëèñà ìîæåò ðåøèòü, ÷òî åå âåðîÿòíîñòü áûòü ñâÿçàííîé óñëîâèÿìè êîíòðàêòà íå äîëæíà ïðåâûøàòü âåðîÿòíîñòü Áîáà áîëüøå, ÷åì íà 2 ïðîöåíòà. Îáîçíà÷èì ðàçëè÷èå Àëèñû êàê a, ðàçëè÷èå Áîáà - êàê b.

(3) Àëèñà ïîñûëàåò Áîáó ïîäïèñàííîå ñîîáùåíèå ñ âåðîÿòíîñòüþ $p = a$.

(4) Áîá ïîñûëàåò Àëèñå ïîäïèñàííîå ñîîáùåíèå ñ $p = a + b$.

(5) Ïóñòü p - ýòî âåðîÿòíîñòü èç ñîîáùåíèÿ, ïîëó÷åííîãî Àëèñîé îò Áîáà íà ïðåäûäóùåì ýòàïå. Àëèñà ïîñûëàåò Áîáó ïîäïèñàííîå ñîîáùåíèå ñ $p' = p + a$ èëè 1, ñìîòðÿ ÷òî ìåíüøå.

(6) Ïóñòü p - ýòî âåðîÿòíîñòü èç ñîîáùåíèÿ, ïîëó÷åííîãî Áîáîì îò Àëèñû íà ïðåäûäóùåì ýòàïå. Áîá ïîñûëàåò Àëèñå ïîäïèñàííîå ñîîáùåíèå ñ $p' = p + b$ èëè 1, ñìîòðÿ ÷òî ìåíüøå.

(7) Àëèñà è Áîá ïðîäîëæàþò âûïîëíÿòü ýòàïû (5) è (6) äî òåõ ïîð, ïîêà îíè íåò íå ïîëó÷àò ñîîáùåíèÿ ñ $p = 1$ èëè ïîêà íå íàñòóïèò ñîãëàñîâàííàÿ íà ýòàïå (1) äàòà.

Ïî ìåðå âûïîëíåíèÿ ïðîòîêîëà è Àëèñà, è Áîá ñîãëàøàþòñÿ, ÷òî îíè îêàçûâàþòñÿ ñâÿçàííûìè êîíòðàêòîì ñî âñå áîëüøåé è áîëüøåé âåðîÿòíîñòüþ. Íàïðèìåð, Àëèñà ìîæåò îòðàäëèòü ñâîå a êàê 2 ïðîöåíòà, à Áîá ñâîå b - êàê 1 ïðîöåíò. (Ëó÷øå áû îíè âûáðàëè áîëüøèå ïðåäàùåíèÿ, à òî ìû çàñòðÿíåì íà ýòîì ìåñòå.) Â ïåðâîì ñîîáùåíèè Àëèñà ñîîáùàåò, ÷òî îíà ñâÿçàíà êîíòðàêòîì ñ âåðîÿòíîñòüþ 2 ïðîöåíòà. Áîá ìîæåò îòâåòèòü, ÷òî îí ñâÿçàí êîíòðàêòîì ñ âåðîÿòíîñòüþ 3 ïðîöåíòà. Ñëåäóþùåå ñîîáùåíèå Àëèñû ìîæåò óòâåðæäàòü, ÷òî îíà ñâÿçàíà êîíòðàêòîì ñ âåðîÿòíîñòüþ 5 ïðîöåíòà è òàê äàëåå, ïîêà âåðîÿòíîñòè îáîèõ íå äîñòèãíóò 100 ïðîöåíòîâ.

Åñëè è Àëèñà, è Áîá çàâåðøèëè ïðîòîêîë ê îãîâîðåííîé äàòå, òî âñå ïðåêðàñíî. Â ïðîòèâíîì ñëó÷àå, ёðáàÿ èç ñòîðîí ìîæåò ïðåäúÿâèòü êîíòðàêò ñóäüå âìåñòå ñ ïîäïèñàííûì ïîñëåäíèì ñîîáùåíèåì ñîîáùåíèå âîçâðàùàåò ïðîòèâíîé ñòîðîíå äîñòèãíóò 100 ïðîöåíòîâ.

Ýòî áàçîâûé ïðîòîêîë, íî ìîãóò èñïîëüçîâàòüñÿ è äîïîëíèòåëüíûå óñëîæíåíèÿ. Ñóäüÿ ìîæåò ïðèíÿòü ðå-

øåíèå â îòñóòñòâèå îäíîé èç ñòîðîí. Ðåøåíèå ñóäüè ñâÿçûâàåò êîíòðàêòíî ëèáî îáå ñòîðîíû, ëèáî íè îäíó èç íèõ. Íå ñóùåñòâóåò ñèòóàöèè, êîãäà îäíà èç ñòîðîí ñâÿçàíà êîíòðàêòíî, à äðóãàÿ - íåò. Áîëåå òîãî, ïðîîôîë çàâåðøèòñÿ, êàê òîëüêî îäíà èç ñòîðîí çàõî÷åò èìåòü õîòü íåìíîãî áîëüøóþ, ÷åì äðóãàÿ, âåðîÿòíîñòü áûòü ñâÿçàííîé êîíòðàêòíî.

Îäíîâðåìåííàÿ ïîäïèñü êîíòðàêòà ääç ïîñðåäíèêà (ñ ïîìîùüþ êðèïòîãðàôèè)

Ýòîò êðèïòîãðàôè÷åñêèé ïðîòîêîë èñïîëüçóåò òò æå ïðèöèï äâóñòîðîííåãî øàãîâ [529]. Äëÿ îïðåäåëåííîñòè èñïîëüçóåòñÿ DES, õîòÿ âìåñòî íåãî ìîæåò áûòü ëþáîé ñèììåòðè÷íûé àëãîðèòì.

(1) È Àëèñà, è Áîá ñëó÷àéíû îáðàçîì âûáèðàþò *2n* êëþ÷åé DES, ñãðóïïèðîâàííûõ ïî äâà ïðèíöèïó ìîíîãàìíîñòè èñïîëüçóåìûõ äëÿ äàííîãî ïðîòîêîëà.

(2) È Àëèñà, è Áîá ñîçäàþò *n* ïàð ñîâùåíèé, L_i è R_i, íàïðèìåð, "Ýòî ëåâàÿ ïîëîâèíà ìîåé *i*-îé ïîäïèñè" è "Ýòî ïðàâàÿ ïîëîâèíà ìîåé *i*-îé ïîäïèñè". Èäåíòèôèêàòîð, *i*, ìåíÿåòñÿ îò 1 äî *n*. Â êàæäîé ñîâùåíèå, âåðîÿòíî, òàêæå áóäåò âõîäèòü öèôðîâàÿ ïîäïèñü êíîïêàòà è ìåòêà âðåìåíè. Êîíòðàêò ñ÷èòàåòñÿ ïîäïèñàííûì, åñëè äóãàÿ ñòîðîíà ìîæåò ïðåäúÿâèòü îáå ïîëîâèíû, L_i è R_i, îäíîé ïàðû ïîäïèñåé.

(3) È Àëèñà, è Áîá øèôðóþò ñâîè ïàðû ñîîáùåíèé ïàðàìè êëþ÷åé DES, ëåâîå ñîîáùåíèå - ëåâûì êëþ÷îì â ïàðå , à ïðàâîå - ïðàâûì.

(4) Àëèñà è Áîá ïîñûëàþò äðóã äðóãó ñâîè ïà÷êè èç *2n* øèôðîâàííûõ ñîîáùåíèé, ïîÿñíÿÿ, êàêèå ñîîáùåíèÿ êàêèì ïîëîâèíàì èç êàêèõ ïàð ÿâëÿþòñÿ.

(5) Àëèñà è Áîá ïîñûëàþò äðóã äðóãó âñå ïàðû êëþ÷åé, èñïîëüçóÿ ïðîòîêîë ðàññåÿííîé ïåðåäà÷è äëÿ êàæäîé ïàðû. Òî åñòü, Àëèñà ïîñûëàåò Áîáó íåçàâèñèìî äëÿ êàæäîé èç *n* ïàð êëþ÷åé ëèáî êëþ÷, èñïîëüçîâàííûé äëÿ øèôðîâàíèÿ ëåâîãî ñîîáùåíèÿ, ëèáî êëþ÷, èñïîëüçîâàííûé äëÿ øèôðîâàíèÿ ïðàâîãî ñîîáùåíèÿ. Áîá äåëàåò òî æå ñàìîå. Îíè ìîãóò ïîñûëàòü ñâîè ïîëîâèíêè ïî î÷åðåäè, èëè ñíà÷àëà îäèí ìîæåò ïîñëàòü âñå 100, à ïîòîì äðóãîé - ýòî íå èìåòî çíà÷åíèÿ. Òåïåðü è ó Àëèñû, è ó Áîáà åñòü ïî îäíîìó êëþ÷ó èç êàæäîé ïàðû, íî íèêòî íå çíàåò, êàêèå èç ïîëîâèíîê ïîëó÷èë ïàðòíåð.

(6) Àëèñà è Áîá, èñïîëüçóÿ ïîëó÷åííûå êëþ÷è, ðàñøèôðîâûâàþò òå ïîëîâèíêè ñîîáùåíèé, êîòîðûå îíè ìîãóò ðàñøèôðîâàòü. Îíè óáåæäàþñÿ, ÷òî ðàñøèôðîâàííûå ñîîáùåíèÿ ïðàâèëüíû.

(7) Àëèñà è Áîá ïîñûëàþò äðóã äðóãó ïåðâûå áèòû âñåõ *2n* êëþ÷åé DES.

(8) Àëèñà è Áîá ïîâòîðÿþò ýòàï (7) äëÿ âòîðûõ áèòîâ âñåõ *2n* êëþ÷åé DES, çàòåì òðåòüèõ áèòîâ è òàê äàëåå, ïîêà âñå áèòû âñåõ êëþ÷åé DES íå áóäóò ïðåäàíû.

(9) Àëèñà è Áîá ðàñøèôðîâûâàþò îñòàâøèåñÿ ïîëîâèíêè ñîîáùåíèé, è êîíòðàêò ïîäïèñàí.

(10) Àëèñà è Áîá îáìåíèâàþòñÿ çàêðûòûìè êëþ÷àìè, èñïîëüçîâàííûìè äëÿ ïðîïîëîã ðàññåÿííîé ïåðåäà÷è íà ýòàïå (5), è êàæäûé èç íèõ óáåæäàåòñÿ â îòñóòñòâèè ìîøåííè÷åñòâà.

Ï î÷åìó Àëèñà è Áîáó íóæíî âûïîëíÿòü âñþ ýòó íóäíóþ ïîñëåäîâàòåëüíîñòü äåéñòâèé? Ïðåäïîëîæèì, ÷òî Àëèñà õî÷åò ñìîøåííè÷àòü, è ïîñìîòðèì, ÷òî ïîëó÷èòñÿ. Íà ýòàïàõ (4) è (5) Àëèñà ìîãëà áû ðàçðóøèòü ïðîòîêîë, ïîñëàâ Áîáó íè÷åãî íå çíà÷àùèå ñòðîêè. Áîá îáðàðóæèë âû ýòî íà ýòàïå (6) ïðè ïîïûòêå ðàñøèôðîâàòü ïîëó÷åííûå ïîêîâèíêè. Áîá ñ ïîëíîé áåçîïàñíîñòüþ ìîæåò îòãàäàòü, à âìåñòî âòîðîãî äî òîãî, êàê Àëèñà ñìîæåò ðàñøèôðîâàòü ëþáóþ èç ïàð ñîîáùåíèé Áîáà.

Åñëè âû Àëèñà áûëà ÷åíü õèòðîé, îíà ìîãëà âû ðàçðóøèòü òîëüêî ïîëîâèíó ïðîòîêîëà. Îíà ìîãëà âû ïîñëàòü îäíó ïîëîâèíêó èç êàæäîé ïàðû ïðàâèëüíî, à âìåñòî âòîðîé òîïðåäèòü áåñïîùåíåíûå ñòðîêè. Âåðîÿòíîñòü Áîáà ïîëó÷èòü ïðàâèëüíóþ ïîëîâèíêó ñîñòàâèò òîëüêî 50 ïðîöåíòîâ, ïîýòîìó â ïîëîâèíå ñëó÷àåâ ìîøåííè÷åñòâî Áîáà íèêîãäà íå óçíàåò ïðàâèëüíîãî îòâåòà. Áîá îáðàðóæèë âû ýòî íà ýòàïå (6) ïðè ïîïûòêå ðàñøèôðîâàòü ïîëó÷åííûå ïîêîâèíêè. Áîá ñ ïîëíîé áåçîïàñíîñòüþ ìîæåò îòãàäàòü, à âìåñòî âòîðîãî äåå ïàðû, ýòîò ñîîñòàâèò ìîøåííè÷åñòâà óäàñòñÿ â 25 ïðîöåíòàõ ñëó÷àåâ. Âîò ïî÷åìó *n* äîëæíî áûòü âåëèêî. Àëèñà íåîáõîäèìî òî÷íî óãàäàòü ðåçóëüòàò *n* ïðîòîêîëîâ ðàññåÿííîé äåéſòâèé, åå âåðîÿòíîñòü äîáèòüſÿ ýòîãî ſîſòàâëÿåò 1 øàíſ èç 2^n. Åſëè $n = 10$, ó Àëèſû 1 øàíſ èç 1024 îáìàíóòü Áîáà.

Àëèſà òàêæå ìîæåò îòïðàâèòü Áîáó ſëó÷àéſûå áèòû íà ýòàïå (8). Âîçſîæſî, Áîá íå óſíàåò, ÷òî îſà ïſſëàëà åſó ſëó÷àéſûå áèòû, ïſêà íå ïſëó÷èò âåſü êëþ÷ è íå ïſïûſàåòſÿ ðàſøèſðîâàòü ïſëîâſíſêſ ſîſòâåſſſòſ Áîáó. Îſ ſíſîâà âåðſÿòſſſòſ íà ſòſðſſíå Áîáà. Î ſ óæå ïſëó÷ëè ſſëîâèſó êëþ÷åé, è Àëèſà íå çſàåò êàêóþ. Åſëè *n* äſſòàòſ÷ſſ âåèëêſ, Àëèſà íàâåðſÿêà ſðèøëò åſó áåſſſſſſſûſ áèò äëÿ êëþ÷à, êſòſðûé ó íſãſ óæå åſòſ, è ſſ íſſàëëåſíſſ óçſàåò, ÷òſ ſſà ſûòàåòſÿ åſſ ſàſàſóòſ.

Âſçſſæſſ, Àëèſà áóäåò âûſſëſÿòſ ýòàſ (8) äſ òàõ ſſð, ſſêà ſſà íå ſſëó÷èò äſſòàòſ÷ſſ áèòſâ êëþ÷åé äëÿ âſêðûòèÿ ãðóáûſ âçëſſſſ, è çàòåſ ſðåêðàòèò ſðåðàä÷ó áèòſâ. Äëéſà êëþ÷à DES - 56 áèòſâ. Åſſëè ſſà ſſëó÷ëëà 40 èç 56 áèòſâ, åé ſſòàſåòſÿ ſðåðááòàòſ 2^{16}, ëëè 65536, êëþ÷åé äëÿ äåøèôðſâêè ſſſàſåéſÿ, à ýòà çàää÷à, ſſðåäåëåſſſ, ſſ ſëëàſ ſſâðåſſåſſſûſ êſſſſüþðåðàſ. Íſ Áſá ſſëó÷èò ðſâſſ ſòſſëûêſ æå áèòſâ åå êëþ÷åé (èëè, â õóäøåſ ſëó÷àå, íà ſàëſ áèò ſåſſüøå), ſëäåſâàòåëüſſſ, ſſ ſſſæåò ſàäëàòü òſ æå ſàſſå. Ó Àëèſû íåò äðóãſãſ âſáſðà, êðſſå êàê ſðſäſëæàòü ſëäåſâàòü ſðſòſêſëó.

Èäåÿ â òîì, ÷òî Àëèñå ïðèäóìûâàåò ñåêðåòíûé ïîòîê ÷èñåë, êîòîðûé îáìåíèâàåòñÿ Áîáîì ñëåäóþùèì îáðàçîì. Â êîíöå ïðîòîêîëà ó îáåèõ ñòîðîí åñòü *n* ïîäïèñàííûõ ïàð ñîâïàäàþùèõ, ëþáûå èç êîòîðûõ äîñòàòî÷íî äëÿ ïðåäâû÷èñëåíèÿ ïîäïèñè.

Ó Àëèñû åñòü òîëüêî îäèí ñïîñîá ñîâåðøåíèè÷àòü - îíà ìîæåò ïîñëàòü Áîáó îäèíàêîâûå ñîîáùåíèÿ íà ýòàïå (5). Áîá íå ñìîæåò îáíàðóæèòü ýòîãî äî êîíöà ïðîòîêîëà, íî îí ñìîæåò èñïîëüçîâàòü ñòåíîãðàììó ïðîòîêîëà, ÷òîáû óáåäèòü Àëèñû.

Ïðîòîêîë ýòîãî òèïà èìåþò äâà ñëàáûõ ìåñòà [138]. Âî ïåðâûõ, ïðîáëåìà âîçíèêàåò, åñëè âû÷èñëèòåëüíàÿ ìîùü îäíîé ñòîðîíû ãîðàçäî áîëüøå, ÷åì ó äðóãîé. Åñëè, íàïðèìåð, Àëèñà ìîæåò âûïîëíèòü âñåõîäíþþ ðåìóëüòèðóþùóþ âû÷èñëèòåëüíóþ çàäà÷ó ñòîèìîñòüþ ñ îäèíàêîâûìè âû÷èñëèòåëüíûìè ïðîáëåìàìè, íî ó íå õâàòèò ðåñóðñîâ çàâåðøèòü âû÷èñëåíèÿ ê íóæíîìó ñðîêó. Ïðîáëåìà ïîÿâëÿåòñÿ, ê ïðèìåðó, åñëè êîíòðàêò ÷òî-òî Àëèñà äîëæíà ñäåëàòü ÷òî-òî ÷åðåç íåäåëþ, à îíà ïðåðûâàåò ïðîòîêîë â òîò ìîìåíò, êîãäà Áîáó äëÿ âû÷èñëåíèÿ åå ïîäïèñè ïîòðåáóþòñÿ öåëûå ãîä ðàñ÷åòîâ. Ðàäëüíàÿ ñëîæíîñòü ïðè ýòîì çàêëþ÷àþòñÿ â áëèçêîé äàòå ïðåäúÿâëåíèÿ êîíòðàêòà, ê êîòîðîé ïðîöåññ íå áóäåò çàâåðøåí îäíîé èëè îäíîé íåäåëè ïîäïèñûâàþùèìè ñòîðîíàìè.

Ýòè ïðîáëåìû ñóùåñòâóþò òàêæå äëÿ ïðîòîêîëîâ ðàçäåëîâ 5.8 è 5.9.

5.8 Ýëåêòðîííàÿ ïî÷òà ñ ïîäòâåðæäåíèåì

Òàêîé æå ïðîòîêîë îäíîâðåìåííî ðàññìîòðåí ïðåðàù÷åíèå, èñïîëüçîâàííûé äëÿ ïîäïèñàíèÿ êîíòðàêòà, ñ íåâîëüøèìè èçìåíåíèÿìè èñïîëüçóåòñÿ äëÿ ýëåêòðîííîé ïî÷òû ñ îïòèìàëüíûì îïòèìàëüíûì ðàçìåðîì çàâåðøèòü âû÷èñëåíèÿ ê íóæíîìó ñðîêó. Ïðîáëåìà ïîÿâëÿåòñÿ, ê ïðèìåðó, åñëè êîíòðàêò ÷òî-òî ÷åðåç íåäåëþ, à îíà ïðåðûâàåò ïðîòîêîë â òîò ìîìåíò, íî ó íå õâàòèò ðåñóðñîâ çàâåðøèòü âû÷èñëåíèÿ, ïîñëàâ Áîáó äëÿ âû÷èñëåíèÿ ïîäïèñè ïîòðåáîâàííûå äàííûå. Áîá, êîòîðîìó äëÿ òàêèõ æå äåéſòâèé ïðîñòî íå õâàòèò âðåìåíè, íå ïîâåçåò.

Âî âòîðûõ, ïðîáëåìà âîçíèêàåò, åñëè îäíà èç ñòîðîí ïðåðâàëàñü ïðîòîêîë ðàíüøå âðåìåíè. Åñëè Àëèñà îáíîâëÿåò âû÷èñëèòåëü ïðîòîêîëà, îáà ñòîëêíóòñÿ ñ îäèíàêîâûì è âû÷èñëèòåëüíûì ïðîáëåìàì, íî ó íå õâàòèò ðåñóðñîâ çàâåðøèòü ê íóæíîìó ñðîêó. Ïðîáëåìà ïîÿâëÿåòñÿ, ê ïðèìåðó, åñëè êîíòðàêò ÷òî-òî ÷åðåç íåäåëþ, à îíà ïðåðûâàåò ïðîòîêîë â òîò ìîìåíò, êîãäà Áîáó äëÿ âû÷èñëåíèÿ åå ïîäïèñè ïîòðåáóþòñÿ öåëûé ãîä ðàñ÷åòîâ. Ðàäëüíàÿ ñëîæíîñòü ïðè ýòîì çàêëþ÷àþòñÿ â áëèçêîé äàòå ïðåäúÿâëåíèÿ êîíòðàêòà, ê êîòîðîé ïðîöåññ íå áóäåò çàâåðøåí îäíîé èëè îáåèõ ñòîðîí. Ðåøåíèå ýòîé ïðîáëåìû ïðè ýòîì çàêëþ÷àåòñÿ â áëèçêîé äàòå ïðåäúÿâëåíèÿ êîíòðàêòà, ê êîòîðîé ïðîöåññ íå áóäåò çàâåðøåí îäíîé èëè îáåèõ ñòîðîí.

Íà ïåðâûé âçãëÿä, ýòó ïðîáëåìó ìîãó áû ðåøèòü ïðîòîêîë îäíîâðåìåííîãî ïîäïèñàíèÿ êîíòðàêòà. Àëèñà ïðîñòî êîïèðóåò ñâîå ñîîáùåíèå êëþ÷îì DES. Åå ïîëîâèíà ïðîòîêîëà âûãëÿäèò ïðèìåðíî òàê: "Ýòî ëåâàÿ ïîëîâèíà êëþ÷à DES: 32f5", à ïîëîâèíà ïðîòîêîëà Áîáà - òàê: "Ýòî ëåâàÿ ïîëîâèíà ìîé êâèòàíöèè." Âñå îñòàëüíîå íå ìåíÿåòñÿ.

