Ãëàâà 21
Ñõåìû èäåíòèôèêàöèè

21.1 FEIGE-FIAT-SHAMIR

Ñõåìà öèôðîâîé ïîäïèñè è ïðîâåðêè ïîäëèííîñòè, ðàçðàáîòàííàÿ Àìîñîì Ôèàòîì (Amos Fiat) è Àäè Øàìèðîì (Adi Shamir), ðàññìàòðèâàåòñÿ â [566, 567]. Óðèåëü Ôåéãå (Uriel Feige), Ôèàò è Øàìèð ìîäèôèöèðîâàëè àëãîðèòì, ïðåâðàòèâ åãî â äîêàçàòåëüñòâî ïîäëèííîñòè ñ íóëåâûì çíàíèåì [544, 545]. Ýòî ëó÷øåå äîêàçàòåëüñòâî ïîäëèííîñòè ñ íóëåâûì çíàíèåì.

9 èþëÿ 1986 ãîäà òðè àâòîðà ïîäàëè çàÿâêó íà ïîëó÷åíèå ïàòåíòà ÑØÀ [1427]. Èç-çà âîçìîæíîãî âîåííîãî ïðèìåíåíèÿ çàÿâêà áûëà ðàññìîòðåíà âîåííûìè. Âðåìÿ îò âðåìåíè ðåçóëüòàòîì ðàáîòû Ïàòåíòíîå áþðî ÿâëÿåòñÿ íå âûäà÷à ïàòåíòà, à íå÷òî, íàçûâàåìîå ñåêðåòíûì ðàñïîðÿæåíèåì. 6 ÿíâàðÿ 1987 ãîäà, çà òðè äíÿ äî èñòå÷åíèÿ øåñòèìåñÿ÷íîãî ïåðèîäà, ïî ïðîñüáå àðìèè Ïàòåíòíîå áþðî èçäàëî òàêîå ðàñïîðÿæåíèå. Çàÿâèëî, ÷òî ". . . ðàñêðûòèå èëè ïóáëèêàöèÿ ïðåäìåòà çàÿâêè . . . ìîæåò ïðè÷èíèòü óùåðá íàöèîíàëüíîé áåçîïàñíîñòè . . ." Àâòîðàì áûëî ïðèêàçàíî óâåäîìèòü âñåõ ãðàæäàí ÑØÀ, êîòîðûå ïî òåì èëè èíûì ïðè÷èíàì óçíàëè î ïðîâîäèìûõ èññëåäîâàíèÿõ, ÷òî íåñàíêöèîíèðîâàííîå ðàñêðûòèå èíôîðìàöèè ìîæåò çàêîí÷èòüñÿ äâóìÿ ãîäàìè òþðåìíîãî çàêëþ÷åíèÿ, øòðàôîì $10,000 èëè òåì è äðóãèì îäíîâðåìåííî. Áîëåå òîãî, àâòîðû äîëæíû áûëè ñîîáùèòü Óïîëíîìî÷åííîìó ïî ïàòåíòàì è òîðãîâûì çíàêàì îáî âñåõ èíîñòðàííûõ ãðàæäàíàõ, êîòîðûå ïîëó÷èëè äîñòóï ê ýòîé èíôîðìàöèè.

Ýòî áûëî íåëåïî. Â òå÷åíèå âòîðîé ïîëîâèíû 1986 ãîäà àâòîðû ïðåäñòàâëÿëè ñâîþ ðàáîòó íà êîíôåðåíöèÿõ â Èçðàèëå, Åâðîïå è Ñîåäèíåííûõ Øòàòàõ. Îíè äàæå íå áûëè àìåðèêàíñêèìè ãðàæäàíàìè, è âñÿ ðàáîòà áûëà âûïîëíåíà â Èíñòèòóòå Âåéöìàíà (Weizmann) â Èçðàèëå.

Ñëóõè îá ýòîì ñòàëè ðàñïðîñòðàíÿòüñÿ â íàó÷íîì ñîîáùåñòâå è ïðåññå. Â òå÷åíèå äâóõ äíåé ñåêðåòíîå ðàñïîðÿæåíèå áûëî àííóëèðîâàíî. Øàìèð è åãî êîëëåãè ñ÷èòàþò, ÷òî çà îòìåíîé ñåêðåòíîãî ðàñïîðÿæåíèÿ ñòîÿëî NSA, õîòÿ íèêàêèõ îôèöèàëüíûõ êîììåíòàðèåâ íå áûëî. Äàëüíåéøèå ïîäðîáíîñòè ýòîé ïðè÷óäëèâîé èñòîðèè ïðèâåäåíû â [936].

Óïðîùåííàÿ ñõåìà èäåíòèôèêàöèè Feige-Fiat-Shamir

Ïåðåä âûäà÷åé ëþáûõ çàêðûòûõ êëþ÷åé àðáèòð âûáèðàåò ñëó÷àéíûé ìîäóëü, n, êîòîðûé ÿâëÿåòñÿ ïðîèçâåäåíèåì äâóõ áîëüøèõ ïðîñòûõ ÷èñåë. Â ðåàëüíîé æèçíè äëèíà n äîëæíà áûòü íå ìåíüøå 512 áèòîâ è ëó÷øå êàê ìîæíî áëèæå ê 1024 áèòàì. n ìîæåò îáùèì äëÿ ãðóïïû êîíòðîëåðîâ. (Èñïîëüçîâàíèå ÷èñåë Áëþìà (Blum) îáëåã÷èò âû÷èñëåíèÿ, íî íå ÿâëÿåòñÿ îáÿçàòåëüíûì äëÿ áåçîïàñíîñòè.)

Äëÿ ãåíåðàöèè îòêðûòîãî è çàêðûòîãî êëþ÷åé Ïåããè äîâåðåííûé àðáèòð âûáèðàåò ÷èñëî v, ÿâëÿþùååñÿ êâàäðàòè÷íûì îñòàòêîì mod n. Äðóãèìè ñëîâàìè âûáèðàåòñÿ v òàê, ÷òîáû óðàâíåíèå $x^2 \equiv v \pmod{n}$ èìåëî ðåøåíèå, è ñóùåñòâîâàë $v^{-1} \bmod n$. Ýòî v è áóäåò îòêðûòûì êëþ÷îì Ïåããè. Çàòåì âû÷èñëÿåòñÿ íàèìåíüøåå s, äëÿ êîòîðîãî $s \equiv \text{sqrt}(v^{-1}) \pmod{n}$. Ýòî áóäåò çàêðûòûé êëþ÷ Ïåããè. Èñïîëüçóåòñÿ ñëåäóþùèé ïðîòîêîë èäåíòèôèêàöèè.

(1) Ïåããè âûáèðàåò ñëó÷àéíîå r, ìåíüøåå n. Çàòåì îíà âû÷èñëÿåò $x = -r^2 \bmod n$ è ïîñûëàåò x Âèêòîðó.

(2) Âèêòîð ïîñûëàåò Ïåããè ñëó÷àéíûé áèò b.

(3) Åñëè $b = 0$, òî Ïåããè ïîñûëàåò Âèêòîðó r. Åñëè $b = 1$, òî Ïåããè ïîñûëàåò Âèêòîðó $y = r*s \bmod n$.

(4) Åñëè $b = 0$, Âèêòîð ïðîâåðÿåò, ÷òî $x = -r^2 \bmod n$, óáåæäàÿñü, ÷òî Ïåããè çíàåò çíà÷åíèå sqrt(x). Åñëè $b = 1$, Âèêòîð ïðîâåðÿåò, ÷òî $x = y^2*v \bmod n$, óáåæäàÿñü, ÷òî Ïåããè çíàåò çíà÷åíèå sqrt(v^{-1}).

Ýòî îäèí ýòàï ïðîòîêîëà, íàçûâàåìûé **àêêðåäèòàöèåé**. Ïåããè è Âèêòîð ïîâòîðÿþò ýòîò ïðîòîêîë t ðàç, ïîêà Âèêòîð íå óáåäèòñÿ, ÷òî Ïåããè çíàåò s. Ýòî ïðîòîêîë "ðàçðåçàòü è âûáðàòü". Åñëè Ïåããè íå çíàåò s, îíà ìîæåò ïîäîáðàòü r òàê, ÷òî îíà ñìîæåò îáìàíóòü Âèêòîðà, åñëè îí ïîøëåò åé 0, èëè îíà ìîæåò ïîäîáðàòü r òàê, ÷òî îíà ñìîæåò îáìàíóòü Âèêòîðà, åñëè îí ïîøëåò åé 1. Îíà íå ìîæåò ñäåëàòü îäíîâðåìåííî è òî, è äðóãîå. Âåðîÿòíîñòü, ÷òî åé óäàñòñÿ îáìàíóòü Âèêòîðà îäèí ðàç, ðàâíà 50 ïðîöåíòàì. Âåðîÿòíîñòü, ÷òî åé óäàñòñÿ îáìàíóòü åãî t ðàç, ðàâíà $1/2^t$.

Âèêòîð ìîæåò ïîïðîáîâàòü âñêðûòü ïðîòîêîë, âûäàâàÿ ñåáÿ çà Ïåããè. Îí ìîæåò íà÷àòü âûïîëíåíèå ïðîòîêîëà ñ ñ äðóãèì êîíòðîëåðîì, Âàëåðèåé. Íà øàãå (1) âìåñòî âûáîðà ñëó÷àéíîãî r åìó îñòàåòñÿ ïðîñòî èñïîëüçîâàòü çíà÷åíèå r, êîòîðîå Ïåããè èñïîëüçîâàëî â ïðîøëûé ðàç. Îäíàêî, âåðîÿòíîñòü òîãî, ÷òî Âàëåðèÿ íà øàãå (2) âûáåðåò òî æå çíà÷åíèå b, êîòîðîå Âèêòîð èñïîëüçîâàë â ïðîòîêîëå ñ Ïåããè, ðàâíà 1/2. Ñëåäîâàòåëüíî, âåðîÿòíîñòü, ÷òî îí îáìàíåò Âàëåðèþ, ðàâíà 50 ïðîöåíòàì. Âåðîÿòíîñòü, ÷òî åìó óäàñòñÿ îáìàíóòü åå t ðàç, ðàâíà $1/2^t$.

×òîáû ýòîò ïðîòîêîë ðàáîòàë, Ïåããè íèêîãäà íå äîëæíà èñïîëüçîâàòü r ïîâòîðíî. Â ïðîòèâíîì ñëó÷àå, åñëè Âèêòîð íà øàãå (2) ïîøëî Ïåããè äðóãîé ñëó÷àéíûé áèò, òî îí ïîëó÷èò îáà îòâåòà Ïåããè. Òîãäà äàæå ïî îäíîìó èç íèõ îí ñìîæåò âû÷èñëèòü s, è äëÿ Ïåããè âñå çàêîí÷èòñÿ.

Ñõåìà èäåíòèôèêàöèè Feige-Fiat-Shamir

Â ñâîèõ ðàáîòàõ [544, 545], Ôåéãà, Ôèàò è Øàìèð ïîêàçàëè, êàê ïàðàëëåëüíàÿ ñõåìà ìîæåò ïîâûñèòü ÷èñëî àêêðåäèòàöèé íà ýòàï è óìåíüøèòü âçàèìîäåéñòâèÿ Ïåããè è Âèêòîðà.

Ñíà÷àëà, êàê è â ïðåäûäóùåì ïðèìåðå, äåíåðèðóåòñÿ n, ïðîèçâåäåíèå äâóõ áîëüøèõ ïðîñòûõ ÷èñåë. Äëÿ åäèíñòâåííîñòè è çàêðûòîñòè êëþ÷åé Ïåããè ñíà÷àëà âûáèðàåòñÿ k ðàçëè÷íûõ ÷èñåë: v_1, v_2, . . . v_k, ãäå êàæäîå v_i ÿâëÿåòñÿ êâàäðàòè÷íûì îñòàòêîì mod n. È íûìè ñëîâàìè, v_i âûáèðàþòñÿ òàê, ÷òîáû $x^2 \equiv v_i \pmod n$ èìåë ðåøåíèå, è ñóùåñòâîâàë $v_i^{-1} \bmod n$. Ñòîðîíà, v_1, v_2, . . . v_k, ñëóæèò îòêðûòûì êëþ÷îì. Çàòåì âû÷èñëÿþòñÿ íàèìåíüøèå s_i, äëÿ êîòîðûõ $s_i \equiv \text{sqrt}\,(v_i^{-1}) \pmod n$. Ñòîðîíà s_1, s_2, . . . s_k, ñëóæèò çàêðûòûì êëþ÷îì.

Âû ïîëíÿåòñÿ ñëåäóþùèé ïðîòîêîë:

(1) Ïåããè âûáèðàåò ñëó÷àéíîå r, ìåíüøåå n. Çàòåì îíà âû÷èñëÿåò $x = -r^2 \bmod n$ è ïîñûëàåò x Âèêòîðó.

(2) Âèêòîð ïîñûëàåò Ïåããè ñòðîêó èç k ñëó÷àéíûõ áèòîâ: b_1, b_2, . . . b_k.

(3) Ïåããè âû÷èñëÿåò $y = r * (s_1^{b_1} * s_2^{b_2} * \ldots * s_k^{b_k}) \bmod n$. (Îíà ïðåìíîæàåò âìåñòå çíà÷åíèÿ s_i, ñîîòâåòñòâóþùèå b_i=1. Åñëè ïåðâûé áèò ðàâåí 1, òî s_1 âîéäåò â ïðîèçâåäåíèå, à åñëè ïåðâûé áèò ðàâåí 0, òî íåò, è ò.ä.) Îíà ïîñûëàåò y Âèêòîðó.

(4) Âèêòîð ïðîâåðÿåò, ÷òî $x = y^2 * (v_1^{b_1} * v_2^{b_2} * \ldots * v_k^{b_k}) \bmod n$. (Îí ïåðåìíîæàåò âìåñòå çíà÷åíèÿ v_i, îñíîâûâàÿñü ãà ñëó÷àéíîé äâîè÷íîé ñòðîêå. Åñëè åãî ïåðâûé áèò ðàâåí 1, òî v_1 âîéäåò â ïðîèçâåäåíèå, à åñëè ïåðâûé áèò ðàâåí 0, òî íåò, è ò.ä.)

Ïåããè è Âèêòîð ïîâòîðÿþò ýòîò ïðîòîêîë t ðàç, ïîêà Âèêòîð íå óáåäèòñÿ, ÷òî Ïåããè çíàåò s_1, s_2, . . . s_k.

Âåðîÿòíîñòü, ÷òî Ïåããè óäàñòñÿ îáìàíóòü Âèêòîð t ðàç, ðàâíà $1/2^{kt}$. Àâòîðû ðåêîìåíäóþò èñïîëüçîâàòü âåðîÿòíîñòü ïîøåíè÷åñòâà $1/2^{20}$ è ïðåäëàãàþò çíà÷åíèÿ $k = 5$ è $t = 4$. Åñëè ó âàñ ñêëîííîñòü ê ìàíèè ïðåñëåäîâàíèÿ, óâåëè÷üòå ýòè çíà÷åíèÿ.

Ïðèìåð

Âçãëÿíåì íà ðàáîòó ýòîãî ïðîòîêîëà íåíåëüíèõ ÷èñëàõ. Åñëè n = 35 (äâà ïðîñòûõ ÷èñëà - 5 è 7), òî âîçìîæíûì è ââàäðàòè÷íûì îñòàòêàì ÿâëÿþòñÿ:

1: $x^2 \equiv 1 \pmod{35}$ èìåò ðåøåíèÿ: x = 1, 6, 29, 34.

4: $x^2 \equiv 4 \pmod{35}$ èìåò ðåøåíèÿ: x = 2, 12, 23, 33.

9: $x^2 \equiv 9 \pmod{35}$ èìåò ðåøåíèÿ: x = 3, 17, 18, 32.

11: $x^2 \equiv 11 \pmod{35}$ èìåò ðåøåíèÿ: x = 9, 16, 19, 26.

14: $x^2 \equiv 14 \pmod{35}$ èìåò ðåøåíèÿ: x = 7, 28.

15: $x^2 \equiv 15 \pmod{35}$ èìåò ðåøåíèÿ: x = 15, 20.

16: $x^2 \equiv 16 \pmod{35}$ èìåò ðåøåíèÿ: x = 4, 11, 24, 31.

21: $x^2 \equiv 21 \pmod{35}$ èìåò ðåøåíèÿ: x = 14, 21.

25: $x^2 \equiv 25 \pmod{35}$ èìåò ðåøåíèÿ: x = 5, 30.

29: $x^2 \equiv 29 \pmod{35}$ èìåò ðåøåíèÿ: x = 8, 13, 22, 27.

30: $x^2 \equiv 30 \pmod{35}$ èìåò ðåøåíèÿ: x = 10, 25.

Îáðàòíûì çíà÷åíèÿì (mod 35) è èõ êâàäðàòíûì êîðíÿì è ÿâëÿþòñÿ:

v	v^{-1}	s=sqrt(v^{-1})
1	1	1
4	9	3
9	4	2
11	16	4

16	11	9
29	29	8

Îáðàòèòå âíèìàíèå, ÷òî ó ÷èñåë 14, 15, 21, 25 è 30 íåò îáðàòíûõ çíà÷åíèé mod 35, òàê êàê îíè íå âçàèìíî ïðîñòû ñ 35. Ýòî èìååò ñìûñë, òàê êàê äîëæíî áûòü (5 - 1) * (7 - 1)/4 êâàäðàòè÷íûõ îñòàòêîâ mod 35, âçàèìíî ïðîñòûõ ñ 35: ÍÎÄ(x, 35) = 1 (ñì. ðàçäåë 11.3).

Èòàê, Ïåããè ïîëó÷àåò îòêðûòûé êëþ÷, ñîñòîÿùèé èç k = 4 çíà÷åíèé: {4,11,16,29}. Ñîîòâåòñòâóþùèì çàêðûòûì êëþ÷îì ÿâëÿåòñÿ {3,4,9,8}. Âîò îäèí ýòàï ïðîòîêîëà.

(1) Ïåããè âûáèðàåò ñëó÷àéíîå r=16, âû÷èñëÿåò 16^2 mod 35 = 11 è ïîñûëàåò åãî Âèêòîðó.

(2) Âèêòîð ïîñûëàåò Ïåããè ñòðîêó ñëó÷àéíûõ áèòîâ: {1, 1, 0, 1}

(3) Ïåããè âû÷èñëÿåò $16*(3^1*4^1*9^0*8^1)$ mod 35 = 31 è ïîñûëàåò åãî Âèêòîðó.

(4) Âèêòîð ïðîâåðÿåò, ÷òî $31^2*(4^1*11^1*16^0*29^1)$ mod 35 =11.

Ïåããè è Âèêòîð ïîâòîðÿþò ýòîò ïðîòîêîë t ðàç, êàæäûé ðàç ñ íîâûì ñëó÷àéíûì r, ïîêà Âèêòîð áóäåò óáåæäåí.

Íåáîëüøèå ÷èñëà, ïîäîáíûå èñïîëüçîâàííûì â ïðèìåðå, íå îáåñïå÷èâàþò ðåàëüíîé áåçîïàñíîñòè. Íî êîãäà äëèíà n ðàâíà 512 è áîëåå áèòàì, Âèêòîð íå ñìîæåò óçíàòü î çàêðûòîì êëþ÷å Ïåããè íè÷åãî êðîìå òîãî ôàêòà, ÷òî Ïåããè äåéñòâèòåëüíî çíàåò åãî.

Óëó÷øåíèÿ

Â ïðîòîêîë ìîæíî âñòðîèòü èäåíòèôèêàöèîííûå äàííûå. Ïóñòü I - ýòî äâîè÷íàÿ ñòðîêà, ïðåäñòàâëÿþùàÿ èäåíòèôèêàòîð Ïåããè: èìÿ, àäðåñ, íîìåð ñîöèàëüíîãî ñòðàõîâàíèÿ, ðàçìåð ãîëîâíîãî óáîðà, ëþáèìûé ñîðò ïðîõëàäèòåëüíîãî íàïèòêà è äðóãàÿ ëè÷íàÿ èíôîðìàöèÿ. Èñïîëüçóåì îäíîíàïðàâëåííóþ õýø-ôóíêöèþ $H(x)$ äëÿ âû÷èñëåíèÿ $H(I,j)$, ãäå j - íåáîëüøîå ÷èñëî, äîáàâëåííîå ê I. Íàéäåì íàáîð j, äëÿ êîòîðûõ $H(I,j)$ - ýòî êâàäðàòè÷íûé îñòàòîê ïî ìîäóëþ n. Ýòè çíà÷åíèÿ $H(I,j)$ ñòàíîâÿòñÿ $v_1, v_2, . . . v_k$ (j íå îáÿçàíû áûòü êâàäðàòè÷íûìè îñòàòêàìè). Òåïåðü îòêðûòûì êëþ÷îì Ïåããè ñëóæèò I è ïåðå÷åíü j. Ïåããè ïîñûëàåò I è ïåðå÷åíü j Âèêòîðó ïåðåä øàãîì (1) ïðîòîêîëà (èëè Âèêòîð çàãðóæàåò ýòè çíà÷åíèÿ ñ êàêîé-òî îòêðûòîé äîñêè îáúÿâëåíèé), È Âèêòîð ãåíåðèðóåò $v_1, v_2, . . . v_k$ èç $H(I,j)$.

Òåïåðü, ïîñëå òîãî, êàê Âèêòîð óñïåøíî çàâåðøèò ïðîòîêîë ñ Ïåããè, îí áóäåò óáåæäåí, ÷òî Òðåíò, êîòîðîìó èçâåñòíî ðàçëîæåíèå ìîäóëÿ íà ìíîæèòåëè, ñåðòèôèöèðîâàë ñâÿçü ìåæäó I è Ïåããè, âûäàâ åé êâàäðàòíûå êîðíè èç v_i, ïîëó÷åííûå èç I. (Ñì. ðàçäåë 5.2.) Ôåéãå, Ôèàò è Øàìèð äîáàâèëè ñëåäóþùèå çàìå÷àíèÿ [544, 545]:

> Äëÿ íåèäåàëüíûõ õýø-ôóíêöèé ìîæíî ïîñîâåòîâàòü ðàíäîìèçèðîâàòü I, äîáàâëÿÿ ê íåìó äëèííóþ ñëó÷àéíóþ ñòðîêó R. Ýòà ñòðîêà âûáèðàåòñÿ àðáèòðîì è îòêðûâàåòñÿ Âèêòîðó âìåñòå ñ I.
>
> Â òèïè÷íûõ ðåàëèçàöèÿõ k äîëæíî áûòü îò 1 äî 18. Áîëüøèå çíà÷åíèÿ k ìîãóò óìåíüøèòü âðåìÿ è òðóäíîñòè ñâÿçè, óìåíüøàÿ êîëè÷åñòâî ýòàïîâ.
>
> Äëèíà n äîëæíà áûòü íå ìåíüøå 512 áèòîâ. (Êîíå÷íî, ñ òåõ ïîð ðàçëîæåíèå íà ìíîæèòåëè çàìåòíî ïðîäâèíóëîñü.)
>
> Åñëè êàæäûé ïîëüçîâàòåëü âûáåðåò ñâîå ñîáñòâåííîå n è îïóáëèêóåò åãî â ôàéëå îòêðûòûõ êëþ÷åé, òî ìîæíî îáîéòèñü è áåç àðáèòðà. Îäíàêî òàêîé RSA-ïîäîáíûé âàðèàíò äåëàåò ñõåìó çàìåòíî ìåíåå óäîáíîé.

Ñõåìà ïîäïèñè Fiat-Shamir

Ïðåâðàùåíèå ýòîé ñõåìû èäåíòèôèêàöèè â ñõåìó ïîäïèñè - ýòî, ïî ñóòè, âîïðîñ ïðåâðàùåíèÿ Âèêòîðà â õýø-ôóíêöèþ. Ãëàâíûì ïðåèìóùåñòâîì ñõåìû öèôðîâîé ïîäïèñè Fiat-Shamir ïî ñðàâíåíèþ ñ RSA ÿâëÿåòñÿ åå ñêîðîñòü: äëÿ Fiat-Shamir íóæíî âñåãî ëèøü îò 1 äî 4 ïðîöåíòîâ ìîäóëüíûõ óìíîæåíèé, èñïîëüçóåìûõ â RSA. Â ýòîì ïðîòîêîëå ñíîâà âåðíåìñÿ ê Àëèñå è Áîáó.

Ñìûñë ïåðåìåííûõ - òàêîé æå, êàê è â ñõåìå èäåíòèôèêàöèè. Âûáèðàåòñÿ n - ïðîèçâåäåíèå äâóõ áîëüøèõ ïðîñòûõ ÷èñåë. Ãåíåðèðóåòñÿ îòêðûòûé êëþ÷, $v_1, v_2, . . . v_k$, è çàêðûòûé êëþ÷, $s_1, s_2, . . . s_k$, ãäå $s_i \equiv \mathrm{sqrt}(v_i^{-1}) \pmod n$.

(1) Àëèñà âûáèðàåò t ñëó÷àéíûõ öåëûõ ÷èñåë â äèàïàçîíå îò 1 äî n - $r_1, r_2, . . ., r_t$ - è âû÷èñëÿåò $x_1, x_2, . . . x_t$, òàêèå ÷òî $x_i = r_i^2$ mod n.

(2) Àëèñà õýøèðóåò îáúåäèíåíèå ñîîáùåíèÿ è ñòðîêè x_i, ñîçäàâàÿ áèòîâûé ïîòîê: $H(m, x_1, x_2, . . . x_t)$. Îíà èñïîëüçóåò ïåðâûå $k*t$ áèòîâ ýòîé ñòðîêè â êà÷åñòâå çíà÷åíèé b_{ij}, ãäå i ïðîáåãàåò îò1 äî t, à j îò 1 äî k.

(3) Àëèñà âû÷èñëÿåò $y_1, y_2, . . . y_t$,, ãäå $y_i = r_i *(s_1^{b_{i1}} * s_2^{b_{i2}} *\ldots*s_k^{b_{ik}})$ mod n

(Äëÿ êàæäîãî i îíà ïåðåìíîæàåò âìåñòå çíà÷åíèÿ s_i, â çàâèñèìîñòè îò ñëó÷àéíûõ çíà÷åíèé b_{ij}. Åñëè b_{ij}=1, òî s_i ó÷àñòâóåò â âû÷èñëåíèÿõ, åñëè b_{ij}=0, òî íåò.)

(4) Àëèñà ïîñûëàåò Áîáó m, âñå áèòû b_{ij}, è âñå çíà÷åíèÿ y_i. Ó Áîáà óæå åñòü îòêðûòûé êëþ÷ Àëèñû: $v_1, v_2, . . . v_k$.

(5) Áîá âû÷èñëÿåò $z_1, z_2, . . . z_t$, ãäå $z_i = y^2*(v_1^{b_{i1}} * v_2^{b_{i2}} *…*v_k^{b_{ik}}) \bmod n$

(È ñíîâà Áîá âûïîëíÿåò óìíîæåíèå â çàâèñèìîñòè îò çíà÷åíèé b_{ij}.) Òàêæå îáðàòèòå âíèìàíèå, ÷òî z_i äîëæíî áûòü ðàâíî x_i.

(6) Áîá ïðîâåðÿåò, ÷òî ïåðâûå $k*t$ áèòîâ $H(m, z_1, z_2, . . . z_t)$ - ýòî çíà÷åíèÿ b_{ij}, êîòîðûå ïðèñëàëà åìó Àëèñà.

Êàê è â ñõåìå èäåíòèôèêàöèè áåçîïàñíîñòü ñõåìû ïîäïèñè ïðîïîðöèîíàëüíà $1/2^{kt}$. Îíà òàêæå çàâèñèò îò ñëîæíîñòè ðàçëîæåíèÿ n íà ìíîæèòåëè. Ôèàò è Øàìèð ïîêàçàëè, ÷òî ïîääåëêà ïîäïèñè îáëåã÷àåòñÿ, åñëè ñëîæíîñòü ðàçëîæåíèÿ n íà ìíîæèòåëè çàìåòíî ìåíüøå 2^{kt}. Êðîìå òîãî, èç-çà âñêðûòèÿ ìåòîäîì äíÿ ðîæäåíèÿ (ñì. ðàçäåë 18.1), îíè ðåêîìåíäóþò ïîâûñèòü $k*t$ îò 20 ïî êðàéíåé ìåðå äî 72, ïðåäëàãàÿ $k = 9$ è $t = 8$.

Óëó÷øåííàÿ ñõåìà ïîäïèñè Fiat-Shamir

Ñèëüâèÿ Ìèêàëè (Silvia Micali) è Àäè Øàìèð óëó÷øèëè ïðîòîêîë Fiat-Shamir [1088]. Îíè âûáèðàëè $v_1, v_2, . . . v_k$ òàê, ÷òîáû îíè áûëè ïåðâûìè k ïðîñòûìè ÷èñëàìè. Òî åñòü

$v_1= 1, v_2= 3, v_3= 5$, è ò.ä.

Ýòî îòêðûòûé êëþ÷. Çàêðûòûì êëþ÷îì, $s_1, s_2, . . . s_k$, ñëóæàò ñëó÷àéíûå êâàäðàòíûå êîðíè, îïðåäåëÿåìûå êàê

$s_i = \mathrm{sqrt}(v_i^{-1}) \pmod n$

Â ýòîé âåðñèè ó êàæäîãî ó÷àñòíèêà äîëæåí áûòü ñâîé n. Òàêàÿ ìîäèôèêàöèÿ îáëåã÷àåò ïðîâåðêó ïîäïèñåé, íå âëèÿÿ íà âðåìÿ ãåíåðàöèè ïîäïèñåé è èõ áåçîïàñíîñòü.

Äðóãèå óëó÷øåíèÿ

Íà îñíîâå àëãîðèòìà Fiat-Shamir ñóùåñòâóåò N-ñòîðîííÿÿ ñõåìà èäåíòèôèêàöèè [264]. Äâà äðóãèõ óëó÷øåíèÿ ñõåìû Fiat-Shamir â [1218]. Åùå îäèí âàðèàíò - â [1368].

Ñõåìà èäåíòèôèêàöèè Ohta-Okamoto

Ýòîò ïðîòîêîë ÿâëÿåòñÿ âàðèàíòîì ñõåìû èäåíòèôèêàöèè Feige-Fiat-Shamir, åãî áåçîïàñíîñòü îñíîâàíà íà òðóäíîñòè ðàçëîæåíèÿ íà ìíîæèòåëè [1198, 1199]. Ýòè æå àâòîðû ðàçðàáîòàëè ñõåìó ñ íåñêîëüêèìè ïîäïèñÿìè (ñì. ðàçäåë 23.1), ñ ïîìîùüþ êîòîðîé ðàçëè÷íûå ëþäè ìîãóò ïîñëåäîâàòåëüíî ïîäïèñûâàòü [1200]. Ýòà ñõåìà áûëà ïðåäëîæåíà äëÿ ðåàëèçàöèè íà èíòåëëåêòóàëüíûõ êàðòî÷êàõ [850].

Ïàòåíòû

Fiat-Shamir çàïàòåíòîâàí [1427]. Ïðè æåëàíèè ïîëó÷èòü ëèöåíçèþ íà àëãîðèòì ñâÿæèòåñü ñ Yeda Research and Development, The Weizmann Institute of Science, Rehovot 76100, Israel.

21.2 GUILLOU-QUISQUATER

Feige-Fiat-Shamir áûë ïåðâûì ïðàêòè÷íûì ïðîòîêîëîì èäåíòèôèêàöèè. Îí ìèíèìèçèðîâàë âû÷èñëåíèÿ, óâåëè÷èâàÿ ÷èñëî èòåðàöèé è àêêðåäèòàöèé íà èòåðàöèþ. Äëÿ ðÿäà ðåàëèçàöèé, íàïðèìåð, äëÿ èíòåëëåêòóàëüíûõ êàðòî÷åê, ýòî íå ñëèøêîì ïîäõîäèò. Îáìåíû ñ âíåøíèì ìèðîì òðåáóþò âðåìåíè, à õðàíåíèå äàííûõ äëÿ êàæäîé àêêðåäèòàöèè ìîæåò áûñòðî èñ÷åðïàòü îãðàíè÷åííûå âîçìîæíîñòè êàðòî÷êè.

Ëóè Ãèëëó (Louis Guillou) è Æàí-Æàê Êèñêàòð (Jean-Jacques Quisquater) ðàçðàáîòàëè àëãîðèòì èäåíòèôèêàöèè ñ íóëåâûì çíàíèåì, êîòîðûé áîëüøå ïîäõîäèò äëÿ ïîäîáíûõ ïðèëîæåíèé [670, 1280]. Îáìåíû ìåæäó Ïåããè è Âèêòîðîì, à òàêæå ïàðàëëåëüíûå àêêðåäèòàöèè â êàæäîì îáìåíå ñâåäåíû ê àáñîëþòíîìó ìèíèìóìó: äëÿ êàæäîãî äîêàçàòåëüñòâà ñóùåñòâóåò òîëüêî îäèí îáìåí, â êîòîðîì - òîëüêî îäíà àêêðåäèòàöèÿ. Äëÿ äîñòèæåíèÿ òîãî æå óðîâíÿ áåçîïàñíîñòè ïðè èñïîëüçîâàíèè ñõåìû Guillou-Quisquater ïîòðåáóåòñÿ âûïîëíèòü â òðè ðàçà áîëüøå âû÷èñëåíèé, ÷åì ïðè Feige-Fiat-Shamir. È, êàê è Feige-Fiat-Shamir, ýòîò àëãîðèòì èäåíòèôèêàöèè ìîæíî ïðåâðàòèòü â àëãîðèòì öèôðîâîé ïîäïèñè.

Ñõåìà èäåíòèôèêàöèè Guillou-Quisquater

Ïåããè - ýòî èíòåëëåêòóàëüíàÿ êàðòî÷êà, êîòîðàÿ ñîáèðàåòñÿ äîêàçàòü ñâîþ ïîäëèííîñòü Âèêòîðó. Èäåíòèôèêàöèÿ Ïåããè ïðîâîäèòñÿ ïî ðÿäó àòðèáóòîâ, ïðåäñòàâëÿþùèõ ñîáîé ñòðîêó äàííûõ ñîäåðæàùèõ íàçâàíèå êàðòî÷êè, ïåðèîä äåéñòâèÿ, íîìåð áàíêîâñêîãî ñ÷åòà è äðóãèå, ïîäòâåðæäàåìûå åå ïðèìåíèìîñòü, äàííûå. Ýòà áèòîâàÿ ñòðîêà íàçûâàåòñÿ J. (Â ðåàëüíîñòè ñòðîêà àòðèáóòîâ ìîæåò áûòü î÷åíü äëèííîé, è â êà÷åñòâå J èñïîëüçóåòñÿ åå õýø-çíà÷åíèå. Ýòî óñëîæíåíèå íèêàê íå âëèÿåò íà ïðîòîêîë.) Ýòà ñòðîêà àíàëîãè÷íà îòêðûòîìó êëþ÷ó. Äðóãîé îòêðûòîé èíôîðìàöèåé, îáùåé äëÿ âñåõ "Ïåããè", êîòîðûå ìîãóò èñïîëüçîâàòü ýòî ïðèëîæåíèå, ÿâëÿåòñÿ ïîêàçàòåëü ñòåïåíè v è ìîäóëü n, ãäå n - ýòî ïðîèçâåäåíèå äâóõ õðàíÿùèõñÿ â ñåêðåòå ïðîñòûõ ÷èñåë. Çàêðûòûì

êëþ÷îì ñëóæèò B, ðàññ÷èòûâàåìîå òàê, ÷òîáû $JB^v \equiv 1 \pmod{n}$.

Ïåãàè ïîñûëàåò Âèêòîðó ñâîè àòðèáóòû J. Òåïåðü îíà õî÷åò äîêàçàòü Âèêòîðó, ÷òî ýòî èìåííî åå àòðèáóòû. Äëÿ ýòîãî îíà äîëæíà óáåäèòü Âèêòîðà, ÷òî åé èçâåñòíî B. Âîò ýòîò ïðîòîêîë:

(1) Ïåãàè âûáèðàåò ñëó÷àéíîå öåëîå r, íàõîäÿùååñÿ â äèàïàçîíå îò 1 äî n-1. Îíà âû÷èñëÿåò $T = r^v \bmod n$ è îòïðàâëÿåò ýòî âû÷èñëåíèå Âèêòîðó.

(2) Âèêòîð âûáèðàåò ñëó÷àéíîå öåëîå d, íàõîäÿùååñÿ â äèàïàçîíå îò 0 äî v-1. Îí ïîñûëàåò d Ïåãàè.

(3) Ïåãàè âû÷èñëÿåò $D = rB^d \bmod n$ è ïîñûëàåò åãî Âèêòîðó.

(4) Âèêòîð âû÷èñëÿåò $T' = D^v J^d \bmod n$. Åñëè $T \equiv T' \pmod{n}$, òî ïîäëèííîñòü Ïåãàè äîêàçàíà.

Ìàòåìàòèêà íåëåøêîì ñëîæíà:

$T' = D^v J^d = (rB^d)^v J^d = r^v B^{dv} J^d = r^v (B^v J)^d = r^v = r' \equiv T \pmod{n}$, òàê êàê $JB^v \equiv 1 \pmod{n}$

Ñõåìà ïîäïèñè Guillou-Quisquater

Ýòó ñõåìó èäåíòèôèêàöèè ìîæíî ïðåäñòàâèòü â ñõåìó ïîäïèñè, òàêæå ïðèãîäíóþ äëÿ ðåàëèçàöèè â èíòåëëåêòóàëüíûõ êàðòî÷êàõ [671, 672]. Îôôûöèàëüíûé è çàêðûòûé êëþ÷è íå ìåíÿþòñÿ. Âîò êàê âûãëÿäèò ïðîòîêîë:

(1) Àëèñà âûáèðàåò ñëó÷àéíîå öåëîå r, íàõîäÿùååñÿ â äèàïàçîíå îò 1 äî n-1. Îíà âû÷èñëÿåò $T = r^v \bmod n$.

(2) Àëèñà âû÷èñëÿåò $d = H(M,T)$, ãäå M - ïîäïèñûâàåìîå ñîîáùåíèå, à $H(x)$ - îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ. Çíà÷åíèå d, ïîëó÷åííîå ñ ïîìîùüþ õýø-ôóíêöèè, äîëæíî áûòü â äèàïàçîíå îò 0 äî v-1 [1280]. Åñëè âûõîä õýø-ôóíêöèè âûõîäèò çà ýòîò äèàïàçîí, îí äîëæåí áûòü ïðèâåäåí ïî ìîäóëþ v.

(3) Àëèñà âû÷èñëÿåò $D = rB^d \bmod n$. Ïîäïèñü ñîîòíîñèò èç ñîîáùåíèÿ M, äâóõ âû÷èñëåííûõ çíà÷åíèé, d and D, è åå àòðèáóòîâ J. Îíà ïîñûëàåò ïîäïèñü ÁÎáó.

(4) ÁÎá âû÷èñëÿåò $T' = D^v J^d \bmod n$. Çàòåì îí âû÷èñëÿåò $d' = H(M,T')$. Åñëè $d \equiv d'$, òî Àëèñà çíàåò B, è åå ïîäïèñü äåéñòâèòåëüíà.

Íåêîòîðûå ïîäïèñè

×òî åñëè íåñêîëüêî ÷åëîâåê çàõîòÿò ïîäïèñàòü îäèí è òîò æå äîêóìåíò? Ïðîùå âñåãî, ÷òîáû îíè ïîäïèñàëè åãî ïîðîçíü, íî ðàññìàòðèâàåìàÿ ñõåìà ïîäïèñè äåëàåò ýòî ëó÷øå. Ïóñòü Àëèñà è ÁÎá ïîäïèñûâàþò äîêóìåíò, à Êýðîë ïðîâåðÿåò ïîäïèñè, íî â ïðîöåññ ïîäïèñàíèÿ ìîæåò áûòü âíåñåíî ïðèçâîëüíîå êîëè÷åñòâî ëþäåé. Êàê è ðàíüøå, Àëèñà è ÁÎá îáëàäàþò óíèêàëüíûìè çíà÷åíèÿìè J è B: (J_A,B_A) è (J_B,B_B). Çíà÷åíèÿ n è v ÿâëÿþòñÿ îáùèìè äëÿ âñåé ñèñòåìû.

(1) Àëèñà âûáèðàåò ñëó÷àéíîå öåëîå r_A, íàõîäÿùååñÿ â äèàïàçîíå îò 1 äî n-1. Îíà âû÷èñëÿåò $T_A = r_A^v \bmod n$ è ïîñûëàåò T_A ÁÎáó.

(2) ÁÎá âûáèðàåò ñëó÷àéíîå öåëîå r_B, íàõîäÿùååñÿ â äèàïàçîíå îò 1 äî n-1. Îí âû÷èñëÿåò $T_B = r_B^v \bmod n$ è ïîñûëàåò T_B Àëèñå.

(3) Àëèñà è ÁÎá, êàæäûé âû÷èñëÿåò $T = (T_A * T_B) \bmod n$.

(4) Àëèñà è ÁÎá, êàæäûé âû÷èñëÿåò $d = H(M,T)$, ãäå M - ïîäïèñûâàåìîå ñîîáùåíèå, à $H(x)$ - îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ. Çíà÷åíèå d, ïîëó÷åííîå ñ ïîìîùüþ õýø-ôóíêöèè, äîëæíî áûòü â äèàïàçîíå îò 0 äî v-1 [1280]. Åñëè âûõîä õýø-ôóíêöèè âûõîäèò çà ýòîò äèàïàçîí, îí äîëæåí áûòü ïðèâåäåí ïî ìîäóëþ v.

(5) Àëèñà âû÷èñëÿåò $D_A = r_A B_A^d \bmod n$ è ïîñûëàåò D_A ÁÎáó.

(6) ÁÎá âû÷èñëÿåò $D_B = r_B B_B^d \bmod n$ è ïîñûëàåò D_B Àëèñå.

(7) Àëèñà è ÁÎá, êàæäûé âû÷èñëÿåò $D = D_A D_B \bmod n$. Ïîäïèñü ñîîòíîñèò èç ñîîáùåíèÿ M, äâóõ âû÷èñëåííûõ çíà÷åíèé, d and D, è àòðèáóòîâ îáîèõ ïîäïèñûâàþùèõ: J_A è J_B.

(8) Êýðîë âû÷èñëÿåò $J = J_A J_B \bmod n$.

(9) Êýðîë âû÷èñëÿåò $T' = D^v J^d \bmod n$. Çàòåì îíà âû÷èñëÿåò $d' = H(M,T')$. Åñëè $d \equiv d'$, òî ìíîæåñòâåííàÿ ïîäïèñü äåéñòâèòåëüíà.

Ýòîò ïðîòîêîë ìîæåò áûòü ðàñøèðåí íà ëþáîå êîëè÷åñòâî ëþäåé. Äëÿ ýòîãî ïîäïèñûâàþùèå ñîîáùåíèå ëþäè äîëæíû ïåðåìíîæèòü ñâîè çíà÷åíèÿ T_i íà ýòàïå (3), è ñâîè çíà÷åíèÿ D_i íà ýòàïå (7). ×òîáû ïðîâåðèòü ìíîæåñòâåííóþ ïîäïèñü, íóæíî íà ýòàïå (8) ïåðåìíîæèòü çíà÷åíèÿ J_i ïîäïèñûâàþùèõ (8). Ëèáî âñå ïîäïèñè ïðàâèëüíû, ëèáî ñóùåñòâóåò ïî êðàéíåé ìåðå îäíà íåïðàâèëüíàÿ ïîäïèñü.

21.3 SCHNORR

Áåçîïàñíîñòü ñõåìû ïðîâåðêè ïîäëèííîñòè è ïîäïèñè Êëàóñà Øíîððà [1396,1397] îïèðàåòñÿ íà òðóäíîñòü âû÷èñëåíèÿ äèñêðåòíûõ ëîãàðèôìîâ. Äëÿ ãåíåðàöèè ïàðû êëþ÷åé ñíà÷àëà âûáèðàþòñÿ äâà ïðîñòûõ ÷èñëà, p è q òàê, ÷òîáû q áûëî ñîìíîæèòåëåì p-1. Çàòåì âûáèðàåòñÿ a, íå ðàâíîå 1, òàêîå ÷òî $a^q \equiv 1 \pmod p$. Âñå ýòè ÷èñëà ìîãóò áûòü ñâîáîäíî îïóáëèêîâàíû è èñïîëüçîâàòüñÿ ãðóïïîé ïîëüçîâàòåëåé.

Äëÿ ãåíåðàöèè êîíêðåòíîé ïàðû êëþ÷åé âûáèðàåòñÿ ñëó÷àéíîå ÷èñëî, ìåíüøåå q. Îíî ñëóæèò çàêðûòûì êëþ÷îì, s. Çàòåì âû÷èñëÿåòñÿ îòêðûòûé êëþ÷ $v = a^{-s} \bmod p$.

Ïðîòîêîë ïðîâåðêè ïîäëèííîñòè

(1) Ïåããè âûáèðàåò ñëó÷àéíîå ÷èñëî r, ìåíüøåå q, è âû÷èñëÿåò $x = a^r \bmod p$. Ýòè âû÷èñëåíèÿ ÿâëÿþòñÿ ïðåäâàðèòåëüíûìè è ìîãóò áûòü âûïîëíåíû çàäîëãî äî ïîÿâëåíèÿ Âèêòîðà.

(2) Ïåããè ïîñûëàåò x Âèêòîðó.

(3) Âèêòîð ïîñûëàåò Ïåããè ñëó÷àéíîå ÷èñëî e, èç äèàïàçîíà îò 0 äî 2^{t-1}. (×òî òàêîå t, ÿ îáúÿñíþ ÷óòü ïîçæå.)

(4) Ïåããè âû÷èñëÿåò $y = (r + se) \bmod q$ è ïîñûëàåò y to Âèêòîðó.

(5) Âèêòîð ïðîâåðÿåò, ÷òî $x = a^y v^e \bmod p$.

Áåçîïàñíîñòü àëãîðèòìà çàâèñèò îò ïàðàìåòðà t. Ñëîæíîñòü âñêðûòèÿ àëãîðèòìà ïðèìåðíî ðàâíà 2^t. Øíîðð ñîâåòóåò èñïîëüçîâàòü p îêîëî 512 áèòîâ, q - îêîëî 140 áèòîâ è t - 72.

Ïðîòîêîë öèôðîâîé ïîäïèñè

Àëãîðèòì Schnorr òàêæå ìîæíî èñïîëüçîâàòü è â êà÷åñòâå ïðîòîêîëà öèôðîâîé ïîäïèñè ñîîáùåíèÿ M. Ïàðà êëþ÷åé èñïîëüçóåòñÿ òà æå ñàìàÿ, íî äîáàâëÿåòñÿ îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ $H(M)$.

(1) Àëèñà âûáèðàåò ñëó÷àéíîå ÷èñëî r, ìåíüøåå q, è âû÷èñëÿåò $x = a^r \bmod p$. Ýòî ñòàäèÿ ïðåäâàðèòåëüíûõ âû÷èñëåíèé.

(2) Àëèñà îáúåäèíÿåò M è x è õýøèðóåò ðåçóëüòàò:

$e = H(M,x)$

(3) Àëèñà âû÷èñëÿåò $y = (r + se) \bmod q$. Ïîäïèñüþ ÿâëÿþòñÿ çíà÷åíèÿ e è y, îíà ïîñûëàåò èõ Áîáó.

(4) Áîá âû÷èñëÿåò $x' = a^y v^e \bmod p$. Çàòåì îí ïðîâåðÿåò, ÷òî õýø-çíà÷åíèå äëÿ îáúåäèíåíèÿ M è x' ðàâíî e.

$e = H(M,x')$

Åñëè ýòî òàê, òî îí ñ÷èòàåò ïîäïèñü âåðíîé.

Â ñâîåé ðàáîòå Øíîðð ïðèâîäèò ñëåäóþùèå íîâûå ñâîéñòâà ñâîåãî àëãîðèòìà:

> Áîëüøàÿ ÷àñòü âû÷èñëåíèé, íóæíûõ äëÿ ãåíåðàöèè ïîäïèñè è íåçàâèñÿùèõ îò ïîäïèñûâàåìîãî ñîîáùåíèÿ, ìîæåò áûòü âûïîëíåíà íà ñòàäèè ïðåäâàðèòåëüíûõ âû÷èñëåíèé. Ñëåäîâàòåëüíî, ýòè âû÷èñëåíèÿ ìîãóò áûòü âûïîëíåíû âî âðåìÿ ïðîñòîÿ è íå âëèÿþò íà ñêîðîñòü ïîäïèñàíèÿ. Âñêðûòèå, íàïðàâëåííîå ïðîòèâ ñòàäèè ïðåäâàðèòåëüíûõ âû÷èñëåíèé, ðàññìàòðèâàåòñÿ â [475], ÿ íå äóìàþ, ÷òî îíî èìååò ïðàêòè÷åñêóþ öåííîñòü.
>
> Ïðè îäèíàêîâîì óðîâíå áåçîïàñíîñòè äëèíà ïîäïèñåé äëÿ Schnorr êîðî÷å, ÷åì äëÿ RSA. Íàïðèìåð, ïðè 140-áèòîâîì q äëèíà ïîäïèñåé ðàâíà âñåãî ëèøü 212 áèòàì, ìåíüøå ïîëîâèíû äëèíû ïîäïèñåé RSA. Ïîäïèñè Schnorr òàêæå íàìíîãî êîðî÷å ïîäïèñåé EIGamal.

Êîíå÷íî, èç ïðàêòè÷åñêèõ ñîîáðàæåíèé êîëè÷åñòâî áèòîâ, èñïîëüçóåìûõ â ýòîé ñõåìå, ìîæåò áûòü óìåíüøåíî: íàïðèìåð, äëÿ ñõåìû èäåíòèôèêàöèè, â êîòîðîé ìîøåííèê äîëæåí âûïîëíèòü äèàëîãîâîå âñêðûòèå âñåãî ëèøü çà íåñêîëüêî ñåêóíä (ñðàâíèòå ñî ñõåìîé ïîäïèñè, êîãäà ìîøåííèê ìîæåò ãîäàìè âåñòè ðàñ÷åòû, ÷òîáû âûïîëíèòü ïîäëîã).

Ìîäèôèêàöèÿ, âûïîëíåííàÿ Ýðíè Áðèêåëëîì (Ernie Brickell) è Êåâèíîì ÌàêÊåðëè (Kevin McCurley), ïîâûñèëà áåçîïàñíîñòü ýòîãî àëãîðèòìà [265].

Ïàòåíòû

Schnorr çàïàòåíòîâàí â Ñîåäèíåííûõ Øòàòàõ [1398] è ìíîãèõ äðóãèõ ñòðàíàõ. Â 1993 ãîäó PKP ïðèîáðåëî ïðàâà íà ýòîò ïàòåíò(ñì. ðàçäåë 25.5). Ñðîê äåéñòâèÿ ïàòåíòà ÑØÀ èñòåêàåò 19 ôåâðàëÿ 2008 ãîäà.

21.4 Ïðåîáðàçîâàíèå ñõåì èäåíòèôèêàöèè â ñõåìû ïîäïèñè

Âîò ñòàíäàðòíûé ìåòîä ïðåîáðàçîâàíèÿ ñõåìû èäåíòèôèêàöèè â ñõåìó ïîäïèñè: Âèêòîð çàìåíÿåòñÿ îäíîíàïðàâëåííîé õýø-ôóíêöèåé. Ïåðåä ïîäïèñàíèåì ñîîáùåíèå íå õýøèðóåòñÿ, âìåñòî ýòîãî õýøèðîâàíèå âñòðàèâà-

åòñÿ â àëãîðèòì ïîäïèñè. Â ïðèíöèïå, òàêóþ ìàíèïóëÿöèþ ìîæíî ïðîäåëàòü ñ ëþáîé ñõåìîé èäåíòèôèêàöèè.

Ãëàâà 22 Àëãîðèòìû îáìåíà êëþ÷àìè

22.1 DIFFIE-HELLMAN

Diffie-Hellman, ïðåäëîæåííûé â èñòîðèè àëãîðèòì ñ îòêðûòûì êëþ÷îì, áûë èçîáðåòåí 1976 ãîäó [496]. Åãî áåçîïàñíîñòü îïèðàåòñÿ íà òðóäíîñòü âû÷èñëåíèÿ äiñêðåòíûõ ëîãàðèôìîâ â êîíå÷íîì ïîëå (â ñðàâíåíèè ñ ëåãêîñòüþ âîçâåäåíèÿ â ñòåïåíü â òîì æå ñàìîì ïîëå. Diffie-Hellman ìîæåò áûòü èñïîëüçîâàí äëÿ ðàñïðåäåëåíèÿ êëþ÷åé - Àëèñà è Áîá ìîãóò âîñïîëüçîâàòüñÿ ýòèì àëãîðèòìîì äëÿ ãåíåðàöèè ñåêðåòíîãî êëþ÷à - íî åãî íåëüçÿ èñïîëüçîâàòü äëÿ øèôðîâàíèÿ è äåøèôðèðîâàíèÿ ñîîáùåíèé.

Ìàòåìàòèêà íåñëîæíà. Ñíà÷àëà Àëèñà è Áîá âûáèðàþò áîëüøèå ïðîñòûå ÷èñëà n è g òàê, ÷òîáû g áûëî ïðèìèòèâíûì mod n. Ýòè äâà öåëûõ ÷èñëà õðàíèòñÿ â ñåêðåòå íåîáÿçàòåëüíî, Àëèñà è Áîá ìîãóò äîãîâîðèòüñÿ îá èç ñïîëüçîâàíèè ïî íåñêîëüêèõ êàíàëàõ. Ýòè ÷èñëà äàæå ìîãóò ñîâìåñòíî èñïîëüçîâàòüñÿ ãðóïïîé ïîëüçîâàòåëåé. Áåç ðàçíèöû. Çàòåì âûïîëíÿþòñÿ ñëåäóþùèé ïðîòîêîë:

(1) Àëèñà âûáèðàåò ñëó÷àéíîå áîëüøîå öåëîå ÷èñëî x è ïîñûëàåò Áîáó

$X = g^x \bmod n$

(2) Áîá âûáèðàåò ñëó÷àéíîå áîëüøîå öåëîå ÷èñëî y è ïîñûëàåò Àëèñå

$Y = g^y \bmod n$

(3) Àëèñà âû÷èñëÿåò

$k = Y^x \bmod n$

(4) Áîá âû÷èñëÿåò

$k' = X^y \bmod n$

È k, è k' ðàâíû $g^{xy} \bmod n$. Íèêòî èç ïîäñëóøèâàþùèõ ýòîò êàíàë íå ñìîæåò âû÷èñëèòü ýòî çíà÷åíèå, èì èçâåñòíî òîëüêî n, g, X è Y. Ïîêà îíè ñìîãóò âû÷èñëèòü äiñêðåòíûé ëîãàðèôì è ðàñêðûòü x èëè y, îíè íå ñìîãóò ðåøèòü ïðîáëåìó. Ïîýòîìó, k - ýòî ñåêðåòíûé êëþ÷, êîòîðûé Àëèñà è Áîá âû÷èñëÿþò íåçàâèñèìî.

Âûáîð g è n ìîæåò çàìåòíî âëèÿòü íà áåçîïàñíîñòü ñèſòåìû. ×èſëî $(n-1)/2$ òàêæå äîëæíî áûòü ïðîſòûì [1253]. È, ſàìîå ãëàâíîå, n äîëæíî áûòü áîëüſèſ: áåçîïàſíîſòü ſèſòåìû îſíîâàſà íà ſèſîæſíſòè ðàçëîæſåſèÿ íà ſíſîſèſèſëè ſèſåſ òîãî æå ðàçſåðà, ſòî è n. Ì îſíî âûáèðàòü ëþáſå g, êîòîðſå ÿâëÿåòſÿ ïðèſèòèâſì mod n; íåò ïðèſèſ, ïſ êîòîðûſ íåëüçÿ áûſ âû áðàòü íàèſåſüſøåſ âſçſſæſſå g - ſáû÷íſ ſäſſðàçðÿäſſå ſèſëſ. (Ê òſſó æå, íà ſàſſ åſëå, g íå äſëæſſ äàæå áûòü ïðèſèòèâſì, ſſſ òſëüêſ äſëæſſ ãåſſåðèðſâàòü äſñòàòſ÷ſ áſëüøóþ ſſäãðóſ ſó ſóëüòèſëèêàòèâſſé ãðóſ ûſ mod n.)

Diffie-Hellman ñ òðåìÿ è áîëåå ó÷àñòíèêàìè *

Ïðîòîêîë îáìåíà êëþ÷àìè Diffie-Hellman ëåãêî ìîæíî ðàſøèðèòü íà ſëó÷àé ſ òðåìÿ è áîëåå ó÷àſſíèêàìè. Â ïðèâîäèìîì ïðèſåðå Àëèſà, Áîá è Êýðîë âſåſòå ãåſåðèðóþò ſåêðåſſûé êëþ÷.

(1) Àëèſà âûáèðàåò ſëó÷àéſſå áſëüøſå öåëſſ ÷èſëſ x è âû÷èſëÿåſ

$X = g^x \bmod n$

(2) Áſá âûáèðàåſ ſëó÷àéſſå áſëüøſå öåëſſ ÷èſëſ y è ïſſûëàåſ Êýðſë

$Y = g^y \bmod n$

(3) Êýðſë âûáèðàåſ ſëó÷àéſſå áſëüøſå öåëſſ ÷èſëſ z è ïſſûëàåſ Àëèſå

$Z = g^z \bmod n$

(4) Àëèſà ïſſûëàåſ Áſáó

$Z'=Z^x \bmod n$

(5) Áſá ïſſûëàåſ Êýðſë *

$X'=X^y \bmod n$

(6) Êýðſë ïſſûëàåſ Àëèſå

$Y'=Y^z \bmod n$

(7) Àëèſà âû÷èſëÿåſ

$k = Y^{x} \bmod n$

(8) Áîá âû÷èñëÿåò

$k = Z^{y} \bmod n$

(9) Êýðîë âû÷èñëÿåò

$k = X^{z} \bmod n$

Ñåêðåòíûé êëþ÷ k ðàâåí $g^{xyz} \bmod n$, è íèêòî èç ïîäñëóøèâàþùèõ êàíàëû ñâÿçè íå ñìîæåò âû÷èñëèòü ýòî çíà÷åíèå. Ïðîòîêîë ìîæíî ëåãêî ðàñøèðèòü äëÿ ÷åòâåðûõ è áîëåå ó÷àñòíèêîâ, ïðîñòî äîáàâëÿòñÿ ó÷àñòíèêè è ýòàïû âû÷èñëåíèé.

Ðàñøèðåííûé Diffie-Hellman

Diffie-Hellman òàêæå ðàáîòàåò â êîìóòàòèâíûõ êîëüöàõ [1253]. Ç. Øìóëè (Z. Shmuley) è Êåâèí ÌàêÊåðëè (Kevin McCurley) èçó÷èëè âàðèàíò àëãîðèòìà, â êîòîðîì ìîäóëü ÿâëÿåòñÿ ñîñòàâíûì ÷èñëîì [1441, 1038]. Â.Ñ. Ìèëëåð (V. S. Miller) è Íèë Êîáëèö (Neal Koblitz) ðàñøèðèëè ýòîò äëãîðèòì, èñïîëüçóÿ ýëëèïòè÷åñêèå êðèâûå [1095, 867]. Òàõåð ÝëüÄæàìàëü (Taher ElGamal) èñïîëüçîâàë îñíîâíîïîëàãàþùóþ èäåþ äëÿ ðàçðàáîòêè àëãîðèòìà øèôðîâàíèÿ è öèôðîâîé ïîäïèñè (ñì. ðàçäåë 19.6).

Ýòîò àëãîðèòì òàêæå ðàáîòàåò â ïîëå Ãàëóà GF(2^k) [1442, 1038]. Â ðÿäå ðåàëèçàöèé èñïîëüçóåòñÿ èìåííî ýòîò ïîäõîä [884, 1631, 1632], òàê êàê âû÷èñëåíèÿ âûïîëíÿþòñÿ íàìíîãî áûñòðåå. Íî è êðèòèêè÷åñêè âû÷èñëåíèÿ âûïîëíÿþòñÿ íàìíîãî áûñòðåå, ïîýòîìó âàæíî òùàòåëüíî âûáèðàòü ïîëå, äîñòàòî÷íî áîëüøîå, ÷òîáû îáåñïå÷èòü íóæíóþ áåçîïàñíîñòü.

Hughes

Ýòîò âàðèàíò àëãîðèòìà Diffie-Hellman ïîçâîëÿåò Àëèñå ãåíåðèðîâàòü êëþ÷ è ïîñëàòü åãî Áîáó [745].

(1) Àëèñà âû÷èñëÿåò ñëó÷àéíîå áîëüøîå öåëîå ÷èñëî x è ãåíåðèðóåò

$k = g^{x} \bmod n$

(2) Áîá âû÷èñëÿåò ñëó÷àéíîå áîëüøîå öåëîå ÷èñëî y è ïîñûëàåò Àëèñå

$Y = g^{y} \bmod n$

(3) Àëèñà ïîñûëàåò Áîáó

$X = Y^{x} \bmod n$

(4) Áîá âû÷èñëÿåò

$z = y^{-1}$

$k' = X^{z} \bmod n$

Åñëè âñå âû÷èñëåíî ïðàâèëüíî, $k = k'$.

Ïðèìóùåñòâîì ýòîãî ïðîòîêîëà íàä Diffie-Hellman ñîñòîèò â òîì, ÷òî k ìîæíî âû÷èñëèòü çàðàíåå, äî âçàèìîäåéñòâèÿ, è Àëèñà ìîæåò øèôðîâàòü ñîîáùåíèÿ ñ ïîìîùüþ k çàäîëãî äî óñòàíîâëåíèÿ ñåàíñà. Îíà ìîæåò ïîñëàòü ñîîáùåíèå ñðàçó ìíæåñòâó ëþäåé, à ïðåäâàòü êëþ÷ ïîçäíåå êàæäîìó ïî òàéíîìó.

Îáìåí êëþ÷îì áåç îáìåíà êëþ÷îì

Åñëè ó âàñ ñîîáùåíèå ïîëüçîâàòåëå, êàæäûé ìîæåò îïóáëèêîâàòü îòêðûòûé êëþ÷, $X = g^{x} \bmod n$, â îáùåé áàçå äàííûõ. Åñëè Àëèñà çàõî÷åò óñòàíîâèòü ñâÿçü ñ Áîáîì, åé ïîíàäîáèòñÿ òîëüêî ïîëó÷èòü îòêðûòûé êëþ÷ Áîáà è ãåíåðèðîâàòü èõ îáùèé ñåêðåòíûé êëþ÷. Îíà ìîæåò çàøèôðîâàòü ñîîáùåíèå ýòèì êëþ÷îì è ïîñëàòü åãî Áîáó. Áîá èçâëå÷åò îòêðûòûé êëþ÷ Àëèñû è âû÷èñëèò îáùèé ñåêðåòíûé êëþ÷.

Êàæäàÿ ïàðà ïîëüçîâàòåëåé ìîæåò èñïîëüçîâàòü óíèêàëüíûé ñåêðåòíûé êëþ÷, íå òðåáóåòñÿ íèêàêèõ ïðåäâàðèòåëüíûõ îáìåíîâ äàííûìè ìåæäó ïîëüçîâàòåëÿìè. Îòêðûòûå êëþ÷è äîëæíû ïðîéòè ñåðòèôèêàöèþ, ÷òîáû ïðåäîòâðàòèòü ìîøåííè÷åñêèå âñêðûòèÿ, è äîëæíû ðåãóëÿðíî ìåíÿòüñÿ, íî â ëþáîì ñëó÷àå ýòî î÷åíü óìíàÿ èäåÿ

Ïàòåíòû

Àëãîðèì îáìåíà êëþ÷àìè Diffie-Hellman çàïàòåíòîâàí â Ñîåäèíåííûõ Øòàòàõ [718] è Êàíàäå [719]. Ãðóïïà, íàçûâàþùàÿñÿ Public Key Partners (PKP, Ïàðòíåðû ïî îòêðûòûì êëþ÷àì), ïîëó÷èëà âìåñòå ñ äðóãèìè ïàòåíòàìè â îáëàñòè êðèïòîãðàôèè ñ òðåõçíà÷íûì êëþ÷àìè ïîëó÷èëà ëèöåíçèþ íà ýòîò ïàòåíò (ñì. ðàçäåë 25.5). Ñðîê äåéñòâèÿ ïàòåíòà ÑØÀ èñòåêàåò 29 àïðåëÿ 1997 ãîäà.

22.2 Ïðîòîêîë "òî÷êà-òî÷êà"

Îáìåí êëþ÷àìè Diffie-Hellman ÷óâñòâèòåëåí ê âñêðûòèþ "÷åëîâåê â ñðåäíåì". Îäíèì èç ñïîñîáîâ ïðåäîòâðàòèòü ýòî, ÿâëÿåòñÿ íåîáõîäèìîñòü äëÿ Àëèñû è Áîáà ïîäïèñûâàòü ñîîáùåíèÿ, êîòîðûå îíè ïîñûëàþò äðóã äðóãó [500].

Ýòîò ïðîòîêîë ïðåäïîëàãàåò, ÷òî ó Àëèñû åñòü ñåðòèôèöèðîâàííûé îòêðûòûé êëþ÷ Áîáà, à ó Áîáà åñòü ñåðòèôèöèðîâàííûé îòêðûòûé êëþ÷ Àëèñû. Ýòè ñåðòèôèêàòû ïîäïèñàíû íåêîòîðûì çàñëóæåííûì îðãàíîì âëàñòè, íàïîìèíàþùèì â ïðîòîêîëå. Âîò êàê Àëèñà è Áîá ãåíåðèðóþò ñåêðåòíûé êëþ÷ k.

(1) Àëèñà ãåíåðèðóåò ñëó÷àéíîå ÷èñëî x è ïîñûëàåò åãî Áîáó.

(2) Áîá ãåíåðèðóåò ñëó÷àéíîå ÷èñëî y. Èñïîëüçóÿ ïðîòîêîë Diffie-Hellman, îí âû÷èñëÿåò îáùèé êëþ÷ k íà áàçå x è y. Îí ïîäïèñûâàåò x è y è øèôðóåò ïîäïèñü êëþ÷îì k. Çàòåì îí ïîñûëàåò ïîëó÷åííûå âìåñòî y Àëèñå.

$$y, E_k(S_B(x,y))$$

(3) Àëèñà òàêæå âû÷èñëÿåò k. Îíà ðàñøèôðîâûâàåò îòòàøóþñü ÷àñòü ñîîáùåíèÿ Áîáà è ïðîâåðÿåò åãî ïîäïèñü. Çàòåì îíà ïîñûëàåò Áîáó ïîäïèñàííîå ñîîáùåíèå, ñîñòîÿùåå èç x è y, çàøèôðîâàííûõ îáùèì êëþ÷îì k.

$$E_k(S_A(x,y))$$

(4) Áîá ðàñøèôðîâûâàåò ñîîáùåíèå è ïðîâåðÿåò ïîäïèñü Àëèñû.

22.3 Òðåõïðîõîäíûé ïðîòîêîë Øàìèðà

Ýòîò èçîáðåòåííûé Àäè Øàìèðîì íî íèêîãäà íå îïóáëèêîâàííûé ïðîòîêîë ïîçâîëÿåò Àëèñå è Áîáó áåçîïàñíî îáìåíèâàòüñÿ èíôîðìàöèåé, íå èñïîëüçóÿ ïðåäâàðèòåëüíîãî îáìåíà íè ñåêðåòíûìè, íè îòêðûòûìè êëþ÷àìè [1008]. Îí ïðåäïîëàãàåò èñïîëüçîâàíèå êîììóòàòèâíîãî øèôðà, äëÿ êîòîðîãî:

$$E_A(E_B(P)) = E_B(E_A(P))$$

Ñåêðåòíûé êëþ÷ Àëèñû - A, à Áîáà - B. Àëèñà õî÷åò ïîñëàòü ñîîáùåíèå M Áîáó. Âîò ýòîò ïðîòîêîë.

(1) Àëèñà øèôðóåò M ñâîèì êëþ÷îì è ïîñûëàåò åãî Áîáó

$$C_1 = E_A(M)$$

(2) Áîá øèôðóåò C_1 ñâîèì êëþ÷îì è ïîñûëàåò Àëèñå

$$C_2 = E_B(E_A(M))$$

(3) Àëèñà ðàñøèôðîâûâàåò C_2 ñâîèì êëþ÷îì è ïîñûëàåò Áîáó

$$C_3 = D_A(E_B(E_A(M))) = D_A(E_A(E_B(M))) = E_B(M)$$

(4) Áîá ðàñøèôðîâûâàåò C_3 ñâîèì êëþ÷îì, ïîëó÷àÿ M.

Êîìóòàòèâíû è îáëàäàþò ñîâåðøåííî áåçîïàñíîñòüþ îäíîðàçîâûå áëîêíîòû, íî ñ ýòèì ïðîòîêîëîì îíè ðàáîòàþò íå áóäóò. Ïðè èñïîëüçîâàíèè îäíîðàçîâîãî áëîêíîòà òðè øèôðîâêñòà áóäóò âûãëÿäåòü ñëåäóþùèì îáðàçîì be:

$$C_1 = M \oplus A$$

$$C_2 = M \oplus A \oplus B$$

$$C_3 = M \oplus B$$

Åâà, çàïèñàâ ýòè òðè ñîîáùåíèÿ, êîòîðûìè îáìåíèâàþòñÿ Àëèñà è Áîá, ïðîñòî âûïîëíèò XOR âñåõ ýòèõ øèôðîâêñòîâ è âîññòàíîâèò ñîîáùåíèå:

$$C_1 \oplus C_2 \oplus C_3 = (M \oplus A) \oplus (M \oplus A \oplus B) \oplus (M \oplus B) = M$$

Î÷åâèäíî, ÷òî òàêîé ñïîñîá ðàáîòàòü íå áóäåò.

Øàìèð (è íåçàâèñèìî Äæèì Îìóðà (Jim Omura)) îïèñàë ïîõîæèé íà RSA àëãîðèòì øèôðîâàíèÿ, êîòîðûé áóäåò ðàáîòàòü ñ ýòèì ïðîòîêîëîì. Ïóñòü p áóäåò áîëüøèì ïðîñòûì ÷èñëîì, ïðè÷åì ìíîæèòåëü p-1 ÿâëÿåòñÿ áîëüøèì ïðîñòûì. Âûáåðåì êëþ÷ øèôðîâàíèÿ e, âçàèìíî ïðîñòîé ñ p-1. Âû÷èñëèì d, äëÿ êîòîðîãî âûïîëíÿåòñÿ $de = 1 \pmod{p-1}$. Äëÿ øèôðîâàíèÿ ñîîáùåíèÿ âû÷èñëÿì

$$C = M^e \bmod p$$

Äëÿ ääøèôðîâàíèÿ ñîîáùåíèÿ âû÷èñëÿåì

$M = C^d \bmod p$

Ïî âêëàäûâàó, ó Åâû íåò ñïîñîáà ïîëó÷èòü M, íå ðåøèâ ïðîáëåìó äèñêðåòíîãî ëîãàðèôìà, íî ýòî íèêîãäà íå áûëî äîêàçàíî.

Êàê è Diffie-Hellman, ýòîò ïðîòîêîë ïîçâîëÿåò Àëèñå íà÷àòü ñåêðåòíûé îáìåí èíôîðìàöèåé ñ Áîáîì, íå çíàÿ íè îäíîãî èç åãî êëþ÷åé. Ïðè èñïîëüçîâàíèè àëãîðèòìà ñ îòêðûòûì êëþ÷îì Àëèñà äîëæíà çíàòü îòêðûòûé êëþ÷ Áîáà. Ïðèìåíÿÿ òðåõïðîõîäíûé àëãîðèòì Øàìèðà, îíà ïðîñòî ïîñûëàåò Áîáó øèôðîâàííûé ñîîáùåíèÿ. Òî æå äåéñòâèå ñ îòêðûòûì àëãîðèòìîì ñ îòêðûòûì êëþ÷îì âûãëÿäèò ñëåäóþùèì îáðàçîì:

(1) Àëèñà çàïðàøèâàåò ó Áîáà (èëè ó KDC) åãî îòêðûòûé êëþ÷.

(2) Áîá (èëè KDC) ïîñûëàåò Àëèñå ñâîé îòêðûòûé êëþ÷.

(3) Àëèñà øèôðóåò M îòêðûòûì êëþ÷îì Áîáà è ïîñûëàåò åãî Áîáó.

Òðåõïðîõîäíûé àëãîðèòì Øàìèðà íå ìîæåò óñòîÿòü ïðåä âñêðûòèåì "÷ëîâåê â ñðåäèíå".

22.4 COMSET

COMSET (COMmunications SETup, óñòàíîâëåíèå ñâÿçè) ýòî ïðîòîêîë îáìåíà ñîîáùåíèÿìè è îáìåíà êëþ÷îì, ðàçðàáîòàííûé äëÿ ïðîåêòà RIPE [1305] (ñì. ðàçäåë 25.7). Ñ ïîìîùüþ êðèïòîãðàôèè ñ îòêðûòûì êëþ÷àìè îí îçâîëÿåò Àëèñå è Áîáó èäåíòèôèöèðîâàòü äðóã äðóãà, ïðè ýòîì îáìåíèâàÿñü ñåêðåòíûì êëþ÷îì.

Ìàòåìàòè÷åñêîé îñíîâîé COMSET ñëóæèò ñõåìà Rabin [1283] (ñì. ðàçäåë 19.5). Ñàìà ñõåìà âïåðâûå áûëà ïðåäëîæåíà â [224]. Ñì. ïîäðîáíîñòè â [1305].

22.5 Îáìåí çàøèôðîâàííûìè êëþ÷àìè

Ïðîòîêîë îáìåíà çàøèôðîâàííûìè êëþ÷àìè (Encrypted Key Exchange, EKE) áûë ðàçðàáîòàí Ñòèâîì Áåëëîâèíîì (Steve Bellovin) è Ìàéêëîì Ìåððèòòîì (Michael Merritt) [109]. Îí îáåñïå÷èâàåò áåçîïàñíîñòü è ïðîâåðêó ïîäëèííîñòè â êîìïüþòåðíûõ ñåòÿõ, ïî íîâîìó èñïîëüçóÿ è ñèììåòðè÷íóþ êðèïòîãðàôèþ, è êðèïòîãðàôèþ ñ îòêðûòûìè êëþ÷àìè: îáùèé ñåêðåòíûé êëþ÷ èñïîëüçóåòñÿ äëÿ øèôðîâàíèÿ ãåíåðèðîâàííîãî ñëó÷àéíûì îáðàçîì îòêðûòîãî êëþ÷à.

Áàçîâûé ïðîòîêîë EKE

Àëèñà è Áîá (äâà ïîëüçîâàòåëÿ, êëèåíò è ñåðâåð, èëè êòî óãîäíî) èìåþò îáùèé ïàðîëü P. Èñïîëüçóÿ ñëåäóþùèé ïðîòîêîë, îíè ìîãóò ïðîâåðèòü ïîäëèííîñòü äðóã äðóãà è âåíåðèðîâàòü îáùèé ñåàíñîâûé êëþ÷ K.

(1) Àëèñà Ñëó÷àéíûì îáðàçîì ãåíåðèðóåò ïàðó "îòêðûòûé êëþ÷/çàêðûòûé êëþ÷". Îíà øèôðóåò îòêðûòûé êëþ÷ K' ñ ïîìîùüþ ñèììåòðè÷íîãî àëãîðèòìà, èñïîëüçóÿ P â êà÷åñòâå êëþ÷à: $E_P(K')$. Îíà ïîñûëàåò Áîáó

$A, E_P(K')$

(2) Áîá çíàåò P. Îí ðàñøèôðîâûâàåò ñîîáùåíèå, ïîëó÷àÿ K'. Çàòåì îí ãåíåðèðóåò ñëó÷àéíûé ñåàíñîâûé êëþ÷ K øèôðóåò åãî îòêðûòûì êëþ÷îì, êîòîðûé îí ïîëó÷èë îò Àëèñû, à çàòåì èñïîëüçóÿ P êà÷åñòâå êëþ÷à. Îí ïîñûëàåò Àëèñå

$E_P(E_{K'}(K))$

(3) Àëèñà ðàñøèôðîâûâàåò ñîîáùåíèå, ïîëó÷àÿ K. Îíà ãåíåðèðóåò ñëó÷àéíóþ ñòðîêó R_A, øèôðóåò åå ñ ïîìîùüþ K è ïîñûëàåò Áîáó

$E_K(R_A)$

(4) Áîá ðàñøèôðîâûâàåò ñîîáùåíèå, ïîëó÷àÿ R_A. Îí ãåíåðèðóåò äðóãóþ ñëó÷àéíóþ ñòðîêó, R_B, øèôðóåò îáå ñòðîêè êëþ÷îì K è ïîñûëàåò Àëèñå ðåçóëüòàò.