×òîáû ïîíÿòü, ïî÷åìó ýòî íå ðàáîòàåò, âñïîìíèòå, ÷òî ïðîòîêîë îïèñàíèÿ íà òî, ÷òî ðàññåÿííàÿ ïåðåäà÷à íà ýòàïå (5) ïðåäïîëàãàåò îò ìîøåíí÷åñòâà îáå ñòîðîíû. Îáà ïàðòíåðà çíàþò, ÷òî îíè ïîñëàëè äóáëèðóþùóþ ïîëîâèíó, íî íèêòî íå çíàåò êâèòó. Îíè íå ìîøåíí÷àþò íà ýòàïå (8), ïîòîì ÷òî âåðîÿòíîñòü âûéòè ñóðè èç âîäû ÷ðåçâû÷àéíî ìàëà. Åñëè Àëèñà ïîñûëàåò Áîáó íå ñîîáùåíèå, à ïîëîâèíó êëþ÷à DES, òî Áîá íå ìîæåò ïðîâåðèòü ïðàâèëüíîñòü êëþ÷à DES íà ýòàïå (6). Àëèñà æå ìîæåò ïðîâåðèòü ïðàâèëüíîñòü êâèòàíöèè Áîáà, ïîýòîìó Áîáó ïðèäîñòü áûò ÷åñòíû. Àëèñà ëåãêî ìîæåò îòïðàâèòü Áîáó íåïðàâèëüíûé êëþ÷ à êîãäà îí íáíàðóæèò ýòî, åãî êâèòàíöèÿ óæå áûëà ó Àëèñû. Âîò íåâåçóõà, Áîá.

Ðåøåíèå ýòîé ïðîáëåìû ïîòðåáóåò íåêîòîðîé êðåïòîãðàôè÷åñêîé ïðîòîêîëà:

(1) Àëèñà øèôðóåò ñâîå ñîîáùåíèå ñëó÷àéíûì êëþ÷îì DES è ïîñûëàåò åãî Áîáó.

(2) Àëèñà ñîçäàåò *n* ïàð êëþ÷åé DES. Ïåðâûé êëþ÷ êàæäîé ïàðû ãåíåðèðóåòñÿ ñëó÷àéíûì îáðàçîì, à âòîðîé ïðåäñòàâëÿåò ñîáîé XOR ïåðâîãî êëþ÷à è êëþ÷à øèôðîâàíèÿ ñîáùåíèÿ.

(3) Àëèñà øèôðóåò ñîîáùåíèå-çàãëóøêó êàæäûì èç ñâîèõ *2n* êëþ÷åé.

(4) Àëèñà ïîñûëàåò Áîáó âñþ ïà÷êó øèôðîâàííûõ ñîîáùåíèé, ïðîâåðÿÿ, ÷òî îí çíàåò, êàêèå ñîîáùåíèÿ êàêèì ïîëîâèíàì êàêèõ ïàð ÿâëÿþòñÿ.

(5) Áîá ñîçäàåò *n* ïàð ñëó÷àéíûõ êëþ÷åé DES.

(6) Áîá ñîçäàåò ïàðó ñîîáùåíèé, îáðàçóþùèõ ïðàâèëüíóþ êâèòàíöèþ. Õîðîøèì âàðèàíòàì ìîãóò ñëóæèòü "Ýòî ëåâàÿ ïîëîâèíà ìîåé êâèòàíöèè" è "Ýòî ëåâàÿ ïîëîâèíà ìîåé êâèòàíöèè" ñ äîáàâëåíèåì êàêîé-íèáóäü ñòðîêè ñëó÷àéíûõ áèòîâ. Îí ñîçäàåò *n* ïàð êâèòàíöèé, íóìåðóÿ êàæäóþ. Êàê è â ïðåäûäóùåì ïðîòîêîëå êâèòàíöèÿ ñ÷èòàåòñÿ ïðàâèëüíîé, åñëè Àëèñà ìîæåò ïðåäúÿâèòü îáå ïîëîâèíû êâèòàíöèè (ñ îäíèì è òåì æå íîìåðîì) è âñå åå êëþ÷è øèôðîâàíèÿ.

(7) Áîá øèôðóåò êàæäóþ ñâîþ ïàðó ñîîáùåíèé ïàðàìè êëþ÷åé DES, *i*-óþ ïàðó ñîîáùåíèé - *i*-îé ïàðîé êëþ÷åé, ëåâîå ñîîáùåíèå - ëåâûì êëþ÷îì â ïàðå, à ïðàâîå - ïðàâûì. â ïàðå.

(8) Áîá ïîñûëàåò Àëèñå ñâîþ ïà÷êó øèôðîâàííûõ ñîîáùåíèé, ïðîâåðÿÿ, ÷òî íà çíàåò, êàêèå ñîîáùåíèÿ êàêèì ïîëîâèíàì êàêèõ ïàð ÿâëÿþòñÿ.

(9) Àëèñà è Áîá ïîñûëàþò äðóã äðóãó âñå ïàðû êëþ÷åé, èñïîëüçóÿ ïðîòîêîë ðàñïðåäíîé ïåðåäà÷è. Òî åñòü,

Àëèñà ïîñûëàåò Áîáó íåçàâèñèìî äëÿ êàæäîé èç *n* ïàð êëþ÷åé ëèáî êëþ÷, èñïîëüçîâàííûé äëÿ øèôðîâàíèÿ ëåâîãî ñîîáùåíèÿ, ëèáî êëþ÷, èñïîëüçîâàííûé äëÿ øèôðîâàíèÿ ïðàâîãî ñîîáùåíèÿ. Áîá äåëàåò òî æå ñàìîå. Îíè ìîãóò ïîñûëàòü ñâîè ïîëîâèíêè ïî î÷åðåäè, èëè ñíà÷àëà îäèí ìîæåò ïîñëàòü âñå *n*, à ïîòîì äðóãîé - ýòî íå èìååò çíà÷åíèÿ. Òåïåðü è ó Àëèñû, è ó Áîáà åñòü ïî îäíîìó êëþ÷ó èç êàæäîé ïàðû, íî íèêòî íå çíàåò, êàêèå èç ïîëîâèíîê ïîëó÷èë ïàðòíåð.

(10) Àëèñà è Áîá ðàñøèôðîâûâàþò òå ïîëîâèíêè ñîîáùåíèé, êîòîðûå ìîãóò è óáåæäàþòñÿ, ÷òî ðàñøèôðîâàííûå ñîîáùåíèÿ ïðàâèëüíû.

(11) Àëèñà è Áîá ïîñûëàþò äðóã äðóãó ïåðâûå áèòû âñåõ *2n* êëþ÷åé DES. (Åñëè îíè áåñïîêîÿòñÿ, ÷òî Åâà ìîæåò ïðî÷èòàòü ýòè ïî÷òîâûå ñîîáùåíèÿ, òî îíè äîëæíû øèôðîâàòü ñâîé îáìåí áèòàìè).

(12) Àëèñà è Áîá ïîâòîðÿþò ýòàï (11) äëÿ âòîðûõ áèòîâ âñåõ *2n* êëþ÷åé DES, çàòåì òðåòüèõ áèòîâ è òàê äàëåå, ïîêà âñå áèòû âñåõ êëþ÷åé DES íå áóäóò ïåðåäàíû.

(13) Àëèñà è Áîá ðàñøèôðîâûâàþò îñòàâøèåñÿ ïîëîâèíêè ñîîáùåíèé. Àëèñà ïîëó÷àåò ïðàâèëüíóþ êâèòàíöèþ îò Áîáà, à Áîá ìîæåò âûïîëíèòü "èñêëþ÷àþùåå èëè" äëÿ ëþáîé ïàðû êëþ÷åé è ïðî÷èòàòü êëþ÷, êîòîðûì çàøèôðîâàíî îðèãèíàëüíîå ñîîáùåíèå.

(14) Àëèñà è Áîá îáìåíèâàþòñÿ çàêðûòûìè êëþ÷àìè, èñïîëüçîâàííûìè äëÿ ïðîòîêîëà ðàññåÿííîé ïåðåäà÷è, è êàæäûé èç íèõ óáåæäàåòñÿ â îòñóòñòâèè ìîøåííè÷åñòâà.

Ýòàïû (5)-(8) äëÿ Áîáà è (9)-(12) äëÿ îáåèõ ñòîðîí íå ìåíÿþòñÿ ïî ñðàâíåíèþ ñ ïðîòîêîëîì ïîäïèñàíèÿ êîíòðàêòà. Îòëè÷èå - â ñîîáùåíèÿõ-çàãëóøêàõ Àëèñû. Îíè ïðåäîñòàâëÿþò Áîáó âîçìîæíîñòü ïðîâåðèòü ïðàâèëüíîñòü åå ðàññåÿííîé ïåðåäà÷è íà ýòàïå (10), ÷òî çàñòàâëÿåò åå îñòàâàòüñÿ ÷åñòíîé íà ýòàïàõ (11)-(13). È, êàê è äëÿ ïðîòîêîëà îäíîâðåìåííîãî ïîäïèñàíèÿ êîíòðàêòà, äëÿ âûïîëíåíèÿ ïðîòîêîëà òðåáóþòñÿ îáå ïîëîâèíû îäíîãî èç ñîîáùåíèé Àëèñû.

5.9 Îäíîâðåìåííûé îáìåí ñåêðåòàìè

Àëèñà çíàåò ñåêðåò *A*, à Áîá - ñåêðåò *B*. Àëèñà ñîáèðàåòñÿ ñîîáùèòü Áîáó *A*, åñëè îí ðàññêàæåò åé *B*. Áîá õî÷åò ñîîáùèòü Àëèñå *B*, åñëè îíà ðàññêàæåò åìó *A*. Ñëåäóþùèé ïðîòîêîë, ïîäñëóøàííûé íà øêîëüíîì äâîðå, ðàáîòàòü íå áóäåò:

(1) Àëèñà: "ß ñêàæó, åñëè òû ñêàæåøü ìíå ïåðâûì."

(2) Áîá: "ß ñêàæó, åñëè òû ñêàæåøü ìíå ïåðâîé."

(3) Àëèñà: "Íåò, òû ïåðâûé."

(4) Áîá: "Íó, õîðîøî." Áîá øåï÷åò Àëèñå.

(5) Àëèñà: "Õà, à ÿ òåáå íå ñêàæó."

(6) Áîá: "Ýòî íå ÷åñòíî."

×åñòíûì ýòî ìîæåò ñäåëàòü êðèïòîãðàôèÿ. Ïðåäûäóùèå äâà ïðîòîêîëà ÿâëÿþòñÿ ðåàëèçàöèÿìè áîëåå îáùåãî ïðîòîêîëà, êîòîðûé è ïîçâîëèò Àëèñå è Áîáó îäíîâðåìåííî îáìåíÿòüñÿ ñåêðåòàìè [529]. ×òîáû íå ïîâòîðÿòü ïîëíîñòüþ âåñü ïðîòîêîë, ÿ íàáðîñàþ íåôîðìàëüíûå èçìåíåíèÿ ïðîòîêîëà ïî÷òû ñ ïîäòâåðæäåíèåì.

Àëèñà âûïîëíÿåò ýòàïû (1)-(4), èñïîëüçóÿ â êà÷åñòâå ñîîáùåíèÿ *A*. Áîá âûïîëíÿåò ýòè æå äåéñòâèÿ, èñïîëüçóÿ â êà÷åñòâå ñâîåãî ñîîáùåíèÿ *B*. Àëèñà è Áîá âûïîëíÿþò ðàññåÿííóþ ïåðåäà÷ó íà ýòàïå (9), ðàñøèôðîâûâàþò íà ýòàïå (10) òå ïîëîâèíêè, êîòîðûå ìîãóò, è âûïîëíÿþò íåôîðìàëüíûå èòåðàöèè íà ýòàïàõ (11) è (12). ×òîáû çàùèòèòüñÿ îò Åâû, îíè äîëæíû øèôðîâàòü ñâîè ñîîáùåíèÿ. Íàêîíåö, è Àëèñà, è Áîá ðàñøèôðîâûâàþò îñòàâøèåñÿ ïîëîâèíû ïàð ñîîáùåíèé è âûïîëíÿþò XOR äëÿ ëþáîé ïàðû êëþ÷åé, ÷òîáû ïîëó÷èòü êëþ÷è, êîòîðûìè çàøèôðîâàíû îðèãèíàëüíûå ñîîáùåíèÿ.

Ýòîò ïðîòîêîë ïîçâîëÿåò Àëèñå è Áîáó îäíîâðåìåííî îáìåíèâàòüñÿ ñåêðåòàìè, íî íå ãàðàíòèðóåò êà÷åñòâà ïåðåäàííûõ ñåêðåòîâ. Àëèñà ìîæåò ïîîáåùàòü Áîáó ïëàí ëàáèðèíòà Ìèíîòàâðà è ïðèñëàòü åìó ñõåìó Áîñòîíñêîãî ìåòðî. Áîá ïîëó÷èò òîëüêî òîò ñåêðåò, êîòîðûé Àëèñà ïðèøëåò åìó. Äðóãèå ïðîòîêîëû îïèñàíû â [1286, 195, 991, 1524, 705, 753, 259, 358, 415].

Ãëàâà 6
Ýçîòåðè÷åñêèå ïðîöåññû

6.1 Áåçîïàñíûå âûáðû

Êîìïüþòåðíîå ãîëîñîâàíèå íåêîòîðûõ áóäåò èñïîëüçîâàíî äëÿ îáû÷íûõ âûáîðîâ, ïîêà íå ïîÿâèòñÿ ïðîöåññîð, êîòîðûé îäíîâðåìåííî ïðåäîòâðàòèò îò ìîøåííè÷åñêèõ è çàùèùàåò òàéíó ëè÷íîñòè. Èäåàëüíûé ïðîöåññ äîëæåí îáëàäàòü, ïî ìåíüøåé ìåðå, ñëåäóþùèìè øåñòüþ ñâîéñòâàìè:

1. Ãîëîñîâàòü ìîãóò òîëüêî òå, êòî èìååò íà ýòî ïðàâî.
2. Êàæäûé ìîæåò ãîëîñîâàòü íå áîëåå îäíîãî ðàçà.
3. Íèêòî íå ìîæåò óçíàòü, çà êîãî ïðîãîëîñîâàë êîíêðåòíûé èçáèðàòåëü.
4. Íèêòî íå ìîæåò ïðîãîëîñîâàòü âìåñòî äðóãîãî. (Ýòî îêàçûâàåòñÿ ñàìûì òÿæåëûì òðåáîâàíèåì.)
5. Íèêòî íå ìîæåò òàéíî èçìåíèòü ÷åé-òî ãîëîñ.
6. Êàæäûé ãîëîñóþùèé ìîæåò ïðîâåðèòü, ÷òî åãî ãîëîñ ó÷èòûâàëñÿ ïðè ïîäñ÷åòå èòîãîâ ãîëîñîâàíèÿ.

Êðîìå òîãî, äëÿ íåêîòîðûõ ñöåí ãîëîñîâàíèÿ ìîæåò ïîíàäîáèòüñÿ ñëåäóþùåå òðåáîâàíèå:

7. Êàæäûé çíàåò, êòî ãîëîñîâàë, à êòî íåò.

Ïðåæäå ÷åì ïîïûòàòüñÿ ñîçäàòü ïðîòîêîë, èìåþùèé ïðèâåäåííûå õàðàêòåðèñòèêè, äàâàéòå âçãëÿíåì íà ðàä ïðîòîêîëîâ ïîïðîùå.

Óïðîùåííûé ïðîòîêîë ãîëîñîâàíèÿ 1

(1) Êàæäûé ãîëîñóþùèé øèôðóåò ñâîé áþëëåòåíü îòêðûòûì êëþ÷îì Öåíòðàëüíîé èçáèðàòåëüíîé êîìèññèè (ÖÈÊ).

(2) Êàæäûé ãîëîñóþùèé ïîñûëàåò ñâîé áþëëåòåíü â ÖÈÊ.

(3) ÖÈÊ ðàñøèôðîâûâàåò áþëëåòåíå, ïîäñ÷èòàåò èòîãè è îïóáëèêîâûâàåò ðåçóëüòàòû ãîëîñîâàíèÿ.

Ýòîò ïðîòîêîë ïðîñòî êøèò ïðîáëåìàìè. ÖÈÊ íå ìîæåò óçíàòü, îòêóäà ïîëó÷åíû áþëëåòåíå, è äàæå, ïðèíàäëåæàò ëè ïðèñëàííûå áþëëåòåíå ïðàâîìî÷íûì èçáèðàòåëÿì. Ó íåå íåò íè ìàëåéøåãî ïðåäñòàâëåíèÿ î òîì, íå ãîëîñîâàëè ëè ïðàâîìî÷íûå èçáèðàòåëè áîëüøå îäíîãî ðàçà. Ïîêàæèòåëüíî ñòðî÷íûé ÿâëÿåòñÿ íåâîçìîæíîñòü èçìåíèòü áþëëåòåíü äðóãîãî ÷åëîâåêà, íî íèêòî è íå áóäåò ïûòàòüñÿ ýòî ñäåëàòü, ïîòîìó ÷òî ãîðàçä ãîëîñîâàòü ïîâòîðíî, äîáàâëÿñü íóæíûõ ðåçóëüòàòîâ âûáîðîâ.

Óïðîùåííûé ïðîòîêîë ãîëîñîâàíèÿ 2

(1) Êàæäûé ãîëîñóþùèé ïîäïèñûâàåò ñâîé áþëëåòåíü ñâîèì çàêðûòûì êëþ÷îì.

(2) Êàæäûé ãîëîñóþùèé øèôðóåò ñâîé áþëëåòåíü îòêðûòûì êëþ÷îì ÖÈÊ.

(3) Êàæäûé ãîëîñóþùèé ïîñûëàåò ñâîé áþëëåòåíü â ÖÈÊ.

(4) ÖÈÊ ðàñøèôðîâûâàåò áþëëåòåíå, ïðîâåðÿåò ïîäïèñè, ïîäâîäèò èòîãè è îïóáëèêîâûâàåò ðåçóëüòàòû ãîëîñîâàíèÿ.

Ýòîò ïðîòîêîë îáëàäàåò ñâîéñòâàìè 1 è 2: Òîëüêî ïðàâîìî÷íûå èçáèðàòåëè ìîãóò ãîëîñîâàòü, è íèêòî íå ìîæåò ãîëîñîâàòü áîëåå îäíîãî ðàçà - ÖÈÊ ìîæåò çàïèñûâàòü áþëëåòåíå, ïîëó÷åííûå íà ýòàïå (3). Êàæäûé áþëëåòåíü ïîäïèñàí çàêðûòûì êëþ÷îì ãîëîñóþùåãî, ïîýòîìó ÖÈÊ çíàåò, êòî ãîëîñîâàë, à êòî íåò, è, êàê ãîëîñîâàë êàæäûé èçáèðàòåëü. Åñëè ïîëó÷åí áþëëåòåíü, êîòîðûé íå ïîäïèñàí ïðàâîìî÷íûì ïîëüçîâàòåëåì, ëèë áþëëåòåíü, ïîäïèñàííûé èçáèðàòåëåì, êîòîðûé óæå ïðîãîëîñîâàë, òî òàêîé áþëëåòåíü èãíîðèðóþòñÿ êîìèññèåé. Êðîìå òîãî, èç-çà öèôðîâîé ïîäïèñè íèêòî íå ìîæåò èçìåíèòü áþëëåòåíü äðóãîãî èçáèðàòåëÿ, äàæå åñëè ñòîëåòî ïåðåõâàòèòü åãî íà ýòàïå (2).

Ïðîáëåìà ýòîãî ïðîòîêîëà â òîì, ÷òî ïîäïèñü äîâåðÿòñÿ ê áþëëåòåíþ, ÖÈÊ çíàåò, êòî çà êîãî ãîëîñîâàë. Øèôðîâàíèå áþëëåòåíå îòêðûòûì êëþ÷îì ÖÈÊ ìåøàåò ïîñòîðîííèì çëîóìûøëåíöó ïðîòîêîëîì è óçíàâàòü, êòî çà êîãî ãîëîñîâàë, íî âàì ïðèäåòñÿ ïîëíîñòüþ äîâåðÿòü ÖÈÊ Ýòî êàê áóäòî â êàéíêå äëÿ ãîëîñîâàíèÿ âàì ÷åðåç ïëå÷î çàãëÿäûâàåò ýëåêòðîííûé ñóäüÿ.

Äâà ñëåäóþùèõ ïðèìåðà ïîêàçûâàþò, êàê òðóäíî îáåñïå÷èòü õîòÿ áû ïðåäâû òðè òðåáîâàíèÿ ê ïðîòîêîëó áåçîïàñíîãî ãîëîñîâàíèÿ.

Ãîëîñîâàíèå ñî ñëåïûìè ïîäïèñÿìè

Íàì íóæíî êàê-òî îòäåëèòü áþëëåòåíü îò ãîëîñóþùåãî, ñîõðàíèâ ïðîöåäóðó èäåíòèôèêàöèè ëè÷íîñòè. Èìåííî ýòî ìîæíî ñäåëàòü ñ ïîìîùüþ ïðîòîêîëà ñëåïîé ïîäïèñè.

(1) Êàæäûé èçáèðàòåëü ñîçäàåò 10 íàáîðîâ ñîîáùåíèé, êàæäûé íàáîð ñîäåðæèò ïðàâèëüíûé áþëëåòåíü äëÿ êàæäîãî âîçìîæíîãî ðåçóëüòàòà (íàïðèìåð, åñëè áþëëåòåíåì ÿâëÿåòñÿ îäèí èç îòâåòîâ "äà"-"íåò", òî êàæäûé íàáîð ñîñòîèò èç äâóõ áþëëåòåíåé, îäíîãî äëÿ "äà", à äðóãîãî äëÿ "íåò"). Êàæäîå ñîîáùåíèå ñîäåðæèò òàêæå ñëó÷àéíûì îáðàçîì ñîçäàííûé èäåíòèôèêàöèîííûé íîìåð, äîñòàòî÷íî áîëüøîé, ÷òîáû èçáåæàòü ïóòàíèöû ñ äðóãèìè èçáèðàòåëÿìè.

(2) Êàæäûé èçáèðàòåëü ëè÷íî ìàñêèðóåò âñå ñîîáùåíèÿ (ñì. ðàçäåë 5.3) è ïîñûëàåò èõ â ÖÈÊ âìåñòå ñ ìàñêèðóþùèìè ìíîæèòåëÿìè.

(3) ÖÈÊ ïî ñâîåé áàçå äàííûõ ïðîâåðÿåò, ÷òî ïîëüçîâàòåëü íå ïðèñûëàë ðàíüøå äëÿ ïîäïèñàíèÿ ñâîè çàìàñêèðîâàííûå áþëëåòåíè. ÖÈÊ îòêðûâàåò 9 èç íàáîðîâ, ïðîâåðÿÿ, ÷òî îíè ïðàâèëüíî ñôîðìèðîâàíû. Çàòåì îíà èíäèâèäóàëüíî ïîäïèñûâàåò êàæäîå ñîîáùåíèå íàáîðà è ïîñûëàåò èõ îáðàòíî èçáèðàòåëþ, ñîõðàíÿÿ èìÿ èçáèðàòåëÿ â ñâîåé áàçå äàííûõ.