$E_K(R_A,R_B)$

(5) Àëèñà ðàñøèôðîâûâàåò ñîîáùåíèå, ïîëó÷àÿ R_A è R_B. Åñëè ñòðîêà R_A, ïîëó÷åííàÿ îò Áîáà, - ýòî òà ñàìàÿ ñòðîêà, êîòîðóþ îíà ïîñëàëà Áîáó íà ýòàïå (3), îíà, èñïîëüçóÿ K, øèôðóåò R_B è ïîñûëàåò åå Áîáó.

$E_K(R_B)$

(6) Áîá ðàñøèôðîâûâàåò ñîîáùåíèå, ïîëó÷àÿ R_B. Åñëè ñòðîêà R_B, ïîëó÷åííàÿ îò Àëèñû, - ýòî òà ñàìàÿ ñòðîêà, êîòîðóþ îí ïîñëàë åé íà ýòàïå (4), çàâåðøåí. Òåïåðü îáå ñòîðîíû ìîãóò îáìåíèâàòüñÿ èíôîðìàöèåé, èñïîëüçóÿ K â êà÷åñòâå ñåàíñîâîãî êëþ÷à.

Íà ýòàïå (3) è Àëèñà, è ÁÎá çíàþò K' è K. K - ýòî ñåàíñîâûé êëþ÷, îí ìîæåò áûòü èñïîëüçîâàí äëÿ øèôðîâàíèÿ âñåõ äðóãèõ ñîîáùåíèé, êîòîðûìè îáìåíèâàþòñÿ Àëèñà è ÁÎá. Ââà, ñèäÿ ìåæäó Àëèñîé è ÁÎáîì, çíàåò òîëüêî $E_P(K')$, $E_P(E_{K'}(K)$ è íåñêîëüêî ñîîáùåíèé, çàøèôðîâàííûõ K. Â äðóãèõ ïðîòîêîëàõ Ââà ìîãëà áû ïîïðîáîâàòü óãàäàòü P (ëþäè âñå âðåìÿ ëþáÿò âûáèðàòü ïëîõèå ïàðîëè, è åñëè Ââà äîñòàòî÷íî óìíà, îíà ìîæåò ýòîò ïàðîëü) è çàòåì ïðîâåðèòü ñâîè ïðåäïîëîæåíèÿ. Â ðàññìàòðèâàåìîì ïðîòîêîëå Ââà íå ìîæåò ïðîâåðÿòü ñâîè ïðåäïîëîæåíèÿ, íå âñêðûâ ïðè ýòîì è àëãîðèòì ñ îòêðûòûì êëþ÷îì. È, åñëè K' è K âûáèðàþòñÿ ñëó÷àéíûì îáðàçîì, òî ýòà ïðîáëåìà áóäåò íåïðåîäîëèìîé.

Îòâåòíàÿ ÷àñòü ïðîòîêîëà, ýòàïû (3) - (6), îáåñïå÷èâàåò ïîäòâåðæäåíèå. Ýòàïû (3) - (5) äîêàçûâàþò Àëèñå, ÷òî ÁÎá çíàåò K, ýòàïû (4) - (6) äîêàçûâàþò ÁÎáó, ÷òî Àëèñà çíàåò K. Îáìåí ìåòêàìè âðåìåíè, èñïîëüçóåìûé â ïðîòîêîëå Kerberos, ðåøàåò òó æå çàäà÷ó.

EKE ìîæåò áûòü ðåàëèçîâàí ñ ìíîæåñòâîì àëãîðèòìîâ ñ îòêðûòûì êëþ÷àìè: RSA, ElGamal, Diffie-Hellman. Ïðîáëåìû ñ áåçîïàñíîñòüþ âîçíèêàþò ïðè ðåàëèçàöèè EKE ñ àëãîðèòìîì ðþêçàêà (äàæå áåç ó÷åòà ïðîáëåì áåçîïàñíîñòè, ïðèñóùèõ ñàìèì àëãîðèòìàì ðþêçàêà): íîìàëüíûå ðàñïðåäåëåíèÿ øèôðîâàííîãî ñîîáùåíèé ñâîäèò íà íåò ïðåèìóùåñòâà EKE.

Ðåàëèçàöèÿ EKE ñ ïîìîùüþ RSA

Àëãîðèòì RSA êàæåòñÿ èäåàëüíûì äëÿ òàêîãî èñïîëüçîâàíèÿ, íî åñòü ðÿä òîíêèõ ïðîáëåì. Àâòîðû ðåêîìåíäóþò øèôðîâàòü íà ýòàïå (1) òîëüêî ïîêàçàòåëü ñòåïåíè, ïîñûëàÿ ìîäóëü. Îáúÿñíåíèå ýòîãî ñîâåòà è äðóãèå òîíêîñòè, ñâÿçàííûå ñ èñïîëüçîâàíèåì RSA, ìîæíî íàéòè [109].

Ðåàëèçàöèÿ EKE ñ ïîìîùüþ ElGamal

Ðåàëèçàöèÿ EKE íà áàçå äëãîðèòìà ElGamal ïðîñòà, ìîæíî äàæå óïðîñòèòü îñíîâíîé ïðîòîêîë. Èñïîëüçóÿ îáîçíà÷åíèÿ èç ðàçäåëà 19.6, g è p ñëóæàò ÷àñòüþ îôôûòîâ êëþ÷à, îâùèè äëÿ âñåõ ïîëüçîâàòåëåé. Çàêðûòûì êëþ÷îì ÿâëÿåòñÿ ñëó÷àéíîå ÷èñëî r. Îòêðûòûì - $g^r \bmod p$. Íà ýòàïå (1) Àëèñà ïîñûëàåò Áîáó ñëåäóþùåå ñîîáùåíèå

Àëèñà, $g^r \bmod p$

Îáðàòèâ âíèìàíèå, ÷òî ýòîò îôôûòîê êëþ÷ íå íóæíî øèôðîâàòü ñ ïîìîùüþ P. Â îáùåì ñëó÷àå ýòî íåâåðíî, íî ýòî òàê äëÿ àëãîðèòìà ElGamal algorithm. Ïîäðîáíîñòè â [109].

Áîá âûáèðàåò ñëó÷àéíîå ÷èñëî R (äëÿ àëãîðèòìà ElGamal, íåçàâèñèìî îò äðóãèõ ñëó÷àéíûõ ÷èñåë, âûáèðàåìûõ äëÿ EKE), è ñîîáùåíèå, êîòîðîå îí ïîñûëàåò Àëèñå íà ýòàïå (2), âûãëÿäèò òàê

$E_P(g^R \bmod p, Kg^{rR} \bmod p)$

Ñóùåñòâóþùèå îãðàíè÷åíèÿ íà âûáîð ïðåìåíîãî äëÿ ElGamal áûëè ïðèâåäåíû â ðàçäåëå 19.6.

Ðåàëèçàöèÿ EKE ñ ïîìîùüþ Diffie-Hellman

Ïðè èñïîëüçîâàíèè ïðîòîêîëà Diffie-Hellman K ãåíåðèðóåòñÿ àâòîìàòè÷åñêè. Îêî÷àòåëüíûé ïðîòîêîë åùå ïðîùå. Çíà÷åíèÿ g è n îïðåäåëÿþòñÿ äëÿ âñåõ ïîëüçîâàòåëåé ñåòè.

(1) Àëèñà âûáèðàåò ñëó÷àéíîå ÷èñëî r_A è ïîñûëàåò Áîáó

$A,\ g^{r_A} \bmod n$

Ïðè èñïîëüçîâàíèè Diffie-Hellman Àëèñå íå íóæíî øèôðîâàòü ñ ïîìîùüþ P ñâîå ïðåäïîëîæåíèå.

(2) Áîá âûáèðàåò ñëó÷àéíîå ÷èñëî r_B è âû÷èñëÿåò

$K = g^{r_A * r_B} \bmod n$

Îí ãåíåðèðóåò ñëó÷àéíóþ ñòðîêó R_B, çàòåì âû÷èñëÿåò è ïîñûëàåò Àëèñå:

$E_Ð(g^{r_B} \bmod n), E_K(R_B)$

(3) Àëèñà ðàñøèôðîâûâàåò ïåðâóþ ïîëîâèíó ñîîáùåíèÿ Áîáà, ïîëó÷àÿ $g^{r_B} \bmod n$. Çàòåì îíà âû÷èñëÿåò K è èñïîëüçóåò åãî äëÿ øèôðîâàíèÿ R_B. Îíà ãåíåðèðóåò äðóãóþ ñëó÷àéíóþ ñòðîêó R_A,, øèôðóåò îáå ñòðîêè êëþ÷îì K è ïîñûëàåò ðåçóëüòàò Áîáó.

$E_K(R_A,,R_B)$

(4) Áîá ðàñøèôðîâûâàåò ñîîáùåíèå, ïîëó÷àÿ R_A, è R_B. Åñëè ïîëó÷åííàÿ îò Àëèñû ñòðîêà R_B ñîâïàäàåò ñ òîé, êîòîðóþ îí ïîñûëàë åé íà ýòàïå (2), îí øèôðóåò R_A êëþ÷îì K è ïîñûëàåò ðåçóëüòàò Àëèñå.

$E_K(R_A)$

(5) Àëèñà ðàñøèôðîâûâàåò ñîîáùåíèå, ïîëó÷àÿ R_A. Åñëè ïîëó÷åííàÿ îò Áîáà ñòðîêà R_A ñîâïàäàåò ñ òîé, êîòîðóþ îíà ïîñûëàëà Áîáó íà ýòàïå (3), ïðîòîêîë çàâåðøàåòñÿ. Òåïåðü ñòîðîíû ìîãóò íàìåíåâàòüñÿ ñîîáùåíèÿìè, èñïîëüçóÿ K â êà÷åñòâå ñåàíñîâîãî êëþ÷à .

Óñèëåíèå EKE

Áåëëîâèí (Bellovin) è Ìåððèòò (Merritt) ïðåäëîæèëè óëó÷øåíèå çàïðîñíî-îòâåòíîé ÷àñòè àëãîðèòìà, êîòîðîå ïîçâîëÿåò èçáåæàòü âîçìîæíîãî âñêðûòèÿ ïðè îáíàðóæåíèè êðèïòîàíàëèòèêîì ñòàðîãî çíà÷åíèÿ K.

Íà áàçîâûé ïðîòîêîë EKE. Íà ýòàïå (3) Àëèñà ãåíåðèðóåò äðóãîå ñëó÷àéíîå ÷èñëî S_A è ïîñûëàåò Áîáó

$E_K(R_A, S_A)$

Íà ýòàïå (4), Áîá ãåíåðèðóåò äðóãîå ñëó÷àéíîå ÷èñëî S_B è ïîñûëàåò Àëèñå

$E_K(R_A,,R_B,S_B)$

Òåïåðü Àëèñà è Áîá ìîãóò âû÷èñëèòü ñòîéêûé ñåàíñîâûé êëþ÷, $S_A \oplus S_B$. Ýòîò êëþ÷ â äàëüíåéøåì èñïîëüçóåòñÿ äëÿ ñîîáùåíèé, êîòîðûå îáìåíèâàþòñÿ Àëèñà è Áîá, K èñïîëüçóåòñÿ â êà÷åñòâå êëþ÷à îáìåíà êëþ÷àìè.

Ïîñìîòðèì íà óðîâíè çàùèùû, ïðåäîñòàâëÿåìûå EKE. Âîññòàíîâëåííûå çíà÷åíèå S íå äàåò Åâå íèêàêîé èíôîðìàöèè î P, òàê êàê P íèêîãäà íå èñïîëüçóåòñÿ äëÿ øèôðîâàíèÿ ÷åãî-òî òàêîãî, ÷òî âåäåò íåïîñðåäñòâåííî ê S. Êðèòè÷åñêîå çíà÷åíèå K òàêæå íåîçíàííî, K èñïîëüçóåòñÿ òîëüêî äëÿ øèôðîâàíèÿ ñëó÷àéíûõ äàííûõ, à S íèêîãäà íå øèôðóåòñÿ îòäåëüíî.

Ðàñøèðåííûé EKE

Ïðîòîêîë EKE ñòðàäàåò îäíèì ñåðüåçíûì íåäîñòàòêîì: îí òðåáóåò, ÷òîáû îáà ñòîðîíû çíàëè P. Â áîëüøèíñòâå ñèñòåì àâòîðèçàöèè äîñòóïà õðàíÿòñÿ çíà÷åíèÿ îäíîíàïðàâëåííîé õýø-ôóíêöèè ïàðîëåé ïîëüçîâàòåëåé, à íå ñàìè ïàðîëè (ñì. ðàçäåë 3.2). Ïðîòîêîë Ðàñøèðåííûé EKE (Augmented EKE, A-EKE) èñïîëüçóåò â âàðèàíòå EKE íà áàçå Diffie-Hellman çíà÷åíèå îäíîíàïðàâëåííîé õýø-ôóíêöèè ïàðîëÿ ïîëüçîâàòåëÿ â êà÷åñòâå êëþ÷à ñâåðõøèôðîâàíèÿ. Çàòåì ïîëüçîâàòåëü ïîñûëàåò äîïîëíèòåëüíîå ñîîáùåíèå, îñíîâàííîå íà ðåàëüíîì ïàðîëå, ýòî ñîîáùåíèå óäîñòîâåðÿåò çàíîâî âûáðàííûé ñàíñîâûé êëþ÷.

Âîò êàê ýòî ðàáîòàåò. Êàê è îáû÷íî, Àëèñà è Áîá õîòÿò ïðîâåðèòü ïîäëèííîñòü äðóã äðóãà è ãåíåðèðîâàòü îáùèé êëþ÷. Îíè âûáèðàþò êàêóþ-íèáóäü ñõåìó öèôðîâîé ïîäïèñè, â êîòîðîé â êà÷åñòâå çàêðûòîãî êëþ÷à ìîæåò èñïîëüçîâàòüñÿ ëþáîå ÷èñëî, à îêðûòûé êëþ÷ – ñîîòâåòñòâóþùàÿ ïàðà ÷èñåë. Íàïðèìåð, â êà÷åñòâå çàêðûòîãî êëþ÷à ìîæåò èñïîëüçîâàòüñÿ ëþáîå ïðîñòîå ÷èñëî, à îòêðûòûé êëþ÷ – ïàðà ÷èñåë g è n, ãäå g – ïåðâîîáðàçíûé ýëåìåíò ïî ìîäóëþ n. Ïîñëå ýòîãî ïðîèñõîäèò îáìåí îòêðûòûìè êëþ÷àìè, è îíè îáà ïîëó÷àþò îáùèé ñåàíñîâûé êëþ÷. Ïîñêîëüêó ïîëó÷åíèå äiñêðåòíîãî ëîãàðèôìà ÿâëÿåòñÿ âû÷èñëèòåëüíî òðóäíîé çàäà÷åé, ïîëó÷åíèå ñåàíñîâîãî êëþ÷à íà îñíîâå îòêðûòîãî êëþ÷à è ïåðåõâàò ïàêåòîâ íå äàþò çëîóìûøëåííèêó âîçìîæíîñòè âû÷èñëèòü ñåàíñîâûé êëþ÷.

Ïîñëå ýòîãî ïðîòîêîë ïåðåõîäèò â ôàçó àóòåíòèôèêàöèè. Íà ýòîì ýòàïå îáà ïîëüçîâàòåëÿ äîêàçûâàþò äðóã äðóãó, ÷òî îíè çíàþò ñåàíñîâûé êëþ÷. Ýòî ìîæíî ñäåëàòü ðàçëè÷íûìè ñïîñîáàìè, íî ìû îïèøåì òîëüêî îäèí èç íèõ, ïîñêîëüêó îí ïîëíîñòüþ îïèñûâàåò ïðèíöèï ðàáîòû ïðîòîêîëà. Ïóñòü $E_K(M)$ – ñèìâîëè÷åñêîå øèôðîâàíèå ñîîáùåíèÿ M ñ ïîìîùüþ êëþ÷à K, à $D_K(M)$ – ñîîòâåòñòâóþùàÿ îïåðàöèÿ äåøèôðîâàíèÿ. Òîãäà ïðîòîêîë ìîæíî îïèñàòü ñëåäóþùèì îáðàçîì:

(1) Àëèñà âûáèðàåò ñëó÷àéíîå ïîêàçàòåëü ñòåïåíè R_a è îòïðàâëÿåò

$E_{D'}(g^{r_B} \bmod n)$

(2) Áîá, êîòîðûé çíàåò òîëüêî P' è íå ìîæåò ïîëó÷èòü èç íåãî P, âûáèðàåò R_b è ïîñûëàåò

$E_D(g^{r_B} \bmod n)$

(3) Àëèñà è Áîá âû÷èñëÿþò îáùèé ñåàíñîâûé êëþ÷ $K= g^{r_A * r_B} \bmod n$. Íàêîíåö Àëèñà äîêàçûâàåò, ÷òî îíà ñàìà çíàåò P, à íå òîëüêî P', ïîñûëàÿ

$E_K(S_P(K))$

Áîá, êîòîðûé çíàåò K è P', ìîæåò ðàñøèôðîâàòü è ïðîâåðèòü ïîäïèñü. Òîëüêî Àëèñà ìîãëà ïðèñëàòü ýòî ñîîáùåíèå, òàê êàê òîëüêî îíà çíàåò P. Ñàìîçâàíäö, äîáûâøèé êîïèþ ôàéëà ïàðîëåé Áîáà, ìîæåò ïîïûòàòüñÿ P, íî îí íå ñìîæåò ïîäïèñàòü ñåàíñîâûé êëþ÷.

Ñõåìà A-EKE íå ðàáîòàåò ñ âàðèàíòîì EKE, èñïîëüçóþùèì îôôëàéí êëþ÷è, òàê êàê â ýòîì ïðîòîêîëå îäíà ñòîðîíà âûáèðàåò ñåàíñîâûé êëþ÷ è íàâÿçûâàåò åãî äðóãîé. Ýòî ïîçâîëÿåò âçëîìùèêó, çàïîëó÷èâøåìó D', âûïîëíèòü âñêðûòèå "÷åîâåê â ñåðåäèíå".

Ïðèìåíåíèå EKE

Áåëëîâèí è Ìåððèòò ïðåäëàãàþò èñïîëüçîâàòü ýòîò ïðîòîêîë äëÿ áåçîïàñíîé òåëåôîííîé ñâÿçè [109]:

> Ïðåäïîëîæèì, ÷òî ðàçâåðíóòà ñåòü øèôðóþùèõ òåëåôîííûõ àïïàðàòîâ. Åñëè êòî-íèáóäü õî÷åò âîñïîëüçîâàòüñÿ òàêèì òåëåôîííûì, òî ïîíàäîáèòñÿ îïðåäåëåííàÿ êëþ÷åâàÿ èíôîðìàöèÿ. Îáû÷íûé ýòàï ðàçâåðíóòü. . . òðåáóþò, ÷òîáû ó çâîíÿùåãî áûë ôèçè÷åñêèé êëþ÷. Âî ìíîãèõ ñèñòåìàõ ýòî íåæåëàòåëüíî. EKE ïîçâîëÿò èñïîëüçîâàòü êîðîòêèé, ââîäèìûé ñëåäîâàòåëüíî ïàðîëü, îáåñïå÷èâàÿ äîðàçâî áîëåå äëèííûé ñåàíñîâûé êëþ÷.
>
> EKE ìîã áû áûòü ïîëåçåí è äëÿ ñîòîâîé ñâÿçè. Ì îãèé÷åñòâî ïðåäñòàâëÿåò ñîáîé áîëüøóþ ïðîáëåìó ñîòîâîé òåëåôîíèè, EKE ìîæåò ïîìî÷ü çàùèòèòüñÿ îò íåãî (è îáñ÷èòü çàêðûòîñòü çâîíêà) çà ñ÷åò ïðîâàæè òåëåôîíîâ, áåñïîëåçíûõ áåç

> âââåäåíèÿ PIN-êîäà. Òàê êàê PIN-êîä íå õðàíèòñÿ â òåëåôîíå, åãî íåâîçìîæíî èçâëå÷ü èç óêðàäåííîãî ýêçåìïëÿðà.

Ãëàâíàÿ ñèëà EKE ñîñòîèò â òîì, ÷òî êðèïòîãðàôèÿ ñ îòêðûòûìè êëþ÷àìè è ñèììåòðè÷íàÿ êðèïòîãðàôèÿ îáúåäèíÿþòñÿ è óñèëèâàþò äðóã äðóãà:

> Â îáùåé ïåðñïåêòèâå EKE ðàáîòàåò êàê *óñèëèòåëü ñåêðåòíîñòè*. Òî åñòü, åãî ìîæíî èñïîëüçîâàòü äëÿ óñèëåíèÿ ñðàâíèòåëüíî ñëàáûõ ñèììåòðè÷íûõ è àñèììåòðè÷íûõ ñèñòåì, èñïîëüçóåìûõ âìåñòå. Ðàññìîòðèì, íàïðèìåð, ðàçìåð êëþ÷à, íåîáõîäèìûé äëÿ îáåñïå÷åíèÿ áåçîïàñíîñòè ïðè èñïîëüçîâàíèè îáìåíà êëþ÷îì - ïîêàçàòåëåì ñòåïåíè. Êàê ïîêàçàëè ËàÌà÷÷à (LaMacchia) è Îäëûæêî (Odlyzko) [934], äàæå ìîäóëè ñ ðàçìåðàìè, ñ÷èòàâøèìèñÿ áåçîïàñíûìè, (à èìåííî, 192 áèòà) ÷óâñòâèòåëüíû ê âñêðûòèþ, çàíèìàþùåìó íåñêîëüêî ìèíóò êîìïüþòåðíîãî âðåìåíè. Íî èõ âñêðûòèå ñòàíîâèòñÿ íåâîçìîæíûì, åñëè íåîáõîäèìî ïåðåä ïðèìåíåíèåì âñêðûòèÿ óãàäàòü ïàðîëü.
>
> Ñ äðóãîé ñòîðîíû, ñëîæíîñòü âñêðûòèÿ îáìåíà êëþ÷àìè - ïîêàçàòåëÿìè ñòåïåíè ìîæåò áûòü èñïîëüçîâàíà äëÿ ñðûâà ïîïûòîê óãàäàòü ïàðîëü. Âîçìîæíîñòü âñêðûòèÿ óãàäûâàíèåì ïàðîëÿ çàâèñèò îò ñêîðîñòè ïðîâåðêè êàæäîãî ïðåäïîëîæåíèÿ. Åñëè äëÿ âûïîëíåíèÿ òàêîé ïðîâåðêè íåîáõîäèìî âûïîëíèòü îáìåí êëþ÷àìè - ïîêàçàòåëÿìè ñòåïåíè, òî îáùåå âðåìÿ ýôôåêòèâíî âîçðàñòàåò.

EKE çàïàòåíòîâàí [111].

22.6 Çàùèùåííûå ïåðåãîâîðû î êëþ÷å

Ýòà ñõåìà òàêæå çàùèùàåò ïåðåãîâîðû î êëþ÷å îò ïëîõîãî âûáîðà ïàðîëåé è âñêðûòèé "÷åëîâåê â ñåðåäèíå" [47, 983]. Â íåé èñïîëüçóåòñÿ õýø-ôóíêöèÿ äâóõ ïåðåìåííûõ, îáëàäàþùàÿ îñîáåííûì ñâîéñòâîì: îíà ÷àñòî ïðèâîäèò ê ñòîëêíîâåíèÿì ïî ïåðâîé ïåðåìåííîé, è ïðàêòè÷åñêè íèêîãäà - ïî âòîðîé.

$H'(x,y) = H(H(k,x) \bmod 2^m, x)$, ãäå $H(k,x)$ - îáû÷íàÿ ôóíêöèÿ k è x

Âîò êàê âûãëÿäèò ýòîò ïðîòîêîë. Àëèñà è Áîá èñïîëüçóþò îáùèé ñåêðåòíûé ïàðîëü P è óæå îáìåíÿëèñü ñåêðåòíûì êëþ÷îì K, èñïîëüçóÿ îáìåí êëþ÷îì Dime-Hellman. Îíè èñïîëüçóþò P äëÿ ïðîâåðêè, ÷òî èõ ñåàíñîâûå êëþ÷è îäèíàêîâû (è ÷òî Åâà íå ïðåäïðèíÿëà âñêðûòèå "÷åëîâåê â ñåðåäèíå"), íå ïîçâîëÿÿ Åâå ïîëó÷èòü P.

(1) Àëèñà ïîñûëàåò Áîáó

$H'(P,K)$

(2) Áîá âû÷èñëÿåò $H'(P,K)$ è ñðàâíèâàåò ðåçóëüòàò ñî çíà÷åíèåì, ïðèñëàííûì Àëèñîé. Åñëè îíè ñîâïàäàþò, îí ïîñûëàåò Àëèñå

$H'(H(P,K))$

(3) Àëèñà âû÷èñëÿåò $H'(H(P,K))$ è ñðàâíèâàåò ðåçóëüòàò ñî çíà÷åíèåì, ïîëó÷åííûì îò Áîáà.

Åñëè Åâà ïûòàåòñÿ âûïîëíèòü âñêðûòèå "÷åëîâåê â ñåðåäèíå", îíà èñïîëüçóåò îäèí êëþ÷, K_1, îáùèé ñ Àëèñîé, è äðóãîé, K_2, îáùèé ñ Áîáîì. ×òîáû îáìàíóòü Áîáà íà ýòàïå (2), åé ïðèäåòñÿ âû÷èñëèòü îáùèé ïàðîëü è çàòåì ïîñëàòü Áîáó $H'(P,K_2)$. Ïðè èñïîëüçîâàíèè îáû÷íîé õýø-ôóíêöèè îíà ìîæåò ïåðåáèðàòü ÷àñòî âñòðå÷àþùèåñÿ ïàðîëè, ïîêà íå óãàäàåò ïðàâèëüíûé, è çàòåì óñïåøíî ïðîíèêíóòü â ïðîòîêîë. Íî ïðè èñïîëüçîâàíèè ïðåäëàãàåìîé õýø-ôóíêöèè, ìíîãèå ïàðîëè äàþò îäíî è òî æå çíà÷åíèå ïðè õýøèðîâàíèè ñ êëþ÷îì K_1. Ïîýòîìó, êîãäà îíà íàõîäèò ñîâïàäåíèå, òî ñêîðåå âñåãî ýòî íåïðàâèëüíûé ïàðîëü, è â ýòîì ñëó÷àå Áîáà îáìàíóòü íå óäàñòñÿ.

22.7 Ðàñïðåäåëåíèå êëþ÷à äëÿ êîíôåðåíöèè è ñåêðåòíàÿ øèðîêîâåùàòåëüíàÿ ïåðåäà÷à

Àëèñà õî÷åò ïåðåäàòü ñîîáùåíèå M ñðàçó íåñêîëüêèì ïîëó÷àòåëÿì. Îäíàêî îíà ñîâñåì íå õî÷åò, ÷òîáû êòî óãîäíî ñìîã ïðî÷åñòü åãî. Â äåéñòâèòåëüíîñòè, åé íóæíî, ÷òîáû òîëüêî ïîëó÷àòåëè èç îïðåäåëåííîãî ïîäìíîæåñòâà ìîãëè ïðàâèëüíî ðàñêðûòü M. Ó âñåõ îñòàëüíûõ äîëæíà ïîëó÷èòüñÿ ÷åïóõà.

Àëèñà ìîæåò èñïîëüçîâàòü äëÿ êàæäîãî ïîëó÷àòåëÿ îòëè÷íûé êëþ÷ (ñåêðåòíûé èëè îòêðûòûé). Îíà øèôðóåò ñîîáùåíèå êàêèì-íèáóäü ñëó÷àéíûì êëþ÷îì K. Çàòåì îíà øèôðóåò êîïèþ K êàæäûì èç êëþ÷åé âûáðàííûõ ïîëó÷àòåëåé ñîîáùåíèÿ. Íàêîíåö îíà øèðîêîâåùàòåëüíî ïîñûëàåò çàøèôðîâàííîå ñîîáùåíèå, à çàòåì âñå çàøèôðîâàííûå K. Ñëóøàþùèé ïåðåäà÷ó Áîá ëèáî ïûòàåòñÿ ðàñøèôðîâàòü âñå K ñâîèì ñåêðåòíûì êëþ÷îì, ïûòàÿñü íàéòè ïðàâèëüíûé, ëèáî, åñëè Àëèñà íå çàáûëà ïåðå÷èñëèòü ïîëó÷àòåëåé ñâîåãî ñîîáùåíèÿ, îí èùåò ñâîå èìÿ, ñîïðîâîæäàåìîå çàøèôðîâàííûì êëþ÷îì. Òàêæå áóäåò ðàáîòàòü è ðàíåå ðàññìîòðåííàÿ êðèïòîãðàôèÿ ñ íåñêîëüêèìè êëþ÷àìè.

Äðóãîé ñïîñîá ïðåäëàãàåòñÿ â [352]. Ñíà÷àëà êàæäûé èç ïîëó÷àòåëåé äîãîâàðèâàåòñÿ ñ Àëèñîé îá îáùåì äëÿ íèõ äâîèõ êëþ÷å, êîòîðûé äëèííåå ëþáîãî âîçìîæíîãî øèôðîâàííîãî ñîîáùåíèÿ. Âñå ýòè êëþ÷è äîëæíû áûòü âçàèìíî ïðîñòûìè. Îíà øèôðóåò ñîîáùåíèå ñëó÷àéíûì êëþ÷îì K. Çàòåì îíà âû÷èñëÿåò îäíî öåëîå ÷èñëî R, êîòîðîå ïî ìîäóëþ ñåêðåòíîãî êëþ÷à êîíãðóýíòíî K, åñëè ýòîò ñåêðåòíûé êëþ÷ ïðåäïîëàãàåòñÿ èñïîëüçîâàòü äëÿ ðàñøèôðîâêè ñîîáùåíèÿ, è êîíãðóýíòíî íóëþ â ïðîòèâíîì ñëó÷àå.

Íàïðèìåð, åñëè Àëèñà õî÷åò, ÷òîáû ñåêðåò ïîëó÷èëè Áîá, Êýðîë è Ýëëåí, íî íå Äýéâ è Ôðýíê, îíà øèôðóåò

ñîîáùåíèå êëþ÷îì K è çàòåì âû÷èñëÿåò òàêîå R, ÷òî

$R \equiv K \pmod{K_B}$

$R \equiv K \pmod{K_C}$

$R \equiv 0 \pmod{K_D}$

$R \equiv K \pmod{K_E}$

$R \equiv 0 \pmod{K_F}$

Ýòî ïðîòèâ àëãåáðàè÷åñêèõ ïðîáëåì, êîòîðûõ ëåãêî ìîæåò áûòü ðåøåíà Àëèñîé. Êîãäà ýòî ñîîáùåíèå áóäåò ïðèíÿòî ïîëó÷àòåëåì, îíè âû÷èñëÿò çíà÷åíèå ïîëó÷åííîãî êëþ÷à ïî ìîäóëþ èõ ñåêðåòíîãî êëþ÷à. Òå, êîìó ïðåäíàçíà÷àëñü ýòî ñîîáùåíèå, â ðåçóëüòàòå âû÷èñëåíèÿ ïîëó÷àò íóæíûé êëþ÷. Â ïðîòèâíîì ñëó÷àå ðåçóëüòàòîì áóäåò 0.

Åùå îäèí, òðåòèé, ïóòü, èñïîëüçóþùèé ïîðîãîâóþ ñõåìó (ñì. ðàçäåë 3.7), ïðåäëàãàåòñÿ â [141]. Êàê è â äðóãèõ ñïîñîáàõ êàæäûé ïîòåíöèàëüíûé ïîëó÷àòåëü ïîëó÷åò ñâîþ ÷àñòü ñåêðåòíîãî êëþ÷à. Ýòîò êëþ÷ ÿâëÿåòñÿ òåíüþ â åùå íå ñîçäàííîé ïîðîãîâîé ñõåìå. Àëèñà ñîðàñïðåäåëÿåò ðÿä ñåêðåòíûõ êëþ÷åé äëÿ ñåáÿ, âîñüì íåîòðèöàòåëüíûõ öåëûõ ÷èñåë, ìåíüøèõ M. Òîãäà äëÿ øèôîâàíèÿ ïðåäàííîãî ñîîáùåíèÿ M Àëèñà øèôóåò M êëþ÷îì K è äåëàåò ñëåäóþùåå.

(1) Àëèñà âûáèðàåò ñëó÷àéíîå ÷èñëî j. Ýòî ÷èñëî ïðèçâàíî çàùèùàòü êîëè÷åñòâî ïîëó÷àåìîé ñîîáùåíèÿ. Î íî íå äîëæíî áûòü ñëèøêîì áîëüøèì è äàæå ìåíüøå ðàâíÿòüñÿ íóëþ.

(2) Àëèñà ñîçäàåò ïîðîãîâóþ ñõåìó $(k + j + 1, 2k + j + 1)$, â êîòîðîé:

K - ýòî ñåêðåò.

Ñåêðåòíûå êëþ÷è äèñêðåòíûõ ñîîáùåíèÿ ñëóæàò òåíÿìè.

Ñåêðåòíûå êëþ÷è ïîëüçîâàòåëåé, êîòîðûõ íåò ñðåäè ïîëó÷àòåëåé ñîîáùåíèÿ, íå ÿâëÿþòñÿ òåíÿìè.

j òåíåé âûáèðàþòñÿ ñëó÷àéíûì îáðàçîì, íå ñîâïàäàÿ íè ñ îäíîì ñåêðåòíûì êëþ÷îì.

(3) Àëèñà øèôîâàùàòåëüíîì ïðåäâû÷èñëåíèè $k + j$ ñëó÷àéíî âûáèðàåò òåíåé, íè îäíà èç êîòîðûõ íå ñîâïàäàåò ñ òåíÿìè ýòàïà (2).

(4) Êàæäûé èç ñëóøàòåëåé, ïðèíÿâøèõ øèôîâàùàòåëüíîå ñîîáùåíèå, äîáàâëÿåò ñâîþ òåíü ê ïîëó÷åííûì $k + j$ òåíÿì. Åñëè äîáàâëåíèå ñâîé òåíè ïîçâîëÿåò ïîëüçîâàòåëþ âû÷èñëèòü ñåêðåò, òî åìó óäàëîñü îòêðûòü êëþ÷. Â ïðîòèâíîì ñëó÷àå - íå óäàëîñü.

Äðóãîé ïîäõîä ìîæíî íàéòè â [885, 886, 1194]. È åùå îäèí - â [1000].

Ðàñïðåäåëåííûå êëþ÷åé äëÿ êîíôåðåíöèè

Ýòîò ïðîòîêîë ïîçâîëÿåò ðóêîâîäèòåëþ n ïîëüçîâàòåëåé äîãîâîðèòüñÿ î ñåêðåòíîì êëþ÷å, èñïîëüçóÿ òîëüêî íåñåêðåòíûå êàíàëû. Ãðóïïà èñïîëüçóåò äâà îáùèõ áîëüøèõ ïðîñòûõ ÷èñëà p è q, à òàêæå ãåíåðàòîð g òîé æå äëèíû, ÷òî è q.

(1) Ï îëüçîâàòåëü i, ãäå i îò 1 äî n, âû÷èñëÿò ÷èñëî r_i, ìåíüøåå q, è øèôîâàùàòåëüíîì îòïðàâëÿåò

$z_i = g^{r_i} \bmod p$

(2) Êàæäûé ïîëüçîâàòåëü ïðîâåðÿåò, ÷òî $z_i^q \equiv 1 \pmod{p}$ äëÿ âñåõ i îò 1 äî n.

(3) i-ûé ïîëüçîâàòåëü øèôîâàùàòåëüíîì ïðåäàåò

$xi = (z_{i+1}/z_{i-1})^{r_i} \bmod p$

(4) i-ûé ïîëüçîâàòåëü âû÷èñëÿåò

$K = (z_{i-1})^{nr_i} * x_i^{n-1} * x_{i+1}^{n-2} * \ldots * x_{i-2} \bmod p$

Âñå âû÷èñëåíèÿ èíäåêñîâ â ïðèâåäåííîì ïðîòîêîëå - i-1, i-2 è i+1 - ïðîâîäÿòñÿ mod n. Ï îêîí÷àíèè ïðîòîêîëà ó âñåõ ÷åñòíûõ ïîëüçîâàòåëåé îêàæåòñÿ îäèí è òîò æå K. À âñå îñòàëüíûå íè÷åãî íå ïîëó÷àò. Îäíàêî ýòîò ïðîòîêîë íå ìîæåò óñòîÿòü ïåðåä âñêðûòèåì "÷åëîâåê â ñðåäíåé". Äðóãîé ïðîòîêîë, íå òàêîé õîðîøèé, ïðèâåäåí â [757].

Tateboyashi-Matsuzaki-Newman

Ýòîò ïðîòîêîë ðàñïðåäåëåíèÿ êëþ÷åé ïîäõîäèò äëÿ èñïîëüçîâàíèÿ â ñåòÿõ [1521]. Àëèñà õî÷åò ñ ïîìîùüþ Òðåíòà, KDC, ãåíåðèðîâàòü êëþ÷ äëÿ ñåàíñà ñâÿçè ñ Áîáîì. Âñåì ó÷àñòíèêàì èçâåñòåí îòêðûòûé êëþ÷ Òðåíòà

n. Òðåòèé èçâåñòíû äâà ïðîñòûõ ìíîæèòåëÿ *n*, è, ñëåäîâàòåëüíî, îí ìîæåò ëåãêî âû÷èñëèòü êâàäðàòíûå êîðíè ìîäóëþ *n*. Ñëåäóþùèé ïðîñòîé íåñìåðæèò íåêîòîðûõ äâóõ, íî ïîçâîëÿåò ïîëó÷èòü îáùåå ïðåäñòàâëåíèå.

(1) Àëèñà âûáèðàåò ñëó÷àéíîå ÷èñëî r_A è ïîñûëàåò Òðåòüþ

$r_A^3 \bmod n$

(2) Òðåòü ñîîáùàåò Áîáó, ÷òî êòî-òî õî÷åò îáìåíÿòüñÿ ñ íèì êëþ÷îì.

(3) Áîá âûáèðàåò ñëó÷àéíîå ÷èñëî $r_Á$ è ïîñûëàåò Òðåòüþ

$r_Á^3 \bmod n$

(4) Òðåòü, èñïîëüçóÿ ñâîé çàêðûòûé êëþ÷, ðàñøèôðîâûâàåò r_A è $r_Á$. Î í ïîñûëàåò Àëèñå

$r_A \oplus r_Á$

(5) Àëèñà âû÷èñëÿåò

$(r_A \oplus r_Á) \oplus r_A = r_Á$

Î íà èñïîëüçóåò $r_Á$ äëÿ áåçîïàñíîãî ñåàíñà ñâÿçè ñ Áîáîì.

Ïðîòîêîë âûãëÿäèò õîðîø, íî ñîäåðæèò çàìåòíûé èçúÿí. Êýðîë ìîæåò ïîäëóøàòü ýòàï(3) è èñïîëüçîâàòü ýòó èíôîðìàöèþ, âîñïîëüçîâàâøèñü ïîìîùüþ äîâåð÷èâîãî Òðåòüà è ñâîåãî ñîîáùíèêà Äýéâà, ÷òîáû ðàñêðûòü [1472].

(1) Êýðîë âûáèðàåò ñëó÷àéíîå ÷èñëî $r_Ñ$ è ïîñûëàåò Òðåòüþ

$r_Á^3 \, r_Ñ^3 \bmod n$

(2) Òðåòü ñîîáùàåò Äýéâó, ÷òî êòî-òî õî÷åò îáìåíÿòüñÿ ñ íèì êëþ÷îì.

(3) Äýéâ âûáèðàåò ñëó÷àéíîå ÷èñëî r_D è ïîñûëàåò Òðåòüþ

$r_D^3 \bmod n$

(4) Òðåòü, èñïîëüçóÿ ñâîé çàêðûòûé êëþ÷, ðàñøèôðîâûâàåò $r_Ñ$ è r_D. Î í ïîñûëàåò Êýðîë

$(r_Á \, r_C \bmod n) \oplus r_D$

(5) Äýéâ ïîñûëàåò r_D Êýðîë.

(6) Êýðîë èñïîëüçóåò r_C è r_D äëÿ ïîëó÷åíèÿ $r_Á$. Î íà èñïîëüçóåò $r_Á$ äëÿ ðàñøèôðîâûâàíèÿ ïåðâîãî Àëèñû è Áîáà.

Ýòî ïëîõî.

Ãëàâà 23
Ñïåöèàëüíûå àëãîðèòìû äëÿ ïðîòîêîëîâ

23.1 Êðèïòîãðàôèÿ ñ íåñåêðåòíûì êëþ÷îì

Ýòî îáîáùåíèå RSA (ñì. ðàçäåë 19.3) [217, 212]. Ì îäóëü n ÿâëÿåòñÿ ïðîèçâåäåíèåì äâóõ ïðîñòûõ ÷èñåë p è q. Îäíàêî âìåñòî e è d, äëÿ êîòîðûõ $ed \equiv 1 \bmod ((p-1)(q-1))$, âûáèðàþòñÿ t êëþ÷åé K_i, äëÿ êîòîðûõ âûïîëíÿåòñÿ

$$K_1 * K_2 * \ldots * K_t \equiv 1 \bmod ((p-1)(q-1))$$

Òàê êàê

$$M^{K_1 * K_2 * \ldots * K_t} = M$$

òî ýòà ñõåìà îêàçûâàåòñÿ ñõåìîé ñ íåñèìåòðè÷íûì êëþ÷îì, îïèñàííàÿ â ðàçäåëå 3.5.

Åñëè, íàïðèìåð, èñïîëüçóåòñÿ ïÿòü êëþ÷åé, òî ñîîáùåíèå, çàøèôðîâàííîå êëþ÷àìè K_3 è K_5, ìîæåò áûòü ðàñøèôðîâàíî ñ ïîìîùüþ K_1, K_2 è K_4.

$$C = M^{K_3 * K_5} \bmod n$$

$$M = C^{K_1 * K_2 * K_4} \bmod n$$

Îäíè èç ïðèìåíåíèé ýòîé ñõåìû ÿâëÿþòñÿ ïîäïèñàíèå äîêóìåíòà íåñèìåòðè÷íûì êëþ÷îì, êîãäà äëÿ òîãî, ÷òîáû äîêóìåíò áûë äåéñòâèòåëåí, îí äîëæåí áûòü ïîäïèñàí è Àëèñîé, è Áîáîì. Èñïîëüçóþòñÿ òðè êëþ÷à: K_1, K_2 è K_3. Àëèñà è Áîá ïîëó÷àþò ïî îäíîìó êëþ÷ó èç ïåðâûõ äâóõ, à òðåòèé ïîúáëèêîâûâàåòñÿ.

(1) Ñíà÷àëà Àëèñà ïîäïèñûâàåò M è ïîñûëàåò åãî Áîáó.

$$M' = M^{K_1} \bmod n$$

(2) Áîá ìîæåò âîññòàíîâèòü M ïî M'.

$$M = M'^{K_3 * K_5} \bmod n$$

(3) Î í ìîæåò òàêæå äîáàâèòü ñâîþ ïîäïèñü.

$$M'' = M'^{K_2} \bmod n$$

(4) Ïðîâåðèòü ïîäïèñè ìîæíî ïðè ïîìîùè îòêðûòîãî êëþ÷à K_3.

$$M = M''^{K_3} \bmod n$$

Îáðàòèâ âíèìàíèå, ÷òî äëÿ ðàáîòîñïîñîáíîñòè ýòîé ñèñòåìû íóæíà çàñëóæèâàþùàÿ äîâåðèÿ ñòîðîíà, êîòîðàÿ óñòàíîâèëà áû ñèñòåìó è âûäàëà êëþ÷è Àëèñå è Áîáó. Òà æå ïðîáëåìà ñóùåñòâóåò è â ñõåìå [484]. Áîëåå òî íåàÿ ñõåìà îïèñàíà â [695, 830, 700], Í î óñëîâíî, ïðåäïðèíÿòûå äëÿ ïðîâåðêè, ïðîïîðöèîíàëüíû êîëè÷åñòâó ïîäïèñûâàþùèõ. Íîâûå ñõåìû [220, 1200], îñíîâàííûå íà ñõåìàõ èäåíòèôèêàöèè ñ íóëåâûì çíàíèåì, ïðåäîëàãàþò ýòè íåäîñòàòêè ïðåäøåñòâóþùèõ ñèñòåì.

23.2 Àëãîðèòìû ðàçäåëåíèÿ ñåêðåòà

Â ðàçäåëå 3.7 ÿ ðàññìàòðèâàë èäåþ, èñïîëüçóþ â ñõåìàõ ðàçäåëåíèÿ ñåêðåòà. ×åòûðå ïðèâåäåííûõ íèæå ðàçëè÷íûõ àëãîðèòìà ïðåäñòàâëÿþò ñîáîé ÷àñòíûå ñëó÷àè îáùåãî òåîðåòè÷åñêîãî ïîäõîäà [883].

Ñõåìà èíòåðïîëÿöèîííîãî ìíîãî÷ëåíà Ëàãðàíæà

Äëÿ ñîçäàíèÿ ïîðîãîâîé ñõåìû Àäè Øàìèð âîñïîëüçîâàëñÿ óðàâíåíèÿì äëÿ ìíîãî÷ëåíîâ â êîíå÷íîì ïîëå [1414]. Âûáåðåì ïðîñòîå ÷èñëî p, êîòîðîå áîëüøå êîëè÷åñòâà âîçìîæíûõ òåíåé è áîëüøå ñàìîãî áîëüøîãî èç âîçìîæíûõ ñåêðåòîâ. ×òîáû ñäåëàòü ñåêðåò îáùèì, ñäåíåðóåì ïðîèçâîëüíîé ìíîãî÷ëåí ñòåïåíè m-1. Íàïðèìåð, åñëè íóæíî ñîçäàòü ïîðîãîâóþ ñõåìó (3,n) (äëÿ âîññòàíîâëåíèÿ M ïîòðåáóþòñÿ òðè òåíè), ãåíåðèðóþòñÿ êâàäðàòè÷íûé ìíîãî÷ëåí

$$(ax^2 + bx + M) \bmod p$$

ãäå p - ýòî ñëó÷àéíîå ïðîñòîå ÷èñëî, áîëüøåå ëþáîãî èç êîýôôèöèåíòîâ. Êîýôôèöèåíòû a è b âûáèðàþòñÿ ñëó÷àéíûì îáðàçîì, îíè õðàíÿòñÿ â òàéíå è îòáðàñûâàþòñÿ ïîñëå òîãî, êàê ðàñïðåäåëÿþòñÿ òåíè. M - ýòî ñîîáùåíèå. Ïðîñòî ÷èñëî äîëæíî áûòü îïóáëèêîâàíî. Òåíè ïîëó÷àþòñÿ ñ ïîìîùüþ âû÷èñëåíèÿ ìíîãî÷ëåíà â n ðàçëè÷íûõ òî÷êàõ:

$k_i = F(x_i)$

Äðóãèì ñëîâàìè, ïåðâîé òåíüþ ìîæåò áûòü çíà÷åíèå ìíîãî÷ëåíà ïðè $x = 1$, âòîðîé òåíüþ - çíà÷åíèå ìíîãî÷ëåíà ïðè $x = 2$, è ò.ä.

Òàê êàê â êâàäðàòè÷íûõ ìíîãî÷ëåíàõ òðè íåèçâåñòíûõ êîýôôèöèåíòà, a, b è M, äëÿ ñîçäàíèÿ òðåõ óðàâíåíèé ìîæíî èñïîëüçîâàòü ëþáûå òðè öåëûå. Îäíîé èëè äâóõ òåñåí íå õâàòèò, à ÷åòûðåõ èëè ïÿòè òåñåí áóäåò ìíîãî.

Íàïðèìåð, ïóñòü M ðàâíî 11. ×òîáû ñîçäàòü ïîðîãîâóþ ñõåìó (3, 5), â êîòîðîé ëþáûå òðîå èç ïÿòè ÷åëîâåê ìîãóò âîññòàíîâèòü M, ñíà÷àëà ïîëó÷èì êâàäðàòè÷íóþ óðàâíåíèå (7 è 8 - ñëó÷àéíî âûáðàííûå ÷èñëà chosen randomly):

$F(x) = (7x^2 + 5x + 11) \bmod 13$

Ïÿòüþ òåíÿìè ÿâëÿþòñÿ:

$k_1 = F(1) = 7 + 8 + 11 \equiv 0 \pmod{13}$

$k_2 = F(2) = 28 + 16 + 11 \equiv 3 \pmod{13}$

$k_3 = F(3) = 63 + 24 + 11 \equiv 7 \pmod{13}$

$k_4 = F(4) = 112 + 32 + 11 \equiv 12 \pmod{13}$

$k_5 = F(5) = 175 + 40 + 11 \equiv 5 \pmod{13}$

×òîáû âîññòàíîâèòü M ïî òðåì òåíÿì, íàïðèìåð, k_2, k_3 è k_5, ðåøàåòñÿ ñèñòåìà ëèíåéíûõ óðàâíåíèé:

$a*2^2 + b*2 + M = 3 \pmod{13}$

$a*3^2 + b*3 + M = 7 \pmod{13}$

$a*5^2 + b*5 + M = 5 \pmod{13}$

Ðåøåíèåì áóäóò $a = 7$, $b = 8$ è $M = 11$. Èòàê, M ïîëó÷åíî.

Ýòó ñõåìó ðàçäåëåíèÿ ìîæíî ëåãêî ðàñøèðèòü äëÿ áîëüøåãî ÷èñëà. Åñëè âû õîòèòå ðàçáèòü ñîîáùåíèå íà 30 ðàâíûõ ÷àñòåé òàê, ÷òîáû âîññòàíîâèòü ñîîáùåíèå ìîæíî áûëî, îáúäèíèâ ëþáûå øåñòü èç íèõ, âûäàéòå êàæäîìó èç 30 ÷åëîâåê çíà÷åíèÿ ìíîãî÷ëåíà ïÿòîé ñòåïåíè.

$F(x) = ax^5 + bx^4 + cx^3 + dx^2 + ex + M \pmod{p}$

Øåñòü ÷åëîâåê ìîãóò øåñòü íåèçâåñòíûõ (âêëþ÷àÿ M), íî ïÿòåðûì íå óäàñòñÿ óçíàòü íè÷åãî îá M.

Íàèáîëåå âïå÷àòëÿþùèì ìîìåíòîì èñïîëüçîâàíèÿ ñåêðåòà ÿâëÿåòñÿ òî, ÷òî, åñëè êîýôôèöèåíòû âûáðàíû ñëó÷àéíûì îáðàçîì, ïÿòè ÷åëîâåê äàæå ïðè ïîìîùè áåñêîíå÷íûõ âû÷èñëèòåëüíûõ ìîùíîñòåé íå ñìîãóò óçíàòü íè÷åãî, êðîìå äëèíû ñîîáùåíèÿ (êòîðàÿ è òàê è èçâåñòíà). Ýòî òàêæå áåçîïàñíî, êàê îäíîðàçîâûé áëîêíîò, ïîïûòêà âûïîëíèòü èñ÷åðïûâàþùèé ïîèñê (òî åñòü, ïåðåáîð âñåõ âîçìîæíûõ øåñòîê òåíåé) ïîêàæåò, ÷òî ëþáîå âîçìîæíîå ñîîáùåíèå îñòàíåòñÿ ñåêðåòíûì. Ýòî ñïðàâåäëèâî äëÿ âñåõ ïðåäûäóùèõ â ýòîé êíèãå ñõåì ðàçäåëåíèÿ ñåêðåòà.

Âåêòîðíàÿ ñõåìà

Äæîðäæ Áëýêëè (George Blakley) èçîáðåë ñõåìó, èñïîëüçóþùóþ ïîíÿòèå òî÷êè â ïðîñòðàíñòâå [182]. Ñîîáùåíèå îïðåäåëÿåòñÿ êàê òî÷êà â m-ìåðíîì ïðîñòðàíñòâå. Êàæäàÿ òåíü - ýòî óðàâíåíèå (m-1)-ìåðíîé ãèïåðïëîñêîñòè, ñîäåðæàùåé ýòó òî÷êó.

Íàïðèìåð, åñëè äëÿ âîññòàíîâëåíèÿ ñîîáùåíèÿ íóæíû òðè òåíè, òî îíî ÿâëÿåòñÿ òî÷êîé â òðåõìåðíîì ïðîñòðàíñòâå. Êàæäàÿ òåíü ïðåäñòàâëÿåò ñîáîé èíóþ ïëîñêîñòü. Çíàÿ îäíó òåíü, ìîæíî óòâåðæäàòü, ÷òî òî÷êà íàõîäèòñÿ ãäå-òî íà ïëîñêîñòè. Çíàÿ âòîðóþ òåíü - ÷òî îíà íàõîäèòñÿ ãäå-òî íà ëèíèè ïåðåñå÷åíèÿ äâóõ ïëîñêîñòåé. Çíàÿ òðè òåíè, ìîæíî òî÷íî îïðåäåëèòü, ÷òî òî÷êà íàõîäèòñÿ íà ïåðåñå÷åíèè òðåõ ïëîñêîñòåé.

Asmuth-Bloom

Â ýòîé ñõåìå èñïîëüçóþòñÿ ïðîñòûå ÷èñëà [65]. Äëÿ (m, n)-ïîðîãîâîé ñõåìû âûáèðàþòñÿ áîëüøîå ïðîñòîå ÷èñëî p, áîëüøåå M. Çàòåì âûáèðàþòñÿ ÷èñëà, ìåíüøèå p - d_1, d_2, . . . d_n, äëÿ êîòîðûõ:

1. Çíà÷åíèÿ d_i óïîðÿäî÷åíû ïî âîçðàñòàíèþ, $d_i < d_{i+1}$
2. Êàæäîå d_i âçàèìíî ïðîñòî ñ ëþáûì äðóãèì d_i
3. $d_1*d_2* \ldots *d_m > p*d_{n-m+2}*d_{n-m+3}* \ldots *d_n$

×òîáû ðàñïðåäåëèòü òåíè, ñíà÷àëà âûáèðàþòñÿ ñëó÷àéíîå ÷èñëî r è âû÷èñëÿþòñÿ

$M' = M + rp$

Òåíÿìè, k_i, ÿâëÿþòñÿ

$k_i = M' \bmod d_i$

Îáúåäèíèâ ëþáûå m òåíåé, ìîæíî âîññòàíîâèòü M, èñïîëüçóÿ êèòàéñêóþ òåîðåìó îá îñòàòêàõ, íî ýòî íåâîçìîæíî ñ ïîìîùüþ ëþáûõ m-1 òåíåé. Ïîäîáíûå ïðèâåäåíû â [65].

Karnin-Greene-Hellman

Â ýòîé ñõåìå èñïîëüçóåòñÿ ìàòðè÷íûå óìíîæåíèå [818]. Âûáèðàþòñÿ n+1 m-ìåðíûõ âåêòîðîâ, V_0, V_1, . . . V_n, òàê, ÷òî ðàíã ëþáîé ìàòðèöû ðàçìåðîì m*m, îáðàçîâàííîé èç ýòèõ âåêòîðîâ, ðàâåí m. Âåêòîð U - ýòî âåêòîð ðàçìåðíîñòè m+1.

M - ýòî ìàòðè÷íûå ïðîèçâåäåíèå $U{\cdot}V_0$. Òåíÿìè ÿâëÿþòñÿ ïðîèçâåäåíèÿ $U{\cdot}V_i$, ãäå i ìåíÿåòñÿ îò 1 äî n.

Ëþáûå m òåíåé ìîæíî èñïîëüçîâàòü äëÿ ðåøåíèÿ ñèſòåìû ëèíåéíûõ óðàâíåíèé ðàçìåðíîñòè m*m, íåèçâåñòíûìè ÿâëÿþòñÿ êîýôôèöèåíòû U. $U{\cdot}V_0$ ìîæíî âû÷èñëèòü ïî U. Èñïîëüçóÿ ëþáûå m-1 òåíåé, ðåøèòü ñèſòåìó óðàâíåíèé è, òàêèì îáðàçîì, âîññòàíîâèòü ñåêðåò íåîçìîæíî.

Áîëåå ñëîæíûå ïðîãîâîðû ñõåìû

Â ïðåäûäóùèõ ïðèìåðàõ ïîêàçàíû òî÷íûå ïðîñòåéøèå ïîðîãîâûå ñõåìû: ñåêðåò äåëèòñÿ íà n òåíåé òàê, ÷òîáû, îáúåäèíèâ ëþáûå m èç íèõ, ìîæíî áûëî ðàſêðûòü ſåêðåò. Íà áàçå ýòèõ àëãîðèòìîâ ìîæíî ſîçäàòü íàſíãî áîëåå ſëîæíûå ſõåìû. Â ſëåäóþſèõ ïðèìåðàõ áóäåò èſïîëüçîâàòüſÿ àëãîðèòì Øàìèðà, õîòÿ áóäóò ðàáîòàòü è âſå îſòàëüſíûå.

×òîáû ſîçäàòü ſõåìó, â êîòîðîé îäíî èç ó÷àſòíèêîâ âàæíåå äðóãèõ, åſó âûäàåſſÿ áîëüſå òåſíåé. Åſëè äëÿ âſſſòàſîâëåſíèÿ ſåêðåòà íóæſî ïÿòü òåſíåé, è ó êîãî-òî åſòü òðè òåſíè, à ó âſåõ îſòàëüſûõ - ïî îäſíé, ýòîſ ÷åſîſåê âìåſòſ ſ ëþáûſè äâóſÿ äðóãſìè ſîæåſ âſſſòàſîâèòü ſåêðåò. Áåç åãî ó÷àſòſÿ äëÿ âſſſòàſîâëåſíèÿ ſåêðåòà ſîòðåáóåſſÿ ſÿòü ÷åſîâê.

Ïî íåſêîſüſî òåſíåé ſîãóſ ſîſó÷èſü äâà ÷åſîâåſê è áſëåå. Êàæäſî ſ ÷åſîâåſó ſîæåſ áûſü âûäàſſ îſëè÷íſå ÷èſſî òåſíåé. Íåçàâèſſſ îſ òſîãſ, ſêſëüſî òåſíåé áûſ ðſçäſſ, äëÿ âſſſòàſîâëåſíèÿ ſåêðåòà ſſòðåáóåſſÿ ëþáûå m èç íèſ. Íſ îäſí ÷åſîâåê, íſ öåäàÿ ãðóſ ſà íåſſſîſóſ âſſſòàſîâſèſü ſåêðåò, ſâſäàäàÿ òſëüſî m-1 òåſÿſ.

Äëÿ äðóãſſ ſõåſ ſſåäſſòàâſ ſ ſöſíàðſéſ ſ äâóſÿ âðàæäåáſſûſ ſ äåſåâàäöſÿſ. Ì îæſî ðàſſðåäſåſſöſ ſåêðåò òàê, ſòſáû äëÿ åãî âſſſòàſîâëåſíèÿ ſſòðåſîâàſſſüſ äâſå èç 7 ó÷àſòſíèêſî äåëåãàöſè A è òðſå èç 12 ó÷àſòſíèêſî äåëåãàöſè B. Ñſçäåòſÿ ſſſîſ÷ëåſ ſòſðſáſ 3, êſòſðûſ ÿâëÿåſÿ ſðſèſâåäåſſåſ ëſíåſſſîſ è êâàäðàòſſîſ âſðåæſſſé. Êàæäſſ ó÷àſòſíèêſ äåëåãàöſè A âſäàåòſÿ òåſſ, êſòſðàÿ ÿâſÿåòſÿ çſà÷åſſåſ ëſíåſſſîſ âſðàæåſſÿ, à ó÷àſòſíèêſſ äåëåãàöſè B âſäàþſÿ çſà÷åſſÿ êâàäðàòſ÷ſſîſ âſðàæåſſÿ.

Äëÿ âſſſòàſîâëåſíèÿ ëſíåſſſîſ âſðàæåſſÿ äſſòàòſ÷ſû ëþáûå äâå òåſè ó÷àſòſíèêſî äåëåãàöſè A, ſſ ſåçàâſſſſſ ſòſ òſîãſ, ſêſëüſî äðóãſſ òåſſé åſſòü ó äåëåãàöſè, åå ó÷àſòſíèêſ ſå ſſſîãóſ ſè÷åſî óſſàòü ſ ſåêðåòà. Àſäſëſîãſ÷ſſî äëÿ äåëåãàöſè B: åå ó÷àſòſíèêſ ſſîãóſ ſëſæèſü òðſ òåſè, âſſſòàſâëſâàÿ êâàäðàòſſſîſå âſðàæåſſſå, ſſ äðóãóþ èſſôſðſàöſþ, ſåſáſîäſſóþ äëÿ âſſſòàſſîâëſſÿ ſåêðåòà â öåſſ, ſſſè ſſëó÷èſü ſå ſſſîãóſ. Òſëüſî ſåðåſſſæſâ ſſâſè âſðàæåſſÿ, ó÷àſòſíèêſ äâóſ äåëåãàöſé ſſſîãóſ âſſſòàſîâſèſü ſåêðåòà [1462, 1463, 1464].

Â ſáſåſ ſëó÷åå, ſſæåò áſûſ ðåäëèçſâàſà ëþáàÿ ſſſëſſſàÿ ſõåſà ðàçäåëſſſÿ ſåêðåòà. Ïſòðåáóåſſÿ òſëüſî íàſèſàòſ ſèſſòåſſſ óðàâſſſé, ſſſòſâåòſſòâóſſſèſ êſſſêðåòſſſé ſèſſòåſſ. Âſò íåſêſëüſî ſðåêðàſſſûſ ſòàòåé íà òåſſ ſáſâſſåſſſûſ ſõåſ ðàçäåëſſſÿ ſåêðåòà [1529, 1463, 1464].

Ðàçäåëſſſå ſåêðåòà ſ ſſøſſſèſſſ

Ýòſò àëãſðèòſ èçſåſÿåò ſòàſſäàðòſſóþ ſſðſſãſâóþ ſõåſó (m, n) äëÿ ſáſàðóæåſſÿ ſſøſſſèſſſâ [1529]. ß ſſſêàæó åãſ èſſſſëüçſſàſſèå ſà áàçå ſõåſû Ëàãðàſæà, ſſ àëãſðèòſ ðàſſòàåò è ſ äðóãèſè ſõåſàſè. Âûáèðàåſſÿ ſðſſòſå ÷èſëſ p, áſëüøåå n è áſëüøåå

$(s - 1)(m - 1)/e + m$

ãäå s - ýòſ ſàſûé áſëüøſé âſçſſæſûé ſåêðåò, à e - âåðſÿòſſſòü óſſſåõà ſſøſſſè÷åſòâà. e ſſæſſ ſäåëàòü ſàſòſſëüêſ ſàëûſ, ſàſêſſëüêſ ýòſ ſåſáſõſäſſſ, ýòſ ſðſſòſ óſëſæſèò âû÷èſëſſÿ. Ïſòðſéóå òåſè êàê ðàſüøå, ſſ âſåſòſ èſſſſëüçſſàſſèÿ 1, 2, 3, . . . , n äëÿ x_i, âûáåðèòå ſëó÷àéſûſ ſſáàçſſ ÷èſëà èç äèàſàçſſà îò 1 äſ p-1.

Òåſſåðü, åſëè Ìýëſſðè ſðè âſſſòàſſâëſèè ſåêðåòà çàſåſèò ſſâſ ÷àſòſ ſſääåëêſé, åãſ òåſü ſ âûſſſêſé ååſſſòſſſüſ ſêàæåòſÿ ſåâſçſſæſſé. Íåſſçſſæſûé ſåêðåò, êſſå÷ſſ æå, ſêàæåòſÿ ſſääåëàſſûſ ſåêðåòſſ. Ìàòåſàòèêà ýòſé ſõåſû ſðèâëäſſà â [1529].

Ê ſſæàëåſèþ, õſòÿ ſſøſſſè÷åſòâſ Ìýëſſðè è áóäåò ſòêſûòſ, åſó óäàſòſÿ óçſàòü ſåêðåò (ſðè óſëſſâèè, ÷òſ âſå ſſòàëüſûå ſóæſûå òåſè ſðàâëëüſû). Îò ýòſſ çàùèſàåò äðóſſé ſðſòſſêſë, ſſèſàſſûé â [1529, 975]. Îſſſâ-

íîé èäåé ÿâëÿåòñÿ èñïîëüçîâàíèå íàáîðà èç k ñåêðåòîâ, òàê ÷òîáû íèêòî èç ó÷àñòíèêîâ çàðàíåå íå çíàë, êàêîé èç íèõ ïðàâèëüíûé. Êàæäûé ñåêðåò, çà èñêëþ÷åíèåì íàñòîÿùåãî, áîëüøå ïðåäûäóùåãî. Ó÷àñòíèêè îáúåäèíÿþò ñâîè òåíè, ïîëó÷àÿ îäèí ñåêðåò çà äðóãèì, ïîêà îíè íå ïîëó÷àò íàèìåíüøåé çíà÷åíèå ñåêðåòà. Ýòîò ñåêðåò è áóäåò ïðàâèëüíûì.

Â ýòîé ñõåìå ìîøåííèêè ëåãêî âûÿâëÿþòñÿ åùå äî ïîëó÷åíèÿ êîíå÷íîãî ñåêðåòà. Ñóùåñòâóåò îïðåäåëåííûå ñëîæíîñòè, åñëè ó÷àñòíèêè ïðåäúÿâëÿþò ñâîè òåíè ïî î÷åðåäè, ïîäôîáíîñòè ìîæíî íàéòè â ëèòåðàòóðå. Â ñëåäóþùèõ ðàáîòàõ òàêæå ðàññìàòðèâàþòñÿ îáîáùåííûå è ïðåäîòâðàùåíèå ìîøåííè÷åñòâà â ïîðîãîâûõ ñõåìàõ [355, 114, 270].

23.3 Ï î äñ î ç íàòåëüí û é êà íàë

Ong-Schnorr-Shamir

Ýòîò ïîäñîçíàòåëüíûé êàíàë (ñì. ðàçäåë 4.2), ðàçðàáîòàííûé Ãóñòàâóñîì Ñèììîíñîì (Gustavus Simmons) [1458, 1459, 1460], èñïîëüçóåò ñõåìó èäåíòè÷íîé Ong-Schnorr-Shamir (ñì. ðàçäåë 20.5). Êàê è â îðèãèíàëüíîé ñõåìå îòðàæåíèå (Àëèñà) âûáèðàåò îáùåäîñòóïíûé ìîäóëü n è çàêðûòûé êëþ÷ k òàê, ÷òîáû n è k áûëè âçàèìíî ïðîñòûìè ÷èñëàìè. Â îòëè÷èå îò îðèãèíàëüíîé ñõåìû k èñïîëüçóåòñÿ ñîâìåñòíî Àëèñîé è Áîáîì, ïîëó÷àåìûì â ïîäñîçíàòåëüíîì êàíàëå. Îòêðûòûé êëþ÷ âû÷èñëÿåòñÿ ñëåäóþùèì îáðàçîì:

$h = -k^2 \bmod n$

Åñëè Àëèñå íóæíî îòïðàâèòü ïîäñîçíàòåëüíîå ñîîáùåíèå M â áåçîáèäíîì ñîîáùåíèè M', îíà ñíà÷àëà ïðîâåðÿåò, ÷òî ïàðû M' è n, à òàêæå M è n ÿâëÿþòñÿ âçàèìíî ïðîñòûìè ÷èñëàìè. Àëèñà âû÷èñëÿåò

$S_1 = 1/2*((M'/M + M)) \bmod n$

$S_2 = 1/2*((M'/M - M)) \bmod n$

Ïàðà ÷èñåë S_1 è S_2 ïðåäñòàâëÿåò ñîáîé ïîäïèñü â òðàäèöèîííîé ñõåìå Ong-Schnortr-Shamir è îáíîâëÿåò ïîñëåäíþþ íîñèòåëü ïîäñîçíàòåëüíîãî ñîîáùåíèÿ.

Òðåòüåé Óîëòð (ïîìíèòå òàêîãî?) ìîæåò ïðîâåðèòü ïîäëèííîñòü ñîîáùåíèÿ, êàê ýòî ïðèíÿòî â Ong-Schnorr-Shamir, íî Áîá ìîæåò ñäåëàòü åùå êîå-÷òî. Î í ìîæåò ïðîâåðèòü ïîäëèííîñòü ñîîáùåíèÿ (Âñåãäà âîçìîæíî, ÷òî Óîëòð ïîïûòàåòñÿ åìó ïîäñóíóòü ïîääåëüíîå ñîîáùåíèå). Î í ïðîâåðÿåò, ÷òî

$S_1^2 - S_2^2 \equiv M' \pmod n$

Åñëè ïîäëèííîñòü ñîîáùåíèÿ äîêàçàíà, ïîëó÷àòåëü ìîæåò èçâëå÷ü è ïîäñîçíàòåëüíîå ñîîáùåíèå, èñïîëüçóÿ ñëåäóþùóþ ôîðìóëó:

$M=M'/(S_1 + S_2 k^{-1}) \bmod n$

Ýòî ðàáîòàåò, íî íå çàáûâàéòå, ÷òî ñàìà ñõåìà Ong-Schnorr-Shamir áûëà âçëîìàíà.

ElGamal

Äðóãîé ïðåäëîæåííûé Ñèìîíîì ïîäñîçíàòåëüíûé êàíàë [1459], îïèñàííûé â [1407, 1473], îñíîâàí íà ñõåìå ïîäïèñè ElGamal ñì. ðàçäåë 19.6).

Ãåíåðàòîð êëþ÷à âûïîëíÿåòñÿ òàêæå, êàê è â îñíîâíîé ñõåìå ïîäïèñè ElGamal. Ñíà÷àëà âûáèðàþòñÿ ïðîñòîå ÷èñëî p è ââà ñëó÷àéíûõ ÷èñëà, g è r, ìåíüøèå p. Çàòåì âû÷èñëÿåòñÿ

$K = g^r \bmod p$

Îòêðûòûì êëþ÷îì ñëóæàò K, g è p. Çàêðûòûì êëþ÷îì ÿâëÿåòñÿ r. Ï î ì è ì Àëèñû r èçâåñòíî è Áîáó, ýòî ÷èñëî èñïîëüçóåòñÿ íå òîëüêî äëÿ ïîäïèñè áåçîáèäíîãî ñîîáùåíèÿ, íî è â êà÷åñòâå êëþ÷à äëÿ îòðàâêè è ÷òåíèÿ ïîäïèñàííîãî ñîîáùåíèÿ.

×òîáû ïîñëàòü ïîäïèñàííîå ñîîáùåíèå M â áåçîáèäíîì ñîîáùåíèè, M', M è p äîëæíû áûòü ïîïàðíî âçàèìíî ïðîñòûì è, êðîìå òîãî, âçàèìíî ïðîñòûì äîëæíû áûòü M è p-1. Àëèñà âû÷èñëÿåò

$X = g^M \bmod p$

è ðåøàåò ñëåäóþùåå óðàâíåíèå äëÿ Y (ñ ïîìîùüþ ðàñøèðåííîãî àëãîðèòìà Ýâêëèäà):

$M' = rX + MY \bmod (p\text{-}1)$

Êàê è â áàçîâîé ñõåìå ElGamal, ïîäïèñü ÿâëÿåòñÿ ïàðà ÷èñåë: X è Y. Óîëòð ìîæåò ïðîâåðèòü ïîäïèñü ElGamal. Î í óáåæäàåòñÿ, ÷òî

$K^X X^Y \equiv g^{M'} \pmod p$

Áîá ìîæåò âîññòàíîâèòü ïîäïîçíàòåëüíîå ñîîáùåíèå. Ñíà÷àëà îí óáåæäàåòñÿ, ÷òî

$(g^r)^X X^Y \equiv g^{M'} \pmod p$

Åñëè ýòî òàê, îí ñ÷èòàåò ñîîáùåíèå ïîäëèííûì (íå ïîääåëàííûì Óîëòåðîì). Çàòåì äëÿ âîññòàíîâëåíèÿ M îí âû÷èñëÿåò

$M = (Y^{-1} (M' - rX)) \bmod (p - 1)$

Íàïðèìåð, ïóñòü $p = 11$, à $g = 2$. Çàêðûòûé êëþ÷ r âûáèðàåòñÿ ðàâíûì 8. Ýòî îçíà÷àåò, ÷òî îòêðûòûì êëþ÷îì, êîòîðûé Óîëòåð ìîæåò èñïîëüçîâàòü äëÿ ïðîâåðêè ïîäïèñè, áóäåò $g^r \bmod p = 2^8 \bmod 11 = 3$.

×òîáû îòïðàâèòü ïîäïèñàííîå ñîîáùåíèå $M = 9$, èñïîëüçóÿ áåçîáèäíîå ñîîáùåíèå $M' = 5$, Àëèñà ïðîâåðÿåò, ÷òî 9 è 11, à òàêæå 5 è 11 ïîïàðíî âçàèìíî ïðîñòû. Îíà òàêæå óáåæäàåòñÿ, ÷òî âçàèìíî ïðîñòû 9 è 11-1=10. Ýòî òàê, ïîýòîìó îíà âû÷èñëÿåò

$X = g^{M'} \pmod p = 2^9 \bmod 11 = 6$

Çàòåì îíà ðåøàåò ñëåäóþ ùåå óðàâíåíèå äëÿ Y:

$5 = 8\ 6 + 9\ Y \bmod 10$

Y= 3, ïîýòîìó ïîäïèñü ïàðà ÷èñåë 6 è 3 (X è Y). Áîá óáåæäàåòñÿ, ÷òî

$(g^r)^X X^Y \equiv g^{M'} \pmod p$

$(2^8)^6 6^3 \equiv 2^5 \pmod{11}$

Ýòî òàê (âû ïîëíèòå àðèôìåòè÷åñêèå äåéñòâèÿ ñàìîñòîÿòåëüíî, åñëè âû íå íà âåðèòå), ïîýòîìó îí ìîæåò ðàñêðûòü ïîäïîçíàòåëüíîå ñîîáùåíèå, âû÷èñëÿÿ

$M = (Y^{-1} (M' - rX)) \bmod (p - 1) = 3^{-1}(5 - 8*6) \bmod 10 = 7(7) \bmod 10 = 49 \bmod 10 = 9$

ESIGN

Ïîäïîçíàòåëüíûé êàíàë ìîæíî äîáàâèòü è ê ESIGN [1460] (ñì. ðàçäåë 20.6). Â ESIGN ñåêðåòíûé êëþ÷ ÿâëÿåòñÿ ïàðîé áîëüøèõ ïðîñòûõ ÷èñåë p è q, à îòêðûòûì êëþ÷îì ñëóæèò $n = p^2q$. Èñïîëüçîâàíèå ïîäïîçíàòåëüíîãî êàíàëà çàêðûòûì êëþ÷îì ÿâëÿþòñÿ òðè ïðîñòûõ ÷èñëà p, q è r, à îòêðûòûì êëþ÷îì - n, òàêîå ÷òî

$n = p^2qr$

Ïåðåìåííàÿ r - ýòî äîïîëíèòåëüíûå äàííûå, íóæíûå Âîáó äëÿ ïðî÷òåíèÿ ïîäïîçíàòåëüíîãî ñîîáùåíèÿ.

×òîáû ïîäïèñàòü îáû÷íîå ñîîáùåíèå, Àëèñà ñíà÷àëà âûáèðàåò ñëó÷àéíîå ÷èñëî x, ìåíüøåå pqr, è âû÷èñëÿò:

w, íàèìåíüøåå öåëîå, êîòîðîå áîëüøå èëè ðàâíî $(H(m) - x^k \bmod n)/pq$

$s = x + ((w/kx^{k-1} \bmod p)\ pq$

$H(m)$ - ýòî õýø-çíà÷åíèå ñîîáùåíèÿ, à k - ïàðàìåòð áåçîïàñíîñòè. Ïîäïèñü ÿâëÿåòñÿ çíà÷åíèå s.

Äëÿ ïðîâåðêè ïîäïèñè Áîá âû÷èñëÿåò $s^k \bmod n$. Êðîìå ýòîãî, îí âû÷èñëÿåò a, íàèìåíüøåå öåëîå, êîòîðîå áîëüøå èëè ðàâíî óäâîåííîìó ÷èñëó áèòîâ n, äåëåííîìó íà 3. Åñëè $H(m)$ ìåíüøå èëè ðàâíà $s^k \bmod n$, è åñëè $s^k \bmod n$ ìåíüøå $H(m)+2^a$, òî ïîäïèñü ñ÷èòàòñÿ ïðàâèëüíîé.