(4) Èçáèðàòåëü ñíèìàåò ìàñêèðîâêó ñ ñîîáùåíèé è ïîëó÷àåò íàáîð áþëëåòåíåé, ïîäïèñàííûõ ÖÈÊ. (Ýòè áþëëåòåíè ïîäïèñàíû, íî íå çàøèôðîâàíû, ïîýòîìó èçáèðàòåëü ëåãêî óâèäèò, êàêîé èç áþëëåòåíåé - "äà", à êàêîé - "íåò".)

(5) Êàæäûé èçáèðàòåëü âûáèðàåò îäèí èç áþëëåòåíåé (î, äåìîêðàòèÿ!) è øèôðóåò åãî îòêðûòûì êëþ÷îì ÖÈÊ.

(6) Èçáèðàòåëü îòïðàâëÿåò ñâîé áþëëåòåíü.

(7) ÖÈÊ ðàñøèôðîâûâàåò áþëëåòåíè, ïðîâåðÿåò ïîäïèñü, ïðîâåðÿåò ïî áàçå äàííûõ óíèêàëüíîñòü èäåíòèôèêàöèîííîãî íîìåðà, ñîõðàíÿåò ïîñëåäîâàòåëüíûé íîìåð è ïîäâîäèò èòîãè. Îíà îïóáëèêîâûâàåò ðåçóëüòàòû ãîëîñîâàíèÿ âìåñòå ñ êàæäûì ïîñëåäîâàòåëüíûì íîìåðîì è ñîîòâåòñòâóþùèì áþëëåòåíåì.

Ìýëëîðè, èçáèðàòåëü-æóëèê, íå ìîæåò îáìàíóòü ýòó ñèñòåìó. Ïðîòîêîë ñëåïîé ïîäïèñè îáåñïå÷èâàåò åäèíñòâåííîñòü åãî áþëëåòåíè. Åñëè îí ïîïûòàåòñÿ îòïðàâèòü òîò æå áþëëåòåíü äâàæäû, ÖÈÊ îáíàðóæèò äóáëèðîâàíèå ïîñëåäîâàòåëüíûõ íîìåðîâ íà ýòàïå (7) è íå áóäåò ó÷èòûâàòü âòîðîé áþëëåòåíü. Åñëè îí ïîïûòàåòñÿ ïîëó÷èòü íåñêîëüêî áþëëåòåíåé íà ýòàïå (2), ÖÈÊ îáíàðóæèò ýòî íà ýòàïå (3). Ìýëëîðè íå ìîæåò ñîçäàòü ñâîè ñîáñòâåííûå áþëëåòåíè, ïîòîìó ÷òî îí íå çíàåò çàêðûòîãî êëþ÷à êîìèññèè. Ïî òîé æå ïðè÷èíå îí íå ìîæåò ïåðåõâàòèòü è èçìåíèòü ÷óæèå áþëëåòåíè.

Ïðîòîêîë "ðàçðåçàòü è âûáðàòü" íà ýòàïå (3) äîëæåí îáåñïå÷èòü óíèêàëüíîñòü áþëëåòåíåé. Áåç ýòîãî ýòàïà Ìýëëîðè ìîã áû ñîçäàòü òî÷íî òàêîé æå, çà èñêëþ÷åíèåì èäåíòèôèêàöèîííîãî íîìåðà, íàáîð áþëëåòåíåé è çàâåðèòü èõ âñå â ÖÈÊ.

Ìîøåííè÷åñêàÿ ÖÈÊ íå ñìîæåò óçíàòü, êàê ãîëîñîâàëè êîíêðåòíûå èçáèðàòåëè. Òàê êàê ïðîòîêîë ñëåïîé ïîäïèñè ìàñêèðóåò ïîñëåäîâàòåëüíûå íîìåðà áþëëåòåíåé äî ìîìåíòà ïîäâåäåíèÿ èòîãîâ, ÖÈÊ íå ñìîæåò óñòàíîâèòü ñâÿçü ìåæäó ïîäïèñàííûì åþ çàìàñêèðîâàííûì áþëëåòåíåì è ïîäûòîæèâàåìûì áþëëåòåíåì. Îïóáëèêîâàíèå ïåðå÷íÿ ïîñëåäîâàòåëüíûõ íîìåðîâ è ñâÿçàííûõ ñ íèìè áþëëåòåíåé ïîçâîëÿåò ïîëüçîâàòåëÿì óáåäèòüñÿ, ÷òî èõ áþëëåòåíè áûëè ïðàâèëüíî ó÷òåíû.

Íî ïðîáëåìû âñå åùå îñòàþòñÿ. Åñëè ýòàï (6) íå àíîíèìåí, è ÖÈÊ ìîæåò çàïèñàòü, êòî êàêîé áþëëåòåíü ïðèñëàë, òî îíà ñìîæåò óçíàòü, êòî çà êîãî ãîëîñîâàë. Îäíàêî, ýòî íåâîçìîæíî, åñëè êîìèññèÿ ïîëó÷àåò áþëëåòåíè â çàïå÷àòàííîé óðíå äëÿ ãîëîñîâàíèÿ è ñ÷èòàåò èõ ïîçæå. Õîòÿ ÖÈÊ è íå ñìîæåò óñòàíîâèòü ñâÿçü ìåæäó èçáèðàòåëÿìè è èõ áþëëåòåíÿìè, îíà ñìîæåò ñîçäàòü áîëüøîå êîëè÷åñòâî ïîäïèñàííûõ è ïðàâèëüíûõ áþëëåòåíåé è ñìîøåííè÷àòü, ïðèñëàâ èõ ñàìà ñåáå. È åñëè Àëèñà îáíàðóæèò, ÷òî ÖÈÊ ïîäìåíèëà åå áþëëåòåíü, îíà íå ñìîæåò äîêàçàòü ýòîãî. Àíàëîãè÷íûé ïðîòîêîë, ïûòàþùèéñÿ óñòðàíèòü ýòè ïðîáëåìû, îïèñàí â [1195, 1370].

Ãîëîñîâàíèå ñ äâóìÿ Öåíòðàëüíûìè êîìèññèÿìè

Îäíèì èç ðåøåíèé ÿâëÿåòñÿ ðàçäåëèòü ÖÈÊ ïîïîëàì. Íè ó îäíîé èç íèõ íå áóäåò äîñòàòî÷íî âëàñòè, ÷òîáû ñìîøåííè÷àòü ïî ñâîåìó óñìîòðåíèþ.

Â ñëåäóþùåì ïðîòîêîëå èñïîëüçóåòñÿ Öåíòðàëüíîå óïðàâëåíèå ðåãèñòðàöèè (ÖÓÐ), çàíèìàþùååñÿ ïðîâåðêîé ïîëüçîâàòåëåé, è îòäåëüíàÿ ÖÈÊ äëÿ ïîäñ÷åòà áþëëåòåíåé [1373].

(1) Êàæäûé èçáèðàòåëü îòïðàâëÿåò ïèñüìî â ÖÓÐ, çàïðàøèâàÿ ðåãèñòðàöèîííûé íîìåð.

(2) ÖÓÐ âîçâðàùàåò èçáèðàòåëþ ñëó÷àéíûé ðåãèñòðàöèîííûé íîìåð. ÖÓÐ âåäåò ñïèñîê ðåãèñòðàöèîííûõ íîìåðîâ. Êðîìå òîãî, ÖÓÐ õðàíèò ñïèñîê ïîëó÷àòåëåé ðåãèñòðàöèîííûõ íîìåðîâ íà ñëó÷àé, åñëè êòî-òî ïîïûòàåòñÿ ïðîãîëîñîâàòü äâàæäû.

(3) ÖÓÐ îòïðàâëÿåò ñïèñîê ðåãèñòðàöèîííûõ íîìåðîâ â ÖÈÊ.

(4) Êàæäûé èçáèðàòåëü âûáèðàåò ñëó÷àéíûé èäåíòèôèêàòîð íîìåð. Îí ñîçäàåò ñîîáùåíèå ñ ýòèì íîìåðîì, ðåãèñòðàöèîííûì íîìåðîì, ïîëó÷åííûì â ÖÓÐ, è ñâîèì áþëëåòåíåì. Îí ïîñûëàåò ýòî ñîîáùåíèå â ÖÈÊ.

(5) ÖÈÊ ïðîâåðÿåò ðåãèñòðàöèîííûå íîìåðà ïî ñïèñêó, ïîëó÷åííîìó îò ÖÓÐ íà ýòàïå (3). Åñëè ðåãèñòðàöèîííûé íîìåð åñòü â ñïèñêå, ÖÈÊ âû÷åðêèâàåò åãî (òàêæå èçáåæàòü ïîâòîðíîãî âêëþ÷åíèÿ). ÖÈÊ äîáàâëÿåò èäåíòèôèêàöèîííûé íîìåð ê ñïèñêó òåõ, êòî ïðîãîëîñîâàë çà îïðåäåëåííîãî êàíäèäàòà, è ïðèáàâëÿåò åäèíè÷íó ê ñîîòâåòñòâóþùåìó èòîãîâîìó ÷èñëó.

(6) Ï îñëå òîãî, êàê âñå áþëëåòåíè áóäóò ïîëó÷åíû, ÖÈÊ ïóáëèêóåò ðåçóëüòàòû âìåñòå ñî ñïèñêàìè, ñîäåðæàùèìè èäåíòèôèêàöèîííûå íîìåðà è ñîîòâåòñòâóþùèå áþëëåòåíè.

Êàê è â ïðåäûäóùåì ïðîòîêîëå êàæäûé èçáèðàòåëü ìîæåò óâèäåòü ñïèñîê èäåíòèôèêàöèîííûõ íîìåðîâ è íàéòè â íåì ñâîé ñîáñòâåííûé. Òàê îí ìîæåò óáåäèòüñÿ, ÷òî åãî áþëëåòåíü ó÷òåí. Êîíå÷íî, âñå ñîîáùåíèÿ, êîòîðûìè îáìåíèâàþòñÿ ó÷àñòíèêè ïðîòîêîëà äîëæíû áûòü çàøèôðîâàíû è ïîäïèñàíû, ÷òîáû ïîìåøàòü êîìó-íèáóäü âûäàòü ñåáÿ çà äðóãîãî èëè ïåðåõâàòèòü ñîîáùåíèÿ.

Ìýëîðè, íå îáëàäàþùèé èçáèðàòåëüíûì ïðàâîì, ìîæåò ïîïûòàòüñÿ ñîøåíè÷àòü, óãàäàâ ïðàâèëüíûé ðåãèñòðàöèîííûé íîìåð. Óãðîçà ýòîãî ìîæåò áûòü ìèíèìèçèðîâàíà, åñëè ìíîæåñòâî âîçìîæíûõ ðåãèñòðàöèîííûõ íîìåðîâ íàìíîãî áîëüøå, ÷åì ìíîæåñòâî ðåãèñòðàöèîííûõ íîìåðîâ: 100-áèòîâîå ÷èñëî äëÿ ìèëëèîíà èçáèðàòåëåé. Êîíå÷íî æå, ðåãèñòðàöèîííûå íîìåðà äîëæíû ãàíäåðîâàòüñÿ ñëó÷àéíûì îáðàçîì.

Íåñìîòðÿ íà ýòî, ÖÓÐ äîëæíà áûòü çàñëóæèâàþùèì äîâåðèÿ îðãàíîì - âåäü îíà ìîæåò çàðåãèñòðèðîâàòü íåïðàâîìî÷íûõ èçáèðàòåëåé. Îíà òàêæå ìîæåò çàðåãèñòðèðîâàòü ïðàâîìî÷íûõ èçáèðàòåëåé íåñêîëüêî ðàç. Ýòîò ðèñê ìîæåò áûòü ñâåäåí ê ìèíèìóì, åñëè ÖÓÐ îïóáëèêóåò ñïèñîê çàðåãèñòðèðîâàòü ïðàâîìî÷íûõ èçáèðàòåëåé (íî áåç èõ ðåãèñòðàöèîííûõ íîìåðîâ). Åñëè ÷èñëî èçáèðàòåëåé â ýòîì ñïèñêå ìåíüøå, ÷åì ÷èñëî ïîäñ÷èòàííûõ áþëëåòåíåé, òî ÷òî-òî íå òàê. Îäíàêî, åñëè çàðåãèñòðèðîâàëîñü áîëüøå èçáèðàòåëåé, ÷åì áûëî ïðèãîòîâëåíî áþëëåòåíåé, òî ýòî, âîçìîæíî, îçíà÷àåò, ÷òî ðÿä çàðåãèñòðèðîâàâøèõñÿ èçáèðàòåëåé íå ïðîãîëîñîâàë. Ì íîãèå, çàðåãèñòðèðîâàâøèñü, íå óòðóäíÿòñÿ áðîñèòü â óðíó ñâîé áþëëåòåíü.

Ýòîò ïðîòîêîë áåççàùèòåí ïðåä ñãîâîðîì ÖÈÊ è ÖÓÐ. Åñëè îíè äåéſòâóþò âìåñòå, íîè ìîãóò îáúåäèíèòü ñâîè áàííûõ è óçíàòü, êòî çà êîãî ãîëîñóåò.

Ãîëîñîâàíèå ñ îäíîé Öåíòðàëüíîé êîìèññèåé

×òîáû èçáåæàòü îïàñíîñòè ñãîâîðà ìåæäó ÖÓÐ è ÖÈÊ ìîæíî èñïîëüçîâàòü áîëåå ñëîæíûé ïðîòîêîë [1373]. Ýòîò ïðîòîêîë èäåíòè÷åí ïðåäûäóùåìó ñ äâóìÿ èçìåíåíèÿìè:

— ÖÓÐ è ÖÈÊ ÿâëÿþòſÿ åäèíîé îðãàíèçàöèåé, è

— äëÿ àíîíèìíîãî ðàñïðåäåëåíèÿ ðåãèñòðàöèîííûõ íîìåðîâ íà ýòàïå (2) èñïîëüçóåòſÿ ANDOS (ſì. ðàçäåë 4.13).

Òàê êàê ïðîòîêîë àíîíèìíîãî ðàñïðåäåëåíèÿ êëþ÷åé íå ïîçâîëÿåò ÖÈÊ óçíàòü, ó êàêîãî èçáèðàòåëÿ êàêîé ðåãèñòðàöèîííûé íîìåð, Ó ÖÈÊ íåò ñïîſíáà ſàÿçàòü ðåãèſòðàöèîííûå íîìåðà è ïîëó÷åííûå áþëëåòåíå. Íî ÖÈÊ äîëæíà áûòü íàäåæíû îðãàíîì, ÷òîáû íå âûäàâàòü ðåãèſòðàöèîííûõ íîìåðîâ íåïðàâîìî÷íûì èçáèðàòåëÿì. Ýòó ïðîáëåìó òàêæå ìîæíî ðåøèòü ſ ïîìüþ ſåëïûõ ïîäïèſåé.

Óëó÷øåííîå îïèſàíèå ſîãíîſòè Öåíòðàëüíîé êîìèſſèé

Â ýòîì ïðîòîêîëå òàêæå èſïîëüçóåòſÿ ANDOS [1175]. Îſ óâîëåòſîðÿåò âſåì øåſòè òðåáîâàíèÿì õîðîøåãî ſðîòîêîëà ãîëſîſâàíèÿ. Îſ íå óâîſåòſâðÿåò ſåäüſîſó òðåáîâàíèþ, íſ îſëèäàåò äâóì ſâîéſòâàì è, äſïîëíÿþùèì ſåðå÷èſëåſíûå â íà÷àëå ðàçäåëà øåſòü ſâîéſòâ:

7. Èçáèðàòåëü ſîæåò èçſåſèòü ſâſå ſſåſèå (ò.å., àſſóëèðîâàòü ſâſé áþëëåòåſü è ſðîãîëſſîâàòü çàſſâſ) â òå÷åſèå çàäàſſîãî ſåðèîäà âðåſåſè.

8. Åſëè èçáèðàòåëü ſâſàðóæèâåò, ſòſ åãî áþëëåòåſü ſſſ÷èòàſ ſåſðàâèëüſſ, ſſ ſſæåò óſòàſſâèòü è èſſïðàâèòü ſðîáëåſó, ſå ðèſêóſ áåçſſàſſſòüſ ſâſåãî áþëëåòåſſ.

Âſò ýòſò ſðſòſêſë:

(1) ÖÈÊ ſóáëèêóåò ſſſèſſê âſåõ ſðàâſſſ÷ſûſ èçáèðàòåëåé.

(2) Â òå÷åſèå ſſſðåäſëſſſſãſ ſðſêà êàæäûé èçáèðàòåëü ſſſáùàåò â ÖÈÊ, ſſáèðàåòſÿ ëè ſſ ãſëſſſſâàòü.

(3) ÖÈÊ ïóáëèêóåò ñïèñîê èçáèðàòåëåé, ó÷àñòâóþ ùèõ â âû÷èñ.

(4) Êàæäûé èçáèðàòåëü ïîëó÷àåò èäåíòèôèêàöèîííûé íîìåð, *I*, ñ ïîìîùüþ ïðîòîêîëà ANDOS.

(5) Êàæäûé èçáèðàòåëü ãåíåðèðóåò ïàðó îòêðûòûé êëþ÷/çàêðûòûé êëþ÷: *k*, *d*. If Åñëè *v* - ýòî áþëëåòåíü, òî èçáèðàòåëü ñîçäàåò è ïîñûëàåò â ÖÈÊ ñëåäóþùåå ñîîáùåíèå:

$I,E_k(I, v)$

Ýòî ñîîáùåíèå äîëæíî áûòü ïîñëàíî àíîíèìíî.

(6) ÖÈÊ ïîäòâåðæäàåò ïîëó÷åíèå áþëëåòåíÿ, ïóáëèêóÿ:

$E_k(I, v)$

(7) Êàæäûé èçáèðàòåëü ïîñûëàåò ÖÈÊ:

I, d

(8) ÖÈÊ ðàñøèôðîâûâàåò áþëëåòåíè. Â êîíöå âûáîðîâ îíà ïóáëèêóåò èõ ðåçóëüòàòû è, äëÿ êàæäîãî âàðèàíòà âûáîðà, ñïèñîê ñîîòâåòſòâóþ ùèé çíà÷åíèé $E_k(I, v)$.

(9) Åñëè èçáèðàòåëü îáíàðóæèâàåò, ÷òî åãî áþëëåòåíü ïîäñ÷èòàí íåïðàâèëüíî, îí ïðîòåſòóåò, ïîñûëàÿ ÖÈÊ:

$I, E_k(I, v), d$

(10) Åñëè èçáèðàòåëü õî÷åò èçìåíèòü ñâîé áþëëåòåíü ñ v íà v', îí ïîñûëàåò ÖÈÊ:

$I, E_k(I, v'), d$

Äðóãîé ïðîòîêîë ãîëîñîâàíèÿ èñïîëüçóåò âìåñòî ANDOS ñëåïûå ïîäïèñè, íî ïî ñóòè ìàëî ÷åì îòëè÷àåòſÿ [585]. Ýòàïû (1) - (3) ýâëÿþſòſÿ ïðåäâàðèòåëüíûìè. Èõ öåëü ñîſòîèò â òîì, ÷òîáû óçíàòü è îïóáëèêîâàòü âñåõ äåéſòâèòåëüíûõ èçáèðàòåëåé. Õîòÿ íåêîòîðûå èç íèõ, âåðîſòíî, íå ïðèíóſ ó÷àſòèſ â ãîëîſîâàíèè, ýòî óſíüøàåſ âîçſîſíîſòſ ÖÈÊ äîáàâèſ ïîääåëüíûå áþëëåòåíè.

Íà ýòàïå (4) äâà èçáèðàòåëÿ ſîãóſ ïîëó÷èſü îſèí è òîſ æå èäåíſèôèêàſîſíûé íîſåð. Ýòà âîſçſîſíîſſòſ ſîſæåſ áſòſ ſèíèſèçèðîâàíà, åſëè ſ÷èſî âſçſîſíîſ èäåíſèôèêàſîſíûſ íîſåðîâ áóäſſ ãîðàçäſ áſëüøå, ſ÷åſ ſ÷èſî ðåàëüíûſ èçáèðàòåëåé. Åſëè äâà èçáèðàòåëÿ ïðèſûſàþſ áþëëåòåíè ſ ſàèſàêſâſû èäåíſèôèêàòſðſ, ÖÈÊ ãåíåðèðóåſ íſâſé èäåíſèôèêàſîſíûé íſåð, *I'*, âſáèðàåſ ſàíſàſ èç èçáèðàòåëåé è ſóáëèêóſſ:

$I',E_k(I, v)$

Âëàäåëåö ýſſàſ áþëëåſåíÿ óçíàſſ ſ ſðſèçſøåäøåé ſóſàſèſå è ſſñſûëàſſ ſâſé áþëëåſåſü ſíſâà, ſſâſſðſÿ ýſàſ (5) ſ íſâſû è èäåíſèôèêàſèſſíſû íſſåðſſ.

Ýſàſ (6) äàſſ êàæäſſſ èçáèðàſſëþ âſçſſæſſſſſ ſðſſâåðſſſ, ÷ſſ ÖÈÊ ſðàâèëüſſſ ſſëó÷èſà åãſ áþëëåſåſü. Åſëè åãſ áþëëåſåſü íåſſðàâèëüſſſ ſſäſ÷èſàſ, ſſ ſſæſſ äſêàçàſſ ýſſ íà ýſàſå (9). Ïðåäſſſêàãàÿ, ÷ſſ áþëëåſåſü èçáèðàſſëÿ íà ýſàſå (6) ſſâèëåſ, ñſſáſſåſèå, êſſſðſſå ſſ ſſſûëàſſ íà ýſàſå (9) äſêàçſâàſſ, ÷ſſ åãſ áþëëåſåſü áſë íåſſðàâèëüſſſ ſſäſ÷èſàſ.

Îäſſſ èç ſðſáëåſ ýſſàſ ſðſſſſêſëà ÿâëÿåſñÿ ſſ, ÷ſſ æſëüſſ÷åſêàÿ ÖÈÊ ſſſæåſ âſſſſſëüçſâàſſüſñÿ ëþäåé, êſſſðſå ſſſáſùèëè ſ íàſåðåſèè ãſëſſſâàſü íà ýſàſå (2), ſſ íå ãſëſſſâàëè â äåéſſàêſåëüſſſſſ. Äðóãſé ſðſáëåſſé ÿâëÿåſñÿ ſëſæſſſſſ ſſðſſſêſëà ANDOS. Àâſſðſ ðåſſſàſáóſ ðàçáèâàſü èçáèðàſåëé íà ſåſüøåſ ãðóſſû, íàſſðèſåð èçáèðàſåëüſſå ſêðóãà.