Äëÿ îòïðàâêè ïîäïîçíàòåëüíîãî ñîîáùåíèÿ M ñ ïîìîùüþ áåçîáèäíîãî ñîîáùåíèÿ M' Àëèñà âû÷èñëÿåò s, èñïîëüçóÿ M âìåñòî of $H(m)$. Ýòî îçíà÷àåò, ÷òî ñîîáùåíèå äîëæíî áûòü ìåíüøå, ÷åì p^2qr. Çàòåì îíà âû÷èñëÿåò ñëó÷àéíîå ÷èñëî u è âû÷èñëÿåò

$x' = M' + ur$

Çàòåì ýòî çíà÷åíèå x' èñïîëüçóåòñÿ â êà÷åñòâå "ñëó÷àéíîãî ÷èñëà" x ïðè ïîäïèñè M'. Ñîîòâåòñòâóþùåå çíà÷åíèå s ïîñûëàåòñÿ â êà÷åñòâå ïîäïèñè.

Óîëòåð ìîæåò ïðîâåðèòü, ÷òî s (âòîðîå s) ÿâëÿåòñÿ ïðàâèëüíîé ïîäïèñüþ M' Òî÷íî òàêæå ïðîâåðèòü ïîäëèííîñü ñîîáùåíèÿ ìîæåò è Áîá. Íî, òàê êàê åìó èçâåñòíî è r, îí ìîæåò âû÷èñëèòü

$s = x' + ypqr = M + ur + ypqr \equiv M \pmod r$

Ýòà ðåàëèçàöèÿ ïîäïîçíàòåëüíîãî êàíàëà íàìíîãî ëó÷øå äâóõ ïðåäûäóùèõ. Â âàðèàíòàõ Ong-Schnorr-Shamir è ElGamal ó Áîáà äîëæåí áûòü çàêðûòûé êëþ÷ Àëèñû. Áîá ñìîæåò íå òîëüêî ÷èòàòü ïîäïîçíàòåëüíûå ñîîáùåíèÿ Àëèñû, íî è âûäàâàòü ñåáÿ çà Àëèñó, ïîäïèñûâàÿ îâû÷íûå äîêóìåíòû. Àëèñà íèêîãî ñ ýòèì íå ñìîæåò ïîäåëàòü, óñòàíàâëèâàÿ òàêîé ïîäïîçíàòåëüíûé êàíàë, åé ïðèäåòñÿ äîâåðÿòü Áîáó.

Ñõåìà ESICN ñòðàäàåò îò ýòîé ïðîáëåìû. Çàêðûòûì êëþ÷îì Àëèñû ñëóæèò íàáîð òðåõ ïðîñòûõ ÷èñåë: p, q

è *r*. Ñåêðåòíûì êëþ÷îì Áîáà ÿâëÿåòñÿ òîëüêî *r*. Îí çíàåò $n = p^2qr$, íî, ÷òîáû ðàñêðûòü *p* è *q*, åìó ïîíàäîáèòñÿ ðàçëîæèòü íà ìíîæèòåëè ýòî ÷èñëî. Åñëè ïðîñòûå ÷èñëà äîñòàòî÷íî âåëèêè, Áîáó áóäåò òåê æå òðóäíî âûäàòü ñåáÿ çà Àëèñó, êàê è Óîëäðó èëè êîìó-íèáóäü åùå.

DSA

Ïîäïèñàòåëüíûé êàíàë ñóùåñòâóåò è â DSA (ñì. ðàçäåë 20.1) [1468, 1469, 1473]. Íà ñàìîì äåëå èõ äàæå ìîæåò áûòü íåñêîëüêî. Ïðîòîêîë øèô ïîäïèñàòåëüíûé êàíàë âêëþ÷àåò âûáîð *k*. Ïðåäïîëàãàåòñÿ, ÷òî ýòî áóäåò 160-áèòîâîå ÷èñëî. Îäíàêî, åñëè Àëèñà âûáåðåò êîíêðåòíîå *k*, òî Áîá, çíàÿ çàêðûòûé êëþ÷ Àëèñû, ñìîæåò ðàñêðûòü ýòî *k*. Àëèñà ïîñûëàòü Áîáó 160-áèòîâîå ïîäïèñàòåëüíîå ñîîáùåíèå â êàæäîé ïîäïèñè DSA, à âñå îñòàëüíûå áóäóò òîëüêî ïðîâåðÿòü ïîäïèñü Àëèñû. Äîïóñêòåëüíîå óñëîâíîå: Òàê êàê *k* äëæíî âûòü ñëó÷àéíû, Àëèñà è Áîá äîëæíû ñîãëàñîâàòü îáùèé îäíîðàçîâûé áëîê è øèôðîâàòü ïîäïèñàòåëüíîå ñîîáùåíèå ñ ïîìîùüþ ýòîãî áëîêà, ãåíåðèðóÿ *k*.

Â DSA åñòü ïîäïèñàòåëüíûå êàíàëû, íå òðåáóþùèå ïåðåäàâàòü Áîáó çàêðûòûé êëþ÷ Àëèñû. Îíè òàêæå ïîäâåðæåíû àòàêàì îáùèé îäíîðàçîâûé áëîê è øèôðîâàòü ïîäïèñàòåëüíîå ñîîáùåíèå ñ ïîìîùüþ ýòîãî áëîêà, ãåíåðèðóÿ *k*.

(1) Àëèñà è Áîá âûáèðàþò ñëó÷àéíîå ïðîñòîå ÷èñëî *P* (îòëè÷àþùåñÿ îò ïàðàìåòðà *p* â ñõåìå ïîäïèñè). Ýòî ñåêðåòíûé êëþ÷ äëÿ ïîäïèñàòåëüíîãî êàíàëà.

(2) Àëèñà ïîäïèñûâàåò áåçîáèäíîñòîáùåíèå *M*. Åñëè îíà õî÷åò îòïðàâèòü Áîáó ïîäïèñàòåëüíûé áèò 1, îíà óáåæäàåòñÿ, ÷òî ïàðàìåòð *r* ïîäïèñè ÿâëÿåòñÿ êâàäðàòè÷íûì îñòàòêîì ïî ìîäóëþ *P*. Åñëè îíà õî÷åò îòïðàâèòü åìó 0, îíà ïðîâåðÿåò, ÷òî ïàðàìåòð *r* ïîäïèñè íå ÿâëÿåòñÿ êâàäðàòè÷íûì îñòàòêîì ïî ìîäóëþ *P*. Îíà äîêàçûâàåò ýòîãî, ïîäïèñûâàÿ ñîîáùåíèå ñ ïîìîùüþ ñëó÷àéíîãî çíà÷åíèé *k*, ïîêà îíà íå ïîëó÷èò ïîäïèñü ñ íóæíûì åé ñâîéñòâîì äëÿ *r*. Òàê êàê ÷èñëà, ÿâëÿþùèåñÿ êâàäðàòè÷íûìè îñòàòêàìè è íå ÿâëÿþùèåñÿ èìè, ðàâíîâåðîÿòíû, òî ýòî íå äîëæíî áûòü ñëèøêîì ñëîæíî.

(3) Àëèñà ïîñûëàåò Áîáó ïîäïèñàííûå ñîîáùåíèå.

(4) Áîá ïðîâåðÿåò ïîäïèñü, óáåæäàÿñü â ïîäëèííîñòè ñîîáùåíèÿ. Çàòåì îí ïðîâåðÿåò, ÿâëÿåòñÿ ëè *r* êâàäðàòè÷íûì îñòàòêîì ïî ìîäóëþ *P* è âîññòàíàâëèâàåò ïîäïèñàííóþ áèò.

Ïåðåäà÷à òàêèì îáðàçîì íåñêîëüêèõ áèòîâ ïîäðàçóìåâàåò ïîäáîð òàêîãî *r*, êîòîðîå ÿâëÿåòñÿ êâàäðàòè÷íûì îñòàòêîì ïî íåñêîëüêèì ìîäóëþ. Ïîäðîáíîñòè ïðèâåäåíû â [1468, 1469].

Ýòà ñõåìà ìîæåò áûòü ëåãêî ðàñøèðåíà äëÿ ïåðåäà÷è íåñêîëüêèõ ïîäñîçíàòåëüíûõ áèòîâ íà ïîäïèñü. Åñëè Àëèñà è Áîá âûáèðàþò äâà ñëó÷àéíûõ ÷èñëà *P* è *Q*, òî Àëèñà ìîæåò ïîñûëàòü âûáèðàåò ñëó÷àéíîå *k* òàê, ÷òîáû *r* ÿâëÿëîñü èëè íå ÿâëÿëîñü êâàäðàòè÷íûì îñòàòêîì mod *P*, à òàêæå ÿâëÿëîñü èëè íå ÿâëÿëîñü êâàäðàòè÷íûì îñòàòêîì mod *Q*. Ñëó÷àéíîå çíà÷åíèå *k* ñ âåðîÿòíîñòüþ 25 ïðîâåðÿåòñÿ ïîçâîëèò ïîëó÷èòü *r* ñ íóæíûìè ñâîéñòâàìè.

Âîò êàê Ìýëîðè, íå÷åòêèé ðåàëèçàòîð DSA, ìîæåò ñîçäàòü àëãîðèòì, èçâëåêàþùèé ïî 10 áèòîâ çàêðûòîãî êëþ÷à Àëèñû èç êàæäîé åå ïîäïèñè.

(1) Ìýëîðè ñòðîèò ñâîþ ðåàëèçàöèþ DSA áàçå óñòîé÷èâîé ê âçëîìó ÑÁÈÑ, ÷òîáû íèêòî íå ñìîã ïðîâåðèòü, êàê îíà ðàáîòàåò. Î ñîçäàò 14 ïîäñîçíàòåëüíûõ êàíàëîâ â ñâîåé ðåàëèçàöèè DSA. Òî åñòü, îí âûáèðàåò 14 ñëó÷àéíûõ ïðîòîêîâ ÷èñëè è èñïîëüçóåò ìèêñîðó, êîòîðàÿ âûáèðàåò çíà÷åíèå *k* òàê, ÷òîáû *r* ÿâëÿëîñü èëè íå ÿâëÿëîñü êâàäðàòè÷íûì îñòàòêîì ïî ìîäóëþ êàæäîãî èç ýòèõ 14 ïðîñòûõ ÷èñåë, â çàâèñèìîñòè îò ïîäïèñûâàåìîãî ñîîáùåíèÿ.

(2) Ìýëîðè âûäàåò ìèêñîðùèê Àëèñå, Áîáó è îñòàëüíûì æåëàþùèì.

(3) Àëèñà îáû÷íûì îáðàçîì ïîäïèñûâàåò ñîîáùåíèå, èñïîëüçóÿ ñâîé çàêðûòûé 160-áèòîâûé êëþ÷ *x*.

(4) Ìèêñîðùèê ñëó÷àéíûì îáðàçîì âûáèðàåò 10-áèòîâûé áëîê *x*: ïåðâûå 10 áèòîâ, âòîðûå 10 áèòîâ, è ò.ä. Òàê êàê ñóùåñòâóåò 16 âîçìîæíûõ 10-áèòîâûõ áëîêîâ, òî íîìåð áëîêà âûðàæàåòñÿ 4-áèòîâûì ÷èñëîì. Ýòîò 4-áèòîâûé èäåíòèôèêàòîð è 10 áèòîâ êëþ÷à è áóäóò 14-áèòîâûì ïîäñîçíàòåëüíûì ñîîáùåíèåì.

(5) Ìèêñîðùèê ïåðåäàåò ñëó÷àéíûå çíà÷åíèÿ *k*, ïîêà íå óäàñòñÿ íàéòè òî, êîòîðîå îáëàäàåò ïðàâèëüíûì êâàäðàòè÷íûì îñòàòêîì, íóæíûì äëÿ ïðåäàê÷è ïîäñîçíàòåëüíîãî. Âåðîÿòíîñòü ñëó÷àéíîãî *k* îáëàäàòü ïðàâèëüíîé ôîðìîé ðàâíà 1/16384. Åñëè ìèêñîðùèê ìîæåò ïðîâåðèòü 10000 çíà÷åíèé *k* â ñåêóíäó, íóæíûå çíà÷åíèå áóäåò íàéäåíî ìåíüøå, ÷åì çà ïàðó ñåêóíä. Ýòè âû÷èñëåíèÿ íå çàâèñÿò îò ñîîáùåíèÿ è ìîãóò áûòü âû÷èñëåíû çàðàíåå, äî òîãî, êàê Àëèñà çàõî÷åò ïîäïèñàòü ñîîáùåíèå.

(6) Ìèêñîðùèê îáû÷íûì îáðàçîì ïîäïèñûâàåò ñîîáùåíèå, èñïîëüçóÿ âûáðàííûå íà ýòàïå (5) çíà÷åíèå *k*.

(7) Àëèñà ïîñûëàåò öèôðîâóþ ïîäïèñü Áîáó, èëè îïóáëèêîâûâàåò åå â ñåòè, èëè åùå ÷òî-íèáóäü äëÿåò.

(8) Ìýëîðè ðàñêðûâàåò *r* è, òàê êàê îí çíàåò 14 ïðîñòûõ ÷èñåë, ðàñøèôðîâûâàåò ïîäñîçíàòåëüíûå

ñîîáùåíèå.

Ñòðàøíåå âñåãî, ÷òî, äàæå åñëè Àëèñà çíàåò, ÷òî ïðîèçîøëî, íîâ íè÷åãî íå ñìîæåò äîêàçàòü. Ïîêà 14 ïðîñòûõ ÷èñåë õðàíÿòñÿ â ñåêðåòå, Ì ýëëîðè â áåçîïàñíîñòè.

Óíè÷òîæåíèå ïîäñîçíàòåëüíîãî êàíäèäàòà â DSA

Ïîäñîçíàòåëüíûé êàíäèäàò îïðåäåëèòü íà òî, ÷òî Àëèñà ìîæåò âûáðàòü *k* äëÿ ïåðâîãî ÷èñëà ïîäñîçíàòåëüíîé èíôîðìàöèè. ×òîáû ñäåëàòü ïîäñîçíàòåëüíûé êàíäèäàò íåâîçìîæíûì, Àëèñå íå äîëæíî áûòü ïîçâîëåíî âûáðàòü *k*. Îäíàêî, âûáîð *k* äîëæåí áûòü çàïðåùåí è äëÿ âñåõ äðóãèõ. Åñëè êòî-òî äðóãîé áóäåò ïîçâîëåíî âûáðàòü *k*, òî ýòî ÷åëîâåê ïîëó÷èò âîçìîæíîñòü ïîääåëàòü ïîäïèñü Àëèñû. Äàëíîâèäíûì ðåøåíèåì äëÿ Àëèñû ÿâëÿåòñÿ ïðîâåäåíèå ãåíåðàöèè *k* âìåñòå ñ äðóãîé ñòîðîíîé, Áîáîì, òàê, ÷òîáû Àëèñà íå ìîãëà êîíòðîëèðîâàòü íè îäèí áèò *k*, à Áîá íå ìîã îïðåäåëèòü íè îäèí áèò *k*. Íà äðóãîé ñòîðîíå ïðîòîêîëà ó Áîáà äîëæíà áûòü âîçìîæíîñòü ïðîâåðèòü, ÷òî Àëèñà èñïîëüçîâàëà èìåííî ñîâìåñòíî ñîãëàñîâàííîå *k*.

Âîò ýòîò ïðîòîêîë [1470, 1472, 1473]

(1) Àëèñà âûáèðàåò *k'* è ïîñûëàåò Áîáó

$u = g^{k'} \bmod p$

(2) Áîá âûáèðàåò *k"* è ïîñûëàåò åãî Àëèñå.

(3) Àëèñà âû÷èñëÿåò $k = k'k'' \bmod (p - 1)$. Î íà èñïîëüçóåò *k*, ÷òîáû ïîäïèñàòü ñâîå ñîîáùåíèå *M*, èñïîëüçóÿ DSA, è ïîñûëàåò Áîáó ñâîþ ïîäïèñü: *r* è *s*.

(4) Áîá ïðîâåðÿåò, ÷òî $((u = g^{k'} \bmod p) \bmod q) = r$

Åñëè ýòî òàê, òî îí çíàåò, ÷òî äëÿ ïîäïèñè *M* èñïîëüçîâàëîñü *k*. Ïîñêå ýòàïà (4) Áîá çíàåò, ÷òî â *r* íå áûëî âêëþ÷åíî íèêàêîé ïîäñîçíàòåëüíîé èíôîðìàöèè. Åñëè îí ÿâëÿåòñÿ äîâåðåííûì ñòîðîííèì, îí ìîæåò ïðîâåðèòü, ÷òî â ïîäïèñè Àëèñû íåò ïîäñîçíàòåëüíîé èíôîðìàöèè. Äðóãèì ïðèäåòñÿ ïîâåðèòü åãî çàÿâëåíèþ, Áîá íå ñìîæåò äîêàçàòü ýòîò ôàêò òðåòüåé ñòîðîíå, âîñïîëüçîâàâøè ïðîòîêîë.

Óäèâèòåëüíî òî, ÷òî Áîá, åñëè çàõî÷åò, ìîæåò èñïîëüçîâàòü ýòîò ïðîòîêîë äëÿ ñîçäàíèÿ ñîáñòâåííîãî ïîäñîçíàòåëüíîãî êàíäèä. Áîá ìîæåò âêëþ÷èòü ïîäñîçíàòåëüíóþ èíôîðìàöèþ â îäíó èç ïîäïèñåé Àëèñû, âûáðàâ *k"* ñ îïðåäåëåííûì õàðàêòåðèñòèêàìè. Êîãäà Ñèìîí îòêðûë òàêóþ âîçìîæíîñòü, îí íàçâàë åå "Êàíàëîì êóêóøêè". Ïîäðîáíîñòè ðàáîòû Êàíäèä êóêóøêè, è ìåøàþùèé ýòîìó òðåõïðîõîäíûé ïðîòîêîë ãåíåðàöèè *k*, ðàññìàòðèâàþòñÿ â [1471, 1473].

Äðóãèå ñõåìû

Ïîäñîçíàòåëüíûé êàíäèä ìîæíî îðãàíèçîâàòü äëÿ ëþáîé ñõåìû ïîäïèñè [1458, 1460, 1406]. Îïèñàíèå ïðîòîêîëà âñòðàèâàíèÿ ïîäñîçíàòåëüíîãî êàíäèäà â ñõåìû Fiat-Shamir è Feige-Fiat-Shamir âìåñòå ñ âîçìîæíûìè çëîóïîòðåáëåíèÿìè ìîæíî íàéòè â [485].

23.4 Íåîòðèöàòåëüíûå öèôðîâûå ïîäïèñè

Àâòîðîì ýòîãî äèãðèòàëüíîé ïîäïèñè (ñì. ðàçäåë 4.3) ÿâëÿåòñÿ Äýâèä ×àóì (David Chaum) [343,327]. Ñíà÷àëà îïóáëèêîâûâàþòñÿ áîëüøîå ïðîñòîå ÷èñëî *p* è ïðèìèòèâíûé ýëåìåíò *g*, êîòîðûå áóäóò îáùåñòâåííî èñïîëüçîâàòüñÿ ãðóïïîé ïîäïèñûâàþùèõ. Ó Àëèñû åñòü çàêðûòûé êëþ÷ *x* è îòêðûòûé êëþ÷ $g^x \bmod p$.

×òîáû ïîäïèñàòü ñîîáùåíèå, Àëèñà âû÷èñëÿåò $z = m^x \bmod p$. Ýòî âñå, ÷òî åé íóæíî ñäåëàòü. Ïðîâåðêà ïîäïèñè íåìíîãî ñëîæíåå.

(1) Áîá âûáèðàåò äâà ñëó÷àéíûõ ÷èñëà, *a* è *b*, ìåíüøèå *p*, è îòïðàâëÿåò Àëèñå:

$c = z^a (g^x)^b \bmod p$

(2) Àëèñà âû÷èñëÿåò $t = x^{-1} \bmod (p-1)$, è îòïðàâëÿåò Áîáó:

$d = c^t \bmod p$

(3) Áîá ïðîâåðÿåò, ÷òî

$d \equiv m^a g^b \pmod p$

Åñëè ýòî òàê, îí ñ÷èòàåò ïîäïèñü èñòèííîé.

Ïðåäïîëàãàÿ, ÷òî Àëèñà è Áîá âûïîëíèëè ýòîò ïðîòîêîë, è Áîá òåïåðü ñ÷èòàåò, ÷òî Àëèñà ïîäïèñàëà ñîîáùåíèå. Áîá õî÷åò óáåäèòü â ýòîì Êýðîë, ïîýòîìó îí ïîêàçûâàåò åé çàïèñü ïðîòîêîëà. Äýâ, îäíàêî, õî÷åò óáåäèòü Êýðîë, ÷òî äîêóìåíò êåì-òî äðóãèì. Î íî ñîçäàåò ïîääåëüíóþ çàïèñü ïðîòîêîëà. Ñíà÷àëà îí ãåíåðèðóåò ñîîáùåíèå íà ýòàïå (1). Çàòåì íà ýòàïå (3) îí ãåíåðèðóåò *d* è êîæóþ ïåðåä÷ó îò äðóãîãî ÷åëîâåêà íà ýòàïå (2).

Íàêîíåö, îí ñîçäàåò ñîîáùåíèå ýòàïà (2). Äëÿ Êýðîë çàïèñè Áîáà è Äýéâà îäíàêîâû. Åå íåâîçìîæíî óáåäèòü â ïðàâèëüíîñòè ïîäïèñè, ïîêà íå âûïîëíèò ïðîòîêîë ñàìîñòîÿòåëüíî.

Êîíå÷íî, åñëè áû îíà ñëåäèëà èç-çà ïëå÷à Áîáà çà òåì, êàê îí âûïîëíÿåò ïðîòîêîë, îíà áûëà áû óáåæäåíà. Êýðîë íóæíî óâèäåòü âûïîëíåíèå ýòàïîâ ïî ïîðÿäêó, òàê, êàê ýòî äåëàë Áîá.

Èñïîëüçóÿ ýòó ñõåìó ïîäïèñè, ìîæíî ñòîëêíóòüñÿ ñ ïðîáëåìîé, íî ÿ íå çíàþ ïîäõîäÿùåãî. Ïðåæäå, ÷åì âîñïîëüçîâàòüñÿ ýòîé ñõåìîé, ïðîìîòðèòå ëèòåðàòóðó.

Äðóãîé ïðîòîêîë âêëþ÷åíèå òîëüêî ïðîòîêîë ïîäòâåðæäåíèÿ - Àëèñà ìîæåò óáåäèòü Áîáà â ïðàâèëüíîñòè ñâîåé ïîäïèñè - íî è ïðîòîêîë îòðèöàíèÿ. Àëèñà ìîæåò ñ ïîìîùüþ èíòåðàêòèâíîãî ïðîòîêîëà ñ íóëåâûì çíàíèåì óáåäèòü Áîáà, ÷òî åå ïîäïèñü íåïðàâèëüíà, åñëè ýòî òàê [329].

Êàê è ïðåäûäóùèé ïðîòîêîë ãðóïïà ïîäïèñûâàþùèõ èñïîëüçóåò îáùåäîñòóïíóþ áîëüøîå ïðîñòîå ÷èñëî p è ïðèìèòèâíûé ýëåìåíò g. Ó Àëèñû åñòü çàêðûòûé êëþ÷ x è îòêðûòûé êëþ÷ $g^x \bmod p$. ×òîáû ïîäïèñàòü ñîîáùåíèå, Àëèñà âû÷èñëÿåò $z = m^x \bmod p$. ×òîáû ïðîâåðèòü ïîäïèñü:

(1) Áîá âûáèðàåò äâà ñëó÷àéíûõ ÷èñëà, a è b, ìåíüøèå p, è îòïðàâëÿåò Àëèñå:

$$c = m^a g^b \bmod p$$

(2) Àëèñà âûáèðàåò ñëó÷àéíîå ÷èñëî q, ìåíüøåå p, à çàòåì âû÷èñëÿåò è îòïðàâëÿåò Áîáó:

$$s_1 = cg^q \bmod p,\ s_2 = (cg^q)^x \bmod p$$

(3) Áîá ïîñûëàåò Àëèñå a è b, ÷òîáû Àëèñà ìîãëà óáåäèòüñÿ, ÷òî Áîá íå ìîøåííè÷àë íà ýòàïå (1).

(4) Àëèñà ïîñûëàåò Áîáó q, ÷òîáû îí ìîãñîãëçîâàòüñÿ m^x è âîññòàíîâèò s_1 è s_2. Åñëè

$$s_1 \equiv cg^q \bmod p$$

$$s_2 \equiv (g^x)^{b+q} z^a \pmod p$$

òî ïîäïèñü ïðàâèëüíà.

Àëèñà ìîæåò òàêæå îòêàçàòüñÿ îò ïîäïèñè z ïîä ñîîáùåíèåì m. Ïîäðîáíîñòè ïðèâåäåíû â [329]. Äîïîëíèòåëüíûå ïðîòîêîëû äëÿ íåîòðèöàíèìîñòè ïîäïèñåé ìîæíî íàéòè â [584, 344]. Ëåéí Õàðí (Lein Harn) è Øóàíü ßíã (Shoubao Yang) ïðåäëîæèëè ñõåìó ãðóïïîâûõ íåîòðèöàíèìûõ ïîäïèñåé [700].

Ïðîáëåìû íåîòðèöàíèÿ ïîäïèñè

Àëãîðèòì äëÿ **ïðîáëåìû íåîòðèöàíèÿ ïîäïèñè**, êîòîðûå ìîæíî ïðîâåðÿòü, îòìåíÿòü è ïðîáëåìû âûâàòü â îáû÷íûå íåîòðèöàíèå ïîäïèñè, ïðèâåäåí â [213]. Î í ñíîâàí íà àëãîðèòìå öèôðîâûõ ïîäïèñåé ElGamal.

Êàê è â ElGamal, ñíà÷àëà âûáèðàþòñÿ äâà ïðîñòûõ ÷èñëà, p è q, òàê, ÷òîáû q áûëî äåëèòåëåì p-1. Òåïåðü íóæíî ñîçäàòü ÷èñëî g, ìåíüøåå q. Â äèàïàçîíå îò 2 äî p-1 âûáèðàåòñÿ ñëó÷àéíîå ÷èñëî h è âû÷èñëÿåòñÿ

$$g=h^{(p-1)/q} \bmod p$$

Åñëè g ðàâíî 1, âûáèðàåòñÿ äðóãîå ñëó÷àéíîå h. Åñëè íåò, èñïîëüçóåòñÿ ïîëó÷åííîå çíà÷åíèå g.

Çàêðûòûì êëþ÷îì ñëóæàò äâà ðàçëè÷íûõ ñëó÷àéíûõ ÷èñëà, x è z, ìåíüøèå q. Îòêðûòûì êëþ÷àìè ÿâëÿþòñÿ p, q, g, y è u, ãäå

$$y = g^x \bmod p$$

$$u=g^{\ddot{y}} \bmod p$$

Äëÿ âû÷èñëåíèÿ ïðåîáðàçóåìîãî íåòðèâèàëüíîãî ïîäïèñè ñîîáùåíèÿ m (êîòîðîå â äåéñòâèòåëüíîñòè ÿâëÿåòñÿ õýø-çíà÷åíèåì ñîîáùåíèÿ), ñíà÷àëà äèàïàçîíå îò 1 äî q-1 âûáèðàåòñÿ ñëó÷àéíîå ÷èñëî t. Çàòåì âû÷èñëÿåòñÿ

$$T = g^r \bmod p$$

è

$$m' = Ttzm \bmod q.$$

Òåïåðü âû÷èñëÿåòñÿ îáû÷íàÿ ïîäïèñü ElGamal äëÿ m'. Âûáèðàåòñÿ ñëó÷àéíîå ÷èñëî R, ìåíüøåå p-1 è âçàèìíî ïðîñòîå ñ íèì. Çàòåì âû÷èñëÿåòñÿ $r = g^R \bmod p$ è, ñ ïîìîùüþ ðàñøèðåííîãî äëãîðèòìà Ýâêëèäà, âû÷èñëÿåòñÿ s, äëÿ êîòîðîãî

$$m' \equiv rx + Rs \pmod q$$

Ïîäïèñü ñëóæàò ïîäïèñü ElGamal (r, s) è T. Âîò êàê Àëèñà ïîäòâåðæäàåò ñâîþ ïîäïèñü Áîáó:

(1) Áîá ãåíåðèðóåò äâà ñëó÷àéíûõ ÷èñëà, a è b, è âû÷èñëÿåò $c = T^{Tma}g^b \bmod p$ è ïîñûëàåò ðåçóëüòàò Àëèñå.

(2) Àëèñà ãåíåðèðóåò ñëó÷àéíîå ÷èñëî k è âû÷èñëÿåò $h_1 = cg^k \bmod p$ è $h_2 = h_1^z \bmod p$, à çàòåì ïîñûëàåò îáà ÷èñëà Áîáó.

(3) Áîá ïîñûëàåò Àëèñå a è b.

(4) Àëèñà ïðîâåðÿåò, ÷òî $c = T^{Tma}g^b \bmod p$. Î íà ïîñûëàåò k Áîáó.

(5) Áîá ïðîâåðÿåò, ÷òî $h_1 = T^{Tma}g^{b+k} \bmod p$, è ÷òî $h_2 = y^{ra}r^{sa}u^{b+k} \bmod p$.

Àëèñà ìîæåò ïðåîáðàçîâàòü âñå ñâîè íåòðèâèàëüíûå ïîäïèñè â îáû÷íûå, îïóáëèêîâàâ z. Òåïåðü ëþáîé ìîæåò ïðîâåðèòü åå ïîäïèñü áåç åå ïîìîùè.

Ñõåìû íåîòðèöàòåëüíîãî ïîäïèñé ìîæíî îáúåäèíèòü ñî ñõåìàìè ðàçäåëåíèÿ ñåêðåòà, ñîçäàâ **ðàñïðåäåëåííûå ïðîòîêîëû íåîòðèöàòåëüíûå ïîäïèñè** [1235]. Êòî-íèáóäü ìîæåò ïîäïèñàòü ñîîáùåíèå, à çàòåì ðàñïðåäåëèòü âîçìîæíîñòü ïîäâåðæäåíèÿ ïðàâèëüíîñòè ïîäïèñè. Î í ìîæåò, íàïðèìåð, ïîðîâíÿòü ÷òîôû â ïðîòîêîëå óáåæäåíèÿ Áîáà â ïðàâèëüíîñòè ïîäïèñè ó÷àñòâîâàëè òðîå èç ïÿòè îáëàäàòåëåé âîçìîæíîñòü ïîäâåðæäåíèÿ ïðàâèëüíîñòè. Â [700, 1369] ïðåäëîæåíû óëó÷øåíèÿ, ïîçâîëÿþùèå îôèçàöüñ îò íåîáõîäèìîñòè äîâåðåííîãî ëèöà - ðàñïðåäåëèòåëÿ.

23.5 Ï î ä ïèñè, ï î äòâåðæäàåì ûå äîâåðåííû ì ëèöî ì

Âîò êàê Àëèñà ìîæåò ïîäïèñàòü ñîîáùåíèå, à Áîá ïðîâåðèò åãî òàê, ÷òîáû è Êýðîë íåìíîãî ïîçæå ìîãëà äîêàçàòü Äýéâó ïðàâèëüíîñòü ïîäïèñè Àëèñû (ñì. ðàçäåë 4.4) [333].

Ñíà÷àëà îïóáëèêîâûâàþòñÿ áîëüøîå ïðîñòîå ÷èñëî p è ïðèìèòèâíûé ýëåìåíò g, êîòîðûå áóäóò ñîâìåñòíî èñïîëüçîâàòüñÿ ãðóïïîé ïîëüçîâàòåëåé. Òàêæå îïóáëèêîâûâàþòñÿ n, ïðîèçâåäåíèå äâóõ ïðîñòûõ ÷èñåë. Ó Êýðîë åñòü çàêðûòûé êëþ÷ z è îòêðûòûé êëþ÷ $h = g^x \bmod p$.

Â ýòîì ïðîòîêîëå Àëèñà ìîæåò ïîäïèñàòü m òàê, ÷òîáû Áîá ìîã ïðîâåðèòü ïðàâèëüíîñòü åå ïîäïèñè, íî íå ìîã óáåäèòü â ýòîì òðåòüåì ñòîðîíó.

(1) Àëèñà âûáèðàåò ñëó÷àéíûå x è âû÷èñëÿåò

$a = g^x \bmod p$

$b = h^x \bmod p$

Î íà âû÷èñëÿåò õýø-çíà÷åíèå m, $H(m)$, è õýø-çíà÷åíèå îáúåäèíåíèÿ a è b, $H(a,b)$, à çàòåì

$j = (H(m) \oplus H(a,b))^{1/3} \bmod n$

è ïîñûëàåò a, b è j Áîáó.

(2) Áîá âûáèðàåò äâà ñëó÷àéíûõ ÷èñëà, s è t, ìåíüøèõ p, è ïîñûëàåò Àëèñå

$c = g^s h^t \bmod p$

(3) Àëèñà âûáèðàåò ñëó÷àéíûå q, ìåíüøåå p, è ïîñûëàåò Áîáó

$d = g^q \bmod p$

$e = (cd)^x \bmod p$

(4) Áîá ïîñûëàåò Àëèñå s è t.

(5) Àëèñà ïðîâåðÿåò, ÷òî

$g^s h^t \equiv c \pmod p$

çàòåì îíà ïîñûëàåò Áîáó q.

(6) Áîá ïðîâåðÿåò

$d \equiv g^q \bmod p$

$e/a^q \equiv a^s b^t \pmod p$

$(H(m) \oplus H(a,b)) = j^{1/3} \bmod n$

Åñëè âñå òî÷íî âûïîëíÿþòñÿ, òî Áîá ñ÷èòàåò ïîäïèñü èñòèííîé.

Áîá íå ìîæåò èñïîëüçîâàòü çàïèñü ýòîãî äîêàçàòåëüñòâà äëÿ óáåæäåíèÿ Äýéâà â èñòèííîñòè ïîäïèñè, íî Äýéâ ìîæåò âûïîëíèòü ïðîòîêîë ñ äîâåðåííûì ëèöîì Àëèñû, Êýðîë. Âîò êàê Êýðîë óáåæäàåò Äýéâà â òî ì, ÷òî a è b îáðàçóþò ïðàâèëüíóþ ïîäïèñü.

(1) Ävéâ âûáèðàåò ñëó÷àéíûå u è v, ìåíüøèå p, è ïîñûëàåò Êýðîë

$k = g^u a^v \bmod p$

(2) Êýðîë âûáèðàåò ñëó÷àéíîå w, , ìåíüøåå p, è ïîñûëàåò Äýéâó

$l = g^w \bmod p$

$y = (kl)^z \bmod p$

(3) Äýéâ ïîñûëàåò Êýðîë u è v.

(4) Êýðîë ïðîâåðÿåò, ÷òî

$g^u a^v \equiv k \pmod p$

Çàòåì îíà ïîñûëàåò Äýéâó w.

(5) Äýéâ ïðîâåðÿåò, ÷òî

$g^w \equiv l \pmod p$

$y/h^w \equiv h^u b^v \pmod p$

Åñëè âñå òî÷íî âûïîëíÿþòñÿ, òî Äýéâ ñ÷èòàåò ïîäïèñü èñòèííîé.

Â äðóãîì ïðîòîêîëå Êýðîë ìîæåò ïðåîáðàçîâàòü ïðîòîêîë äîâåðåííîãî ëèöà â îáû÷íóþ öèôðîâóþ ïîäïèñü. Ïîäðîáíîñòè â [333].

23.6 Âû÷èñëåíèÿ ñ çàøèôðîâàííûìè äàííûìè

Ïðîáëåìà äèñêðåòíîãî ëîãàðèôìà

Ñóùåñòâóåò áîëüøîå ïðîñòîå p è ãåíåðàòîð g. Àëèñà õî÷åò äëÿ êîíêðåòíîãî x íàéòè òàêîå e, äëÿ êîòîðîãî

$g^e \equiv x \pmod p$

Ýòî òðóäíàÿ ïðîáëåìà, è Àëèñå íå õâàòàåò âû÷èñëèòåëüíûõ ìîùíîñòåé äëÿ âû÷èñëåíèÿ ðåçóëüòàòà. Ó Âîáà åñòü òàêàÿ âîçìîæíîñòü - îí ïðåäñòàâëÿåò ïðàâèëüíîñòü, èëè ìîùíûé âû÷èñëèòåëüíûé öåíòð, èëè åùå êàêóþ-íèáóäü âèðòóàëüíóþ îðãàíèçàöèþ. Âîò êàê Àëèñà ìîæåò ïîëó÷èòü ïîìîùü Âîáà, íå ðàñêðûâ åìó x [547, 4]:

(1) Àëèñà âûáèðàåò ñëó÷àéíîå ÷èñëî r, ìåíüøåå p.

(2) Àëèñà âû÷èñëÿåò

$x' = xg^r \bmod p$

(3) Àëèñà ïðîñèò Âîáà ðåøèòü

$g^{e'} \equiv x' \pmod p$)

(4) Âîá âû÷èñëÿåò e' è ïîñûëàåò åãî Àëèñå.

(5) Àëèñà âîññòàíàâëèâàåò e, âû÷èñëÿÿ

$e = (e' - r) \bmod (p - 1)$

Àíàëîãè÷íûå ïðîòîêîëû äëÿ ïðîáëåì êâàäðàòè÷íûõ îñòàòêîâ è ïðèìèòèâíûõ êîðíåé ïðèâåäåíû â [3, 4]. (Ñì. òàêæå ðàçäåë 4.8.)

23.7 Áðîñàíèå "÷åñòíîé" ìîíåòû

Ñëåäóþùèå ïðîòîêîëû ïîçâîëÿþò Àëèñå è Âîáó áðîñàòü ÷åñòíóþ ìîíåòó â ñåòè ïåðåäà÷è äàííûõ (ñì. ðàçäåë 4.9) [194]. Ýòî ïðèìåð áðîñàíèÿ ìîíåòû â êîëîäó (ñì. ðàçäåë 4.10). Ñíà÷àëà òîëüêî Âîá óçíàåò ðåçóëüòàò áðîñêà è ñîîáùàåò åãî Àëèñå. Çàòåì Àëèñà ìîæåò ïðîâåðèòü, ÷òî Âîá ñîîáùèë ïðàâèëüíûé ðåçóëüòàò áðîñêà.