Åùå ſäſſé, áſëåå ſåðüåçſſé ſſðſáëſſé ÿâëÿåſñÿ ſſ, ÷ſſ ÖÈÊ ſſæåſ íå ſſäſ÷èſàſü êàêſé-íèáóäü áþëëåſåſü. Ýſà ſſðſáëåſà íåðàçðåøèſà: Àëèſà óſâåðæäåſ, ÷ſſ ÖÈÊ íàſåðåſſſ ſſðåſááðåã åå áþëëåſåſà, à ÖÈÊ óſâåðæäåſ, ÷ſſ Àëèſà íèêſſäàà íå ãſëſſſâſà.

Ãſëſſſâàſèå áåç Öåſòðàëüſſé èçáèðàſåüſſé êſſèſſñèè

Â ſëåäóþùåſ ſðſſòſêſëå ÖÈÊ íå èſſſëüçóåſſÿ, èçáèðàſåëè ſëåäÿſ äðóã çà äðóãſſ. Ýſſò ſðſſòſêſſ, ſſçäàſſſûé Ìàéêëſſ Ìåðèſſſ [452, 1076, 453], íàſòſëüêſ ãðſſſçâſ, ÷ſſ âſçſſæſſſſòü åãſ ðåàëèçàſèè áſëüøå ÷åſ äëÿ ſÿſè ÷åëſâåê ſſſſſéſåëüſà, ſſ âñå æå ſſçſàêſſſèſüſñÿ ſ íèſ áſäåſ ſſſåçſ.

Àëèſà, Áſá, Êýðſë è Äýéâ ãſëſſñóſ (äà/íåſ èëè 0/1) ſſ êàêſſó-òſ âſſðſſñ. Ïóſòſ ó êàæäſãſ èçáèðàſåëÿ åſòſ ſſêðſûſé è çàêðſûſé êëþ÷è. Ïóſòſ òàêæå âſå ſſêðſûſå êëþ÷è èçâåſòſû âſå.

(1) Êàæäûé ãſëſſñóþ ùèé ðåøåſò, êàê ãſëſſñſâàòſ, è äåëåſò ſëåäóþ ùåå:

(a) Äſáàâëÿåſ ſëó÷àéſóþ ſòðſêó ê ſâſåſó áþëëåſåíþ.

(b) Øèſðóåſ ðåçóëüſàſ (à) ſſêðſûſſ êëþ÷ſſ Äýéâà.

(c) Øèſðóåſ ðåçóëüſàſ (b) ſſêðſûſſ êëþ÷ſſ Êýðſë.

(d) Øèôðóåò ðåçóëüòàò ýòàïà (c) îòêðûòûì êëþ÷îì Áîáà.

(e) Øèôðóåò ðåçóëüòàò ýòàïà (d) îòêðûòûì êëþ÷îì Àëèñû.

(f) Äîáàâëÿåò íîâóþ ñëó÷àéíóþ ñòðîêó ê ðåçóëüòàòó ýòàïà (e) è øèôðóåò ïîëó÷åííûå îòêðûòûì êëþ-÷îì Äýéâà. Î í çàïèñûâàåò çíà÷åíèå ñëó÷àéíîé ñòðîêè.

(g) Äîáàâëÿåò íîâóþ ñëó÷àéíóþ ñòðîêó ê ðåçóëüòàòó ýòàïà (f) è øèôðóåò ïîëó÷åííûå îòêðûòûì êëþ-÷îì Êýðîë. Î í çàïèñûâàåò çíà÷åíèå ñëó÷àéíîé ñòðîêè.

(h) Äîáàâëÿåò íîâóþ ñëó÷àéíóþ ñòðîêó ê ðåçóëüòàòó ýòàïà (g) è øèôðóåò ïîëó÷åííûå îòêðûòûì êëþ-÷îì Áîáà. Î í çàïèñûâàåò çíà÷åíèå ñëó÷àéíîé ñòðîêè.

(i) Äîáàâëÿåò íîâóþ ñëó÷àéíóþ ñòðîêó ê ðåçóëüòàòó ýòàïà (g) è øèôðóåò ïîëó÷åííûå îòêðûòûì êëþ-÷îì Àëèñû. Î í çàïèñûâàåò çíà÷åíèå ñëó÷àéíîé ñòðîêè.

Åñëè E - ýòî ôóíêöèÿ øèôðîâàíèÿ, R_i - ñëó÷àéíàÿ ñòðîêà, à V - áþëëåòåíü , òî åãî ñîîáùåíèå áóäåò âûãëÿäåòü ñëåäóþ ùèì îáðàçîì:

$$E_A(R_5,E_B(R_4,E_C(R_3,E_D(R_2,E_A(E_B(E_C(E_D(V,R_1)))))))$$

Êàæäûé ãîëîñóþ ùèé ñîõðàíÿåò ïðîìåæóòî÷íûå ðåçóëüòàòû íà êàæäîì ýòàïå âû÷èñëåíèé. Ýòè ðåçóëüòàòû áóäóò èñïîëüçîâàòüñÿ íà äàëüíåéøèõ ýòàïàõ ïðîòîêîëà äëÿ ïîäòâåðæäåíèÿ, ÷òî áþëëåòåíü äàííîãî èçáèðàòåëÿ áóäåò ó÷òåí.

(2) Êàæäûé ãîëîñóþ ùèé îòïðàâëÿåò ñîîáùåíèå Àëèñå.

(3) Àëèñà ðàñøèôðîâûâàåò âñå áþëëåòåíè, èñïîëüçóÿ ñâîé çàêðûòûé êëþ÷, è óäàëÿåò âñå ñëó÷àéíûå ñòðîêè íà ýòîì óðîâíå.

(4) Àëèñà ïåðåòàñîâûâàåò âñå áþëëåòåíè è ïîñûëàåò ðåçóëüòàò Áîáó.

Òåïåðü êàæäûé áþëëåòåíü áóäåò âûãëÿäåòü ñëåäóþ ùèì îáðàçîì:

$$E_B(R_4,E_C(R_3,E_D(R_2,E_A(E_B(E_C(E_D(V,R_1)))))))$$

(5) Áîá ðàñøèôðîâûâàåò âñå áþëëåòåíè, èñïîëüçóÿ ñâîé çàêðûòûé êëþ÷, ïðîâåðÿåò, åñòü ëè åãî áþëëåòåíü ñðåäè ïðèñëàííûõ áþëëåòåíåé, óäàëÿåò âñå ñëó÷àéíûå ñòðîêè íà ýòîì óðîâíå, òàñóåò áþëëåòåíè è ïîñûëàåò ðåçóëüòàò Êýðîë.

Òåïåðü êàæäûé áþëëåòåíü áóäåò âûãëÿäåòü ñëåäóþ ùèì îáðàçîì:

$$E_C(R_3,E_D(R_2,E_A(E_B(E_C(E_D(V,R_1)))))))$$

(6) Êýðîë ðàñøèôðîâûâàåò âñå áþëëåòåíè, èñïîëüçóÿ ñâîé çàêðûòûé êëþ÷, ïðîâåðÿåò, åñòü ëè åå áþëëåòåíü ñðåäè ïðèñëàííûõ áþëëåòåíåé, óäàëÿåò âñå ñëó÷àéíûå ñòðîêè íà ýòîì óðîâíå, òàñóåò áþëëåòåíè è ïîñûëàåò ðåçóëüòàò Äýéâó.

Òåïåðü êàæäûé áþëëåòåíü áóäåò âûãëÿäåòü ñëåäóþ ùèì îáðàçîì:

$$E_D(R_2,E_A(E_B(E_C(E_D(V,R_1)))))$$

(7) Äýéâ ðàñøèôðîâûâàåò âñå áþëëåòåíè, èñïîëüçóÿ ñâîé çàêðûòûé êëþ÷, ïðîâåðÿåò, åñòü ëè åãî áþëëåòåíü ñðåäè ïðèñëàííûõ áþëëåòåíåé, óäàëÿåò âñå ñëó÷àéíûå ñòðîêè íà ýòîì óðîâíå, òàñóåò áþëëåòåíè è ïîñûëàåò ðåçóëüòàò Àëèñå.

Òåïåðü êàæäûé áþëëåòåíü áóäåò âûãëÿäåòü ñëåäóþ ùèì îáðàçîì:

$$E_A(E_B(E_C(E_D(V,R_1))))$$

(8) Àëèñà ðàñøèôðîâûâàåò âñå áþëëåòåíè, èñïîëüçóÿ ñâîé çàêðûòûé êëþ÷, ïðîâåðÿåò, åñòü ëè åå áþëëåòåíü ñðåäè ïðèñëàííûõ áþëëåòåíåé, ïîäïèñûâàåò âñå áþëëåòåíè è ïîñûëàåò ðåçóëüòàò Áîáó, Êýðîë è Äýéâó.

Òåïåðü êàæäûé áþëëåòåíü áóäåò âûãëÿäåòü ñëåäóþ ùèì îáðàçîì:

$$S_A\,(E_B(E_C(E_D(V,R_1))))$$

(9) Áîá ïðîâåðÿåò è óäàëÿåò ïîäïèñè Àëèñû. Î í ðàñøèôðîâûâàåò âñå áþëëåòåíè, èñïîëüçóÿ ñâîé çàêðûòûé êëþ÷, ïðîâåðÿåò, åñòü ëè åãî áþëëåòåíü ñðåäè ïðèñëàííûõ áþëëåòåíåé, ïîäïèñûâàåò âñå áþëëåòåíè è ïîñûëàåò ðåçóëüòàò Àëèñå, Êýðîë è Äýéâó.

Òåïåðü êàæäûé áþëëåòåíü áóäåò âûãëÿäåòü ñëåäóþ ùèì îáðàçîì:

$$S_B(E_C(E_D(V,R_1)))$$

(10) Êýðîë ïðîâåðÿåò è óäàëÿåò ïîäïèñè Áîáà. Î íà ðàñøèôðîâûâàåò âñå áþëëåòåíè, èñïîëüçóÿ ñâîé çàêðûòûé

êëþ÷, ïðîâåðÿåò, åñòü ëè åå áþëëåòåíü ñðåäè ïðèñëàííûõ áþëëåòåíåé, ïîäïèñûâàåò âñå áþëëåòåíè è ïîñûëàåò ðåçóëüòàò Àëèñå, Áîáó è Äýéâó.

Òåïåðü êàæäûé áþëëåòåíü áóäåò âûãëÿäåòü ñëåäóþùèì îáðàçîì:

$S_C(E_D(V,R_1))$

(11) Äýéâ ïðîâåðÿåò è óäàëÿåò ïîäïèñü Êýðîë. Îí ðàñøèôðîâûâàåò âñå áþëëåòåíè, èñïîëüçóÿ ñâîé çàêðûòûé êëþ÷, ïðîâåðÿåò, åñòü ëè åãî áþëëåòåíü ñðåäè ïðèñëàííûõ áþëëåòåíåé, ïîäïèñûâàåò âñå áþëëåòåíè è ïîñûëàåò ðåçóëüòàò Àëèñå, Áîáó è Êýðîë.

Òåïåðü êàæäûé áþëëåòåíü áóäåò âûãëÿäåòü ñëåäóþùèì îáðàçîì:

$S_D(V,R_1)$

(12) Âñå ïðîâåðÿþò è óäàëÿþò ïîäïèñü Äýéâà. Îíè óáåæäàþòñÿ, ÷òî èõ áþëëåòåíè íàõîäÿòñÿ ñðåäè ïîëó÷åííûõ (íàõîäÿ ñâîþ ñëó÷àéíóþ ñòðîêó).

(13) Âñå óäàëÿþò ñëó÷àéíûå ñòðîêè èç êàæäîãî áþëëåòåíÿ è ñóììèðóþò áþëëåòåíè.

Ýòîò ïðîòîêîë íå òîëüêî ðàáîòàåò, îí ñàì ÿâëÿåòñÿ ñâîèì àðáèòðîì. Àëèñà, Áîá, Êýðîë è Äýéâ íåìåäëåííî óçíàþò, åñëè êòî-íèáóäü èç íèõ ïîïûòàåòñÿ ìîøåííè÷àòü. Íå íóæíî íèêàêèõ ÖÈÊ è ÖÓÐ. ×òîáû óâèäåòü, êàê ýòî ðàáîòàåò, ïîïûòàåìñÿ ñìîøåííè÷àòü.

Åñëè êòî-íèáóäü ïûòàåòñÿ äîáàâèòü áþëëåòåíü, Àëèñà îáíàðóæèò ýòó ïîïûòêó íà ýòàïå (3), êîãäà îíà ïîëó÷èò áþëëåòåíåé áîëüøå ÷åì êîëè÷åñòâî ëþäåé, ó÷àñòâóþùèõ â ãîëîñîâàíèè. Åñëè Àëèñà ïîïûòàåòñÿ äîáàâèòü áþëëåòåíü, Áîá îáíàðóæèò ýòî íà ýòàïå (4).

Áîëåå ëîâêîé ÿâëÿåòñÿ ïîäìåíà îäíîãî áþëëåòåíÿ äðóãèì. Òàê êàê áþëëåòåíè øèôðóþòñÿ ðàçëè÷íûìè îòêðûòûìè êëþ÷àìè, êàæäûé ìîæåò ñîçäàòü ñòîëüêî ïðàâèëüíûõ áþëëåòåíåé, ñêîëüêî íóæíî. Ïðîòîêîë äåøèôðèðîâàíèÿ ñîñòîèò èç äâóõ ÷àñòåé: ïåðâàÿ âêëþ÷àåò ýòàïû (3)-(7), à âòîðàÿ - ýòàïû (8)-(11). Ïîäìåíà ãîëîñà íà ðàçëè÷íûõ ýòàïàõ îáíàðóæèâàåòñÿ ïî ðàçíîìó.

Åñëè êòî-íèáóäü çàìåíèò îäèí áþëëåòåíü äðóãèì âî âòîðîé ÷àñòè, åãî äåéñòâèÿ áóäóò îáíàðóæåíû íåìåäëåííî. Íà êàæäîì ýòàïå áþëëåòåíè ïîäïèñûâàþòñÿ è ïîñûëàþòñÿ âñåì èçáèðàòåëÿì. Åñëè îäèí èçáèðàòåëü (èëè íåñêîëüêî) îáíàðóæèâàåò, ÷òî åãî áþëëåòåíÿ áîëüøå íåò ñðåäè íàáîðà áþëëåòåíåé, îí íåìåäëåííî ïðåêðàùàåò âûïîëíåíèå ïðîòîêîëà. Òàê êàê áþëëåòåíè ïîäïèñûâàþòñÿ íà êàæäîì ýòàïå, è òàê êàê êàæäûé ìîæåò âåðíóòüñÿ âî âòîðîé ÷àñòè ïðîòîêîëà íà íåñêîëüêî øàãîâ íàçàä, òî îáíàðóæèòü ìîøåííèêà, ïîäìåíèâøåãî áþëëåòåíè, ëåãêî.

Çàìåíà îäíîãî áþëëåòåíÿ äðóãèì â ïåðâîé ÷àñòè ïðîòîêîëà áîëåå òîíêà. Àëèñà íå ìîæåò ñäåëàòü çàìåíó íà ýòàïå (3), ïîòîìó ÷òî Áîá, Êýðîë è Äýéâ îáíàðóæàò ýòî íà ýòàïàõ (5), (6) èëè (7). Áîá ìîæåò ïîïðîáîâàòü íà ýòàïå (5). Åñëè îí çàìåíèò áþëëåòåíè Êýðîë è Äýéâà (ïîìíèòå, îí íå çíàåò, êàêîé áþëëåòåíü ÷åé), Êýðîë èëè Äýéâ çàìåòÿò ýòî íà ýòàïàõ (6) èëè (7). Îíè íå áóäóò çíàòü, êòî ïîäìåíèë èõ áþëëåòåíè (õîòÿ ýòî äîëæåí áûòü êòî-òî, óæå îáðàáîòàâøèé áþëëåòåíè), íî îíè áóäóò çíàòü, ÷òî èõ ãîëîñà ïîäìåíåíû. Åñëè Áîáó ïîâåçëî, è åìó óäàëîñü ïîäìåíèòü áþëëåòåíü Àëèñû, îíà íå çàìåòèò ýòîãî äî âòîðîé ÷àñòè ïðîòîêîëà. Òîãäà îíà îáíàðóæèò èñ÷åçíîâåíèå ñâîåãî ãîëîñà íà ýòàïå (8), íî íå ñìîæåò óçíàòü, êòî ïîäìåíèë áþëëåòåíü. Â ïåðâîé ÷àñòè áþëëåòåíè ïåðåòàñîâûâàþòñÿ íà êàæäîì ýòàïå è íå ïîäïèñûâàþòñÿ, ïîýòîìó íèêòî íå ñìîæåò îòðàáîòàòü ïðîòîêîë îáðàòíî è îïðåäåëèòü, êòî ïîäìåíèë áþëëåòåíè.

Äðóãîé ôîðìîé ìîøåííè÷åñòâà ÿâëÿåòñÿ ïîïûòêà óçíàòü, êòî çà êîãî ïðîãîëîñîâàë. Èç-çà ïåðåòàñîâêè áþëëåòåíåé â ïåðâîé ÷àñòè íèêòî íå ñìîæåò îòðàáîòàòü ïðîòîêîë îáðàòíî è ñâÿçàòü áþëëåòåíè è ãîëîñóþùèõ. Óäàëåíèå ñëó÷àéíûõ ñòðîê â ïåðâîé ÷àñòè òàêæå ÿâëÿåòñÿ ðåøàþùèì äëÿ ñîõðàíåíèÿ àíîíèìíîñòè. Åñëè ñòðîêè íå óäàëÿþòñÿ, ïåðåìåøèâàíèå ãîëîñîâ ìîæåò áûòü èíâåðòèðîâàíî ïðè ïîìîùè ïîâòîðíîãî øèôðîâàíèÿ ïîëó÷àåìûõ ãîëîñîâ îòêðûòûì êëþ÷îì òîãî, êòî èõ òàñîâàë. Êîãäà ïðîòîêîë îñòàíîâèòñÿ, êîíôèäåíöèàëüíîñòü áþëëåòåíåé ñîõðàíèòñÿ.

Áîëåå òîãî, èç-çà íà÷àëüíîé ñëó÷àéíîé ñòðîêè, R_1, äàæå îäèíàêîâûå áþëëåòåíè øèôðóþòñÿ ïî ðàçíîìó íà êàæäîì ýòàïå ïðîòîêîëà. Íèêòî íå ìîæåò óçíàòü çíà÷åíèå áþëëåòåíÿ äî ýòàïà (11).

Êàêîâû ïðîáëåìû ýòîãî ïðîòîêîëà? Âî ïåðâûõ, äëÿ âûïîëíåíèÿ ïðîòîêîëà íóæíû ãðîìàäíûå âû÷èñëåíèÿ. Â ïðèâåäåííîì ïðèìåðå â ãîëîñîâàíèè ïðèíèìàþò ó÷àñòèå òîëüêî ÷åòâåðî, íî è îí *óæå* ñëîæåí. Òàêîé ïðîòîêîë íå ñìîæåò ðàáîòàòü ïðè ðåàëüíûõ âûáîðàõ ñ äåñÿòêàìè òûñÿ÷ ãîëîñóþùèõ. Âî âòîðûõ, Äýéâ óçíàåò ðåçóëüòàòû âûáîðîâ ðàíüøå îñòàëüíûõ. Õîòÿ îí è íå ìîæåò ïîâëèÿòü íà ðåçóëüòàò, îí ïîëó÷àåò îïðåäåëåííîå ïðåèìóùåñòâî. Ñ äðóãîé ñòîðîíû òàêîå òàêæå âîçìîæíî è ïðè öåíòðàëèçîâàííîé ñõåìå ãîëîñîâàíèÿ.

Òðåòüÿ ïðîáëåìà çàêëþ÷àåòñÿ â òîì, ÷òî Àëèñà ìîæåò ñêîïèðîâàòü áþëëåòåíü äðóãîãî ó÷àñòíèêà, äàæå íå çíàÿ åãî ñîäåðæàíèÿ çàðàíåå. ×òîáû ïîíÿòü, ïî÷åìó ýòî ìîæåò ñòàòü ïðîáëåìîé, ðàññìîòðèì âûáîðû äëÿ òðåõ ãîëîñóþùèõ - Àëèñû, Áîáà è Åâû. Åâå íå âàæíû ðåçóëüòàòû âûáîðîâ, íî îíà õî÷åò çíàòü, êàê ãîëîñîâàëà Àëèñà. Ïîýòîìó îíà êîïèðóåò áþëëåòåíü Àëèñû, è ðåçóëüòàò âûáîðîâ áóäåò ñîîòâåòñòâîâàòü áþëëåòåíþ Àëèñû.

Äðóãèå ñõåìû ãîëîñîâàíèÿ

Áûëî ïðåäëîæåíî ìíîãî ñëîæíûõ áåçïàñíûõ ïðîòîêîëîâ âûáîðà. Èõ ìîæíî ðàçäåëèòü íà äâà òèïà. Ñóùåñòâóþò ïðîòîêîëû ñ ïåðâè÷íûì ðàçäåëåíèåì, êàê "Âîëîñîâàíèå áåç Öåíòðàëüíîé èçáèðàòåëüíîé êîìèññèè", â êîòîðûõ âñå áþëëåòåíè ïåðâè÷íîé ïîäïèñàíî ÷òî-òî íåêîòîðûì îáðàçîì, è ïðîòîêîëû ñ öåíòðàëèçîâàííûì ïîäñ÷åòîì. Ýòè ïðîòîêîëû Ýòè ïðîòîêîëû çàùèùàþòñÿ îò íåñàíêöèîíèðîâàííîãî èçáèðàòåëåì òîëüêî, åñëè ðàçëè÷íûå "÷àñòè" ïðàâèòåëüñòâà (èëè êòî áû íå ïðîâîäèë ãîëîñîâàíèå) íå ñãîâàðèâàþòñÿ ïðîòèâ èçáèðàòåëÿ. (Èäåÿ ðàçáèòü öåíòðàëüíûé îðãàí íà íåñêîëüêî ÷àñòåé, êîòîðûå ïîëüçóþòñÿ äîâåðåíî, òîëüêî êîãäà îíè äåéſòâóþò ïàðàëëåëüíî, ïðèøëà èç [316].)

Îäíî èç ïðîòîêîëîâ ñ ðàçäåëåíèåì ïðåäëîæåí â [1371]. Îñíîâíàÿ èäåÿ ñîñòîèò â òîì, ÷òî êàæäûé èçáèðàòåëü äåëèòñÿ íà íåñêîëüêî ÷àñòåé. Íàïðèìåð, åñëè áû áþëëåòåíü ñîäåðæàë "äà" èëè "íåò", 1 îáîçíà÷àëà áû "äà", à 0 - "íåò", èçáèðàòåëü ìîã áû ñîçäàòü íåñêîëüêî ÷åñë, êîòîðûå â ñóììå äàâàëè áû 0 èëè 1. Ýòè äîëè ïîñûëàþòñÿ ñ÷åòíûì êîìèññèÿì, êàæäîé ïî îäíîé, è òàêæå øèôðóþòñÿ è ñîõðàíÿþòñÿ. Êàæäûé öåíòð ñóììèðóåò ïîëó÷åííûå äîëè (ñóùåñòâóþò ïðîòîêîëû, îáåñïå÷èâàþùèå ïðàâèëüíîñòü èòîãà), è îêî÷àòåëüíûé èòîã ÿâëÿåòñÿ ñóììîé âñåõ ïðîìåæóòî÷íûõ èòîãîâ. Ñóùåñòâóþò òàêæå ïðîòîêîëû, ãàðàíòèðóþùèå, ÷òî äîëè êàæäîãî èçáèðàòåëÿ áóäóò ñëîæåíû äëÿ ïîëó÷åíèÿ 0 èëè 1.

Äðóãîé ïðîòîêîë, ïðåäëîæåííûé Äýâèäîì ×àóì [322], ïîçâîëÿåò ïðîñëåäèòü èçáèðàòåëÿ, êîòîðûé ïûòàåòñÿ ìîøåíè÷àòü. Îäíàêî, âûíûõ ïðèâîäèò ïîâòîðíî, èñêëþ÷èâ ìåøàþùåãî ïîëüçîâàòåëÿ. Ýòî ïîäõîä íà ïðèìåðå íà ïðàêòèêå äëÿ âûíîñíîãî áîëüøèíñòâà (ñì. [770, 771]. Ñóùåñòâóåò äâæå ïðîòîêîë, èñïîëüçóþùèé øèôðû ñî ìíîãèì êëþ÷àìè [219]. Äðóãîé ïðîòîêîë, êîòîðûé, êàê óòâåðæäàþò, ïîäõîäèò äëÿ êðèïòîãðàôè÷åñêè ñòîéêèõ âû÷èñëåíèé â [585]. À [347] ïîçâîëÿåò èçáèðàòåëÿì íå ãîëîñîâàòü.

Ïðîòîêîëû ãîëîñîâàíèÿ ðàíîàþò, îíè äàæå îáëåã÷àþò ïðîäàæó è ïîêóïêó ãîëîñîâ. Êîãäà ïîêóïàòåëü ìîæåò áûòü óâåðåí, ÷òî ïðîäàâåö ïðîãîëîñóåò, êàê îáû÷íî ïîñòóïàåò ñòàíäàðòíûé **áåç ïîäòâåðæäåíèÿ**, íå ïîçâîëÿÿ èçáèðàòåëþ äîêàçàòü êîìó-ëèáî åùå, ÷òî îí ïðîãîëîñîâàë îïðåäåëåííûì îáðàçîì [117, 1170, 1372].

6.2 Áåçîïàñíûå âû÷èñëåíèÿ ñ íåñêîëüêèìè ó÷àñòíèêàìè

Áåçîïàñíûå âû÷èñëåíèÿ ñ íåñêîëüêèìè ó÷àñòíèêàìè ïðåäñòàâëÿò ñîáîé ïðîòîêîë, ñ ïîìîùüþ êîòîðîãî ãðóïïà ëþäåé ìîæåò îïðåäåëåííûì îáðàçîì âû÷èñëèòü ôóíêöèþ ìíîãèõ ïåðåìåííûõ. Êàæäûé â ãðóïïå îáðàùàåòñÿ ê îäíîìó öåíòðàëèçîâàííîìó óçëó, êîòîðûé âû÷èñëÿåò è ñîõðàíÿåò ñòàíäàðòíûé èçâåñòíûé çíà÷åíèå, íî íèêòî íå çíàåòñÿ , ïðåäïîëàãàåìûå äðóãèì ÷ëåíàìè ãðóïïû, åñëè ýòî íå ÿâëÿåòñÿ î÷åâèäíûì èç ðåçóëüòàòà âû÷èñëåíèé. Íèæå ïðèâåäåíî íåñêîëüêî ïðèìåðîâ:

Ïðîòîêîë 1

Êàê ìîæåò ãðóïïà ëþäåé âû÷èñëèòü ñâîþ ñðåäíþþ çàðïëàòó áåç òîãî, ÷òîáû çàðïëàòà îäíîãî ñòàëà èçâåñòíà ãðóãîìó?

(1) Àëèñà äîáàâëÿåò ñåêðåòíîå ñëó÷àéíîå ÷èñëî ê ñóììå ñâîåé çàðïëàòû, øèôðóåò ðåçóëüòàò îòêðûòûì êëþ÷îì Áîáà è îñûëàåò åãî Áîáó.

(2) Áîá ðàñøèôðîâûâàåò ðåçóëüòàò ñâîèì çàêðûòûì êëþ÷îì. Îí äîáàâëÿåò ñóììó ñâîåé çàðïëàòû ê ïîëó÷åííîìó îò Àëèñû çíà÷åíèþ, øèôðóåò ðåçóëüòàò îòêðûòûì êëþ÷îì Êýðîë è ïîñûëàåò åãî Êýðîë.

(3) Êýðîë ðàñøèôðîâûâàåò ðåçóëüòàò ñâîèì çàêðûòûì êëþ÷îì. Îíà äîáàâëÿåò ñóììó ñâîåé çàðïëàòû ê ïîëó÷åííîìó îò Áîáà çíà÷åíèþ, øèôðóåò ðåçóëüòàò îòêðûòûì êëþ÷îì Äýéâà è ïîñûëàåò åãî Äýéâó.

(4) Äýéâ ðàñøèôðîâûâàåò ðåçóëüòàò ñâîèì çàêðûòûì êëþ÷îì. Îí äîáàâëÿåò ñóììó ñâîåé çàðïëàòû ê ïîëó÷åííîìó îò Êýðîë çíà÷åíèþ, øèôðóåò ðåçóëüòàò îòêðûòûì êëþ÷îì Àëèñû è ïîñûëàåò åãî Àëèñå.

(5) Àëèñà ðàñøèôðîâûâàåò ðåçóëüòàò ñâîèì çàêðûòûì êëþ÷îì. Îíà âû÷èòàåò ñëó÷àéíîå ÷èñëî, ïðèáàâëÿåò íà ýòàïå (1), ïîëó÷àÿ ñóììó âñåõ çàðïëàò.

(6) Àëèñà äåëèò ðåçóëüòàò íà ÷èñëî ëþäåé (â äàííîì ñëó÷àå íà ÷åòûðå) è îáúÿâëÿåò ðåçóëüòàò.

Ýòîò ïðîòîêîë ïîäðàçóìåâàåò, ÷òî êàæäûé ó÷àñòíèê ÷åñòåí - îíè õîòÿ è ìîãóò ëþáîïûòñòâîâàòü, íî ñëåäóþò ïðîòîêîëó. Åñëè ëþáîé èç ó÷àñòíèêîâ ñîëãàòü î ñâîåé çàðïëàòå, ñðåäíÿÿ çàðïëàòà áóäåò ðàññ÷èòàíà íåïðàâèëüíî. Áîëåå ñåðüåçíàÿ ïðîáëåìà ñîñòîèò â òîì, ÷òî Àëèñà ìîæåò èñêàæàòü èòîãîâûé ðåçóëüòàò. Îíà ìîæåò âû÷åñòü íà ýòàïå (5) ëþáîå ÷èñëî, êîòîðîå åå óñòðàèâàåò, è íèêòî îá ýòîì íå óçíàåò. Ïîìåøàòü Àëèñå ñäåëàòü ýòî ìîæíî, ïîðóøàÿ îò íåå âðó÷èòü åé ñëó÷àéíîå ÷èñëî ñ ïîìîùüþ îáùåãî çàøèôðîâàííîãî ïîëÿ, íî êîãäà

íía îòêðîåò ñâîå ñëó÷àéíîå ÷èñëî â êîíöå ïðîòîêîëà Áîá ñìîæåò óçíàòü åå çàðïëàòó.

Ïðîòîêîë ¹2

Àëèñà è Áîá âìåñòå â ðåñòîðàíå è ñïîðÿò î òîì, êòî ñòàðøå. Íèêòî, îäíàêî, íå õî÷åò ñîîáùèòü äðóãîìó ñâîé âîçðàñò. Êàæäûé èç íèõ ìîã áû ïðîøåïòàòü ñâîé âîçðàñò íà óøêî äîâåðåííîé íåéòðàëüíîé ñòîðîíå (íàïðèìåð, îôèöèàíòó), êòî ìîã áû ñðàâíèòü ÷èñëà â óìå è îáúÿâèòü ðåçóëüòàò è Àëèñå, è Áîáó.

Ó ïðèâåäåííîãî ïðîòîêîëà åñòü äâå ïðîáëåìû. Âî ïåðâûõ, âû÷èñëèòåëüíûå ñïîñîáíîñòè ñðåäíåãî îôèöèàíòà íå ïîçâîëÿþ åìó îáðàáîòàòü ñèòóàöèè áîëåå ñëîæíûå, ÷åì ïîðåøèòü äâóõ ÷èñåë. È âî âòîðûõ, åñëè áû Àëèñà è Áîá äåéñòâèòåëüíî çàáîòèëèñü î ñîõðàíåíèè ñâîé èíôîðìàöèè â òàéíå, èì ïðèøëîñü áû óòî÷íèòü îôèöèàíòà â âàííå ñ ìèíåðàëüíîé âîäîé, ÷òîáû îí íè÷åãî íå ðàçáîëòàë áóôåò÷èêó.

Êðèïòîãðàôèÿ ñ îòêðûòûì êëþ÷àìè ïðåäëàãàåò ñóùåñòâîâíî ìåíåå æåñòîêîå ðåøåíèå. Ñóùåñòâóåò ïðîòîêîë, â ñîîòâåòſòâèè ñ êîòîðûì Àëèñà, çíàÿ çíà÷åíèå *a*, è Áîá, çíàÿ *b*, ìîãóò ñîâìåñòíî îïðåäåëèòü âåðíî ëè, ÷òî *a<b*, òàê, ÷òîáû Àëèñà íå ïîëó÷èëà èíôîðìàöèè î *b*, à Áîá - îá *a*. Êðîìå òîãî, è Àëèñà, è Áîá óáåæäåíû â ïðîâåðêå ïðàâèëüíîñòè âû÷èñëåíèé. Òàê êàê èñïîëüçóåìûé êðèïòîãðàôè÷åñêèé àëãîðèòì ÿâëÿåòſ ñóùåſòâóþùèì ïðîòîêîëîì, ïîäõîäÿùèì ìåíüøå ÷åì íà îäíó äåñÿòè÷íóþ öèôðó, ïîýòîìó ïðîòîêîë, îïèſàííûé âûſå, ñîîáſåíèå ñ âåſîſòíîſòüſ 23.14.

Êîíå÷íî, ýòî ïðîòîêîë íå çàùèùàåò îò àêòèâíûõ ìîøåííèêîâ. Íè÷òî íå ñìîæåò ïîìåøàòü Àëèñå (èëè Áîáó, êàêàÿ ðàçíèöà) ñîëãàòü î ñâîåì âîçðàſſå. Åſëè áû Áîá áûë êîìüþòåðſíîé ïðîãðàìſìé, êîòîðàÿ ñëåïî ïðîãîíſëà áû ïðîòîêîëó, Àëèſſà ìîãëà áû óçíàòü åſî âîçðàſſ (ÿâëÿåòſÿ ëè âîçðàſſîì êîìüþòåſíîé ïðîãðàìſìû îòåçîê âðåìåíè ſ ìîſſåíòà åå íàïèſàſèÿ èëè ſ îſſåíòà åå çàïóſêà?), ïîâòſðſſ âû ïſëíÿÿ ïðîòſêſë. Àëèſà ſſãëà áû óêàçàòü, ÷òſ åå âſçðàſſ - 60 ëåò. Óſíàâ, ÷òſ ſſà ſòàðøå, ſſà ſſãëà áû âû ſſëſèòü ïðſòſêſë ſſſâà, óêàçàâ, ÷òſ åå âſçðàſſ - 30 ëåò. Óſíàâ, ÷òſ Áſá ſòàðøå, ſſà ſſãëà áû ſſſâà âû ſſëſèòü ïðſòſêſë, óêàçàâ, ÷òſ åå âſçðàſſ - 45 ëåò, è òàê äàëåå, ſſêà Àëèſà íå óſíàåò âſçðàſſ Áſáà ſ ëþáſé íóæſſé åé ſòåſſåſſüſ òſ÷ſſſòè.

Ïðè óſëſſâèè, ÷òſ ó÷àſòſêêè íå ſáſàſſûâàþò ſſſåöèàëüſſſ, ýòſò ïðſòſêſë ëåãêſ ðàſøèðèòü äëÿ íåſêſſëüêèõ ó÷àſòſêêſâ. Ëþáſå êſëë÷åſòâſ ëþäåé ſſæåò ſſſðåäåëèòü ſſðÿſſê èõ âſçðàſòſâ ſ ſſſſſüſþ ſſſëåſſſâſòåëüſſûõ ÷åſòſſûõ ſðèſåſſéſ ſſðſòſêſëà, è ſèêàêſé ó÷àſòſêê íå ſſſæåò óçſàòü âſçðàſò äðóãſãſ.

Ïðîòîêîë ¹3

Àëèſà ſðàâèòſÿ çàáàâëÿòüſÿ ſ ſëþ øåâû ſè ſåäåääÿſè. Â ýðſòè÷åſſêõ ôàſòàçèÿõ Áſáà âàæſſå ſåſòſ çàſè-ſàþò ſðàſſſðſûå ſòſëû. Sáà âåſüſà ſòåſſſýþòſÿ ſſâſèõ ſſðêâû÷åê, ſſ ſ óáſâſſëüſòâèſ ſàøëè áû êſãſ-ſèáóäü, êòſ ðàçäåëèë áû ſ ſèſè èõ... ãſ... ſáðàç æèçſè.

Â Ñëóæáå áåçſſſàſſſûõ âû÷èſëſſéſ ſ ſåſêſſëüêſſè ó÷àſòſêêàſè ſû ſſðſåêòſðſâàëè ſðſòſêſëſ äëÿ ſſäſâſáſûõ ëþäåé. S û çàſóſåðſâàëè âſå÷àòëÿþſùèſ ſſſèſſê èõ ſſðèſòðàſòſèſ ſò "àſðêèſáſſêêõ ſóðàâûåäſâ" äſ "ÿáëſ÷ſûõ ſſèſſãſâ". Ðàçäåëſſſſûå ſſäåſſſſſſ ëſſſåſé ſâÿçè, Àëèſà è Áſá ſſãóò ó÷àſòſâſàòſ â áåçſſäſſſſ ſðſòſêſëå ſ íå-ſêſſëüêſſſ ó÷àſòſêêàſſ. Sſſè âſſåſòå ſſãóò ſſðåäåëèòü, åſòſ ëè ó íèſ ſáſſèå ſðèâû÷êè. Åſëè åſòſ, ſſſè ſſãëè áû óſòðåſſèòſſÿ ſ ſáſſſſſſſſſ ſſſðſòſêſëå ſ íåſêſſëüêſſſ ó÷àſòſêêàſſ. Sſſè âſſåſòå ſſãóò ſſðåäåëèòü ſſðÿſſê èõ âſçðàſòſâſ ſ ſſſſſüſþ ſſſëåſſſâſòåëüſſûõ ſſðſòſêſëà, è ſèêàêſé ó÷àſòſêê íå ſſſæåò óçſàòſ âſçðàſò äðóãſãſ.

Ïðîòîêîë ¹4

Âſò äðóãàÿ ſðſſáſåſſà äſÿ áåçſſſàſſſûõ âû÷èſëſſéſ ſſ ſſſſãſſſ ó÷àſòſêêàſſ [1373]: ſſſâåò ſåſſ ðåãóſÿðſſ

âñòðå÷àåòñÿ, ÷òîáû òàéíî ïðîãîëîñîâàòü ïî íåêîòîðûì âîïðîñàì. (Âñå â ïîðÿäêå, îíè óïðàâëÿþò ìèðîì - íå ãîâîðèòå íèêîìó, ÷òî ÿ âàì ïðîãîâîðèëñÿ.) Âñå ÷ëåíû ñîâåòà ìîãóò ãîëîñîâàòü "äà" èëè "íåò". Êðîìå òîãî, äâå ñòîðîíû íáëàäàþò "ñóïåð-áþëëåòåíü": 5-äà è 5-íåò. Îíè íå îáÿçàíû èñïîëüçîâàòü ýòè "ñóïåð-áþëëåòíèå" è, åñëè õîòÿò, ìîãóò âîñïîëüçîâàòüñÿ îáû÷íûìè áþëëåòåíÿìè. Åñëè íèêòî íå èñïîëüçóåò "ñóïåð-áþëëåòíè", òî âîïðîñ ðåøàåòñÿ ïðîñòûì áîëüøèíñòâîì ãîëîñîâ. Â ñëó÷àå ïðèìåíåíèÿ îäíîãî èëè äâóõ ýêâèâàëåíòíûõ "ñóïåð-áþëëåòíûå" âñå îáû÷íûå ãîëîñà èãíîðèðóþòñÿ. Â ñëó÷àå ãðóïïîâîãî ïîäñ÷åòà ïîäñ÷èòàþòñÿ áîëüøèíñòâî ïîëó÷åííûõ "ñóïåð-áþëëåòíûå" ãîëîñîâ.

Ñëåäóþùèå äâà ïðèìåðà èëëþñòðèðóþò ïðîáëåìû. Ïóñòü ó÷àñòâóþò ïÿòü îáû÷íûõ èçáèðàòåëåé, îò N_1 äî N_5, è äâà ñóïåðèçáèðàòåëÿ: S_1 è S_2. Âîò ãîëîñîâàíèå ïî âîïðîñó ¹ 1:

S_1	S_2	N_1	N_2	N_3	N_4	N_5
Ñóïåð-äà	íåò	íåò	íåò	íåò	äà	äà

Â ýòîì ïðèìåðå äåéñòâóåò òîëüêî îäèí "ñóïåð-áþëëåòåíü" S_1, è ðåçóëüòàò ãîëîñîâàíèÿ - "äà". À âîò ãîëîñîâàíèå ïî âîïðîñó ¹ 2:

S_1	S_2	N_1	N_2	N_3	N_4	N_5
Ñóïåð-äà	Ñóïåð-íåò	íåò	íåò	íåò	äà	äà

Â ýòîì ïðèìåðå äâà "ñóïåð-áþëëåòíèê" íáéòðàëèçóþò äðóãà äðóãà, è âîïðîñ ðåøàåòñÿ áîëüøèíñòâîì îáû÷íûõ "íåò".

Åñëè íå òðåáóåòñÿ ñêðûòü èíôîðìàöèþ î òîì, îáû÷íûé èëè ñóïåðáþëëåòåíü áûë ðåøàþùèì, òî ýòî ïðîñòî ïðèìåíåíèå áåçîïàñíîãî ïðîòîêîëà ãîëîñîâàíèÿ. Ñîêðûòèå ýòîé èíôîðìàöèè ïîòðåáóåò áîëåå ñëîæíîãî áåçîïàñíîãî ïðîòîêîëà âû÷èñëåíèé ñ íåñêîëüêèì óðàâíåíèåì.

Ýòî âèä ãîëîñîâàíèÿ ìîæåò ïðîèçîéòè â ðåàëüíîé æèçíè. Ýòî ìîæåò áûòü ÷àñòè îðãàíèçàöèîííîé ñòðóêòóðû êîðïîðàöèè, ãäå íåêîòîðûå ëþäè îáëàäàþò áîëüøåé âëàñòüþ ÷åì äðóãèå, èëè ÷àñòü ïðîöåäóðû Î Î Í, ãäå îäíè ãîñóäàðñòâà èìåþò áîëüøå çíà÷åíèå, ÷åì äðóãèå.

Áåçóñëîâíûå áåçîïàñíûå ïðîòîêîëû ñ íåñêîëüêèì ó÷àñòíèêàìè

Ýòî òîëüêî ÷àñòíûé ñëó÷àé îáùåé òåîðåìû: ëþáàÿ ôóíêöèÿ ñ *n* âõîäàìè ìîæåò áûòü âû÷èñëåíà *n* èãðîêàìè ñïîñîáíî, êòîðûé ïîçâîëèò âñåì óçíàòü çíà÷åíèå ôóíêöèè, íî ëþáîå êîëè÷åñòâî èãðîêîâ, ìåíüøåå, ÷åì *n/2*, íå ñìîæåò ïîëó÷èòü íèêàêîé äîïîëíèòåëüíîé èíôîðìàöèè, íå ñëåäóþùåé èç èõ ñîáñòâåííûõ âõîäîâ è ðåçóëüòàòà âû÷èñëåíèé. Ïîäðîáíîñòè ìîæíî íàéòè â [136, 334, 1288, 621].

Áåçîïàñíàÿ îöåíêà ñõåìû

Âõîä Àëèñû - *a*, à Áîáà - *b*. Îíè âìåñòå õîòÿò âû÷èñëèòü íåêîòîðóþ ôóíêöèþ *f(a,b)* òàê, ÷òîáû Àëèñà íå ñìîãëà íè÷åãî óçíàòü î âõîäå Áîáà, à Áîá - î âõîäå Àëèñû. Ãëàâíàÿ ïðîáëåìà áåçîïàñíûõ âû÷èñëåíèé ñ íåñêîëüêèìè ó÷àñòíèêàìè òàêæå íàçûâàåòñÿ **áåçîïàñíîé îöåíêîé ñõåìû**. Àëèñà è Áîá ìîãóò ñîçäàòü ïðîèçâîëüíóþ ëîãè÷åñêóþ ñõåìó. Ýòà ñõåìà ïîëó÷åò íà âõîä çíà÷åíèÿ Àëèñû è Áîáà è âûäàñò ðåçóëüòàò. Áåçîïàñíàÿ îöåíêà ñõåìû ÿâëÿåòñÿ ïðîòîêîëîì, êîòîðûé ðåàëèçóåò ñëåäóþùèå òðè òðåáîâàíèÿ:

1. Àëèñà ìîæåò âûñòè ñâîå çíà÷åíèå òàê, ÷òî Áîá íå ñìîæåò åãî óçíàòü.
2. Áîá ìîæåò âûñòè ñâîå çíà÷åíèå òàê, ÷òî Àëèñà íå ñìîæåò åãî óçíàòü.
3. È Àëèñà, è Áîá ìîãóò âû÷èñëèòü ðåçóëüòàò, ïðè÷åì îáà óäóò óâåðåíû â òîì, ÷òî ðåçóëüòàò ïðàâèëåí è íå ïîäâåðãíóò íè îäíîé ñòîðîíîé.