Áðîñàíèå "÷åñòíîé" ìîíåòû ñ ïîìîùüþ êâàäðàòíûõ êîðíåé

Ïîäïðîòîêîë áðîñàíèÿ ÷åñòíîé ìîíåòû:

(1) Àëèñà âûáèðàåò äâà âîëüøèõ ïðîñòûõ ÷èñëà, p è q, è ïîñûëàåò èõ ïðîèçâåäåíèå n Âîáó.

(2) Âîá âûáèðàåò ñëó÷àéíîå ïîëîæèòåëüíîå öåëîå ÷èñëî r, ìåíüøåå $n/2$. Âîá âû÷èñëÿåò

$z = r^2 \bmod n$

è ïîñûëàåò z Àëèñå.

(3) Àëèñà âû÷èñëÿåò ÷åòûðå êâàäðàòíûõ êîðíÿ $z \pmod n$. Îíà ìîæåò ñäåëàòü ýòî, òàê êàê îíà çíàåò ðàçëîæåíèå n íà ìíîæèòåëè. Íàçîâåì èõ $+x$, $-x$, $+y$ è $-y$. Îáîçíà÷èì êàê x' ìåíüøåå èç ñëåäóþùèõ âåëè÷èí:

$x \bmod n$

$-x \bmod n$

Àíàëîãè÷íî, îáîçíà÷èì êàê y' ìåíüøåå èç ñëåäóþùèõ âåëè÷èí:

$y \bmod n$

$-y \bmod n$

Îáðàòèòå âíèìàíèå, ÷òî r ðàâíî ëèáî x', ëèáî y'.

(4) Àëèñà äåëàåò ïûòàþùóþñÿ óãàäàòü, êàêîå èç çíà÷åíèé ðàâíî $r - x'$ èëè y', è ïîñûëàåò ñîþ äîãàäêó Áîáó.

(5) Åñëè äîãàäêà Àëèñû ïðàâèëüíà, ðåçóëüòàòîì áðîñêà ìîíåòû ÿâëÿåòñÿ "îðåë", à åñëè íåïðàâèëüíà - "ðåøêà". Áîá îáúÿâëÿåò ðåçóëüòàò áðîñêà ìîíåòû.

Ïîäðîáíîñòè ïðîâåðêè:

(6) Àëèñà ïîñûëàåò p è q Áîáó.

(7) Áîá âû÷èñëÿåò x' è y' è ïîñûëàåò èõ Àëèñå.

(8) Àëèñà âû÷èñëÿåò r.

Ó Àëèñû íåò âîçìîæíîñòè óçíàòü, ïîýòîìó îíà äåéñòâèòåëüíî óãàäûâàåò. Îíà íà ýòàïå (4) ñîîáùàåò Áîáó òîëüêî îäèí áèò ñâîé äîãàäêè, íå äàâàÿ Áîáó ïîëó÷èòü è x', è y'. Åñëè Áîá ïîëó÷èò îáà ýòèõ ÷èñëà, îí ìîæåò èçìåíèòü r ïîñëå ýòàïà (4).

Áðîñàíèå "÷åñòíîé" ìîíåòû ñ ïîìîùüþ âîçâåäåíèÿ â ñòåïåíü ïî ìîäóëþ p

Â ýòîì ïðîòîêîëå â êà÷åñòâå îäíîíàïðàâëåííîé ôóíêöèè èñïîëüçóåòñÿ âîçâåäåíèå â ñòåïåíü ïî ìîäóëþ ïðîñòîãî ÷èñëà p [1306]:

Ïîäïðîòîêîë áðîñàíèÿ ÷åñòíîé ìîíåòû:

(1) Àëèñà âûáèðàåò ïðîñòîå ÷èñëî p òàê, ÷òîáû ìíîæèòåëè p-1 áûëè èçâåñòíû, è ñðåäè íèõ áûëî ïî êðàéíåé ìåðå îäíî áîëüøîå ïðîñòîå ÷èñëî.

(2) Áîá âûáèðàåò äâà ïðèìèòèâíûõ ýëåìåíòà, h è t, â GF(p). Îí ïîñûëàåò èõ Àëèñå.

(3) Àëèñà óáåæäàåòñÿ, ÷òî h è t ÿâëÿþòñÿ ïðèìèòèâíûìè ýëåìåíòàìè, è çàòåì âûáèðàåò ñëó÷àéíîå ÷èñëî x, âçàèìíî ïðîñòîå ñ p-1. Çàòåì îíà âû÷èñëÿåò îäíî èç âåëè÷èí:

$y = h^x \bmod p$, èëè $y = t^x \bmod p$

Îíà ïîñûëàåò y Áîáó.

(4) Áîá ïûòàåòñÿ óãàäàòü, âû÷èñëèâ Àëèñà y êàê ôóíêöèþ h èëè êàê ôóíêöèþ t, è ïîñûëàåò ñâîå ïðåäïîëîæåíèå Àëèñå.

(5) Åñëè äîãàäêà Áîáà ïðàâèëüíà, ðåçóëüòàòîì áðîñàíèÿ ìîíåòû ÿâëÿåòñÿ "îðåë", â ïðîòèâíîì ñëó÷àå - "ðåøêà". Àëèñà îáúÿâëÿåò ðåçóëüòàò áðîñêà ìîíåòû.

Ïîäïðîòîêîë ïðîâåðêè:

(6) Àëèñà ðàñêðûâàåò Áîáó çíà÷åíèå x. Áîá âû÷èñëÿåò $h^x \bmod p$ è $t^x \bmod p$, óáåæäàÿñü, ÷òî Àëèñà èãðàëà ÷åñòíî è ïðîâåðÿÿ ðåçóëüòàò áðîñêà. Î í òàêæå ïðîâåðÿåò, ÷òî x è p-1 - âçàèìíî ïðîñòûå ÷èñëà.

×òîáû Àëèñà ìîãëà ñìîøëèòü, îíà äîëæíà çíàòü äâà öåëûõ ÷èñëà, x è x', äëÿ êîòîðûõ âûïîëíÿåòñÿ $h^x \equiv t^{x'} \bmod p$. Äëÿ òîãî, ÷òîáû óçíàòü ýòè çíà÷åíèÿ, åé íóæíî âû÷èñëèòü:

$\log_t h = x'x^{-1} \bmod p$-1 è $\log_t h = xx'^{-1} \bmod p$-1.

Ýòî òðóäíûå ïðîáëåìû.

Àëèñà ñìîãëà áû ñäåëàòü ýòî, åñëè áû îíà çíàëà $\log_t h$, íî Áîá âûáèðàåò h è t íà ýòàïå (2). Ó Àëèñû íåò äðóãîãî ñïîñîáà êðàòêî, êàê ïîïûòàòüñÿ âû÷èñëèòü äèñêðåòíûé ëîãàðèôì. Àëèñà ìîæåò òàêæå ïîïûòàòüñÿ ñìîøåííè÷àòü, âûáðàâ x, êîòîðîå íå ÿâëÿåòñÿ âçàèìíî ïðîñòûì ñ p-1, íî Áîá îáìàíåò ýòî íà ýòàïå (6).

Áîá ìîæåò ñìîøåííè÷àòü, åñëè h è t íå ÿâëÿþòñÿ ïðèìèòèâíûìè ýëåìåíòàìè â ïîëå in GF(p), íî Àëèñà ñìîæåò ëåãêî ïðîâåðèòü ýòî ïîñëå ýòàïà (2), òàê êàê åé èçâåñòíî ðàçëîæåíèå p-1 íà ïðîñòûå ìíîæèòåëè.

Óäà÷íûì â ýòîì ïðîòîêîëå ÿâëÿåòñÿ òî, ÷òî åñëè Àëèñà è Áîá çàõîòÿò áðîñèòü íåñêîëüêî ìîíåò, îí7è ñìîãóò èñïîëüçîâàòü îäíè è òå æå çíà÷åíèÿ *p*, *h* è *t*. Àëèñà ïðîñòî ãåíåðèðóåò íîâîå *x*, è ïðîòîêîë ïðîäîëæàåòñÿ ñ ýòàïà (3).

Áðîñàíèå "÷åñòíîé" ìîíåòû ñ ïîìîùüþ öåëûõ ÷èñåë Áëþìà

Â ïðîòîêîëå áðîñàíèÿ ìîíåòû ìîæíî èñïîëüçîâàòü ÷åëûå ÷èñëà Áëþìà.

(1) Àëèñà ãåíåðèðóåò öåëîå ÷èñëî Áëþìà *n*, ñëó÷àéíîå *x*, âçàèìíî ïðîñòîå ñ *n*, $x_0 = x^2 \bmod n$ è $x_1 = x_0^2 \bmod n$. Îíà ïîñûëàåò Áîáó *n* è x_1.

(2) Áîá óãàäûâàåò, ÷åòíû ìëè íå÷åòíû ÿâëÿåòñÿ x_0.

(3) Àëèñà ïîñûëàåò *x* Áîáó.

(4) Áîá ïðîâåðÿåò, ÷òî *n* ÿâëÿåòñÿ öåëûì ÷èñëîì Áëþìà (Àëèñà íóæíî ïðåäàòü Áîáó ìíîæèòåëè *n* è äîêàçàòåëüñòâà òîãî, ÷òî îíè ÿâëÿþòñÿ ïðîñòûìè, èëè âû ïîëíîìó íåêîððåêòíî ñ óêàçàííûì çíà÷åíèì, óáåæäàþ ùèé Áîáà, ÷òî *n* - ýòî öåëîå ÷èñëî Áëþìà), è ÷òî $x_0 = x^2 \bmod n$ è $x_1 = x_0^2 \bmod n$. Åñëè âñå ïðîâåðêè âûïîëíÿþòñÿ, è Áîá óâåðåí ïðàâèëüíî, îí âûâîäèò áðîñîê.

Ýòî âàæíî, ÷òîáû *n* áûë ÷èñëîì Áëþìà. Èíà÷å Àëèñà ñìîæåò íàéòè òàêîå x'_0, ÷òî $x'^2_0 \bmod n = x_0^2 \bmod n = x_1$, ãäå x'_0 òàêæå ÿâëÿåòñÿ êâàäðàòè÷íûì îñòàòêîì. Åñëè áû x_0 áûë ÷åòíûì, à x'_0 - íå÷åòíûì (èëè íàîáîðîò), Àëèñà ìîãëà áû ìîøåííè÷àòü.

23.8 Îäíîíàïðàâëåííûå ñóì ìàòîðû

Ñóùåñòâóåò ïðîñòàÿ ôóíêöèÿ îäíîíàïðàâëåííîãî ñóì ìàòîðà [116] (ñì. ðàçäåë 4.12.):

$A(x_i, y) = x_{i-1}^{\,y} \bmod n$

×èñëà *n* (ÿâëÿþùåéñÿ ïðîèçâåäåíèåì äâóõ ïðîñòûõ ÷èñåë) è x_0 äîëæíû áûòü çàðàíåå ñîãëàñîâàíû. Òîãäà ñóì ìèðîâàíèÿ y_1, y_2 è y_3 áóäåò

$((x_0^{\,y_1} \bmod n)^{y_2} \bmod n)^{y_3} \bmod n$

Ýòî âû÷èñëåíèå íå çàâèñèò îò ïîðÿäêà y_1, y_2 è y_3.

23.9 Ðàñøèðåííûå ñåðâåðíî-"âñå èëè íè÷åãî"

Ýòîò ïðîòîêîë ïîçâîëÿåò íåñêîëüêèì ñòîðîíàì (äëÿ ðàâíîò ïðîòîêîëà íóæíî íå ìåíüøå äâóõ ó÷àñòíèêîâ) ïîêóïàòü ðàçëè÷íûå ñåðâåðû ó îäíîãî ïðîäàâöà (ñì. ðàçäåë 4.13) [1374, 1175]. Íà÷íåì ñ ïîñëåäíåãî. Âîçüìåì äâå ñòðîêè áèòîâ, *x* è *y*. Ôèêñèðîâàííûì áèòîâûì èíäåêñîì (fixed bit index, **FBI**) *x* è *y* íàçûâàþòñÿ ïîñëåäíèå áèòû ýòèõ ñòðîê.

Íàïðèìåð:

x = 110101001011

y = 101010000110

FBI(*x*, *y*) = {1, 4, 5, 11}

(Ì û ÷èòàåì áèòû ñïðàâà íàëåâî, ñ÷èòàÿ íóëåâûì êðàéíèé ïðàâûé áèò.)

Òåïåðü âîò êàê âûãëÿäèò ïðîòîêîë. Àëèñà áóäåò ïðîäàâöîì. Áîá è Êýðîë - ïîêóïàòåëüì. Ó Àëèñû åñòü *k n*-áèòîâûõ ñåêðåòîâ: S_1, S_2, . . . S_k. Áîá õî÷åò êóïèòü ñåêðåò S_b, Êýðîë - ñåêðåò S_c.

(1) Àëèñà ãåíåðèðóåò ïàðó "îòêðûòûé êëþ÷/çàêðûòûé êëþ÷"è ñîîáùàåò Áîáó (íî íå Êýðîë) îòêðûòûé êëþ÷. Îíà ãåíåðèðóåò äðóãóþ ïàðó "îòêðûòûé êëþ÷/çàêðûòûé êëþ÷"è ñîîáùàåò Êýðîë (íî íå Áîáó) îòêðûòûé êëþ÷.

(2) Áîá ãåíåðèðóåò *k n*-áèòîâûõ ñëó÷àéíûõ ÷èñåë, B_1, B_2, . . . B_k, è ñîîáùàåò èõ Êýðîë. Êýðîë ãåíåðèðóåò *k n*-áèòîâûõ ñëó÷àéíûõ ÷èñåë, C_1, C_2, . . . C_k, è ñîîáùàåò èõ Áîáó.

(3) Áîá øèôðóåò C_b (íàïîìíè, îí õî÷åò êóïèòü ñåêðåò S_b) îòêðûòûì êëþ÷îì, ïîëó÷åííûì îò Àëèñû. Î í âû÷èñëÿåò FBI äëÿ C_b è òîëüêî ÷òî çàøèôðîâàííûõ ðåçóëüòàòà. Î í ïîñûëàåò ýòî FBI Êýðîë.

Êýðîë øèôðóåò B_c (íàïîìíè, îíà õî÷åò êóïèòü ñåêðåò S_c) îòêðûòûì êëþ÷îì, ïîëó÷åííûì îò Àëèñû. Î íà âû÷èñëÿåò FBI äëÿ B_c è òîëüêî ÷òî çàøèôðîâàííûõ ðåçóëüòàòà. Î íà ïîñûëàåò ýòî FBI Áîáó.

(4) Áîá áåðåò êàæäîå èç *n*-áèòîâûõ ÷èñåë B_1, B_2, . . . B_k è çàìåíÿåò êàæäûé áèò, íî ìåðà êîòîðîãî íåò â FBI, ïîëó÷åííîì îò Êýðîë, åãî äîïîëíåíèÿì. Î í ïîñûëàåò ýòî íîâûé ñïèñîê *n*-áèòîâûõ ÷èñåë B'_1, B'_2, . . . B'_k

Àëèñå.

Êýðîë áåðåò êàæäîå èç n-áèòîâûõ ÷èñåë C_1, C_2, . . . C_k è çàøèôðóåò êàæäûé áèò, íî ìåðà êîòîðîãî íåò â FBI, ïîëó÷åííî îò Áîáà, åãî äîïîëíåíèå. Îíà ïîñûëàåò ýòî íîâûé ñïèñîê n-áèòîâûõ ÷èñåë C'_1, C'_2, . . . C'_k Àëèñå.

(5) Àëèñà ðàñøèôðîâûâàåò âñå C'_i çàêðûòûì êëþ÷îì Áîáà, ïîëó÷àÿ k n-áèòîâûõ ÷èñåë C''_1, C''_2, . . . C''_k. Îíà âû÷èñëÿåò $S_i \oplus C''_i$ äëÿ $i = 1, \ldots k$, è ïîñûëàåò ðåçóëüòàòû Áîáó.

Àëèñà ðàñøèôðîâûâàåò âñå B'_i çàêðûòûì êëþ÷îì Êýðîë, ïîëó÷àÿ k n-áèòîâûõ ÷èñåë B''_1, B''_2, . . . B''_k. Îíà âû÷èñëÿåò $S_i \oplus B''_i$ äëÿ $i = 1, \ldots k$, è ïîñûëàåò ðåçóëüòàòû Êýðîë.

(6) Áîá âû÷èñëÿåò S_b, âûïîëíÿÿ XOR C_b è b-ãî ÷èñëà, ïîëó÷åííîãî îò Àëèñû.

Êýðîë âû÷èñëÿåò S_c, âûïîëíÿÿ XOR B_c è c-ãî ÷èñëà, ïîëó÷åííîãî îò Àëèñû..

Âñå òàê ñëîæíî. Ïîÿñíèì ýòè äåéñòâèÿ íà ïðèìåðå.

Ó Àëèñû åñòü äëÿ ïðîäàæè âîñåìü 12-áèòîâûõ ñåêðåòîâ: S_1 = 1990, S_2 = 471, S_3 = 3860, S_4 = 1487, S_5 = 2235, S_6 = 3751, S_7 = 2546 è S_8 = 4043. Áîá õî÷åò êóïèòü S_7, à Êýðîë - S_2.

(1) Àëèñà èñïîëüçóåò àëãîðèòì RSA. Â äèàëîãå ñ Áîáîì îíà èñïîëüçóåò ñëåäóþùóþ ïàðó êëþ÷åé: n = 7387, e = 5145 è d = 777, à â äèàëîãå ñ Êýðîë - n = 2747, e = 1421 è d = 2261. Îíà ñîîáùàåò Áîáó è Êýðîë èõ îòêðûòûå êëþ÷è.

(2) Áîá åãíåðèðóåò âîñåìü 12-áèòîâûõ ÷èñåë, B_1= 743, B_2= 1988, B_3= 4001, B_4= 2942, B_5= 3421, B_6= 2210, B_7=2306 è B_8= 222, è ñîîáùàåò èõ Êýðîë. Êýðîë ãåíåðèðóåò âîñåìü 12-áèòîâûõ ÷èñåë, C_1= 1708, C_2 = 711, C_3= 1969, C_4 = 3112, C_5 = 4014, C_6 = 2308, C_7 = 2212 è C_8 = 222, è ñîîáùàåò èõ Áîáó.

(3) Áîá õî÷åò êóïèòü S_7, ïîýòîìó îí òèðûòûì êëþ÷îì, âûäàíûì Àëèñîé, øèôðóåò C_7.

$2212^{5145} \bmod 7387 = 5928$

Òåïåðü:

2212 = 0100010100100

5928 = 1011100101000

Ñëåäîâàòåëüíî, FBI ýòèõ äâóõ ÷èñåë ðàâåí {0, 1, 4, 5, 6}. Îí ïîñûëàåò åãî Êýðîë.

Êýðîë õî÷åò êóïèòü S_2, ïîýòîìó îíà îòêðûòûì êëþ÷îì, âûäàíûì Àëèñîé, øèôðóåò B_2 è âû÷èñëÿåò FBI B_2 è ðåçóëüòàòà øèôðîâàíèÿ. Îíà ïîñûëàåò Áîáó{0, 1, 2, 6, 9, 10}.

(4) Áîá áåðåò B_1, B_2, . . . B_8 è çàøèôðóåò êàæäûé áèò, èíäåêñ êîòîðîãî îòñóòñòâóåò â íàáîðå {0, 1, 2, 6, 9, 10} åãî äîïîëíåíèå. Íàïðèìåð:

B_2= 111111000100 = 1988

B'_2 = 011001111100 = 1660

Îí ïîñûëàåò B'_1, B'_2, . . . B'_8 Àëèñå.

Êýðîë áåðåò C_1, C_2, . . . C_8 è çàøèôðóåò êàæäûé áèò, èíäåêñ êîòîðîãî îòñóòñòâóåò â íàáîðå {0, 1, 4, 5, 6}åãî äîïîëíåíèå. Íàïðèìåð:

C_7 = 0100010100100 = 2212

C'_7 = 1011100101000 = 5928

Îíà ïîñûëàåò C'_1, C'_2, . . . C'_8 Àëèñå.

(5) Àëèñà ðàñøèôðîâûâàåò âñå C'_i çàêðûòûì êëþ÷îì Áîáà è âûïîëíÿåò XOR ðåçóëüòàòîâ ñ S_i. Íàïðèìåð, äëÿ i = 7:

$5928^{777} \bmod 7387 = 2212$; $2546 \oplus 2212 = 342$

Îíà ïîñûëàåò ðåçóëüòàò Áîáó.

Àëèñà ðàñøèôðîâûâàåò âñå B'_i çàêðûòûì êëþ÷îì Êýðîë è âûïîëíÿåò XOR ðåçóëüòàòîâ ñ S_i. Íàïðèìåð, äëÿ i = 2:

$1660^{2261} \pmod{2747} = 1988$; $471 \oplus 1988 = 1555$

Îíà ïîñûëàåò ðåçóëüòàò Êýðîë.

(6) Áîá âû÷èñëÿåò S_7, âûïîëíÿÿ XOR C_7 è ñðàâíèâàÿ ÷èñëà, ïîëó÷åííîãî èì îò Àëèñû:

$2212 \oplus 342 = 2546$

Êýôîë âû÷èñëÿåò S_2, âû ïîëíÿÿ XOR B_2 è âòîðîãî ÷èñëà, ïîëó÷åííîãî åé îò Àëèñû.

$1988 \oplus 1555 = 471$

Ïðîòîêîë ðàáîòàåò äëÿ ëþáîãî êîëè÷åñòâà ïîëüçîâàòåëåé. Åñëè Âîá, Êýðîë è Äýéâ õîòÿò êóïèòü ñåêðåòû, Àëèñà âûäàåò êàæäîìó ïîëüçîâàòåëþ äâà îòêðûòûõ êëþ÷à, ïî îäíîìó íà êàæäîãî äðóãîãî ïîëüçîâàòåëÿ. Êàæäûé ïîëüçîâàòåëü ïîëó÷àåò íàáîð ÷èñåë îò êàæäîãî äðóãîãî ïîëüçîâàòåëÿ. Çàòåì îíè âûïîëíÿþò ïðîòîêîë ñ Àëèñîé äëÿ êàæäîãî èç ñâîèõ íàáîðîâ íîìåðîâ è âûïîëíÿþò XOR âñåõ ïîëó÷åííûõ îò Àëèñû ðåçóëüòàòîâ, ïîëó÷àÿ ñâîè ñåêðåòû. Áîëåå ïîäðîáíî ýòî îïèñàíî â [1374, 1175].

Ê ñîæàëåíèþ, ïðàêòè÷åñêèå ó÷àñòíûå ñìîøåíèè÷àòü. Àëèñà è Êýðîë, äâéñòâóÿ íà ïàðó, ìîãóò ëåãêî ïîíÿòü, êàêîé ñåêðåò ïîëó÷èë Âîá: åñëè îíè çíàþò FBI C_b è àëãîðèòì øèôðîâàíèÿ Âîáà, îíè ìîãóò ïîäûñêàòü òàêîå b, ÷òî ó C_b áóäåò ïðàâèëüíûé FBI. À Âîá è Êýðîë, äâéñòâóÿ âìåñòå, ìîãóò ëåãêî çàïîëó÷èòü âñå ñâåðåíû Àëèñû.

Åñëè âû ñ÷èòàåòå, ÷òî ó÷àñòíèêè ÷åñòíû, ìîæíî èñïîëüçîâàòü ïðîòîêîë ïîïðîùå [389].

(1) Àëèñà øèôðóåò âñå ñâåðåíû RSA è ïîñûëàåò èõ Âîáó:

$C_i = S_i^e \bmod n$

(2) Âîá âûáèðàåò ñâîé ñâåðåò C_b, ãåíåðèðóåò ñëó÷àéíîå ÷èñëî r è ïîñûëàåò Àëèñå.

$C' = C_b r^e \bmod n$

(3) Àëèñà ïîñûëàåò Âîáó^

$P' = C'^d \bmod n$

(4) Âîá âû÷èñëÿåò P'

$S_b = P' r^{-1} \bmod n$

Åñëè ó÷àñòíèêè ìîãóò æóëüíè÷àòü, Âîá ìîæåò äîêàçàòü ñ íóëåâûì çíàíèåì, ÷òî îí çíàåò íåîòðèöàòåëüíîãî r, òàêîå ÷òî $C' = C_b r^e \bmod n$, è õðàíèòü â b ñåêðåòå, ïîêà Àëèñà íå ïðåäàñòàâèò óíà ýòàïå (3) P' [246].

23.10 ×åñòíûå è îòêàçîóñòîé÷èâûå êðèïòîñèñòåìû

×åñòíàÿ ñõåìà Diffie-Hellman

×åñòíûå êðèïòîñèñòåìû ïðåäñòàâëÿþò ñîáîé ïðîãðàììíûé ñïîñîá óñëîâíîãî âðó÷åíèÿ äîêóìåíòîâ (ñì. ðàçäåë 4.14). Ýòîò ïðèìåð âçÿò èç ðàáîò Ñèëüâèè Ìèêàëè (Silvia Micali) [1084, 1085]. Î í çàïàòåíòîâàí [1086, 1087].

Â áàçîâîé ñõåìå Diffie-Hellman ãðóïïà ïîëüçîâàòåëåé èñïîëüçóåò îáùåå ïðîñòîå ÷èñëî p è ãåíåðàòîð g. Çàêðûòûì êëþ÷îì Àëèñû ÿâëÿåòñÿ s, à åå îòêðûòûì êëþ÷îì $t = g^s \bmod p$. Âîò êàê ñäåëàòü ñõåìó Diffie-Hellman ÷åñòíîé (â ýòîì ïðèìåðå èñïîëüçóåòñÿ ïÿòü äîâåðåííûõ ëèö).

(1) Àëèñà âûáèðàåò ïÿòü öåëûõ ÷èñåë, s_1, s_2, s_3, s_4, s_5, ìåíüøèõ p-1. Çàêðûòûì êëþ÷îì Àëèñû ÿâëÿåòñÿ

$s = (s_1 + s_2 + s_3 + s_4 + s_5) \bmod p\text{-}1$

à åå îòêðûòûì êëþ÷îì

$t = g^s \bmod p$

Àëèñà òàêæå âû÷èñëÿåò

$t_i = g^{s_i} \bmod p$, äëÿ $i = 1, \ldots 5$.

Îòêðûòûì ÷àñòÿì Àëèñû ÿâëÿþòñÿ t_i, à çàêðûòûì - s_i.

(2) Àëèñà ïîñûëàåò çàêðûòóþ è ñîîòâåòñòâóþùóþ îòêðûòóþ ÷àñòè êàæäîìó äîâåðåííîìó ëèöó. Íàïðèìåð, îíà ïîñûëàåò s_1 è t_2 äîâåðåííîìó ëèöó 1. Î íà ïîñûëàåò t â KDC.

(3) Êàæäîå äîâåðåííîå ëèöî ïðîâåðÿåò, ÷òî

$t_i = g^{s_i} \bmod p$

Åñëè ýòî òàê, äîâåðåííîå ëèöî ïîäïèñûâàåò t_i è ïîñûëàåò åãî â KDC. Äîâåðåííîå ëèöî ñîõðàíÿåò s_i â áåçîïàñíîì ìåñòå.

(4) Ï îñëå âñå ïÿòü îòêðûòûõ ÷àñòåé, KDC ïðîâåðÿåò, ÷òî

$t=(t_1 * t_2 * t_3 * t_4 * t_5) \bmod p$

Åñëè ýòî òàê, KDC ïðèçíàåò îòêðûòûé êëþ÷.

Â ýòîì ìîìåíò KDC çíàåò, ÷òî ó êàæäîãî äîâåðåííîãî ëèöà åñòü ïðàâèëüíàÿ ÷àñòü, è ÷òî îíè ïðè íåîáõîäèìîñòè ñîãóò âîññòàíîâèòü çàêðûòûé êëþ÷. Îäíàêî íè KDC, íè ëþáûå ÷åòûðå äîâåðåííûõ ëèöà íå ìîãóò âîññòàíîâèòü çàêðûòûé êëþ÷ Àëèñû.

Ðàáîòû Ì èêàëè [1084, 1085] òàêæå ñîäåðæàò ïîñëåäîâàòåëüíîñòü äâóñòîðîíí èõ ïðîòîêîëîâ, ïîçâîëÿþùèé *m* äîâåðåííûì ëèöàì èç *n* âîññòàíîâèòü çàêðûòûé êëþ÷.

Îòêðûòûé ÷åâàÿ ñõåìà Diffie-Hellman

Êàê è â ïðåäûäóùåì ïðîòîêîëå ó ãðóïïû ïîëüçîâàòåëåé åñòü îáùåå ïðîñòîå ÷èñëî *p* è ãåíåðàòîð *g*. Çàêðûòûì êëþ÷îì Àëèñû ÿâëÿåòñÿ *s*, à åå îòêðûòûì êëþ÷îì $t = g^s \bmod p$.

(1) KDC âûáèðàåò ñëó÷àéíîå ÷èñëî *B* èç äèàïàçîíà îò 0 äî *p*-2 è âðó÷àåò *B* ñ ïîìîùüþ ïðîòîêîëà âðó÷åíèÿ áèòîâ (ñì. ðàçäåë 4.9).

Àëèñà âûáèðàåò ñëó÷àéíîå ÷èñëî *A* èç äèàïàçîíà îò 0 äî *p*-2. Îíà ïîñûëàåò KDC $g^A \bmod p$.

(2) Ï îëüçîâàòåëü "ðàçäåëÿåò" *A* ñ êàæäûì äîâåðåííûì ëèöîì, èñïîëüçóÿ ñõåìó ïîäòâåðæäåíèÿ ïîäëèííîñòè ñîîáùåíèÿ ñåðâåðà (ñì. ðàçäåë 3.7).

(3) KDC ðàñïðîñòðàíÿåò *B* Àëèñå.

(4) Àëèñà ïðîâåðÿåò âðó÷åíèå ýòàïà (1). Çàòåì îíà óñòàíàâëèâàåò ñâîé îòêðûòûé êëþ÷ ðàâíûì

$t = g^A g^B \bmod p$

à çàêðûòûé êëþ÷ ðàâíûì

$s = (A + B) \bmod (p\text{-}1)$

Äîâåðåííûå ëèöà ìîãóò âîññòàíîâèòü *A*. Òàê êàê KDC çíàåò *B*, ýòîãî äîñòàòî÷íî äëÿ âîññòàíîâëåíèÿ *s*. È Àëèñà íå ñìîæåò èñïîëüçîâàòü íèêàêèõ ïîäñìîòðåííûõ êàíàëîâ äëÿ ïððàà÷è íåñàíêöèîíèðîâàííîé èíôîðìàöèè. Ýòîò ïðîòîêîë, ðàññìîòðåííûé â [946, 833] â íàñòîÿùåå âðåìÿ ïàòåíòóåòñÿ.

23.11 ZERO-KNOWLEDGE PROOFS OF KNOWLEDGE

Äîêàçàòåëüñòâî ñóëåâûì çíàíèåì äëÿ äèñêðåòíîãî ëîãàðèôìà

Ï åãàè õî÷åò äîêàçàòü Âèêòîðó, ÷òî åé èçâåñòíî *x*, ÿâëÿþùåéñÿ ðåøåíèåì

$A^x \equiv B \pmod p$

ãäå *p* - ïðîñòîå ÷èñëî, à *x* - ïðîèçâîëüíîå ÷èñëî, âçàèìíî ïðîñòîå ñ *p*-1. ×èñëà *A*, *B* è *p* îáùåäîñòóïíû, à *x* õðàíèòñÿ â ñåêðåòå. Âîò êàê Ï åãàè, íå ðàñêðûâàÿ çíà÷åíèÿ *x*, ìîæåò äîêàçàòü, ÷òî îíî åé èçâåñòíî (ñì. ðàçäåë 5.1) [338, 337].

(1) Ï åãàè ãåíåðèðóåò *t* ñëó÷àéíûõ ÷èñåë, $r_1, r_2, \ldots r_t$, ïðè÷åì âñå r_i ìåíüøå *p*-1.

(2) Ï åãàè âû÷èñëÿåò $h_i = A^{r_i} \bmod p$ äëÿ âñåõ çíà÷åíèé *i* è ï îñûëàåò èõ Âèêòîðó.

(3) Ï åãàè è Âèêòîð, âîñïîëüçîâàâøèñü ïðîòîêîëîì áðîñàíèÿ ì îíåòû ãåíåðèðóþò *t* áèòîâ: $b_1, b_2, \ldots b_t$.

(4) Äëÿ âñåõ *t* áèòîâ Ï åãàè âû ï îëíÿåò îäíó èç ñëåäóþ ùèõ ï ðåäàöèé:

a) Åñëè $b_i = 0$, îíà ï îñûëàåò Âèêòîðó r_i

b) Åñëè $b_i = 1$, îíà ï îñûëàåò Âèêòîðó $s_i = (r_i - r_j) \bmod (p\text{-}1)$, ãäå *j* - íàèìåíüøåå çíà÷åíèå èíäåêñà, ïðè êîòîðîì $b_j = 1$

(5) Äëÿ âñåõ *t* áèòîâ Âèêòîð ïðîâåðÿåò îäíî èç ñëåäóþ ùèõ óñëîâèé:

a) Ï ðè $b_i = 0$ ÷òî $A^{r_i} \equiv h_i \pmod p$

b) Ï ðè $b_i = 1$ ÷òî $A^{s_i} \equiv h_i h_j^{-1} \pmod p$

(6) Ï åãàè ï îñûëàåò Âèêòîðó *Z*, ãäå

$Z = (x - r_j) \bmod (p\text{-}1)$

(7) Âèêòîð ïðîâåðÿåò, ÷òî $A^Z \equiv B h_j^{-1} \pmod p$

Âåðîÿòíîñòü óäà÷íîãî ìîøåííè÷åñòâà Ïåããè ðàâíà $1/2^t$.

Äîêàçàòåëüñòâî ñóùåñòâîâàíèÿ äëÿ âîçìîæíîñòè âñêðûòü RSA

Àëèñà çíàåò çàêðûòûé êëþ÷ Êýðîë. Ì îæåò áûòü îíà âçëîìùèêîì RSA, à ìîæåò îíà âçëîìùèêà äâåðü êâàðòèðû Êýðîë è âûêðàëà êëþ÷. Àëèñà õî÷åò óáåäèòü ÁÎáà, ÷òî åé èçâåñòåí êëþ÷ Êýðîë. Îäíàêî îíà íå õî÷åò íè ñîîáùàòü ÁÎáó êëþ÷, íè äàæå ðàñøèôðîâàòü äëÿ ÁÎáà îäíî èç ñîîáùåíèé Êýðîë. Äàëåå ïðèâåäåí ïðîòîêîë ñ óòâåðæäåíèåì, ñ ïîìîùüþ êîòîðîãî Àëèñà óáåæäàåò ÁÎáà, ÷òî îíà çíàåò çàêðûòûé êëþ÷ Êýðîë [888]. Ïóñòü îòêðûòûé êëþ÷ Êýðîë - *e*, åå çàêðûòûé êëþ÷ - *d*, à ìîäóëü RSA - *n*.

(1) Àëèñà è ÁÎá âûáèðàþò ñëó÷àéíûå *k* è *m*, äëÿ êîòîðûõ

$km \equiv e \pmod{n}$

×èñëà îíè äîëæíû âûáèðàòüñÿ òàêèìè, ÷òîáû ïðîèçâåäåíèå *k* ïðîòèâíè ìîíåòû, à çàòåì âû÷èñëÿÿ *m*. Åñëè è *k*, è *m* áîëüøå 3, ïðîòîêîë ïðîäîëæàåòñÿ. Â ïðîòèâíîì ñëó÷àå ÷èñëà âûáèðàþòñÿ çàíîâî.

(2) Àëèñà è ÁÎá ãåíåðèðóþò ñëó÷àéíûé øèôðîâàííûé *C*. È ñíîâà îíè äîëæíû âîñïîëüçîâàòüñÿ ïðîòîêîëîì áðîñàíèÿ ìîíåòû.

(3) Àëèñà, èñïîëüçóÿ çàêðûòûé êëþ÷ Êýðîë, âû÷èñëÿåò

$M = C^d \bmod n$

Çàòåì îíà âû÷èñëÿåò

$X = M^k \bmod n$

è ïîñûëàåò *X* ÁÎáó.

(4) ÁÎá ïðîâåðÿåò, ÷òî $X^m \bmod n = C$. Åñëè ýòî òàê, òî îí óáåæäàåòñÿ â ïðàâèëüíîñòè çàÿâëåíèÿ Àëèñû.

Àíàëîãè÷íûé ïðîòîêîë ìîæíî èñïîëüçîâàòü äëÿ äàëüíîñòíîé ñâÿçè ïîñðåäñòâîì ïðîâåäåíèÿ äèñêðåòíîãî ëîãàðèôìà [888].

Äîêàçàòåëüñòâî ñóùåñòâîâàíèÿ òîãî, ÷òî ïðîáëåìû ÷èñëî Áëþìà

Ïîêà íåèçâåñòíî ýêâèâåíòíî ïðàêòè÷íûõ äîêàçàòåëüñòâ òîãî, ÷òî $n = pq$, ãäå p è q - ïðîñòûå ÷èñëà, êîíãðóýíòíûå 3 ïî ìîäóëþ 4. Îäíàêî åñëè n èìåòü âèä $p^r q^s$, ãäå r è s íå÷åòíû, òî ó ÷èñëà n ñîððàíÿþòñÿ ñâîéñòâà, êîòîðûå äåëàþò ÷èñëà Áëþìà ïîëåçíûìè äëÿ êðèïòîãðàôèè. È òîãäà ñóùåñòâóåò äîêàçàòåëüñòâî ñ íóëåâûì çíàíèåì òîãî, ÷òî n èìåò òàêóþ âíåøíþþ ôîðìó.

Ïðåäïîëîæèì, ÷òî Àëèñà èçâåñòíî ðàçëîæåíèå íà ìíîæèòåëè ÷èñëà Áëþìà n, ãäå n îáëàäàåò ðàñïîòðåíí îé âûøå âíåøíåé. Âîò êàê îíà ìîæåò äîêàçàòü ÁÎáó, ÷òî n èìåò òàêóþ âíåøíþþ [660].