Äåòàëè ïðîòîêîëà áåçîïàñíîé îöåíêè ñõåìû ìîæíî íàéòè â [831].

6.3 Àíîíèìíàÿ øèðîêîâåùàòåëüíàÿ ïðåäàà÷à ñîîáùåíèé

Âàì íå óäàñòñÿ ïîíáäàòü ñ êîì ïàíåå êðèïòîãðàôà è íå îêàçàòüñÿ ñðåäè îæåñòî÷åííîé ïðåíàëèê. Â [321] Äýâèä ×àóì ââîäèò Ïðîáëåìó îáùàåò ôðèïòîãðàôà:

> Òðè êðèïòîãðàôà ñèäÿò çà îáåäîì â ñâîåì ëþáèìîì ðåñòîðàíå. Èõ îôèöèàíò ñîîáùàåò èì, ÷òî ìåòðäîòàëü ïðèíÿë íåîáõîäèìûå ìåðû, ÷òîáû ñ÷åò ìîæíî áûëî îïëàòèòü àíîíèìíî. Çà îáåä ìîã áû çàïëàòèòü îäèí èç êðèïòîãðàôîâ ëèê NSA. Òðè êðèïòîãðàôà î÷åíü óâàæàþò ïðàâî êàæäîãî èç íèõ çàïëàòèòü àíîíèìíî, íî èì õîòåëîñü áû çíàòü, çàïëàòèò ëè NSA.

Êàê êðèïòîãðàôàì Àëèñå, Áîáó è Êýðîë óçíàòü, íå çàïëàòèë ëè çà îáåä êòî-íèáóäü èç íèõ, è â òî æå âðåìÿ íå

íàðóøèòü àíîíèìíîñòü ïëàòåëüùèêà? ×àói ðåøàåò ïðîáëåìó:

> Êàæäûé êðèïòîãðàô áðîñàåò íåñìåùåííóþ ìîíåòó, ïðèêðåïëåííóþ ê êîíâåðòó, ìåæäó íèì è êðèïòîãðàôîì ñïðàâà îò íåãî òàê, ÷òî òîëüêî îíè äâîå ìîãóò âèäåòü ðåçóëüòàò. Çàòåì êàæäûé êðèïòîãðàô ãðîìêî îáúÿâëÿåò, óíàäëè ëè äâå ìîíåòû - îäíà åãî è îäíà åãî ëåâîãî ñîñåäà - íà îäíó ëèø íà ðàçëè÷íûå ñòîðîíû. Åñëè ïëàòåëüùèê - îäèí èç êðèïòîãðàôîâ, òî åãî óòâåðæäåíèå ïðîòèâîïîëîæíî òîìó, ÷òî îí âèäèò. Í÷åòíî ÷èñëî çàÿâëåííûõ ðàçëè÷èé çà ñòîëî òèêñîâ óâåëè÷èâàåò êðèïòîãðàô; ÷åòíî ÷èñëî ðàçëè÷èé - ÷òî NSA (ïðè óñëîâèè, ÷òî îáëà ìîæåò áûòü îïëà÷åí òîëüêî îäèí ðàç). Îäíàêî, åñëè îáëà îïëà÷èâàåò êðèïòîãðàô, íèêòî èç äâóõ äðóãèõ íå óçíàåò èç ñäåëàííûõ çàÿâëåíèé, êòî æå êîíêðåòíî îïëàòèë îáëà.

×òîáû óâåëè÷èòü, êàê ýòî ðàáîòàåò, ÷òî Àëèñà ïûòàåòñÿ ïîíÿòü, êòî èç äâóõ äðóãèõ êðèïòîãðàôîâ çàïëàòèë çà îáëà (ïðè óñëîâèè, ÷òî íå îíà è íå NSA). Åñëè îíà âèäèò äâå ðàçëè÷íûõ ìîíåòû, òî ëèáî îáà äðóãèõ êðèïòîãðàôà (Áîá è Êýðîë) ñêàçàëè, "Ïàéíâîâûå" èëè îáà ñêàçàëè, "ðàçíûå". (Ï î ì íèòå, íå÷åòíå ÷èñëî êðèïòîãðàôîâ, ãîâîðÿùèõ "ðàçíûå" óêàçûâàåò, ÷òî îïëàòèë êòî-òî èç íèõ.). Åñëè îáà ñêàçàëè "ðàçíûå", òî ïëàòåëüùèê - êðèïòîãðàô, ñèäÿùèé áëèæå ðåäêî ê ìîíåòå, ðåçóëüòàò áðîñêà êîòîðîé òîò æå, ÷òî è ó ñêðûòîé ìîíåòû (áðîøåííîé ìåæäó Áîáîì è Êýðîë). Åñëè îáà ñêàçàëè "îäèíàêîâûå", òî ïëàòåëüùèê - êðèïòîãðàô, ñèäÿùèé áëèæå ðåäêî ê ìîíåòå, ðåçóëüòàò áðîñêà êîòîðîé îòëè÷àåòñÿ îò ðåçóëüòàòà áðîñêà ñêðûòîé ìîíåòû. Îäíàêî, åñëè Àëèñà âèäèò äâå îäèíàêîâûõ ìîíåòû, òî ëèë Áîá ñêàçàë, "îäèíàêîâûå", à Êýðîë - "ðàçíûå", èëè Áîá ñêàçàë "ðàçíûå", à Êýðîë - "îäèíàêîâûå". Åñëè ëè ñêðûòàÿ ìîíåòà - òàêàÿ æå êàê è âèäèìûå åé äâå ìîíåòû, òî ïëàòåëüùèê - êðèïòîãðàô, êîòîðûé ñêàçàë, "ðàçíûå". Åñëè ñêðûòàÿ ìîíåòà îòëè÷íà îò âèäèìûõ åé äâóõ ìîíåò, òî ïëàòåëüùèê - êðèïòîãðàô, êîòîðûé ñêàçàë "îäèíàêîâûå". ×òîáû îïðåäåëèòü, êòî ïëàòèë, âî âñåõ ýòèõ ñëó÷àÿõ Àëèñà äîëæíà çíàòü ðåçóëüòàò áðîñêà ìîíåòû ìåæäó Áîáîì è Êýðîë.

Ýòîò ïðîòîêîë ìîæåò áûòü îáúåäèíåí íà ëþáîå êîëè÷åñòâî êðèïòîãðàôîâ, êîòîðûå ñèäÿò î êðóãó è áðîñàþò ìîíåòû ìåæäó ñîáîé. Êàæäàÿ ïàðà êðèïòîãðàôîâ âûïîëíÿåò ïðîòîêîë. Êîíå÷íî, îíè çíàþò, êòî ïëàòèò, íî êòî-òî, íàáëþäàþùèé çà ïðîòîêîëîì ìîæåò ñêàçàòü òîëüêî, ÷òî çàïëàòèë îäèí èç êðèïòîãðàôîâ ëèë NSA, íî íå ñîæåò óêàçàòü, êàêîé èç êðèïòîãðàôîâ ïëàòèë.

Ïðèìåíèì ýòîò ïðîòîêîë âûõîäèò äàëåêî çà ïðåäåëû îáëàäíîãî ñòîëà. Âîò ïðèìåð **áåçóñëîâíîãî îòïðàâèòåëÿ è íåîòëåæèâàåìîãî îòïðàâèòåëÿ**. Åðóïïà ïîëüçîâàòåëåé ñåòè ìîæåò èñïîëüçîâàòü ýòîò ïðîòîêîë äëÿ îòïðàâëåíèÿ àíîíèìíûõ ñîîáùåíèé.

(1) Ï îëüçîâàòåëè óïîðÿäî÷èâàþòñÿ ïî êðóãó.

(2) ×åðåç ðåãóëÿðíûå èíòåðâàëû âðåìåíè ñîñåäíèå ïàðû ïîëüçîâàòåëåé áðîñàþò ìåæäó ñîáîé ìîíåòó, èñïîëüçóÿ êàêîé-íèáóäü áåçîïàñíûé îò çëîóìûøëåíèêîâ ïðîòîêîë áðîñàíèÿ "÷åñòíî" ìîíåòû.

(3) Ï îñëå êàæäîãî áðîñêà êàæäûé ïîëüçîâàòåëü îáúÿâëÿåò ëèáî "îäèíàêîâûå", ëèáî "ðàçíûå".

Åñëè Àëèñà õî÷åò ïåðåäàòü øèðîêîâåùàòåëüíîå ñîîáùåíèå, îíà ïðîñòî íà÷èíàåò èíâåðòèðîâàòü ñâîå óòâåðæäåíèå â òåõ ðàóíäàõ, êîòîðûå ñîîòâåòñòâóþò 1 â äâîè÷íîì ïðåäñòàâëåíèè åå ñîîáùåíèÿ. Íàïðèìåð, åñëè åå ñîîáùåíèå áûëî "1001", îíà èíâåðòèðóåò åå óòâåðæäåíèå, ñîîáùèò ïðàâó, ñîîáùèò ïðàâó, è çàòåì èíâåðòèðóåò ñîîâà óòâåðæäåíèå. Ïðè óñëîâèè, ÷òî ðåçóëüòàòîì åå áîñêîâ áûëî "ðàçíûå", "îäèíàêîâûå", "îäèíàêîâûå", "îäèíàêîâûå", îíà áóäåò ãâîñòèò "îäèíàêîâûå", "îäèíàêîâûå ", "îäèíàêîâûå", "ðàçíûå".

Åñëè Àëèñà çàìå÷àåò, ÷òî ïîëíûé ðåçóëüòàò íå ñîîòâåòñòâóåò ñîîáùåíèþ, êîòîðîå îíà ïðîáóåò ïîñûëàòü, îíà ïîíèìàåò, ÷òî â ýòî æå âðåìÿ êòî-òî åùå ïûòàåòñÿ ïîñûëàòü ñîîáùåíèå. Òîãäà îíà ïðåðâàåò ïðåäàч ñîîáùåíèÿ è âûæèäàåò ñëó÷àéíîå êîëè÷åñòâî âðåìåíè. Òî÷íûå ïàðàìåòðû äîëæíû áûòü âûðàáîòàíû íà ïñíîâå òðåòüåãî ñîîáùåíèé â ñåòè, íî èäåÿ äîñòàòî÷íî ïîíÿòíà.

×òîáû ñäåëàòü äåëî åùå áîëåå èíòåðåñíûì, ýòè ñîîáùåíèÿ ìîãóò áûòü çàøèôðîâàíû îòêðûòûì êëþ÷îì äðóãîãî ïîëüçîâàòåëÿ. Çàòåì, êîãäà êàæäûé ïðèíèìàåò ñîîáùåíèå (ïðåòè÷åñêàÿ ðåàëèçàöèÿ äîëæíà âêëþ÷àòü ñòàíäàðòíûå çàãîëîâêè è îêîí÷àíèÿ ñîîáùåíèé), òîëüêî îòðåäàêòèðîâàííûé ïîëó÷àòåëü ñìîæåò ðàñøèôðîâàòü è ïðî÷åñòü ñîîáùåíèå. Íèêòî äðóãîé íè÷åãî íå óçíàåò ïðî ìåòàäàííûå çàÿâëåíèé, òî÷íîå èç äâóõ äðóãèõ íå óçíàåò òî, æå ñàìóþ ïîñëåäîâàòåëüíîñòü ïîñåùåíèé è ñîáëþäåíèé ôîðìû ìåæïîëüçîâàòåëüñêîãî îáùåíèÿ, òî àíàëèç òðàôèêà, îòñëåæèâàþùèé è ñîáëþäåíèé ôîðìû ìåæïîëüçîâàòåëüñêîãî îáùåíèÿ.

×òîáû ñäåëàòü äåëî åùå áîëåå èíòåðåñíûì, ýòè ñîîáùåíèÿ ìîãóò áûòü çàøèôðîâàíû îòêðûòûì êëþ÷îì äðóãîãî ïîëüçîâàòåëÿ. Çàòåì, êîãäà êàæäûé ïðèíèìàåò ñîîáùåíèå (ïðåòè÷åñêàÿ ðåàëèçàöèÿ äîëæíà âêëþ÷àòü ñòàíäàðòíûå çàãîëîâêè è îêîí÷àíèÿ ñîîáùåíèé), òîëüêî îòðåäàêòèðîâàííûé ïîëó÷àòåëü ñìîæåò ðàñøèôðîâàòü è ïðî÷åñòü ñîîáùåíèå. Íèêòî äðóãîé íè÷åãî íå óçíàåò ïðî ìåòàäàííûå çàÿâëåíèé, òî÷íîå èç äâóõ äðóãèõ íå óçíàåò òî, æå ñàìóþ ïîñëåäîâàòåëüíîñòü ïîñåùåíèé è ñîáëþäåíèé ôîðìû ìåæïîëüçîâàòåëüñêîãî îáùåíèÿ, òî àíàëèç òðàôèêà, îòñëåæèâàþùèé è ñîáëþäåíèé ôîðìû ìåæïîëüçîâàòåëüñêîãî îáùåíèÿ, äåñïîëåçåí.

Àëüòåðíàòèâíî ìîæíî ìåæäó ñîîáùåíèÿìè ñòîðîíàìè ìîãëî áûòü çàïèñàíî íà CD-ROM, èëè îäèí ëåíèâûé ïàðòíåð áûë ïîñëàí ñ äîñòàâêîé íà äîì. Âîçìîæíî, ñòîðîíû ìîãëè áû õðàíèòü ôàéë (êîíå÷íî, â çàøèôðîâàííîì âèäå). Èëè, îíè ìîãëè áû äîãîâîðèòüñÿ èñïîëüçîâàòü ñîâìåñòíûé êðèïòîãðàôè÷åñêè áåçîïàñíûé ãåíåðàòîð ïñåâäîñëó÷àéíûõ ÷èñåë, è êàæäûé èç íèõ ñìîã áû ãåíåðèðîâàòü äëÿ ïðîòîêîëà òó æå ñàìóþ ïîñëåäîâàòåëüíîñòü ïñåâäîñëó÷àéíûõ áèòîâ.

Ïðîáëåìîé ýòîãî ïðîòîêîëà ÿâëÿåòñÿ òî, ÷òî õîòÿ ìîøåííè÷àþùèé ó÷àñòíèê è íå ñìîæåò ÷èòàòü íèêàêèõ ñîîáùåíèé, îí ìîæåò íåçàìåòíî èñïîðòèòü âñþ ñèñòåìó, ïîñòîÿííî îáìàíûâàÿ íà ýòàïå (3). Ñóùåñòâóåò ìîäèôèêàöèÿ ïðåäûäóùåãî ïðîòîêîëà, ïîçâîëÿþùàÿ îáíàðóæèòü âðåäîíîñíûõ [1578, 1242]. Ýòà ïðîáëåìà íàçûâàåòñÿ "Îáùàþùèå êðèïòîãðàôû â äèñêîòåêå".

6.4 Ýëåêòðîííûå íàëè÷íûå

Íàëè÷íûå äåíüãè - ýòî ïðîáëåìà. Ðàçäðàæåò èõ íîñèòü, îíè ñïîñîáíû âûçâàòü ðàñïðîñòðàíåíèå ìèêðîáîâ, ëþäè ìîãóò êðàñòü èõ ó Âàñ. ×åêè è êðåäèòíûå êàðòî÷êè óìåíüøèëè êîëè÷åñòâî íàëè÷íûõ äåíåã, îáîðîòû êîòîðûõ, íî ïîëíîå óäàëåíèå íàëè÷íûõ äåíåã îáåñöåíèëî áû ýêîíîìèêó. Ýòîãî íèêîãäà íå ïðîèçîéäåò; òîðãîâöû íàðêîòèêàìè è ïîëèòèê÷åñêèå äåÿòåëè íèêîãäà ýòîãî íå äîïóñòÿò. ×åêè è êðåäèòíûå êàðòî÷êè ìîæíî ïðîñëåäèòü, âû íå ìîæåòå ñêðûòüñÿ îò òîãî, êîìó äàëè äåíüãè.

Ñ äðóãîé ñòîðîíû, ÷åêè è êðåäèòíûå êàðòî÷êè ïîçâîëÿþò ëþäÿì âòîðãàòüñÿ â âàøó ëè÷íóþ æèçíü êàê íèêîãäà ïðåæäå. Âû íèêîãäà íå äîïóñòèëè áû, ÷òîáû ïîëèöèÿ âñþ æèçíü õîäèëà çà âàìè ïî ïÿòàì, íî ïîëüçîâàòåëè ìîãóò ïðîñëåäèòü âàøè ôèíàíñîâûå îïåðàöèè. Î íè ìîãóò âëàäåü, ãäå âû ïîêóïàåòå ãàç, ãäå âû ïîêóïàåòå åäó, êîìó âû çâîíèòå ïî òåëåôîíó, è âñå ýòî íå îòðûâàÿñü îò ñâîèõ êîìïüþòåðíûõ òåðìèíàëîâ. Ëþäè äîëæíû óìåòü çàùèòèòü ñâîþ àíîíèìíîñòü, ÷òîáû çàùèòèòü ñâîè ëè÷íûå òàéíû.

Ê ñ÷àñòüþ, ñóùåñòâóþò ñëîæíûé ïðîòîêîë, êîòîðûé ðàçðåøàåò èñïîëüçîâàíèå çàâåðåííûõ, íî íåîòëåæèâàåìûõ ñîîáùåíèé. Ëîááèñò Àëèñà ìîæåò ïðåäàòü **ýëåêòðîííûå äåíüãè** êîíãðåññìåíó Áîáó òàê, ÷òîáû ãàçåòíûé ðåïîðòåð Åâà íè÷åãî íå óçíàëà áû îá Àëèñå. Áîá ìîæåò çàòåì âîñïèòü ýòè ýëåêòðîííûå äåíüãè íà ñâîé áàíêîâñêèé ñ÷åò, äàæå åñëè áàíê íå òðåáóåò îò Àëèñû íèêàêîãî ïðåäñòàâëåíèÿ. Íî åñëè Àëèñà ïðîáóåò ïîêóïàòü êîêàèí íà òó æå ñàìóþ ïîðöèþ ýëåêòðîííûõ äåíåã, êîòîðóþ îíà èñïîëüçîâàëà äëÿ ïîäêóïà Áîáà, îíà áóäåò îáíàðóæåíà áàíêîì. È åñëè Áîá ïðîáóåò âîñïèòü ïðöèþ äåíåã íà äâà ðàçëè÷íûõ ñ÷åòà, ýòî áóäåò îáíàðóæåíî, íî Áîá, êàê è Àëèñà, îñòàíåòñÿ î àíîíèìíû. È íîâàÿ ýòî íàçûâàåòñÿ **àíîíèìíûì ýëåêòðîííûì äåíüãàìè**, ÷òîáû ìîæíî áûëî îöèôðîâàòü òî òðåáîâàíèå ýëåêòðîííûõ äåíåã, òèïà êðåäèòíûõ êàðòî÷åê.

Â ïîäîáíûõ âåùàõ ñóùåñòâóåò áîëüøàÿ îùåñòâåííàÿ íåîáõîäèìîñòü. Ñ ðîñòîì èñïîëüçîâàíèÿ Internet äëÿ êîìåð÷åñêèõ îïåðàöèé ðàñòåò è ïîòðåáíîñòè â ñåêðåòíîñòè ïðåäàâàòåìî ïî ñåòè èíôîðìàöèè è àíîíèìíîñòè ïðè ïîêóïêàõ â Internet.) Ñ äðóãîé ñòîðîíû, áàíêè è ïðàâèòåëüñòâà, ïî âèäèìîìó, íå ïîæåëàþò óñòóïèòü êîíòðîëü íàä ñîâðåìåííûìè áàíêîâñêèìè ñèñòåìàìè. Õîòÿ èì ïðèäåòñÿ ýòî ñäåëàòü. Âñå, ÷òî ïîòðåáóåòñÿ, ÷òîáû ýëåêòðîííûå äåíüãè âîøëè â ìîäó, - ýòî ïîÿâëåíèå íåêîòîðîãî çàñëóæåííàþùåãî äîâåðèÿ óíåæäåíèÿ, æåëàþùåãî ïðåáûâàíèÿ öèôðû â ðåàëüíûå äåíüãè.

Ïðîòîêîëû ýëåêòðîííûõ äåíåã î÷åíü ñëîæíû. Äàëüøå ìû øàã çà øàãîì ïîñòðîèì îäèí èç íèõ. Áîëåå ïîäðîáíî îá ýòîì ïðîòîêîëå ìîæíî ïðî÷èòàòü â [318, 339, 325, 335, 340]. Íî ïîìíèòå, ýòî òîëüêî îäèí èç íèõ. Áîëüøèíñòâî ýëåêòðîííûõ äåíåã, ñóùåñòâóþò è äðóãèå.

Ïðîòîêîë ¹1

Ïåðâûå íåñêîëüêî ïðîòîêîëîâ ïðåäñòàâëÿþò ñîáîé ôèçè÷åñêèå àíàëîãè ôèçè÷åñêèõ ïðîòîêîëîâ. Ñëåäóþùèé ïðîòîêîë ÿâëÿåòñÿ óïðîùåííûì ôèçè÷åñêèì ïðîòîêîëîì äëÿ àíîíèìíûõ äåíåæíûõ ÷åêîâ:

(1) Àëèñà ãîòîâèò 100 àíîíèìíûõ äåíåæíûõ ÷åêîâ ïî $1000 êàæäûé.

(2) Àëèñà âêëàäûâàåò êàæäûé èç íèõ è ëèñòîê êîïèðîâàëüíîé áóìàãè â 100 ðàçëè÷íûõ êîíâåðòîâ è îòíîñèò âñå êîíâåðòû â áàíê.

(3) Áàíê îòêðûâàåò 99 êîíâåðòîâ è óáåæäàåòñÿ, ÷òî êàæäûé ÷åê âûïèñàí íà $1000.

(4) Áàíê ïîäïèñûâàåò äâóñòîðîííþ îñòàøéñÿ íåðàñïå÷àòàííûì êîíâåðò. Ñ ïîìîùüþ êîïèðîâàëüíîé áóìàãè ïîäïèñü ïåðåíîñèò íà ÷åê. Áàíê âîçâðàùàåò íåðàñïå÷àòàííûé êîíâåðò Àëèñå è ñïèñûâàåò $1000 ñ åå ñ÷åòà.

(5) Àëèñà âñêðûâàåò êîíâåðò è îòäàåò äåíåæíûé ÷åê ïðîäàâöó.

(6) Ïðîäàâåö ïðîâåðÿåò áàíêîâñêóþ ïîäïèñü, óáåæäàÿñü â çàêîííîñòè äåíåæíîãî ÷åêà.

(7) Ïðîäàâåö îòíîñèò äåíåæíûé ÷åê â áàíê.

(8) Áàíê ïðîâåðÿåò ñâîþ ïîäïèñü è íà÷èñëÿåò $1000 íà ñ÷åò ïðîäàâöà.

Ýòîò ïðîòîêîë ðàáîòàåò. Áàíê íå âèäèò äåíåæíûé ÷åê, êîòîðûé îí ïîäïèñûâàåò, ïîýòîìó, êîãäà ïðîäàâåö ïðèíåñåò ÷åê â áàíê, áàíê íèêîãäà íå óçíàåò, ÷òî ýòî ÷åê Àëèñû. Áëàãîäàðÿ ïîäïèñè áàíêà óâåæàåí â çàêîííîñòè ÷åêà. À èç-çà ïðîòîêîëà "ðàçðåçàòü è âûáðàòü" (ñì. ðàçäåë 5.1) áàíê óâåðåí, ÷òî íåðàñïå÷àòàííûé äåíåæíûé ÷åê - íà ñóìó $1000 (à íå $100000 èëè $100000000). Î í ïðîâåðÿåò îñòàëüíûå 99 êîíâåðòîâ, ïîýòîìó âåðîÿòíîñòü îáìàíà áàíêà Àëèñîé ñîñòàâëÿåò òîëüêî 1 ïðîöåíò. Êîíå÷íî, áàíê íàçíà÷èò çà îáìàí äîñòàòî÷íî áîëüøîé øòðàô, òàêîé, ÷òîáû íå ñòîèëî ìîøåííè÷àòü. Âåäü åñëè áàíê ïðîñò îòêàæåòñÿ ïîäïèñàòü ïîñëåäíèé ÷åê (åñëè Àëèñà ïîéìàíà íà îáìàíå), íå øòðàôóÿ Àëèñó, îíà ïðîäîëæèò ñâîè ïîïûòêè, ïîêà åé íå ïîâåçåò. Ëó÷øåå ñðåäñòâî óñòðàøåíèÿ - ýòî òþðåìíîå çàêëþ÷åíèå.

Ïðîòîêîë ¹2

Ïðåäûäóùèé ïðîòîêîë íå äàåò Àëèñå íàïèñàòü ÷åê íà ñóì ìó, îòëè÷íóþ îò çàÿâëåííîé, íî îí íå ìåøàåò åé îòêðûòîìó ïðîòîêîëó è èñïîëüçîâàòü åãî äâàæäû. Ýòî íàçûâàåòñÿ **ïðîáëåìîé ïîâòîðíîé îïëàòû**; äëÿ åå ðåøåíèÿ ïðèäóìàíû óñëîæíåíèÿ ïðîòîêîëà:

(1) Àëèñà ãîòîâèò 100 àíîíèìíûõ äâóõôàçíûõ ÷åêîâ ïî $1000 êàæäûé. Ê êàæäîìó äâóõôàçíîìó ÷åêó îíà äîáàâëÿåò óíèêàëüíóþ ñòðîêó, âûðàæåíóþ ñëó÷àéíûì îáðàçîì è äîñòàòî÷íî äëèííóþ, ÷òîáû âåðîÿòíîñòü èñïîëüçîâàíèÿ ýòîé ñòðîêè äðóãèì ÷åëîâåêîì áûëà ïðåíåáðåæèìî ìàëà.

(2) Àëèñà âêëàäûâàåò êàæäûé èç íèõ è ëèñòîê êîïèðîâàëüíîé áóìàãè â 100 ðàçëè÷íûõ êîíâåðòîâ è îòíîñèò âñå êîíâåðòû â áàíê.

(3) Áàíê îòêðûâàåò 99 êîíâåðòîâ è óáåæäàåòñÿ, ÷òî êàæäûé ÷åê âûïèñàí íà $1000.

(4) Áàíê ïîäïèñûâàåò åäèíñòâåííûé îñòàâøèéñÿ íåðàñïå÷àòàííûì êîíâåðò. Ñ ïîìîùüþ êîïèðîâàëüíîé áóìàãè ïîäïèñü ïåðåíîñèòñÿ íà ÷åê. Áàíê âîçâðàùàåò íåðàñïå÷àòàííûé êîíâåðò Àëèñå è ñîîáùàåò $1000 ñ åå ñ÷åòà.

(5) Àëèñà âñêðûâàåò êîíâåðò è îòäàåò äåíåæíûé ÷åê ïðîäàâöó.

(6) Ïðîäàâåö ïðîâåðÿåò áàíêîâñêóþ ïîäïèñü, óáåæäàÿñü â çàêîííîñòè äåíåæíîãî ÷åêà.

(7) Ïðîäàâåö îòíîñèò äåíåæíûé ÷åê â áàíê.

(8) Áàíê ïðîâåðÿåò ñâîþ ïîäïèñü è ïî ñâîåé áàçå äàííûõ óáåæäàåòñÿ, ÷òî äåíåæíûé ÷åê ñ òàêîé óíèêàëüíîé ñòðîêîé ðàíåå íå äåïîíèðîâàëñÿ. Åñëè ýòî òàê, áàíê íà÷èñëÿåò $1000 íà ñ÷åò ïðîäàâöà è çàïèñûâàåò óíèêàëüíóþ ñòðîêó â áàçó äàííûõ.

(9) Åñëè äåíåæíûé ÷åê óæå áûë äåïîíèðîâàí ðàíåå, áàíê îòêàçûâàåòñÿ ïðèíÿòü åãî.

Òàïåðü, åñëè Àëèñà ïîïûòàåòñÿ ðàñïëàòèòüñÿ êñåðîêîïèåé äåíåæíîãî ÷åêà èëè ïðîäàâöó ïîïûòàåòñÿ äåïîíèðîâàòü äåíåæíûé ÷åê ïîâòîðíî, èñïîëüçóÿ êñåðîêîïèþ, áàíê óçíàåò îá ýòîì.

Ïðîòîêîë ¹3

Ïðåäûäóùèé ïðîòîêîë çàùèùàåò áàíê îò ìîøåííèêîâ, íî íå óñòàíàâëèâàåò èõ ëè÷íîñòü. Áàíê íå çíàåò, ïîïûòàëñÿ ëè ÷åëîâåê, êîòîðûé ïîëó÷èë ÷åê (áàíê íè÷åãî íå çíàåò îá Àëèñå), îòìàíóòü ïðîäàâöà, èëè ïðîäàâåö ïûòàåòñÿ îáìàíóòü áàíê. Ýòà íåîäíîçíà÷íîñòü èñïðàâëÿåòñÿ ñëåäóþùèì ïðîòîêîëîì:

(1) Àëèñà ãîòîâèò 100 àíîíèìíûõ äâóõôàçíûõ ÷åêîâ ïî $1000 êàæäûé. Ê êàæäîìó äâóõôàçíîìó ÷åêó îíà äîáàâëÿåò óíèêàëüíóþ ñòðîêó, âûðàæåíóþ ñëó÷àéíûì îáðàçîì è äîñòàòî÷íî äëèííóþ, ÷òîáû âåðîÿòíîñòü èñïîëüçîâàíèÿ ýòîé ñòðîêè äðóãèì ÷åëîâåêîì áûëà ïðåíåáðåæèìî ìàëà.

(2) Àëèñà âêëàäûâàåò êàæäûé èç íèõ è ëèñòîê êîïèðîâàëüíîé áóìàãè â 100 ðàçëè÷íûõ êîíâåðòîâ è îòíîñèò âñå êîíâåðòû â áàíê.

(3) Áàíê îòêðûâàåò 99 êîíâåðòîâ è óáåæäàåòñÿ, ÷òî êàæäûé ÷åê âûïèñàí íà $1000, è ÷òî âñå ñëó÷àéíûå ñòðîêè ðàçëè÷íû.

(4) Áàíê ïîäïèñûâàåò åäèíñòâåííûé îñòàâøèéñÿ íåðàñïå÷àòàííûì êîíâåðò. Ñ ïîìîùüþ êîïèðîâàëüíîé áóìàãè ïîäïèñü ïåðåíîñèòñÿ íà ÷åê. Áàíê âîçâðàùàåò íåðàñïå÷àòàííûé êîíâåðò Àëèñå è ñîîáùàåò $1000 ñ åå ñ÷åòà.

(5) Àëèñà âñêðûâàåò êîíâåðò è îòäàåò äåíåæíûé ÷åê ïðîäàâöó.

(6) Ïðîäàâåö ïðîâåðÿåò áàíêîâñêóþ ïîäïèñü, óáåæäàÿñü â çàêîííîñòè äåíåæíîãî ÷åêà.

(7) Ïðîäàâåö ïðîñèò Àëèñó íàïèñàòü ñëó÷àéíóþ èäåíòèôèêàöèîííóþ ñòðîêó íà äåíåæíîì ÷åêå.

(8) Àëèñà âûïîëíÿåò ýòî.

(9) Ïðîäàâåö îòíîñèò äåíåæíûé ÷åê â áàíê.

(10) Áàíê ïðîâåðÿåò ñâîþ ïîäïèñü è ïî ñâîåé áàçå äàííûõ óáåæäàåòñÿ, ÷òî äåíåæíûé ÷åê ñ òàêîé óíèêàëüíîé ñòðîêîé ðàíåå íå äåïîíèðîâàëñÿ. Åñëè ýòî òàê, áàíê íà÷èñëÿåò $1000 íà ñ÷åò ïðîäàâöà è çàïèñûâàåò óíèêàëüíóþ ñòðîêó â áàçó äàííûõ.

(11) Åñëè óíèêàëüíàÿ ñòðîêà óæå åñòü â áàçå äàííûõ, áàíê îòêàçûâàåòñÿ ïðèíÿòü äåíåæíûé ÷åê è ñðàáîòàåò èäåíòèôèêàöèîííóþ ñòðîêó íà äåíåæíîì ÷åêå ñ õðàíèìîé â áàçå äàííûõ. Åñëè îíè ñîâïàäàþò, òî áàíê óáåæäàåòñÿ, ÷òî êîïèÿ áûëà ñîçäàíà ïðîäàâöîì. Åñëè èäåíòèôèêàöèîííûå ñòðîêè ðàçëè÷íû, òî áàíê çíàåò, ÷òî ÷åê áûë ñêîïèðîâàí ÷åëîâåêîì, êîòîðûé åãî âîîáùå.

Â ýòîì ïðîòîêîëå ïðåäïîëàãàåòñÿ, ÷òî ïðîäàâåö íå ìîæåò èçìåíèòü èäåíòèôèêàöèîííóþ ñòðîêó ïîñëå òîãî,

êàê Àëèñà íàïèøåò åå íà äâíàäöàòè÷åêå. Íà äâíàäöàòè÷åêå ìîãó áû íàõîäèòüñÿ ðÿä íåáîëüøèõ êâàäðàòîâ, êîòîðûå ïî ðàçìåðàì îòðàæàþò òîðãîâöà Àëèñà äîëæíà çàïîëíèòü êðåñòèêàìè èëè íîëèêàìè. Äâíàäöàòûé ÷åê ìîãó áûòü ñäåëàí èç áóìàãè, êîòîðàÿ ðâåòñÿ ïðè èñïàðåíèÿõ.

Òàê êàê ïðîäâåö è áàíê âçàèìîäåéñòâóþò ïîñëå òîãî, êàê Àëèñà ïîðàçèò äåíüãè, ïðîäàâöó ìîãóò âñ÷èòü ïëîñêîäííóþ ÷åê. Ïðàêòè÷åñêè ðåàëèçàöèè ýòîãî ïðîòîêîëà ìîãëè áû ïîðåãóëèðîâàòü îò Àëèñû ïîäîæäàòü ó êàññîâîãî àïïàðàòà, ïîêà ïðîäâåö áóäåò ðàçáèðàòüñÿ ñ áàíêîì, òî÷íî òàêæå, êàê ýòî ïðîèñõîäèò ñåãîäíÿ ïðè îáðàáîòêå ïëàòåæåé ñ èñïîëüçîâàíèåì êðåäèòíûõ êàðòî÷åê.

Àëèñà òàêæå ìîæåò ïðèñîåäèíèòüñÿ è ê ýòîìó. Îíà ìîæåò ïîðàòèòü êîïèþ äåíåæíîãî ÷åêà âòîðîé ðàç, íàïèñàâ òó æå ñàìóþ èäåíòèôèêàöèîííóþ ñòðîêó íà ýòàïå (7). Åñëè ïðîäàâåö íå âåäåò áàçó äàííûõ óæå ïîëó÷åííûõ äåíåæíûõ ÷åêîâ, îí áóäåò ââåäåí â çàáëóæäåíèå. Ýòó ïðîáëåìó óñòðàíÿåò ñëåäóþùèé ïðîòîêîë.

Ïðîòîêîë ¹4

Åñëè îêàæåòñÿ, ÷òî ÷åëîâåê, âûïèñàâøèé áàíêîâñêèé ÷åê, ïîïûòàëñÿ îáìàíóòü ïðîäàâöà, òî áàíê ìîæåò çàõîòåòü ëè÷íîñòü ýòîãî ÷åëîâåêà. ×òîáû ñäåëàòü ýòî, ïðèäåòñÿ âåðíóòüñÿ îò ôèçè÷åñêîãî àíàëîãèé â ìèð êðèïòîãðàôèè.

×òîáû ñïðÿòàòü èìÿ Àëèñû â ýëåêòðîííîì ÷åêå, ìîæíî âîñïîëüçîâàòüñÿ ìåòîäèêîé ðàçäåëåíèÿ ñåêðåòà.

(1) Àëèñà ãîòîâèò *n* àíîíèìíûõ äâîè÷íûõ ÷åíîâ íà çàäàííóþ ñóììó.

Êàæäûé èç ÷åíîâ ñîäåðæèò óíèêàëüíóþ ñòðîêó, *X*, ïîëó÷åííóþ ñëó÷àéíûì îáðàçîì è äîñòàòî÷íî äëèííóþ, ÷òîáû âåðîÿòíîñòü ïîÿâëåíèÿ âäâóõ îäèíàêîâûõ ñòðîê áûëà ïðåíåáðåæèìî ìàëà.

Íà êàæäîì ÷åêå åñòü òàêæå *n* ïàð áèòîâûõ ñòðîê èäåíòèôèêàòîðè, I_1, I_2, ..., I_n. (Èìåííî òàê, *n* ðàçëè÷íûõ ïàð íà *êàæäîì* ÷åêå.) Êàæäàÿ èç ýòèõ ïàð ãåíåðèðóåòñÿ ñëåäóþùèì îáðàçîì: Àëèñà ñîçäàò ñòðîêó, ñîäåðæàùóþ åå èìÿ, àäðåñ è ïðî÷èå ñâåäåíèÿ, òðåáóåìûå áàíêîì. Çàòåì îíà äåëèò ýòó ñòðîêó íà äâà ÷àñòè, èñïîëüçóÿ ïðîòîêîë äåëåíèÿ ñåêðåòà (ñì. ðàçäåë 3.6) è âðó÷àò êàæäóþ ÷àñòü, èñïîëüçóÿ ïðîòîêîë âðó÷åíèÿ áèòîâ.

Íàïðèìåð, I_{37} ñîñòîèò èç äâóõ ÷àñòåé: I_{37_L} è I_{37_R}. Êàæäàÿ ÷àñòü ïðåäñòàâëÿåò ñîáîé ïàêåò âðó÷åííûõ áèòîâ, êîòîðûé Àëèñó ìîãóò ïîïðîñèòü îòêðûòü, è ÷üå îòêðûòèå ñîäåðæàíèå ìîæåò áûòü ìãíîâåííî ïðîâåðåíî. Ëþáàÿ ïàðà (íàïðèìåð, I_{37_L} è I_{37_R}, íî íå I_{37_L} è I_{38_R}), ðàñêðûâàåò ëè÷íîñòü Àëèñû. Êàæäûé èç ÷åíîâ âûãëÿäèò ñëåäóþùèì îáðàçîì:

Ñóììà

Óíèêàëüíàÿ ñòðîêà: *X*

Ñòðîêè èäåíòèôèêàöèè: $I_1 = (I_{1_L}, I_{1_R})$

$I_2 = (I_{2_L}, I_{2_R})$

....

$I_n = (I_{n_L}, I_{n_R})$

(2) Àëèñà ìàñêèðóåò âñå *n* ÷åêîâ ñ ïîìîùüþ ïðîòîêîëà ñëåïîé ïîäïèñè è îòíîñèò ÷åêè â áàíê.

(3) Áàíê ïðîñèò Àëèñó ñíÿòü ìàñêèðîâêó ñ *n-1* äâíàäöàòè ÷åêîâ è óâåäîìèòü, ÷òî âñå îíè ïðàâèëüíî îòìå÷åíû. Áàíê ïðîâåðÿåò ñóììó, óíèêàëüíóþ ñòðîêó è ïðîñèò Àëèñó ðàñêðûòü âñå ñòðîêè èäåíòèôèêàöèè.

(4) Åñëè áàíê óâîëåíåíîðåí, íå îáíàðóæèâ ïîïûòîê ìîøåííè÷åñòâà, îí ïîäïèñûâàåò îòâåòíóþ çàìàñêèðîâàííóþ äâîè÷íóþ ÷åê Àëèñå è ñîîáùàåò ñóììó ñ åå ñ÷åòà.

(5) Àëèñà ñíèìàåò ìàñêèðîâêó ñ ÷åêà è òðàòèò åãî ó ïðîäàâöà.

(6) Ïðîäàâåö ïðîâåðÿåò áàíêîâñêóþ ïîäïèñü, óâåæäàÿñü â çàêîííîñòè äâîè÷íîãî ÷åêà.

(7) Ïðîäàâåö ñëó÷àéíûì îáðàçîì ïðîñèò Àëèñó ðàñêðûòü ëèáî ëâûå, ëèáî ïðàâûå ïîëîâèíû âñåõ ñòðîê èäåíòèôèêàöèè íà ÷åêå. Ï î ñóòè, ïðîäàâåö âûäàåò Àëèñå ñëó÷àéíóþ *n*-áèòîâóþ **ñòðîêó-ñåëåêòîð**, b_1, b_2, ..., b_n. Ëâóþ èëè ïðàâóþ ïîëîâèíó I_i îòêðûâàåò Àëèñà, çàâèñèò îò çíà÷åíèÿ b_i, 0 èëè 1.

(8) Àëèñà âûïîëíÿåò ýòî.

(9) Ïðîäàâåö îòíîñèò äåíåæíûé ÷åê â áàíê.

(10) Áàíê ïðîâåðÿåò ñâîþ ïîäïèñü è ïî ñâîåé áàçå äàííûõ óâåæäàåòñÿ, ÷òî äåíåæíûé ÷åê ñ òàêîé óíèêàëüíîé ñòðîêîé ðàíåå íà äàííîêðîâàëñÿ. Åñëè ýòî òàê, áàíê íà÷èñëÿåò óêàçàííóþ ñóììó íà ñ÷åò ïðîäàâöà è çàïè-

ñûâàåò óíèêàëüíóþ ñòðîêó â áàçó äàííûõ.

(11) Åñëè óíèêàëüíàÿ ñòðîêà óæå åñòü â áàçå äàííûõ, áàíê îòêàçûâàåòñÿ ïðèíÿòü äåíåæíûé ÷åê è ñðàâíèâàåò èäåíòèôèêàöèîííóþ ñòðîêó íà äåíåæíîì ÷åêå ñ õðàíèìîé â áàçå äàííûõ. Åñëè îíè ñîâïàäàþò, òî áàíê óáåæäàåòñÿ, ÷òî ÷åê áûë ñêîïèðîâàí ïðîäàâöîì. Åñëè èäåíòèôèêàöèîííûå ñòðîêè ðàçëè÷íû, òî áàíê çíàåò, ÷òî ÷åê áûë ñêîïèðîâàí ÷åëîâåêîì, êîòîðûé ãîòîâèë ýòîò äåíåæíûé ÷åê. Òàê êàê âòîðîé ïðîäàâöû, ïîëó÷èâøèé ÷åê, âûäàë Àëèñå äóáëèêàò, ÷åì ïåðâûé, ñòðîêó-ñåëåêòîð, áàíê îáíàðóæèò, ÷òî äëÿ êàêîé-òî èç ïîçèöèé Àëèñà îòêðûëà ëåâóþ ïîëîâèíó ïðîäàâöû, à ïðàâóþ - äóáëîì. Âûïîëíèâ íàä ýòèì ïîëîâèíàì ñòðîê èäåíòèôèêàöèè îïåðàöèþ XOR, áàíê îïðåäåëèò ëè÷íîñòü Àëèñû.

Ýòî âåñüìà èíòåðåñíûé ïðîòîêîë, ïîýòîìó ïîñìîòðèì íà íåãî ñðàçíûõ ñòîðîí.

Ì îæåò ëè Àëèñà ñìîøåííè÷àòü? Åå ýëåêòðîííûå äåíüãè ïðåäñòàâëÿò ñîáîé ïðîñòî áèòû, êîòîðûå îíà ëåãêî ìîæåò ñêîïèðîâàòü. Ï îòðàòèòü èõ â ïåðâûé ðàç - íå ïðîáëåìà, îíà ïðîñòî âûïîëíèò ïðîòîêîë, è âñå ïðîéäåò áåç ïðîáëåì. Ïðîáëåìà âûçâàíà åé íà ýòàïå (7) ñëó÷àéíóþ *n*-áèòîâóþ ñòðîêó-ñåëåêòîð, è Àëèñà îòêðîåò ëèáî ëåâóþ, ëèáî ïðàâóþ ïîëîâèíó êàæäîé I_i íà ýòàïå (8). Íà ýòàïå (10) áàíê çàïèøåò âñå ýòè äàííûå â ìåñòà ñ óíèêàëüíîé ñòðîêîé äåíåæíîãî ÷åêà.