(1) Àëèñà ïîñûëàåò ÁÎáó ÷èñëî u, ÷åé ñìîâîë ßêîáè ðàâåí -1 ïî ìîäóëþ n.

(2) Àëèñà è ÁÎá ñîâìåñòíî âûáèðàþò ñëó÷àéíûå áèòû: $b_1, b_2, \ldots b_k$.

(3) Àëèñà è ÁÎá ñîâìåñòíî âûáèðàþò ñëó÷àéíûå ÷èñëà: $x_1, x_2, \ldots x_k$.

(4) Äëÿ êàæäîãî $i = 1, 2, \ldots k$ Àëèñà ïîñûëàåò ÁÎáó êâàäðàòíûé êîðåíü ïî ìîäóëþ n äëÿ îäíîãî èç ÷åòûðåõ ÷èñåë: x_i, $-x_i$, ux_i, $-ux_i$. Ñìîâîë ßêîáè êâàäðàòíîãî êîðíÿ äîëæåí áûòü ðàâåí b_i.

Âåðîÿòíîñòü óäà÷íîãî ìîøåííè÷åñòâà Àëèñû ðàâíà $1/2^k$.

23.12 Ñëåïûå ïîäïèñè

Ïîíÿòèå ñëåïîãî ïîäïèñè (ñì. ðàçäåë 5.3) áûëî ïðèäóìàíî Äýâèäîì ×àóì (David Chaum) [317, 323], êîòîðûé òàêæå ïðåäëîæèë è ïðåâîþ ðåàëèçàöèþ ýòîãî ïîíÿòèÿ [318]. Îíà èñïîëüçóåò àëãîðèòì RSA.

Ó ÁÎáà åñòü îòêðûòûé êëþ÷ *e*, çàêðûòûé êëþ÷ *d* è îòêðûòûé ìîäóëü *n*. Àëèñà õî÷åò, ÷òîáû ÁÎá âñëåïóþ, íå ÷èòàÿ, ïîäïèñàë ñîîáùåíèå *m*.

(1) Àëèñà âûáèðàåò ñëó÷àéíîå ÷èñëî *k* èç äèàïàçîíà îò 1 äî *n*. Çàòåì îíà ìàñêèðóåò *m*, âû÷èñëÿÿ

$t = mk^e \bmod n$

(2) ÁÎá ïîäïèñûâàåò *t*

$t^d = (mk^e)^d \bmod n$

(3) Àëèñà ñíèìàåò ìàñêèðîâêó ñ t^d, âû÷èñëÿÿ

$s = t^d/k \bmod n$

(4) Ðåçóëüòàòîì ÿâëÿåòñÿ

$s = m^d \bmod n$

Ýòî ìîæíî ëåãêî ïîêàçàòü

$t^d \equiv (mk^e)^d \equiv m^d k \pmod n$, ïîýòîìó $t^d/k = m^d k/k \equiv m^d \pmod n$.

×àùå ïðèäóìàë öåëîå ñåìåéñòâî áîëåå ñëîæíûõ àëãîðèòìîâ ñëåïîé ïîäïèñè [320, 324], íàçûâàåìûõ íåîæèäàííûìè ñëåïûìè ïîäïèñÿìè. Ñõåìû ýòèõ ïîäïèñåé ñëîæíåå, íî îíè äàþò áîëüøå âîçìîæíîñòåé.

23.13 Ïåðåäà÷à ñçáûâàíèå

Â ýòîì ïðîòîêîëå, ïðåäëîæåííîì Ìàéêëîì Ðàáèíûì (Michael Rabin) [1286], Àëèñà ñ âåðîÿòíîñòüþ 50 ïðîöåíòîâ óâåäîìëÿ ïðåäâàðèòåëüíûé ÁÎáó äâà ïðîñòûõ ÷èñëà, p è q. Àëèñà íå çíàåò, óñïåøíî ëè ïðîøëà ïðåäâà÷à (Ñì. ðàçäåë 5.5.) (Ýòîò ïðîòîêîë ìîæíî èñïîëüçîâàòü äëÿ ïðåäâà÷è ÁÎáó ëþáîãî ñîîáùåíèÿ ñ 50-ïðîöåíòíîé âåðîÿòíîñòüþ óñïåøíîé ïðåäâà÷è, åñëè p è q ðàñêðûâàþò çàêðûòûé êëþ÷ RSA.)

(1) Àëèñà ïîñûëàåò ÁÎáó ïðîèçâîëüíîå äâóõ ïðîñòûõ ÷èñåë: $n = pq$.

(2) ÁÎá âûáèðàåò ñëó÷àéíîå ÷èñëî x, ìåíüøåå n è âçàèìíî ïðîñòîå ñ n. Î í ïîñûëàåò Àëèñå:

$a = x^2 \bmod n$

(3) Àëèñà, çíàÿ p è q, âû÷èñëÿåò ÷åòûðå êâàäðàòíûõ êîðíÿ a: x, n-x, y è n-y. Î íà ñëó÷àéíûì îáðàçîì âûáèðàåò ëþáîé èç ýòèõ êîðíåé è ïîñûëàåò åãî ÁÎáó.

(4) Åñëè ÁÎá ïîëó÷àåò y ëèáî n-y, îí ìîæåò âû÷èñëèòü íàèáîëüøèé îáùèé äåëèòåëü $x+y$ è n, êîòîðûì áóäåò ëèáî p, ëèáî q. Çàòåì, êîíå÷íî æå, $n/p = q$. Åñëè ÁÎá ïîëó÷àåò x ëèáî n-x, îí íå ìîæåò íè÷åãî âû÷èñëèòü.

Ó ýòîãî ïðîòîêîëà ìîæåò áûòü ñëàáîå ìåñòî: âîçìîæíà ñèòóàöèÿ, êîãäà ÁÎá ìîæåò âû÷èñëèòü òàêîå ÷èñëî a, ÷òî ïðè èçâåñòíîì êîäèðîâàíèè êîíêðåòíîãî a îí ñìîæåò âñå âðåìÿ ðàñêëàäûâàòü n íà ìíîæèòåëè.

23.14 Áåçîïàñíûå âû÷èñëåíèÿ ñ íåñêîëüêèìè óчàñòíèêàìè

Ýòîò ïðîòîêîë âçÿò èç [1373]. Àëèñà çíàåò öåëîå ÷èñëî i, à ÁÎá - öåëîå ÷èñëî j. Àëèñà è ÁÎá âìåñòå õîòÿò óçíàòü, ÷òî ïðàâäèâî - $i \le j$ èëè $i > j$, íî íè Àëèñà, íè ÁÎá íå õî÷åò ðàñêðûòü ñâîå ÷èñëî ïàðòíåðó. Ýòîò îñîáûé ñëó÷àé áåçîïàñíûõ âû÷èñëåíèé ñ íåñêîëüêèìè ó÷àñòíèêàìè (ñì. ðàçäåë 6.2) èíîãäà íàçûâàþò **ïðîáëåìîé ìèëëèîíåðà ßî** [162, 7].

Â ïðèâåäåííîì ïðèìåðå ïðåäïîëàãàåòñÿ, ÷òî i è j âûáèðàþòñÿ èç äèàïàçîíà îò 1 äî 100. Ó ÁÎáà åñòü îòêðûòûé è çàêðûòûé êëþ÷è.

(1) Àëèñà âûáèðàåò áîëüøîå ñëó÷àéíîå ÷èñëî x è øèôðóåò åãî îòêðûòûì êëþ÷îì ÁÎáà.

$c = E_B(x)$

(2) Àëèñà âû÷èñëÿåò c-j è ïîñûëàåò ðåçóëüòàò ÁÎáó.

(3) ÁÎá âû÷èñëÿåò ñëåäóþùèå 100 ÷èñåë:

$y_u = D_B(c-i+u)$, äëÿ $1 \le u \le 100$

D_B îáîçíà÷àåò äåøèôðîâàíèå çàêðûòûì êëþ÷îì ÁÎáà.

Î í âûáèðàåò áîëüøîå ñëó÷àéíîå ÷èñëî p. (Ðàçìåð p äîëæåí áûòü íåìíîãî ìåíüøå x. Áîá íå çíàåò x, íî Àëèñà ìîæåò ëåãêî ñîîáùèòü åìó ðàçìåð x.) Î í âû÷èñëÿåò ñëåäóþùèå 100 ÷èñåë:

$z_u = (y_u \bmod p)$, äëÿ $1 \le u \le 100$

Äàëåå î í ïðîâåðÿåò, ÷òî äëÿ âñåõ $u \ne v$

$|z_u - z_i| \ge 2$

è ÷òî äëÿ âñåõ u

$0 < z_u < p$-1

Åñëè ýòî íå òàê, òî ÁÎá âûáèðàåò äðóãîå ïðîñòîå ÷èñëî è ïðîáóåò ñíîâà.

(4) Áîá ïîñûëàåò Àëèñå ýòó ïîñëåäîâàòåëüíîñòü ÷èñåë, ñîâåðøàÿ èõ òî÷íûé ïîðÿäîê:

$z_1, z_2, \ldots z_j, z_{j+1}+1, z_{j+2}+1, \ldots z_{100}+1, p$

(5) Àëèñà ïðîâåðÿåò, êîíãðóýíòåí ëè *i*-ûé ÷ëåí ïîñëåäîâàòåëüíîñòè *x* mod *p*. Åñëè ýòî òàê, îíà äåëàåò âûâîä, ÷òî *i*≤*j*. Â ïðîòèâíîì ñëó÷àå îíà ðåøàåò, ÷òî *i*> *j*.

(6) Àëèñà ñîîáùàåò Áîáó ñâîè âûâîäû.

Ïðîâåðêà, êîòîðóþ Áîá âûïîëíÿåò íà ýòàïå (3), äîëæíà ãàðàíòèðîâàòü, ÷òî íè îäíî ÷èñëî íå ïîÿâèòñÿ äâàæäû â ïîñëåäîâàòåëüíîñòè, ãåíåðèðîâàííîé íà ýòàïå (4). Â ïðîòèâíîì ñëó÷àå, åñëè $z_a = z_b$, Àëèñà óçíàåò, ÷òî $a \le j < b$.

Íåäîñòàòêîì ýòîãî ïðîòîêîëà ÿâëÿåòñÿ òî, ÷òî Àëèñà óçíàåò ðåçóëüòàòû âû÷èñëåíèé ðàíüøå Áîáà. Íè÷òî íå ïîìåøàåò åé çàâåðøèòü ïðîòîêîë íà ýòàïå (5), îòêàçàâøèñü ñîîáùàòü Áîáó ðåçóëüòàòû. Îíà äàæå ìîæåò ñîêãàòü Áîáó íà ýòàïå (6).

Ïðèìåð ïðîòîêîëà

Ïóñòü îíè èñïîëüçóþò RSA. Îòêðûòûé êëþ÷îì Áîáà ÿâëÿåòñÿ 7, à çàêðûòûì - 23. *n* = 55. Ñåêðåòíûå ÷èñëî Àëèñû, *i*, ðàâíî 4, ñåêðåòíîå ÷èñëî Áîáà, *j* - 2. (Ïðåäïîëîæèì, ÷òî ÷èñëà *i* è *j* ìîãóò ïðèíèìàòü òîëüêî çíà÷åíèÿ 1, 2, 3 è 4.)

(1) Àëèñà âûáèðàåò *x* = 39 è $c = E_B(39) = 19$.

(2) Àëèñà âû÷èñëÿåò *c*-*i*=19-4=15. Îíà ïîñûëàåò 15 Áîáó.

(3) Áîá âû÷èñëÿåò ñëåäóþ ùèå ÷åòûðå ÷èñëà:

$y_1 = D_B\{15+l) = 26$

$y_2 = D_B\{15+2) = 18$

$y_3 = D_B\{15+3) = 2$

$y_4 = D_B\{15+4) = 39$

Îí âûáèðàåò *p* = 31 è âû÷èñëÿåò:

$z_1 = (26 \bmod 31) = 26$

$z_2 = (18 \bmod 31) = 18$

$z_3 = (2 \bmod 31) = 2$

$z_4 = (39 \bmod 31) = 8$

Îí âûïîëíÿåò âñå ïðîâåðêè è óáåæäàåòñÿ, ÷òî ïîñëåäîâàòåëüíîñòü ïðàâèëüíà.

(4) Áîá ïîñûëàåò Àëèñå ýòó ïîñëåäîâàòåëüíîñòü ÷èñåë, ñîáðàííóþ èõ ïîðÿäîê:

26, 18, 2+1, 8+1, 31, ò.å., 26, 18, 3, 9, 31

(5) Àëèñà ïðîâåðÿåò, êîíãðóýíòíî ëè ÷åòâåðòîå ÷èñëî *X* mod *p*. Òàê êàê $9 \neq 39 \pmod{31}$, òî *i* > *j*.

(6) Àëèñà ñîîáùàåò îá ýòîì Áîáó.

Ýòîò ïðîòîêîë ìîæíî èñïîëüçîâàòü äëÿ ñîçäàíèÿ íàìíîãî áîëåå ñëîæíûõ ïðîòîêîëîâ. Ãðóïïà ëþäåé ìîæåò ïðîâîäèòü ñâîåîáðàçíûé àóêöèîí ïî ñåòè. Îíè ëãàë÷åñêè óïðàâëÿò ñåáÿ ïî êðóãó è, ñ ïîìîùüþ ïîïàðíûõ ñðàâíåíèé, îïðåäåëÿò, êòî ïðåäëîæèë áîëüøóþ öåíó. ×òîáû ïîìåøàòü ëþäÿì óæå èçìåíÿòü ñäåëàííûå ïðåäëîæåíèÿ â ñåðåäèíå àóêöèîíà äîëæåí èñïîëüçîâàòüñÿ êàêîé-òî ïðîòîêîë âðó÷åíèÿ áèòâ. Åñëè àóêöèîí ïðîâîäèòñÿ ïî âîëíàì ñîòîâîãî ñîòîâîãî ïîêîëåíèÿ, òî ïðåäëîæåâøèé íàèâûñøóþ öåíó ïîëó÷àò ïðåèìóùåñòâî ïåðåä ïðîòèâíèêîì ñòàíîâèòüñÿ îäíèì èç ïîáåäèòåëåé.) Àíàëîãè÷íûå èäåè ïðèìåíèìû ïðè çàêëþ÷åíèè ñäåëîê, ïðåäâîñõèùàþùèõ è àðáèòðàæ.

23.15 Âåðîÿòíîñòíûå øèôðîâàíèå

Ïîíÿòèå **âåðîÿòíîñòíîãî øèôðîâàíèÿ** áûëî èçîáðåòåíî Øàôè Ãîëäâàññåðîì (Shafi Goldwasser) è Ñèëüâèåé Ìèêàëè [624]. Õîòÿ èõ òåîðèÿ ïîçâîëÿåò ñîçäàòü áåçîïàñíóþ èç èçíáðàòåëüíûõ êðèïòîñèñòåì, ðàíüøå áûëè ðåàëèçàöèè áûëà íåýôôåêòèâíîé [625]. Íî áîëåå ïîçäíèå ðåàëèçàöèè âñå èçìåíèëè.

Èäåé âåðîÿòíîñòíîãî øèôðîâàíèÿ ÿâëÿåòñÿ óñòðàíåíèå óòå÷êè èíôîðìàöèè â êðèòîãðàôèè ñ îòêðûòûì êëþ÷îì. Òàê êàê êðèïòîàíàëèòèê âñåãäà ìîæåò ðàñøèôðîâàòü ñîîáùåíèÿ îòêðûòûì êëþ÷îì, îí ìîæåò ïîëó÷èòü íåêîòîðóþ èíôîðìàöèþ. Ïðè óñëîâèè, ÷òî ó íåãî åñòü øèôðîâêè $C = E_K(M)$, è îí ïûòàåòñÿ ïîëó÷èòü îòêðûòûé òåêñò *M*, îí ìîæåò âûáðàòü ñëó÷àéíîå ñîîáùåíèå *M′* è çàøèôðîâàòü âåñ: $C' = E_K(M')$. Åñëè $C' = C$, òî îí óãàäàë ïðàâèëüíûé îòêðûòûé òåêſò. Â ïðîòèâíîì ñëó÷àå îí äåëàåò ñëåäóþ ùóþ ïîïûòêó.

Êðîìå òîãî, âåðîÿòíîñòíûå øèôðîâàíèå ïîçâîëÿåò èçáåæàòü äàæå ÷àñòè÷íîé óòå÷êè èíôîðìàöèè îá îðèãèíàëüíîì ñîîáùåíèè. Ïðè èñïîëüçîâàíèè êðèïòîãðàôèè ñ îòêðûòûì êëþ÷àìè êðèïòîàíàëèòèê èíîãäà ìîæåò óçíàòü êîä-÷òî î áèòàõ: XOR 5-ãî, 17-ãî è 39-ãî áèòîâ ðàâíî 1, è ò.ï.. Ïðè âåðîÿòíîñòíîì øèôðîâàíèè îñòàåòñÿ ñêðûòîé è òàéíîé èíôîðìàöèÿ.

Òàêèì ñïîñîáîì ìîæíî èçâëå÷ü íå ìíîãî èíôîðìàöèè, íî ïîòåíöèàëüíî âîçìîæíîñòü êðèïòîàíàëèòèêà ðàñøèôðîâûâàòü ñëó÷àéíûå ñîîáùåíèÿ âàøèì îòêðûòûì êëþ÷îì ìîæåò ñîçäàòü ïðåäåëåííûå ïðîáëåìû. Êàæäûé ðàç, øèôðóÿ ñîîáùåíå, êðèïòîàíàëèòèê ìîæåò èçâëå÷ü íåìíîãî èíôîðìàöèè. Íèêòî íå çíàåò, íàñêîëüêî çíà÷èòåëüíà ýòà èíôîðìàöèÿ.

Âåðîÿòíîñòíûå øèôðîâàíèå ïûòàåòñÿ óñòðàíèòü ýòó óòå÷êó. Öåëü ýòîãî ìåòîäà ñîñòîèò â òîì, ÷òîáû íè âû÷èñëåíèÿ, ïðîâîäèìûå íàä øèôðîòåêñòîì, íè ïðîâåðêà ëþáûõ äóãèõ îòêðûòûõ òåêñòîâ íå ñìîãëè äàòü êðèïòîàíàëèòèêó íèêàêîé èíôîðìàöèè î ñîîòâåòñòâóþùåì îòêðûòîì òåêñòå.

Ïðè âåðîÿòíîñòíîì øèôðîâàíèè äëãîðèòì øèôðîâàíèÿ ÿâëÿåòñÿ âåðîÿòíîñòíûì, à íå äåòåðìèíèðîâàííûì. Äóãèìè ñëîâàìè, ìíîãèå øèôðîòåêñòû ïðè ðàñøèôðîâêå äàþò äàííûé îòêðûòûé òåêñò, è êîíêðåòíûé øèôðîòåêñò, èñïîëüçóåìûé â ëþáîì êîíêðåòíîì øèôðîâàíèè, âûáèðàåòñÿ ñëó÷àéíûì îáðàçîì.

$C_1 = E_K(M)$, $C_2 = E_K(M)$, $C_3 = E_K(M)$, . . . $C_i = E_K(M)$

$M = D_K(C_1) = D_K(C_2) = D_K(C_3) = \ldots = D_K(C_i)$

Ïðè âåðîÿòíîñòíîì øèôðîâàíèè êðèòîàíàëèòèêó áîëüøå íå óäàñòñÿ øèôðîâàòü ïðîèçâîëüíûå îòêðûòûå òåêñòû â îòëè÷èå îò ñëó÷àéíûõ øèôðîòåêñòà. Äëÿ èëëþñòðàöèè ó êðèòîàíàëèòèêà åñòü øèôðîòåêñò $C_i = E_K(M)$. Äàæå åñëè îí ïðàêòè÷åñêè M, ïîëó÷åííûé ïðè øèôðîâàíèè $E_K(M)$ ðåçóëüòàò áóäåò ñîâåðøåííî äðóãèì øèôðîòåêñòîì C: C_j. Ñðàâíèâàÿ C_i è C_j, îí íå ìîæåò ïî èõ ñîâïàäåíèþ îïðåäåëèòü ïðàâèëüíîñòü ñîâåé äîãàäêè.

Ýòî ïîðàçèòåëüíî. Äàæå åñëè ó êðèòîàíàëèòèêà åñòü îòêðûòûé êëþ÷ øèôðîâàíèÿ, îòêðûòûé òåêñò è øèôðîòåêñò, îí íå ìîæåò áåç çàêðûòîãî êëþ÷à äøèôðîâàíèÿ äîêàçàòü, ÷òî øèôðîòåêñò ÿâëÿåòñÿ ðåçóëüòàòîì øèôðîâàíèÿ êîíêðåòíîãî òåêñòà. Äàæå âûïîëíèâ èñ÷åðïûâàþùèé ïîèñê, îí ìîæåò äîêàçàòü òîëüêî, ÷òî êàæäûé âîçìîæíûé îòêðûòûé òåêñò ÿâëÿåòñÿ âîçìîæíûì îòêðûòûì òåêñòîì.

Â ýòîé ñòàòüå øèôðîòåêñò âñåãäà áóäåò îòêðûòûì òåêñòà. Ýòîãî íåâîçìîæíî èçáåæàòü, ýòî ÿâëÿåòñÿ ðåçóëüòàòîì òîãî, ÷òî ìíîãèå øèôðîâàíèÿ ñ îòêðûòûì ðàñøèôðîâûâàþòñÿ â îäèí è òîò æå îòêðûòûé òåêñò. Â ïåðâîé ñòàòüå âåðîÿòíîñòíîãî øèôðîâàíèÿ [625] øèôðîòåêñò ïîëó÷àëñÿ íàñòîëüêî áîëüøå îòêðûòîãî òåêñòà, ÷òî îí áûë áåçîïàñíûì.

Îäíàêî Ìàíóýëü Áëþì (Manual Blum) è Ãîëäâàññåð (Goldwasser) ïîëó÷èëè ýôôåêòèâíóþ ðåàëèçàöèþ âåðîÿòíîñòíîãî øèôðîâàíèÿ ñ îòêðûòûì ãåíåðàòîðà ïñåâäîñëó÷àéíûõ áèòîâ Blum Blum Shub (BBS), îïèñàííîãî â ðàçäåëå 17.9 [199].

Åãåíåðàòîð BBS îñíîâàí íà òåîðèè êâàäðàòè÷íûõ îñòàòêîâ. Ñóùåñòâóþò äâà ïðîñòûõ ÷èñëà, p è q, êîíãðóýíòíûõ 3 ïî ìîäóëþ 4. Ýòî çàêðûòûé êëþ÷. Èõ ïðîèçâåäåíèå, $pq = n$, ÿâëÿåòñÿ îòêðûòûì êëþ÷îì. (Çàìåòèì ñâîè p è q, áåçîïàñíîñòü ñõåìû îïèðàåòñÿ íà ñëîæíîñòü ðàçëîæåíèÿ n íà ìíîæèòåëè.)

Äëÿ øèôðîâàíèÿ ñîîáùåíèÿ M ñíà÷àëà âûáèðàåòñÿ ñëó÷àéíîå x, âçàèìíî ïðîñòîå ñ n. Çàòåì âû÷èñëÿåòñÿ

$x_0 = x^2 \bmod n$

x_0 ñëóæèò ñòàðòîâîé ïîñëåäîâàòåëüíîñòüþ äëÿ ãåíåðàòîðà ïñåâäîñëó÷àéíûõ áèòîâ BBS, à âûõîä ãåíåðàòîðà èñïîëüçóåòñÿ â êà÷åñòâå ïîòîêîâîãî øèôðà. Ïîáèòîâî âûïîëíÿåòñÿ XOR M ñ âûõîäîì ãåíåðàòîðà. Åãåíåðàòîð âûäàåò áèòû b_i (ìëäøèé çíà÷àùèé áèò x_i, ãäå $x_i = x_{i-1}^2 \bmod n$), ïîýòîìó

$M=M_1, M_2, M_3, \ldots M_t$

$c = M_1 \oplus b_1, M_2 \oplus b_2, M_3 \oplus b_3, \ldots \ M_t \oplus b_t$

ãäå t - ýòî äëèíà îòêðûòîãî òåêñòà

Äîáàâüòå ïîñëåäíåå âû÷èñëåííîå çíà÷åíèå, x_t, ê êîíöó ñîîáùåíèÿ, è äëî ñåãèíî.

Ðàñøèôðîâàòü ýòî ñîîáùåíèå ìîæíî òîëüêî îäíèì ñïîñîáîì - ïîëó÷èòü x_0 è ñ ýòîé ñòàðòîâîé ïîñëåäîâàòåëüíîñòü çàïóñòèòü ãåíåðàòîð BBS, âû ïîíÿòü XOR âûõîäà ñ øèôðîòåêñòîì. Òàê êàê ãåíåðàòîð BBS áåçîïàñåí âëâîî, çíà÷åíèå x_t áåñïîëåçíî äëÿ êðèòîàíàëèòèêà. Òîëüêî òîò, êòî ìóä èçâåñòíû p è q, ìîæåò ðàñøèôðîâàòü ñîîáùåíèå. Âîò êàê íà ÿçûêå C âûãëÿäèò äëãîðèòì ïîëó÷åíèÿ x_0 èç x_t:

```
int xO (int p, int q, int n, int t, int xt) {
    int a, b, u, v, w, z;
    /* ìû óæå çíàåì, ÷òî ÍÎÄ(p,q) == 1 */
    (void)extended_euclidian(p, q, &a, &b);
```

```
    u = modexp ((p+1)/4, t, p-1);
    v = modexp ((q+1)/4, t, q-1);
    w = modexp (xt%p, u, p);
    z = modexp (xt%p, v, q);
    return (b*q*w + a*p*z) % n;
}
```

Ïðè íàëè÷èè x_0 äâîè÷íîãî ïðåäñòàâëåíèÿ íåñëîæíî. Ïðîñòî çàäàéòå ñòàðòîâóþ ïîñëåäîâàòåëüíîñòü ãåíåðàòîðà BBS è âû÷èñëèòå XOR ðåçóëüòàòà ñ øèôðîâàííûì.

Ýòó ñõåìó ìîæíî äàëåå óñëîæíÿòü, èñïîëüçóÿ âñå èçâåñòíûå áàçîâûå áëîêè x_i, à íå òîëüêî ìëàäøèé çíà÷àùèé áèò. Ñ òàêèì óëó÷øåíèåì âåðîÿòíîñòíûå øèôðîâàíèå Blum-Goldwasser îêàçûâàåòñÿ áûñòðåå RSA è íå äîïóñêàåò óòå÷êè èíôîðìàöèè îá îòêðûòîì òåêñòå. Êðîìå òîãî, ìîæíî äîêàçàòü, ÷òî ñëîæíîñòü âñêðûòèÿ ýòîé ñõåìû ðàâíà ñëîæíîñòè ðàçëîæåíèÿ n íà ìíîæèòåëè.

Ñ äðóãîé ñòîðîíû, ýòà ñõåìà ñîâåðøåííî íåäåçîïàñíà ïî îòíîøåíèþ ê âñêðûòèþ ñ âûáðàííûì øèôðîòåêñòîì. Ïî ìèãàøè çíà÷àùèì áèòàì ïðàêòè÷åñêè íåâîçìîæíî âû÷èñëèòü êâàäðàòè÷íûõ îñòàòêîâ ìîäóëî n, äàæå çíàÿ åãî ðàçëîæåíèå. Ïîäîáíûé ôàêò óäàñòñÿ, òî óäàñòñÿ è ðàçëîæåíèå íà ìíîæèòåëè. Ïîäðîáíîñòè âû÷èñëèòåëüíîé ñëîæíîñòè ýòîé çàäà÷è ìîæíî íàéòè â [1570, 1571, 35, 36].

23.16 Êâàíòîâàÿ êðèïòîãðàôèÿ

Êâàíòîâàÿ êðèïòîãðàôèÿ ââîäèò åñòåñòâåííóþ íåîïðåäåëåííîñòü êâàíòîâîãî ìèðà. Ñ åå ïîìîùüþ ìîæíî ñîçäàâàòü ëèíèè ñâÿçè, êîòîðûå íåâîçìîæíî ïîñëóøàòü, íå âîâëåêàÿ â ïðåäà÷ó. Çàêîíûôèçèêè íàäåæíî çàùèùàþò òàêîé êâàíòîâûé êàíàë, äàæå åñëè ïîäñëóøèâàþùèé ìîæåò ïðåäïðèíèìàòü ëþáûå äåéſòâèÿ, äàæå åñëè îí èìåò äîñòóï ê íåîãðàíè÷åííîé âû÷èñëèòåëüíîé ìîùíîſòè, äàæå åñëè **P = NP**. Øàðëü Áåííåò (Charles Bennett), Æèëü Áðàññàð (Gilles Brassard), Êëîä Êðåïî (Claude Crepeau) è äðóãèå ðàñøèðèëè ýòó èäåþ, îïèñàâ êâàíòîâîå ðàñïðåäåëåíèå êëþ÷åé, êâàíòîâîå áðîñàíèå ìîíåòû, êâàíòîâîå âðó÷åíèå áèòà, êâàíòîâóþ ïåðåäà÷ó ñ çàáûâàíèåì è êâàíòîâûå âû÷èñëåíèÿ ñ íåñêîëüêèìè ó÷àſòíèêàìè. Îſèñàíèå èõ ðåçóëüòàòîâ ìîæíî íàéſè â [128, 129, 123, 124, 125, 133, 126, 394, 134, 392, 243, 517, 132, 130, 244, 393, 396]. Ëó÷øèì îáçîðîì ſî êâàíòîâîé êðèſòîãðàôèè ſâëſåòſſ [131]. Äðóãèì õîðîøèì íåòåõíè÷åñêèì îáçîðîì ſîæåſ ſëóæèòſ [1651]. Sîſíóſ áèáëèîãðàôèſ ſî êâàíòîâîé êðèſòîãðàôèè ſîæſſ íàéòè â [237].

Ýòè èäåè òàê è îſòàëèſſ áû ſðåäſåòſſ îáſóæäåſſÿ ôàſàòèêîâ êðèſòîãðàôèè, íî Áåſſå è Áðàſſàð ðàçðàáſòàëè äåéſòâóſſóſ ſſſîſſſ [127, 121, 122]. Òåſðüſ ó íàſ åſòſſ *ýêſſåðſſſſàſſòàëüſſàÿ* êâàſſòſſâàÿ êðèſòſſãðàôèÿ.

Èòàê óſòðſéòåſſü ſſóäſäſſåå, íàëåéòå ſåáå ſåãſ-íèáóäü âûſèòü è ðàſſſëàáüòåſſü. ß ſſſſðſáóþ ſáúÿſſéòü âàì, ſòſ ýòſ òàêſå.

Â ſſſòſååòſòâèè ſ çàêſſàſè êâàſòſâſé ſåðàſêêê ſàſòèöû íà ſàſſſ äåëå íå íàðſäÿòſſ â ſäſſſ ſåſòå, à ſ ſſ-ðåääëåſſſſé åâðſÿòſſſſòüþ ſóſåſòåſóþò ſðàçſ âſ ſſſãèſò ſåſòàſ. Säſàêſ ýſ òàê òſêüſê äſ òåſ ſſð, ſſêà íå ſðèſſſäèò ó÷åſſûé è íå ſàſåðÿåò ſàſòèó, "ſêàçàâøóþſÿ" â äàſſſſ êſſíêðåòſſſ ſåſòå. Íſ èçſåðèòü âñå ſàðàſåòðû ſàſòèöû (íàſðèſåð, êſſðäèſàòû è ſêſðſſòü) ſäſſâðåſſåſſ íåâſçſſſæſſ. Åſëè èçſåðèòü ſàſó èç ýòèſ äâóſ âåëè÷èſ, ſàſ àêò èçſåðåſëÿ óſè÷òſæàåò âſÿêóþ âſçſſæſſſòü èçſåðèòü äðóáóþ âåëè÷èſó. Íåſſïðåäåëåſſſſòü ÿâëÿåòſÿ ôóſäàſåſòàëüſû ſ ſâſéſòſðſſòſſ êâàſòſâſ ſèðà, è íèêóäà ſò ýòſ íå äåſåøüſÿ.

Ýòó íåſïðåäåëåſſſòü ſſæſſ èſſſſëüçſâàòü äëÿ ãåſåðàöèè ſåêðåòſſſ êëþ÷à. Ïóòåøåſòâóÿ, ôſòſſû êſëåáëþòſÿ â ſïðåäåëåſſſſ íàïðàâëåſèè, ââåðõ-âſèç, âëåâſ-âſðàâſ, èëè, ÷òſ áſëåå âåðſÿòſſ, ſſä êàêèſ-òſ óãëſ. Îáû÷íûé ñſëſå÷íûé ſâåò íåſſëÿðèçſâàſ, ôſòſſû êſëåáëþòſÿ âſ åſſõ âſçſſæſſûõ íàſðàâëåſèÿõ. Êſãàà íàſðàâëåſèå êſëåáàſéſ ſſſãèõ ôſòſſſû ſſâſäàäàåò, ſſſ ÿâëÿþòſÿ **ſſëÿðèçſâàſſûſè**. Ïſëÿðèçäöèſſſûå ôëëüòðû ſðſſſóſêàþò òſëüſêſ òå ôſòſſû, êſòſðûå ſſëÿðèçſâàſſû â ſſðåäåëåſſſſ íàſðàâëåſèè, à ſñòàëüſûå áëſêèðóþòſÿ. Íàſðèſåð, ãſðèçſſòàëüſûé ſſëÿðèçäöèſſſûé ôëëüòð ſðſſóſêàåò òſëüſêſ ôſòſſû ſ ãſðèçſſòàëüſſé ſſëÿðèçàöèſåé. Ïſâåðſſå ýòſ ôëëüòð íà 90 ãðàäóſſâ, è òåſðüſ ſêâſçü ſåſſ áóäó ſðſſſäèòü òſëüſêſ âåðòèêàëüſſ ſſëÿðèçſâàſſûå ôſòſſû.

Ïóſòü ó âàſ åſòü èſ ſóëüſſ ãſðèçſſòàëüſſ ſſëÿðèçſâàſſûſ ôſòſſâ. Åſëè ſſè ſſſðſáóþò ſðſſóè ÷åðåç ãſðèçſſòàëüſûé ôëëüòð, òſ ó íèſ ó âſåſ ſðåðèſſſ ſſëó÷èſſ. Åſëè ſåëëſſſ ſſſâſðà÷èàòü ôëëüòð íà 90 ãðàäóſſâ, êſëë÷åſòſâ ſðſſſóſêàåſ ſſſãèſò ôſòſſû áóäåò ſòàſſâèòüſſ âſå ſåſüøå è ſåſüøå, è íàêſſåö íè ſäèſ ôſòſſ íå ſðſé-äåò ÷åðåç ôëëüòð. Ýòſ ſðſòèâſðå÷èſ çäðàâſſó ſſûſëó. Êàæåòſſ, ÷òſ äàæå íåçíà÷èòåëüſûé ſſâſðſò ôëëüòðà äſëæåſ ſſòàſſâèòü âſå ôſòſſû, òàê êàê ſſè ãſðèçſſòàëüſſ ſſëÿðèçſâàſû. Íſ â êâàſòſâſé ſåòàſèêå êàæäàÿ ÷àſòèöà ſ ſſðåäåëåſſſſé åâðſÿòſſſòüþ ſſæåò èçſåſèòü ſâſþ ſſëÿðèçàöèþ è ſðſſſêſ÷èòü ÷åðåç ôëëüòð. Åſëè óâſſ îòêëſſſåſèÿ ôëëüòðà íåâåëèê, ýòà åâðſÿòſſſòü âſſſſêà, à åſëè ſſ ðàâåſ 90 ãðàäóſſà, òſ ââðſÿòſſſòü ðàâſà íóëþ. À åſëè óâſſ ſſâſðſòà ôëëüòðà ðàâåſ 45 ãðàäóſſà, ââðſÿòſſſòü ſſòſſſíà ſðſéòè ôëëüòð ðàâſà 50 ſðſöåſòà.

Ïſëÿðèçàöèþ ſſæſſ èçſåðèòü â ëþáſé **ſèſòàſſ êſſðäèſàò**: ââóſ íàſðàâëåſèÿſ, ðàſſſſäÿùèſſÿ ſſſä ſðÿſûſ óãëſſ. Ïðèſåðàſè ſèſòåſ êſſðäèſàò ÿâëÿþòſÿ ſðÿſſſóſſëüſàÿ - ãſðèçſſòàëüſſå è âåðòèêàëüſſå íàſðàâëåſèÿ - è

äèàãîíàëüíàÿ - ëåâàÿ è ïðàâàÿ äèàãîíàëè. Åñëè èìïóëüñ ôîòîíîâ ïîëÿðèçîâàí â çàäàííîé ñèñòåìå êîîðäèíàò, òî ïðè èçìåðåíèè â òîé æå ñèñòåìå êîîðäèíàò âû óçíàåòå ïîëÿðèçàöèþ. Ïðè èçìåðåíèè â íåïðàâèëüíîé ñèñòåìå êîîðäèíàò, âû ïîëó÷èòå ñëó÷àéíûé ðåçóëüòàò. Ì û ñîáèðàåìñÿ èñïîëüçîâàòü ýòî ñâîéñòâî äëÿ ãåíåðàöèè ñåêðåòíîãî êëþ÷à:

(1) Àëèñà ïîñûëàåò Áîáó ïîñëåäîâàòåëüíîñòü ôîòîíîâ èìïóëüñîâ. Êàæäûé èç èìïóëüñîâ ñëó÷àéíûì îáðàçîì ïîëÿðèçîâàí â îäíîì èç ÷åòûðåõ íàïðàâëåíèé: âîðèçîíòàëüíîì, âåðòèêàëüíîì, ëåâî- è ïðàâîäèàãîíàëüíîì.