Êîãäà îíà ïîïûòàåòñÿ èñïîëüçîâàòü òå æå ýëåêòðîííûå äåíüãè âòîðîé ðàç, ïðîäàâøè (òîò æå èëè èíîé) âûäàñò åé íà ýòàïå (7) äóáëèðóþùóþ *n*-áèòîâóþ ñòðîêó-ñåëåêòîð. Àëèñà äîëæíà âûïîëíèòü ýòàï (8), åå îòêàç íåìåäëåííî âñòðåâîæèò ïðîäàâöà. Òåïåðü, êîãäà ïðîäàâåö ïðèíñèò äåíüãè â áàíê íà ýòàïå (10), áàíê íåìåäëåííî çàìåòèò, ÷òî äåíåæíûé ÷åê ñ ýòîé óíèêàëüíîé ñòðîêîé óæå áûë äåïîíèðîâàí. Áàíê ñðàâíèâàåò îòêðûòûå ïîêàçàòåëè ñòðîê èäåíòèôèêàöèè. Âåðîÿòíîñòü, ÷òî ïåðâàÿ ïîëîâèíà êîòîðîé ñîâïàäåò ñ ýòîé óíèêàëüíîé ñòðîêîé óæå áûë äåïîíèðîâàí. Áàíê ñðàâíèâàåò îòêðûòûå ïîêàçàòåëè ñîîòâåòñòâóþùèõ 2^n, ýòîãî íå ñëó÷èòñÿ äî ñëåäóþùåãî îëåäåíåíèÿ. Òàïåðü áàíê íàõîäèò ïàðó, ïåðâàÿ ïîëîâèíà êîòîðîé áûëà îòêðûòà â ïåðâûé ðàç, à âòîðàÿ - âî âòîðîé, âûïîëíÿåò íàä ýòèìè ïîëîâèíàìè îïåðàöèþ XOR è èçâëåêàåò èìÿ Àëèñû. Òàê áàíê óçíàåò, êòî ïîïûòàëñÿ âîñïîëüçîâàòüñÿ ÷åêîì äâàæäû.

×òî ýòî ïðîòîêîë íå ìåøàåò Àëèñå ìîøåíè÷àòü, íî åå ìîøåíè÷åñòâî ïî÷òè íàâðÿêà áóäåò îáíàðóæåíî. Ñìîøåíè÷àâ, Àëèñà íå ñìîæåò ñîõðàíèòü â òàéíå ñâîþ ëè÷íóþ ñòîèìîñòü, è ïðîäàâåö íåìåäëåííî çàìåòèò ýòî íà ýòàïå (6).

Àëèñà ìîãëà áû ïîïûòàòüñÿ ïîäñóíóòü áàíêó ïëîõîé äåíåæíûé ÷åê, òàêîé, íà êîòîðîì ñòðîêè èäåíòèôèêàöèè íå ðàñõîäÿòñÿ áóäåò îáíàðóæåíî. Ñòðîêè íå ñîâïàäóò, íî êàêóþ-íèáóäü èç ñòðîê èäåíòèôèêàöèè, èíà÷å èñïîðòèòñÿ áàíêîâñêàÿ ïîäïèñü, è ïðîäàâåö íåìåäëåííî çàìåòèò ýòî íà ýòàïå (6).

Àëèñà ìîãëà áû ïîïûòàòüñÿ ïîäñóíóòü áàíêó ïëîõîé äåíåæíûé ÷åê, òàêîé, íà êîòîðîì ñòðîêè èäåíòèôèêàöèè íå ðàñõîäÿòñÿ ñòðîêè-ñåëåêòîðû. Îíà íå ìîæåò èçìåíèòü íè îäèí áèò, íå çíàÿ ñîîòâåòſòâóþùèõ áèòîâ èñõîäíûõ ñòðîê. Îíà íå ìîæåò èçìåíèòü íè îäèí áèò, íå íàðóøèâ ïîäïèñü. Îíà íå ìîæåò èçìåíèòü íè îäèí áèò, íå ïîòåðÿâ ñòðîêè èäåíòèôèêàöèè. Âåðîÿòíîñòü, ÷òî òàêàÿ óãîâêà ïîñòîÿííî, íî åñëè øòðàô çà ìîøåííè÷åñòâî áûë äîñòàòî÷íî âûñîêèì, òî áàíê íå ñìîæåò ìîøåííè÷àòü, îáâèíÿÿ Àëèñó, òàê êàê òîëüêî îíà ìîæåò îòêðûòü ëþáóþ ñòðîêó èäåíòèôèêàöèè.

Íå ïîìîæåò îáìàíóòü áàíê è ëþáîé ñâîáîä ìåæäó Àëèñîé è ïðîäàâöîì. Åñëè áàíê ïîäïèñàë äåíåæíûé ÷åê ñ óíèêàëüíîé ñòðîêîé, îí ìîæåò áûòü óâåðåí â òîì, ÷òî ýòîò ÷åê áóäåò îïëà÷åí òîëüêî îäèí ðàç.

À êàê íàñ÷åò áàíêà? Ì îæåò ëè îí âû÷èñëèòü, ÷òî äåíåæíûé ÷åê, ïîëó÷åííûé îò ïðîäàâöà, ýòî è åñòü òîò ñàìûé ÷åê, êîòîðûé íàì ñêàçàë Àëèñà? Íà ýòàïàõ (2)-(5) Àëèñà çàùèùåíà ïðîòîêîëîì ñëåïîé ïîäïèñè. Áàíê íå ìîæåò ñâÿçàòü Àëèñó è ÷åê, äàæå åñëè îí îïëà÷åí. Áàíê ìîæåò ïîäïèñàòü ñîîáùåíèå, ñîäåðæàùåå ñëó÷àéíûå áèòû, è ïîòîì ïîïðîñèòü Àëèñó ðàñøèôðîâàòü åãî. Íî ýòî íå äàñò áàíêó íèêàêîé èíôîðìàöèè î òîì, êàêîå ñîîáùåíèå áûëî çàøèôðîâàíî. Ïîñêîëüêó ñîîáùåíèå áûëî ñëó÷àéíûì, îíî íå ñîäåðæèò íèêàêîé ñòàòèſòè÷åſêîé èíôîðìàöèè, êîòîðóþ ìîæíî áû èçâëå÷ü.

Ýëåêòðîííûå íàëè÷íûå è èäåàëüíîå ïðèâàòíîſòè

Ó ýëåêòðîííûõ íàëè÷íûõ åñòü è ñâîſ òåì íàſ ñòîðîíà. Èíîãäà ëþäſì íå íóæíî òàê ìíîãî ñåêðåòíſòè. Ñì îòðèå, êàê Àëèñà ñîâåðøàåò èäåàëüíîå ïðåñòóïëåíèå [1575]:

(1) Àëèñà êðàäåò ðåáåíêà.

(2) Àëèñà ãîòîâèò 10000 àíîíèìíûõ äåíåæíûõ ÷åêîâ ïî $1000 (èëè äðóãîå êîëè÷åñòâî ÷åêîâ íóæíîãî åé äîñòàòî÷íîñòâà).

(3) Àëèñà ìàñêèðóåò âñå 10000 äåíåæíûõ ÷åêîâ, èñïîëüçóÿ ïðîïîëî ñëåïîé ïîäïèñè. Îíà ïîñûëàåò èõ âëàäåëüöó ñóãðîçíé óâèäåíèå, åñëè íå áóäóò âûïîëíåíû ñëåäóþùèå èíñòðóêöèè:

(a) Âñå 10000 äåíåæíûõ ÷åêîâ äîëæíû áûòü ïîäïèñàíû áàíêîì.

(b) Ðåçóëüòàòû îïóáëèêîâàíû â ãàçåòå.

(4) Âëàñòè ñîãëàøàþòñÿ.

(5) Àëèñà ïîêóïàåò ãàçåòó, ñíèìàåò ìàñêèðîâêó ñ äåíåæíûõ ÷åêîâ è íà÷èíàåò òðàíçèò èõ. Íå ñìîãóò íàéòè åå, ïðîñëåäèâ çà äåíåæíûìè ÷åêàìè.

(6) Àëèñà îñâîáîæäàåò ðåáåíêà.

Çàìåòüå, ÷òî ýòà ñèòóàöèÿ ãîðàçäî õóæå ÷åì ïðè èñïîëüçîâàíèè ëþáûõ ôèçè÷åñêèõ íîñèòåëåé, íàïðèìåð, íàëè÷íûõ. Áåç ôèçè÷åñêîãî êîíòàêòà ó ïîëèöèè ãîðàçäî ìåíüøå øàíñîâ çàäåðæàòü ïîõèòèòåëÿ.

Îäíàêî, â îáùåì ñëó÷àå ýëåêòðîííûå íàëè÷íûå íå ñëèøêîì óäîáíû äëÿ ïðåñòóïíèêîâ. Ïðîáëåìà â òîì, ÷òî àíîíèìíîñòü ðàâíîçíà òîëüêî äëÿ îäíîé ñòîðîíû - ïîêóïàòåëü àíîíèì, à ïðîäàâåö íåò. Áîëåå òîãî, ïðîäàâåö íå ñìîæåò ñêðûòü ôàêò ïîëó÷åíèÿ äåíåã. Ýëåêòðîííûå íàëè÷íûå ïîìîãóò ïðàêòè÷åñêè ïîðåâîëþöèè, ñêîëüêî äåíåã âû çàðàáàòûâàåòå, íî îïðåäåëèòü, êàê âû èõ òðàòèòå, îñòàíåòñÿ íåâîçìîæíûì.

Ðàçëè÷íûå ýëåêòðîííûå íàëè÷íûå

Ãîëëàíäñêàÿ êîìïàíèÿ, DigiCash, âêëàäåò áîëüøóþ ÷àñòü ïàòåíòîâ â îáëàñòè ýëåêòðîííûõ íàëè÷íûõ è ðàçëè÷íàÿ ïðîïðèåòàðíàÿ ýëåêòðîííûå íàëè÷íûå â ðàáîòàþùèõ ïðîäóêòàõ owns. Åñëè âû çàèíòåðåñîâàíû ýòèì, îáðàòèòåñü â DigiCash BV, Kruislaan 419, 1098 VA Amsterdam, Netherlands.

Äðóãèå ïðîòîêîëû ýëåêòðîííûõ íàëè÷íûõ

Ñóùåñòâóþò è äðóãèå ïðîòîêîëû ýëåêòðîííûõ íàëè÷íûõ, ñì. [707, 1554, 734, 1633, 973]. Ðÿä èç íèõ èñïîëüçóåò âåñüìà èçîùðåííóþ ìàòåìàòèêó. Ðàçëè÷íûå ïðîòîêîëû ýëåêòðîííûõ íàëè÷íûõ ìîæíî ðàçäåëèòü íà ðàçëè÷íûå êàòåãîðèè. **Äèâèäåíäû** ñèñòåìû òðåáóþò, ÷òîáû ïðîäàâåö ñâÿçûâàëñÿ ñ áàíêîì ïðè êàæäîé ïðîäàæå, ÷òî î÷åíü ïîõîæå íà ñåãîäíÿøíèé ïðîòîêîë äëÿ êðåäèòíûõ êàðòî÷åê. Åñëè âîçíèêàò êàêèå-íèáóäü ïðîáëåìû, áàíê íå ïðèíèìàò íàëè÷íûå, è Àëèñà íå ìîæåò ñìîøåííè÷àòü.

Àâòîíîìíûå ñèñòåìû, ïîäîáíûå ïðîòîêîë ¹4, íå òðåáóþò ñîâäèíåíèÿ ìåæäó ïðîäàâöîì è áàíêîì äî îêîí÷àíèÿ òðàíçàêöèè ìåæäó ïðîäàâöîì è ïîêóïàòåëåì. Ýòè ñèñòåìû íå ïîìøàþò Àëèñå ìîøåííè÷àòü, íî âìåñòî ýòîãî îáíàðóæàò åå ìîøåííè÷åñòâî. Ïðîòîêîë ¹4 îáíàðóæèâàåò ìîøåííè÷åñòâî Àëèñû, ðàñêðûâàÿ åå ëè÷íîñòü ïðè ïîêóïêå ìîøåííè÷àòü. Àëèñà çíàåò î ïîñëåäñòâèÿõ è, ïîýòîìó, íå ìîøåííè÷àåò.

Äðóãîé ïóòü ñîñòîèò â ñîçäàíèè ñïåöèàëèçèðîâàííûõ êîðïîðàöèé (ñì. Ðàçäåë 24.13), ñîäåðæàùåé çàùèùåííóþ ìèêðîñõåìó, íàçûâàåìóþ **íàáëþäàòåëåì** [332, 341, 387]. Ìèêðîñõåìà-íàáëþäàòåëü õðàíèò ìèíèìóì äàííûõ âñåõ ÷àñòåé ýëåêòðîííûõ íàëè÷íûõ, ïîòðåáíûõ äëÿ ïðîâåðêè ïîäëèííîñòè ýëåêòðîííûõ íàëè÷íûõ è ïîäàòåëåé. Ýòè äàííûå íå ïîçâîëÿþò íàáëþäàòåëþ óçíàòü ñóììó, íàïðèìåð, ïîêóïîê, êîòîðûå îíè, íàêîïëåíèé áóäóò äåìîíñòðèðîâàòü, áàíê ìîæåò ïðîâåðèòü íàëè÷íûå è îïðåäåëèòü ìîøåííè÷à, åñëè ïðîèçîøëè îøèáêè.

Äðóãîé ïóòü ñîñòîèò â ñîçäàíèè ñïåöèàëèçèðîâàííûõ êîðïîðàöèé (ñì. Ðàçäåë 24.13), ñîäåðæàùåé çàùèùåííóþ ìèêðîñõåìó, íàçûâàåìóþ **íàáëþäàòåëåì** [332, 341, 387]. Ìèêðîñõåìà-íàáëþäàòåëü õðàíèò ìèíèìóì äàííûõ âñåõ ÷àñòåé ýëåêòðîííûõ íàëè÷íûõ, ïîòðåáíûõ äëÿ ïðîâåðêè ïîäëèííîñòè ýëåêòðîííûõ íàëè÷íûõ è ïîäàòåëåé. Ýòè äàííûå íå ïîçâîëÿþò íàáëþäàòåëþ óçíàòü ñóììó, íàïðèìåð, ïîêóïîê, êîòîðûå îíè, íàêîïëåíèé áóäóò äåìîíñòðèðîâàòü, áàíê ìîæåò ïðîâåðèòü íàëè÷íûå è îïðåäåëèòü ìîøåííè÷à, åñëè ïðîèçîøëè îøèáêè.

Ïðîòîêîëû ýëåêòðîííûõ íàëè÷íûõ ìîæíî ðàçäåëèòü è ïî äðóãîìó ïðèçíàêó. Íîñèòåë **ýëåêòðîííûõ ìîíåò** ôèêñèðîâàí, ëþäÿì, èñïîëüçóþùèì òàêóþ ñèñòåìó, íóæåí ðÿä ìîíåò ðàçëè÷íûõ íîìèíàëîâ. **Ýëåêòðîííûå ÷åêè** ìîãóò áûòü èñïîëüçîâàíû äëÿ ëþáûõ ñóìì äî çàäàííîãî ìàêñèìóìà, à íåïîðà÷åííûé îñòàòîê ìîæåò áûòü âîçâðàùåí íà ñ÷åò.

Äâóìÿ îòëè÷íûìè ñîâðåìåííî îòëè÷àþùèìèñÿ äðóãà îò äðóãà àâòîíîìíûìè ïðîòîêîëàìè ýëåêòðîííûõ ìîíåò ÿâëÿþòñÿ [225, 226, 227] è [563, 564, 565]. Òàêæå ìîæíî ïðåäëîæèòü ñèñòåìà NetCash (Ñåòåâûå íàëè÷íûå) ñ áîëåå ñëàáûìè ñâîéñòâàìè [1048, 1049]. Äðóãîé íîâîé ñèñòåìîé ÿâëÿåòñÿ [289].

Â [1211] Òàòóàêè Îêàìîòî (Tatsuaki Okamoto) è Êàçóî Îõòà (Kazuo Ohta) ïðåä÷èñëèëè øåñòü ñâîéſòâ èäåàëüíîé ñèſòåìû ýëåêòðîííûõ íàëè÷íûõ:

1. Íåçàâèſèìîſòü. Áåçîſàſíîſòü ýëåêòðîííûõ íàëè÷íûõ íå çàâiſèſò îò ìåſòîſàõîæäåſèÿ. Íàëè÷íûå ìîãóò áûòü ïåðåäàſû ïî êîìïüſòåðſûì ſåòÿì.
2. Áåçîſàſíîſòü. Ýſåêſòðîſſûå íàëè÷íûå íåëüçÿ ſêîſèðîâàòü è ſîâòîðſî èſſîſüçîâàòü.
3. Òàéſà ëè÷íſòè (Íåſòſåæèâàìſòü). Òàéſà ëè÷íſòè ſſëüçîâàòåëÿ çàùèùåſà, ſâÿçü ìåæäó ſſëüçſ-

âàòåëåì è åãî ïîêóïêàìè îáîðóäîâàíèå íåîçìîæíî.

4. Àâòîíîìíûé ïëàòåæ. Êîãäà ïîëüçîâàòåëü ðàñïëà÷èâàåòñÿ çà ïîêóïêó ýëåêòðîííûìè íàëè÷íûìè, ïðîòîêîë ìåæó ïîëüçîâàòåëåì è ïðîäàâöîì âûïîëíÿåòñÿ àâòîíîìíî. Òî åñòü, ìàãàçèíó íå íóæíî ñîâåðøàòü ñ öåíòðàëüíûì êîìïüþòåðîì äëÿ îáðàáîòêè ïëàòåæà ïîëüçîâàòåëÿ.
5. Ïåðåìåùàåìîñòü. Íàëè÷íûå ìîãóò ïåðåäàâàòüñÿ äóãèì ïîëüçîâàòåëþ.
6. Äëèòåëüíîñòü. Çàäíÿÿ ñòìà ýëåêòðîííûõ íàëè÷íûõ ìîæåò áûòü ïîäåëåíà íà ÷àñòè ìåíüøåé ñóìì. (Êîíå÷íî, îáùàÿ ñóìà â êîíöå äîëæíà ñîéòèñü.)

Ðàíåå ïðèâåäåííûå óäîâëåòâîðþò òðåáîâàíèÿì 1, 2, 3 è 4, íî íå óäîâëåòâîðþò òðåáîâàíèþ 5 è 6. Ðÿä äèàëîãîâûõ ñèñòåì ýëåêòðîííûõ íàëè÷íûõ óâîëåòâîðÿåò âñåì òðåáîâàíèÿì êðîìå 4 [318, 413, 1243]. Ïåðâàÿ àâòîíîìíàÿ ñèñòåìà, óâîëåòâîðþùàÿ òðåáîâàíèÿì 1, 2, 3 è 4, ïîõîæàÿ íà îäíó èç îïèñàííûõ, áûëà ïðåäëîæåíà [339]. Îêàìîòî è Îõòà ïðåäëîæèëè ñèñòåìó, óâîëåòâîðþùàÿ òðåáîâàíèÿì ñ 1 ïî 5 [1209], îíè òàêæå ïðåäëîæèëè ñèñòåìó, óâîëåòâîðþùóþ òðåáîâàíèÿì ñ 1 ïî 6, îáúåì äàííûõ äëÿ îäíîãî ïëàòåæà ñîñòàâëÿë ïðèáëèçèòåëüíî 200 ìåãàáàéò. Äðóãàÿ àâòîíîìíàÿ ñèñòåìà ýëåêòðîííûõ ìîíåò ñ âîçìîæíîñòüþ äåëåíèÿ îïëàòû â [522].

Ñõåìà ýëåêòðîííûõ íàëè÷íûõ, ïðåäëîæåííàÿ òåì æå àâòîðàìè [1211], óâîëåòâîðÿåò òðåáîâàíèÿì ñ1 ïî 6 áåç íåîáõîäèìîñòè òàêîãî îãðîìíîãî îáúåìà äàííûõ. Îáùèé îáúåì äàííûõ äëÿ îäíîãî ýëåêòðîííîãî ïëàòåæà ñîñòàâëÿåò îêîëî 20 êèëîáàéò, è ïðîòîêîë ìîæåò áûòü âûïîëíåí çà íåñêîëüêî ñåêóíä. Àâòîðû ðàññìàòðèâàþò ýòó ñõåìó êàê ïåðâóþ èäåàëüíóþ ñèñòåìó íåòñëåæèâàåìûõ ýëåêòðîííûõ íàëè÷íûõ.

Àíîíèìíûå êðåäèòíûå êàðòî÷êè

Ýòîò ïðîòîêîë [988] äëÿ çàùèòû ëè÷íîñòè êëèåíòà èñïîëüçóåò íåñêîëüêî ðàçëè÷íûõ áàíêîâ. Êàæäûé êëèåíò èìåò ñ÷åò â äâóõ ðàçëè÷íûõ áàíêàõ. Ïåðâûé áàíê, êîòîðîìó èçâåñòíà ëè÷íîñòü ÷åëîâåêà, ìîæåò çà÷èñëÿòü äåíüãè íà åãî ñ÷åò. Âòîðîé áàíê çíàåò êëèåíòà òîëüêî ïîä ïñåâäîíèìîì (ïîäîáíî íîìåðíîìó ñ÷åòó â øâåéöàðñêîì áàíêå).

Êëèåíò ìîæåò áðàòü äåíüãè èç âòîðîãî áàíêà, äîêàçûâàÿ, ÷òî îí ÿâëÿåòñÿ âëàäåëüöåì ñ÷åòà. Í î, ýòî áàíê íå çíàåò ëè÷íîñòè ÷åëîâåêà è íå ìîæåò çà÷èñëÿòü äåíüãè íà åãî ñ÷åò. Ïåðâûé áàíê çíàåò êëèåíòà è ïåðå÷èñëÿåò äåíüãè âî âòîðîé áàíê, íå çíàÿ ïñåâäîíèìà. Çàòåì êëèåíò àíîíèìíî òðàòèò ýòè äåíüãè. Â êîíöå ìåñÿöà âòîðîé áàíê âûñûëàåò ñ÷åò ïåðâîìó áàíêó, âåðÿ, ÷òî îí åãî ïîëàòèò. Êîãäà êëèåíò îïëà÷èâàåò ñ÷åò, ïåðâûé áàíê ïåðå÷èñëÿåò äîïîëíèòåëüíûå äåíüãè âî âòîðîé áàíê. Âñå òðàíçàêöèè ïðîâîäÿòñÿ ÷åðåç ïîñðåäíèêà, êîòîðûé äåéſòâóåò îò èìåíè Ôåäåðàëüíîãî Ðåçåðâó: îïëà÷èâàåò áàíêîâñêèå ñ÷åòà, ðåãèſòðèðóåò ñîîáùåíèÿ è ñîçäàåò êîíòðîëüíûé ñëåä.

Îáùåíû ìåæó êëèåíòîì, ïðîäàâöîì è ðàçëè÷íûìè áàíêàìè îñíâí âûäåëåíû â [988]. Åñëè âñå íå ñãîâàðèâàþòñÿ ïðîòèâ êëèåíòà, åãî àíîíèìíîñòü ãàðàíòèðîâàíà. Îäíàêî, ýòî íå ýëåêòðîííûå íàëè÷íûå, áàíê ñèſòåìû ìîæåò ìîøåííè÷àòü. Ïðîòîêîë ïîçâîëÿåò êëèåíòàì ïîëüçîâàòüſÿ ïðåìóſùåſòâàìè êðåäèòíûõ êàðòî÷åê, íå ðàſêðûâàÿ ſâîé ëè÷íîſòè.