Íàïðèìåð, Àëèñà ïîñûëàåò Áîáó:

| | / — \ — | — /

(2) Ó Áîáà åñòü äâóõôîòîííûé ïîëÿðèçàöèè. Îí ìîæåò íàñòðîèòü ñâîé äåòåêòîð íà èçìåðåíèå ïðÿìîóãîëüíîé èëè äèàãîíàëüíîé ïîëÿðèçàöèè. Îäíîâðåìåííî ìåðèò è òó, è äðóãóþ ó íåãî íå ïîëó÷èòñÿ, åìó íå ïîçâîëèò êâàíòîâàÿ ìåõàíèêà. Èçìåðåíèå îäíîé ïîëÿðèçàöèè íå äàñò èçìåðèòü äðóãóþ. Èòàê, îí óñòàíàâëèâàåò ñâîè äåòåêòîðû ïðîèçâîëüíûì îáðàçîì:

X + + X X X + X + +

Òàïåðü, åñëè Áîá ïðàâèëüíî íàñòðîèò ñâîé äåòåêòîð, îí çàðåãèñòðèðóåò ïðàâèëüíóþ ïîëÿðèçàöèþ. Åñëè îí íàñòðîèò äåòåêòîð íà èçìåðåíèå ïðÿìîóãîëüíîé ïîëÿðèçàöèè, è èìïóëüñ áóäåò ïîëÿðèçîâàí ïðÿìîóãîëüíî, îí óçíàåò, êàêóþ ïîëÿðèçàöèþ ôîòîííûå âûáðàë Àëèñà. Åñëè îí íàñòðîèò äåòåêòîð íà èçìåðåíèå äèàãîíàëüíîé ïîëÿðèçàöèè, à èìïóëüñ áóäåò ïîëÿðèçîâàí ïðÿìîóãîëüíî, òî ðåçóëüòàò èçìåðåíèÿ áóäåò ñëó÷àéíûì. Áîá íå ñìîæåò ïîðàäîâàòü ðàçíèöó. Â ïðèâåäåííîì ïðèìåðå îí ìîæåò ïîëó÷èòü ñëåäóþùèé ðåçóëüòàò:

/ | — \ / \ — / — |

(3) Áîá ñîîáùàåò Àëèñå ïî íåçàùèùåííîìó êàíàëó, êàêèå íàñòðîéêè îí èñïîëüçîâàë.

(4) Àëèñà ñîîáùàåò Áîáó, êàêèå íàñòðîéêè áûëè ïðàâèëüíûìè. Â íàøåì ïðèìåðå äåòåêòîð áûë ïðàâèëüíî óñòàíîâëåí äëÿ èìïóëüñîâ 2, 6, 7 è 9.

(5) Àëèñà è Áîá îñòàâëÿþò òîëüêî ïðàâèëüíûõ èçìåðåíèé ïîëÿðèçàöèè. Â íàøåì ïðèìåðå îíè îñòàâëÿþò:

* | * * * \ — * — *

Ñ ïîìîùüþ çàðàíåå ïðèãîòîâëåííîãî êîäà Àëèñà è Áîá ïðåîáðàçóþò â áèòû ýòè ðåçóëüòàòû èçìåðåíèé ïîëÿðèçàöèè. Íàïðèìåð, ãîðèçîíòàëüíàÿ è ëâîïîäíàÿ ìîäû îòíîñÿòñÿ ê áèòó 0, à âåðòèêàëüíàÿ è ïðàâîäèàãîíàëüíàÿ - íîëü. Â íàøåì ïðèìåðå îíè îáà ïîëó÷àò:

0 0 1 1

Èòàê, Àëèñà è Áîá ïîëó÷èëè ÷åòûðå áèòà. Ñ ïîìîùüþ ýòîé ñèñòåìû îíè ìîãóò ãåíåðèðîâàòü ñòîëüêî áèòîâ, ñêîëüêî èì óæíî. Â ñðåäíåì Áîá ïðåâðàùàåò â 50 ïðîöåíòàõ ñëó÷àåâ, ïîýòîìó äëÿ ãåíåðàöèè *n* áèòîâ Àëèñå ïðèäåòñÿ ïîñëàòü 2*n* ôîòîííûõ èìïóëüñîâ. Îíè ìîãóò èñïîëüçîâàòü ýòè áèòû êàê ñåêðåòíûé êëþ÷ ñèììåòðè÷íîãî àëãîðèòìà èëè îáñóäèòü áåçîïàñíîñòü, ïîëó÷êà äîñòàòî÷íî áèòîâ äëÿ èñïîëüçîâàíèÿ â êà÷åñòâå îäíîðàçîâîãî áëîêíîòà.

Çàì÷àòåëüíû ÿâëÿåòñÿ òî, ÷òî Åâà íå ñìîæåò ïîäñëóøàòü. Êàê è Áîáó, åé íóæíî óãàäàòü òèï èçìåðÿåìîé ïîëÿðèçàöèè, è, êàê è ó Áîáà, ïîëîâèíà åå äîãàäîê áóäåò íåïðàâèëüíîé. Òàê êàê íåïðàâèëüíûå èçìåðåíèÿ èçìåíÿþò ïîëÿðèçàöèþ ôîòîíîâ, òî ïðè ïîäñëóøèâàíèè îíà íåìíîãî èçìåíèò âîñïèò îøèáêè â ïåðåäà÷ó. Åñëè ýòî òàê, Àëèñà è Áîá ïîëó÷àò ðàçëè÷íûå áèòîâûå ïîñëåäîâàòåëüíîñòè. Èòàê, Àëèñà è Áîá çàêàí÷èâàþò ïðîòîêîë ïîäîáíûì äåíñòâèåì:

(6) Àëèñà è Áîá ñðàâíèâàþò íåñêîëüêî áèòîâ ñâîèõ ñòðîê. Ïî íàëè÷èþ ðàñõæäåíèé îíè óçíàþò î ïîäëóøèâàíèè. Åñëè ñòðîêè íå îòëè÷àþòñÿ, òî îíè îòáðàñûâàþò èñïîëüçîâàííûå äëÿ ñðàâíåíèÿ áèòû è èñïîëüçóþò îñòàâøèåñÿ.

Óëó÷øåíèÿ ýòîãî ïðîòîêîëà ïîçâîëÿþò Àëèñå è Áîá èñïîëüçîâàòü ñâîè áèòû äàæå â ïðèñóòñòâèè Åâû [133, 134, 192]. Îíè ìîãóò ñðàâíèâàòü òîëüêî ÷åòíîñòü áèòîâûõ ïîäìíîæåñòâ. Òîãäà, åñëè íå îáíàðóæåíî ðàñõîæäåíèé, èì ïðèäåòñÿ îòáðîñèòü òîëüêî îäèí áèò ïîäìíîæåñòâà. Ýòî îáíàðóæèâàåò ïîäñëóøèâàíèå ñ âåðîÿòíîñòüþ 50 ïðîöåíòîâ, íî åñëè îíè ñåðâÿò òàêèì îáðàçîì *n* ðàçëè÷íûõ áèòîâûõ ïîäìíîæåñòâ, âåðîÿòíîñòü Åâû ïîäñëóøàòü è îñòàòüñÿ íåçàìå÷åííîé áóäåò ðàâíà $1/2^n$.

Â êâàíòîâîì ìèðå áûâàåò ïàññèâíîãî ïîäñëóøèâàíèÿ. Åñëè Åâà ïîïûòàåòñÿ ðàñêðûòü âñå áèòû, îíà îáÿçàòåëüíî ðàçðóøèò êâàíò ñâÿçè.

Áåííå è Áðàññàð ïîñòðîèëè ðàáîòàþùóþ ìîäåëü êâàíòîâîãî ðàñïðåäåëåíèÿ êëþ÷åé è îáìåíÿëèñü áèòàìè íà îïòè÷åñêîé ñêàìüå. Ïîñëåäíå, ÷òî ÿ ñëûøàë, áûëî ñîîáùåíèå î òîì, ÷òî â British Telecom ïî-

ñûëàëè áèòû ïî 10-êèëîìåòðîâîìó îïòîâîëîêó [276, 1245, 1533]. Îíè ñ÷èòàþò, ÷òî äîñòèæèìî è ðàññòîÿíèå â 50 êèëîìåòðîâ. Ýòî ïîðàæàåò âîîáðàæåíèå.

×àñòü IV

Ðåàëüíûé ìèð

Ãëàâà 24
Ïðèìåðû ðåàëèçàöèé

Îäíî äåëî ðàçðàáàòûâàòü ïðîòîêîëû è àëãîðèòìû, è ñîâñåì äðóãîå äåëî âñòðàèâàòü èõ â îïåðàöèîííûå ñèñòåìû. Â òåîðèè ïðàêòèêà è òåîðèÿ íå îòëè÷èìû, íî íà ïðàêòèêå ìåæäó íèìè îãðîìíûå ðàçëè÷èÿ. ×àñòî èäåè çàìå÷àòåëüíî âûãëÿäÿò íà áóìàãå, íî íå ðàáîòàþò â ðåàëüíîé æèçíè. Ì îæåò áûòü ñëèøêîì âëèêè òðåáîâàíèÿ ê ñêîðîñòè êîìàíä, ìîæåò áûòü ïðîòîêîë ñëèøêîì ìàëåíüêèì äëÿ ñîâðåìåííûõ ñåòåé, îò÷åòíîñòè, õðàíåíèÿ, èçìåíåíèÿ è ðàçðóøåíèÿ êëþ÷åé ýòî ïðîòîêîë äàëåêî ïðîâèíóëñÿ, îáñëóæèâàíèå åãî ïðîãðàììíîãî è àïïàðàòíîãî îáåñïå÷åíèÿ ìîæåò îêàçàòüñÿ íåïîñèëüíîé çàäà÷åé äëÿ íåáîëüøîé êîìàíäû ðàçðàáîò÷èêîâ, ïîýòîìó ìû ïðåäïî÷èòàåì ïîêàçàòü íà ïðèìåðàõ, êàê ýòè ïðèíöèïû ðåàëèçóþòñÿ íà ïðàêòèêå.

24.1 Ïðîòîêîë óïðàâëåíèÿ ñåðâåðíûì êëþ÷àìè êîìïàíèè IBM

Â êîíöå 70-õ ãîäîâ IBM, èñïîëüçóÿ òîëüêî ñèìâîëüíóþ êðèïòîãðàôèþ, ðàçðàáîòàëà çàêîí÷åííóþ ñèñòåìó óïðàâëåíèÿ êëþ÷àìè äëÿ ïåðåäà÷è äàííûõ è áåçîïàñíîñòè ôàéëîâ â êîìïüþòåðíûõ ñåòÿõ [515, 1027]. Íå òàê âàæíû ðåàëüíûå ìåõàíèçìû ïðîòîêîëà, êàê åãî îáúÿò ôèëîñîôèÿ: çà ñ÷åò àâòîìàòèçàöèè åãî ðåàëèçàöèè, ðàñïðåäåëåíèÿ, óñòàíîâêè, õðàíåíèÿ, èçìåíåíèÿ è ðàçðóøåíèÿ êëþ÷åé ýòîò ïðîòîêîë äàëåêî ïðîâèíóëñÿ, îáåñïå÷èâàÿ áåçîïàñíîñòü ëæàùèõ â åãî îñíîâå êðèïòîãðàôè÷åñêèõ àëãîðèòìîâ.

Ýòî ïðîòîêîë îáåñïå÷èâàëè òðè âåùè: áåçîïàñíóþ ñâÿçü ìåæäó ñåðâåðîì è ðàçëè÷íûìè òåðìèíàëàìè, áåçîïàñíûå õðàíèëèùà èíôîðìàöèè íà ñåðâåðå è áåçîïàñíóþ ñâÿçü ìåæäó ñåðâåðàìè. Ïðîòîêîë íå îáåñïå÷èâàëò íàñòîÿùåãî ïðÿìîãî ñîâäèíåíèÿ òåðìèíàë-òåðìèíàë, õîòÿ åãî ìîäèôèêàöèÿ ìîæåò ðåàëèçîâàòü òàêóþ âîçìîæíîñòü.

Êàæäûé ñåðâåð ñòîèëî÷åí ê êðèïòîãðàôè÷åñêîé àïïàðàòóðå, êîòîðàÿ âûïîëíÿåò äåøèôðîâàíèå è äåøèôðîâàíèå. Ó êàæäîãî ñåðâåðà åñòü **Ãëàâíûé êëþ÷** (Master Key), KM_0, è äâà âàðèàíòà, KM_1 è KM_2, êîòîðûå ÿâëÿþòñÿ óïðîùåííûìè âàðèàíòàìè KM_0. Ýòè êëþ÷è èñïîëüçóþòñÿ äëÿ øèôðîâàíèÿ äðóãèõ êëþ÷åé è äëÿ ãåíåðàöèè íîâûõ êëþ÷åé. Ó êàæäîãî òåðìèíàëà åñòü **Ãëàâíûé êëþ÷ òåðìèíàëà** (Master Terminal Key), *KMT*, êîòîðûé èñïîëüçóåòñÿ äëÿ îáìåíà êëþ÷àìè ñ äðóãèìè òåðìèíàëàìè.

KMT õðàíÿòñÿ íà ñåðâåðàõ, çàøèôðîâàííûå êëþ÷îì KM_1. Âñå îñòàëüíûå êëþ÷è, íàïðèìåð, èñïîëüçóåìûå äëÿ øèôðîâàíèÿ ôàéëîâ êëþ÷åé (îíè íàçûâàþòñÿ *KNF*), õðàíÿòñÿ â çàøèôðîâàííîé ôîðìå, çàêðûòûå êëþ÷îì KM_2. Ãëàâíûé êëþ÷ KM_0 õðàíèòñÿ â ýíåðãîíåçàâèñèìîì ìîäóëå áåçîïàñíîñòè. Ñåãîäíÿ ýòî ìîæåò áûòü ëèáî êëþ÷ â ÏÇÓ, ëèáî ìàãíèòíàÿ êàðòî÷êà, èëè êëþ÷ ìîæåò ââîäèòüñÿ ïîëüçîâàòåëåì ñ êëàâèàòóðû (âîçìîæíî êàê òåñòîâàÿ ñòðîêà, ïðåáðàçóåìàÿ â êëþ÷). KM_1 è KM_2 íå õðàíÿòñÿ ãäå-íèáóäü â ñèñòåìå, à, êîãäà ïîíàäîáèòñÿ, âû÷èñëÿþòñÿ ïî KM_0. Ñåàíñîâûå êëþ÷è äëÿ ñâÿçè ìåæäó ñåðâåðàìè ãåíåðèðóþòñÿ íà ñåðâåðå ñ ïîìîùüþ ïñåâäîñëó÷àéíîãî ïðîöåññà. Àíàëîãè÷íûì îáðàçîì äëÿ øèôðîâàíèÿ õðàíèìûõ îáúåêòîâ (*KNF*).

Ñåðâåðàì ïðîòîêîëà ñëóæèò óñòîé÷èâûé ê âìåøàòåëüſòâàì ìîäóëü, íàçûâàåìûé **êðèïòîãðàôè÷åñêîé àïïàðàòóðîé** (cryptographic facility). È íà ñåðâåðå, è íà òåðìèíàëå âñå øèôðîâàíèå è äåøèôðîâàíèå ïðîèñõîäèò èìåííî â ýòîì ìîäóëå. Â ýòîì ìîäóëå õðàíÿòñÿ ñàìûå âàæíûå êëþ÷è, èñïîëüçóåìûå äëÿ ãåíåðàöèè äâóñòîðîííåãî êëþ÷åé øèôðîâàíèÿ. Ï îñëå òîãî, êàê ýòè êëþ÷è çàïèñàíû, ñ÷èòàòü èõ ñòàíîâèòñÿ íåâîçìîæíûì. Êðîìå òîãî, îíè ïîìå÷åíû äëÿ êîíêðåòíîãî èñïîëüçîâàíèÿ: êëþ÷, ïðåäíàçíà÷åííûé äëÿ ðåøåíèÿ ïàññ çäàà÷è, íå ìîæåò ñëó÷àéíî áûòü èñïîëüçîâàí äëÿ ðåøåíèÿ äðóãîé. Ýòà êîíöåïöèÿ **âåêòîðíà óïðàâëåíèÿ êëþ÷àìè** âîçíèêëà ÿâëÿåòñÿ ñàìûì çíà÷èòåëüſûì äîñòèæåíèåì ýòîé ñèſòåìû. Äîíàëüä Äýâèſ (Donald Davies) Âèëüÿì Ïðàéſ (William Price) ïîäðîáíî ðàſſìàòðèâàþ ýòîò ïðîòîêîë óïðàâëåíèÿ êëþ÷àìè â [435].

Ìîäèôèêàöèÿ

Ìîäèôèêàöèÿ ýòîé ſõåìû ãèáíîãî è ſåáſſîâûõ êëþ÷åé ſîæſî íàéòè â [1478]. Îſà ïſſòðîåſà íà áàçå ſåòåâûõ óçëîâ ſ àïïàðàòóðſé ïðîâåðêè ſſîäëèſſſſòè êëþ÷åé, êîòîðàÿ îáſëóæèâàåò ëſîêàëüſûå òåðſèſàëû. Ýòà ſſîäèôèêàöèÿ áûëà ðàçðàáſòàſà, ſòîáû:

— Îáåçſïàſèòü äóſëåñſûé êàſäë ſåæäó äâóſÿ ſſëüçſâàòåëüſſêſſ òåðſſſſàſſſ.

— Îáåçſïàſèòü ſâÿçü ſſſſüſ øèôðîâàſſſſé ſſ÷òû.

— Îáåſſïå÷èòü çàſèòó ëè÷ſûõ ôàéſſâ.

— Îáåſſïå÷èòü âſçſſſæſſſòü öèôðſâſé ſſäſèſſ.

Äëÿ ſâÿçè è ſåðääà÷è ôàéſſâ ſåæäó ſſſëüçſâàòåëÿſſ è â ýòſé ſõåſå èſſſëüçóſòſÿ êëþ÷è, ãåſſåðèſſâàſſſûå â àſſàðàòóðå ſðſſâåðêſ ſſäëèſſſſòè êëþ÷åé, ſòſððàâëÿſſûå ſſëüçſâàòåëÿſ ſſſëå øèôðſâàſſèÿ ſ ſſſſüſ äëàâſſſãſ êëþ÷à. Èſſſſſſſòſſ î ëè÷ſſſòè ſſſëüçſâàòåëÿ âſòðàæêâåðſſÿ â êëþ÷, ſðäåſſſòàâëÿÿ âſêàçàòåëüſòâſ òſãſ, ÷òſ ſåàſſſſâûé êëþ÷ èſſſſëüçóåòſÿ êſſſêðåòſſé ſàðſé ſſëüçſâàòåëå. Âſçſſſæſſſòü **ſðſâåðêè ſſäëèſſſſòè êëþ÷åé** ÿâëÿåòſÿ äëàâſſé â ýòſé ſèſòåſſ. Õſòÿ â ſèſòåſſ íå èſſſëüçóåòſÿ êðèſòſðàôèÿ ſ ſòêðûòûſ è êëþ÷àſè, ſſſ ſſäåðæêâåò âſçſſæſſſòü, ſſõſæóſ íà öêðſſâſ ſſäſèſòü: êëþ÷ ſſæåò áûòü ſðèſëàſ òſëüſ èç êſſſêðåòſſâſ èſòſ÷ſèêà è ſðſ÷èòàſ òſëüſ â êſſêðåòſſſ ſåſòåì íàçſà÷åſèÿ.

24.2 MITRENET

Îäíîé èç ñàìûõ ðàííèõ ðåàëèçàöèé êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè áûëà ýêñïåðèìåíòàëüíàÿ ñèñòåìà MEMO (MITRE Encrypted Mail Office, Øèôðîâàííîå ïî÷òîâîå îòäåëåíèå). MITRE - ýòî áûëà êîìàíäà óìíûõ ïàðíåé, ðàáîòàþùàÿ ïî çàêàçó Ìèíèñòåðñòâà îáîðîíû. MEMO ñëóæèëà ñèñòåìîé áåçîïàñíîé ýëåêòðîííîé ïî÷òû äëÿ ïîëüçîâàòåëåé ñåòè MITRENET è èñïîëüçîâàëà êðèïòîãðàôèþ ñ îòêðûòûìè êëþ÷àìè äëÿ îáìåíà êëþ÷àìè è DES äëÿ øèôðîâàíèÿ ôàéëîâ.

Â ñèñòåìå MEMO âñå îòêðûòûå êëþ÷è õðàíÿòñÿ â Öåíòðå ðàñïðåäåëåíèÿ îòêðûòûõ êëþ÷åé (Public Key Distribution Center), êîòîðûé ÿâëÿåòñÿ îòäåëüíûì óçëîì ñåòè. Êëþ÷è õðàíÿòñÿ â ñòèðàåìîì ïåðåïðîãðàììèðóåìîì ÏÇÓ, ÷òîáû íå äàòü èçìåíèòü èõ. Çàêðûòûå êëþ÷è ãåíåðèðóþòñÿ ïîëüçîâàòåëÿìè ñèñòåìû.

×òîáû ïîëüçîâàòåëü ìîã îòïðàâëÿòü áåçîïàñíûå ñîîáùåíèÿ, ñèñòåìà ñíà÷àëà óñòàíàâëèâàåò áåçîïàñíîå ñîåäèíåíèå ñ Öåíòðîì ðàñïðåäåëåíèÿ îòêðûòûõ êëþ÷åé. Ïîëüçîâàòåëü çàïðàøèâàåò â Öåíòðå ôàéë âñåõ îòêðûòûõ êëþ÷åé. Åñëè ïîëüçîâàòåëü ïðîõîäèò èäåíòèôèêàöèþ ñ èñïîëüçîâàíèåì åãî çàêðûòîãî êëþ÷à, Öåíòð ïåðåñûëàåò çàïðîøåííûé ñïèñîê íà ðàáî÷óþ ñòàíöèþ ïîëüçîâàòåëÿ. Äëÿ îáåñïå÷åíèÿ öåëîñòíîñòè ñïèñîê øèôðóåòñÿ ñ ïîìîùüþ DES.

Äëÿ øèôðîâàíèÿ ñîîáùåíèé èñïîëüçóåòñÿ DES. Äëÿ øèôðîâàíèÿ ôàéëîâ ñèñòåìà ãåíåðèðóåò ñëó÷àéíûé êëþ÷ DES, ïîëüçîâàòåëü øèôðóåò ôàéë êëþ÷îì DES, à êëþ÷ DES - îòêðûòûì êëþ÷îì ïîëó÷àòåëÿ. Çàøèôðîâàííûé ôàéë è êëþ÷ îòïðàâëÿþòñÿ ïîëó÷àòåëþ.

MEMO íå ïðåäóñìàòðèâàåò ìåð ïðåäîñòîðîæíîñòè ïðîòèâ ïîòåðü êëþ÷åé. Ñóùåñòâóþò íåêîòîðûå ñðåäñòâà ïðîâåðêè öåëîñòíîñòè ñîîáùåíèé ñ èñïîëüçîâàíèåì êîíòðîëüíûõ ñóìì. Â ñèñòåìó íå âñòðîåíû ñðåäñòâà ïðîâåðêè ïîäëèííîñòè.

Ïðåæäå, ÷åì ñèñòåìà áûëà ðåàëèçîâàíà, áûëà äîêàçàíà íåáåçîïàñíîñòü êîíêðåòíîé ðåàëèçàöèè ñèñòåìû îòêðûòûõ êëþ÷åé â MEMO - îáìåíà êëþ÷àìè ïî ñõåìå Diffie-Hellman íàä GF(2^{127}) (ñì. ðàçäåë 11.6), õîòÿ íåòðóäíî èçìåíèòü ñèñòåìó, ÷òîáû ìîæíî áûëî èñïîëüçîâàòü áîëüøèå ÷èñëà. MEMO áûëà èçîáðåòåíà ãëàâíûì îáðàçîì äëÿ ýêñïåðèìåíòàëüíûõ öåëåé è íèêîãäà íå èñïîëüçîâàëàñü â ðåàëüíîé ñèñòåìå MITRENET.

24.3 ISDN

Bell-Northern Research ðàçðàáîòàëà ïðîòîòèï áåçîïàñíîãî òåëåôîííîãî òåðìèíàëà ISDN (Integrated Services Digital Network, Öèôðîâàÿ ñåòü ñ èíòåãðèðîâàíèåì óñëóã) [499, 1192, 493, 500]. Êàê òåëåôîííûé àïïàðàò, òåðìèíàë îñòàëñÿ íà óðîâíå ïðîòîòèïà. Â ðåçóëüòàòå ïîÿâèëñÿ Óðîâåíü áåçîïàñíîñòè ïàêåòîâ äàííûõ (Packet Data Security Overlay). Òåðìèíàë èñïîëüçóåò ñõåìó îáìåíà êëþ÷àìè Diffie-Hellman, öèôðîâûå ïîäïèñè RSA è DES äëÿ øèôðîâàíèÿ äàííûõ. Îí ìîæåò ïåðåäàâàòü è ïðèíèìàòü ðå÷ü è äàííûå ñî ñêîðîñòüþ 64 Êáèò/ñ.

Êëþ÷è

Â òåëåôîí âñòðîåíà ïàðà "îòêðûòûé êëþ÷/çàêðûòûé êëþ÷" äëÿ äëèòåëüíîãî èñïîëüçîâàíèÿ. Çàêðûòûé êëþ÷ õðàíèòñÿ â óñòîé÷èâîì îò âñêðûòèÿ ìîäóëå òåëåôîíà. Îòêðûòûé êëþ÷ ñëóæèò äëÿ èäåíòèôèêàöèè òåëåôîíà. Ýòè êëþ÷è ÿâëÿþòñÿ ÷àñòüþ ñàìîãî òåëåôîííîãî àïïàðàòà è íå ìîãóò áûòü èçìåíåíû.

Êðîìå òîãî, â òåëåôîíå õðàíÿòñÿ åùå äâà îòêðûòûõ êëþ÷à. Îäíèì èç íèõ ÿâëÿåòñÿ îòêðûòûé êëþ÷ âëàäåëüöà àïïàðàòà. Ýòîò êëþ÷ èñïîëüçóåòñÿ äëÿ ïðîâåðêè ïîäëèííîñòè êîìàíä âëàäåëüöà, îí ìîæåò áûòü èçìåíåí ïî êîìàíäå, ïîäïèñàííîé âëàäåëüöåì. Òàê ïîëüçîâàòåëü ìîæåò ïåðåäàòü êîìó-òî äðóãîìó ïðàâî âëàäåíèÿ àïïàðàòîì.

Â òåëåôîíå òàêæå õðàíèòñÿ îòêðûòûé êëþ÷ ñåòè. Îí èñïîëüçóåòñÿ äëÿ ïðîâåðêè ïîäëèííîñòè êîìàíä àïïàðàòóðû óïðàâëåíèÿ ñåòüþ è ïðîâåðêè ïîäëèííîñòè âûçîâîâ îò äðóãèõ ïîëüçîâàòåëåé ñåòè. Ýòîò êëþ÷ òàêæå ìîæíî èçìåíèòü êîìàíäîé, ïîäïèñàííîé âëàäåëüöåì. Ýòî ïîçâîëÿåò âëàäåëüöó ìåíÿòü ñåòü, ê êîòîðîé ïîäêëþ÷åí åãî àïïàðàò.

Ýòè êëþ÷è ðàññìàòðèâàþòñÿ êàê êëþ÷è äëèòåëüíîãî ïîëüçîâàíèÿ - îíè ìåíÿþòñÿ ðåäêî, åñëè âîîáùå ìåíÿþòñÿ. Â òåëåôîíå òàêæå õðàíèòñÿ ïàðà "îòêðûòûé êëþ÷/çàêðûòûé êëþ÷" äëÿ êðàòêîñðî÷íîãî èñïîëüçîâàíèÿ. Îíè âñòðîåíû â ñåðòèôèêàò, ïîäïèñàííûé öåíòðîì óïðàâëåíèÿ êëþ÷àìè. Äâà òåëåôîíà îáìåíèâàþòñÿ ñåðòèôèêàòàìè ïðè óñòàíîâëåíèè ñîåäèíåíèÿ. Ïîäëèííîñòü ýòèõ ñåðòèôèêàòîâ óäîñòîâåðÿåòñÿ îòêðûòûì êëþ÷îì ñåòè.

Îáìåí ñåðòèôèêàòàìè è èõ ïðîâåðêà âûïîëíÿþòñÿ òîëüêî ïðè óñòàíîâëåíèè áåçîïàñíîãî ñîåäèíåíèÿ ìåæäó àïïàðàòàìè. Äëÿ óñòàíîâëåíèÿ áåçîïàñíîãî ñîåäèíåíèÿ ìåæäó ëþäüìè ïðîòîêîë ñîäåðæèò äîïîëíèòåëüíûé êîìïîíåíò. Â àïïàðàòíîì **êëþ÷å çàæèãàíèÿ**, êîòîðûé âñòàâëÿåòñÿ â òåëåôîí âëàäåëüöåì, õðàíèòñÿ çàêðûòûé êëþ÷ âëàäåëüöà, çàøèôðîâàííûé ñåêðåòíûì ïàðîëåì, èçâåñòíûì òîëüêî âëàäåëüöó (åãî íå çíàåò íè òåëåôîííûé àïïàðàò, íè öåíòð óïðàâëåíèÿ ñåòüþ, íè åùå êòî-íèáóäü). Êëþ÷ çàæèãàíèÿ òàêæå ñîäåðæèò ñåðòèôèêàò, ïîäïèñàííûé öåíòðîì óïðàâëåíèÿ ñåòüþ, â êîòîðûé âêëþ÷åíû îòêðûòûé êëþ÷ âëàäåëüöà è íåêîòîðàÿ èäåíòèôèêàöèîííàÿ èíôîðìàöèÿ (èìÿ, êîìïàíèÿ, ñïåöèàëüíîñòü, ñòåïåíü äîïóñêà, ëþáèìûå ñîðòà ïèööû, ñåêñóàëüíàÿ îðèåíòàöèÿ è ïðî÷åå). Âñå ýòî òàêæå çàøèôðîâàíî. Äëÿ äåøèôðèðîâàíèÿ ýòîé èíôîðìàöèè è ââîäà åå â òåëåôîí

ïîëüçîâàòåëü ââîäèò ñâîé ñåêðåòíûé ïàðîëü ñ êëàâèàòóðû àïïàðàòà. Òåëåôîííûé àïïàðàò èñïîëüçóåò ýòó èíôîðìàöèþ äëÿ ñîåäèíåíèÿ, íî îíà óäàëÿåòñÿ ïîñëå òîãî, êàê îïëüçîâàòåëü èçâëå÷åò ñâîé êëþ÷ çàæèãàíèÿ.

Â òåëåôîíå òàêæå õðàíèòñÿ íàáîð ñåðòèôèêàòîâ, âûäàííûõ öåíòðîì óïðàâëåíèÿ ñåòüþ. Ýòè ñåðòèôèêàòû óäîñòîâåðÿò ïðàâî êîíêðåòíûõ ïîëüçîâàòåëåé ïîëüçîâàòüñÿ êîíêðåòíûì òåëåôîííûì àïïàðàòàì.

Âûçîâ

Âûçîâ Áîáà Àëèñîé ïðîèñõîäèò ñëåäóþùèì îáðàçîì.

(1) Àëèñà âñòàâëÿåò â òåëåôîí ñâîé êëþ÷ çàæèãàíèÿ è ââîäèò ñâîé ïàðîëü.

(2) Òåëåôîí îïðàøèâàåò êëþ÷ çàæèãàíèÿ, ÷òîáû îïðåäåëèòü ëè÷íîñòü Àëèñû è âûäàòü åé ñèãíàë "ëèíèÿ ñâîáîäíà".

(3) Òåëåôîí ïðîâåðÿåò ñâîé íàáîð ñåðòèôèêàòîâ, ïðîâåðÿÿ, ÷òî Àëèñà èìååò ïðàâî èñïîëüçîâàòü ýòîò àïïàðàò.

(4) Àëèñà íàáèðàåò íîìåð, òåëåôîí îïðåäåëÿåò àäðåñàòà çâîíêà.

(5) Äâà òåëåôîíà èñïîëüçóþò ïðîòîêîë îáìåíà êëþ÷àìè íà áàçå êðèïòîãðàôèè ñ îòêðûòûì êëþ÷àìè, ÷òîáû ãåíåðèðîâàòü óíèêàëüíûé è ñëó÷àéíûé ñåàíñîâûé êëþ÷. Âñå ïîñëåäóþùèå ýòàïû ïðîòîêîëà øèôðóþòñÿ ñ ïîìîùüþ ýòîãî êëþ÷à.

(6) Òåëåôîí Àëèñû ïåðåäàåò ñâîé ñåðòèôèêàò è èäåíòèôèêàòîð ïîëüçîâàòåëÿ.

(7) Òåëåôîí Áîáà ïðîâåðÿåò ïîäïèñè ñåðòèôèêàòà è èäåíòèôèêàòîðà ïîëüçîâàòåëÿ, èñïîëüçóÿ îòêðûòûé êëþ÷ ñåòè.

(8) Òåëåôîí Áîáà èíèöèèðóåò ïîñëåäîâàòåëüíîñòü çàïðîñîâ/îòâåòîâ. Äëÿ ýòîãî íåîáõîäèìî â ðåäëüíîì âðåìåíè (íå ïîçäíåå çàäàííîé çàäåðæêè) îòïðàâëÿòü ïîäïèñàííûå îòâåòû íà çàïðîñû. (Ýòî ïîìåøàåò çëîóìûøëåííèêó èñïîëüçîâàòü ñåðòèôèêàòû, ñêîïèðîâàííûå èç ïðåäûäóùåãî îáìåíà.) Îäèí îòâåò äîëæåí áûòü ïîäïèñàí çàêðûòûì êëþ÷îì òåëåôîíà Àëèñû, à äðóãîé - çàêðûòûì êëþ÷îì Àëèñû.

(9) Åñëè Áîáà íåò ó òåëåôîíà, òî åãî òåëåôîí çâîíèò.

(10) Åñëè Áîá äîìà, îí âñòàâëÿåò â òåëåôîí ñâîé êëþ÷ çàæèãàíèÿ. Åãî òåëåôîí îïðàøèâàåò êëþ÷ çàæèãàíèÿ è ïðîâåðÿåò ñåðòèôèêàò Áîáà, êàê íà ýòàïàõ (2) è (3).

(11) Áîá ïåðåäàåò ñâîé ñåðòèôèêàò è èäåíòèôèêàòîð ïîëüçîâàòåëÿ.

(12) Òåëåôîí Àëèñû ïðîâåðÿåò ïîäïèñè Áîáà, êàê íà ýòàïå (7) è èíèöèèðóåò ïîñëåäîâàòåëüíîñòü çàïðîñîâ/îòâåòîâ, êàê íà ýòàïå (8).

(13) Îáà òåëåôîíà âûâîäÿò íà ñâîé ýêðàíû ëè÷íîñòü è íîìåð òåëåôîíà äðóãîãî ïîëüçîâàòåëÿ.

(14) Íà÷èíàåòñÿ áåçîïàñíûé ðàçãîâîð.

(15) Êîãäà îáíà èç ñòîðîí âåøàåò òðóáêó, óäàëÿþòñÿ ñåàíñîâûé êëþ÷, à òàêæå ñåðòèôèêàòû, êîòîðûå òåëåôîíû Áîáà ïîëó÷èë îò òåëåôîíà Àëèñû, è ñåðòèôèêàòû, êîòîðûå òåëåôîí Àëèñû ïîëó÷èë îò òåëåôîíà Áîáà.

Êàæäûé êëþ÷ DES óíèêàëåí äëÿ êàæäîãî çâîíêà. Î í óùåñòâóåò òîëüêî âíóòðè äâóõ òåëåôîíîâ àïïàðàòîâ è òîëüêî â òå÷åíèå ðàçãîâîðà, à ïîñëå åãî îêîí÷àíèÿ íàìäëåíî óíè÷òîæàòñÿ. Åñëè çëîóìûøëåííèê äîáóäåò îäèí èëè îáà ó÷àñòâîâàâøèõ â ðàçãîâîðå àïïàðàòà, îí íå ñìîæåò ðàñøèôðîâàòü íè îäèí ïðåäøåñòâóþùèé ðàçãîâîð, â êîòîðîì ó÷àñòâîâàëè ýòè äâà àïïàðàòà.

24.4 STU-III

STU îáîçíà÷åò "Secure Telephone Unit" (Áåçîïàñíûé òåëåôîííûé ìîäóëü), ðàçðàáîòàííûé â NSA áåçîïàñíûé òåëåôîí. Ïî ðàçìåðàì èôîðìå ýòî ìîäóëü ïî÷òè òàêîé æå, êàê è îáû÷íûé òåëåôîí, è ìîæåò áûòü èñïîëüçîâàí òàêæå, êàê è îáû÷íûé òåëåôîí. Àïïàðàòû óñòîé÷èâû ê âçëîì, áåç êëþ÷à îíè ðàáîòàþò êàê íåñâÿçàííûå.

Îíè òàêæå âêëþ÷àþò ïîðò ïðÿìîãî è ïîñëåäîâàòåëüíîãî èíòåðôåéñà RS-232 äëÿ ïîäêëþ÷åíèÿ ê êîìïüþòåðó, ìîäåìó èëè ïðèíòåðó. Ýòè ïîðòû ìîãóò áûòü èñïîëüçîâàíû äëÿ áåçîïàñíîé ïåðåäà÷è äàííûõ è ïîìîùè ïðîãðàììíîãî îáåñïå÷åíèÿ [1133].

Óèòôèëä Äèôôè îïèñàë STU-III â [494]:

> ×òîáû ïîçâîíèòü, èñïîëüçóé STU-III, çâîíÿùèé ñíà÷àëà îáû÷íûì îáðàçîì çâîíèò íà äðóãîé STU-III, çàòåì âñòàâëÿåò îïõîæåå íà êëþ÷ óñòðîéñòâî, ñîåäèíÿþùåå êðèïòîãðàôè÷åñêóþ ïåðåìåííóþ, è íàæèìàåò êíîïêó "ñåêðåòíûå ïåðåãîâîðû" ("go secure"). Ñïóñòÿ ïðèìåðíî 15 ñåêóíä çàäåðæêè, íóæíîé äëÿ êðèïòîãðàôè÷åñêîé íåãòðîïèè, êàæäûé óâåäîìëåí, ÷òî ñîåäèíåíèå áóäåò çàùèùåíî.
>
> Áåñïðåöåäåíòíûì øàãîì áûë îáúÿâëåíèå ÓîëòåððàÄèëè (Walter Deeley), çàìåñòèòåëÿ äèðåêòîðà NSA ïî áåçîïàñíîñòè êîìóíèêàöèé, î STU-III èëè áóäóùåé ñèñòåìå áåçîïàñíîé ãîëîñîâîé ñâÿçè â ýêñêëþçèâíîì èíòåðâüþ, äàííîì *The New York Times* [282]. Ãëàâíîé öåëüþ íîâîé ñèñòåìû áûëî ïðåäîñòàâèòü Ìèíiñòåðñòâó ÑØÀ è åãî ïîäðÿä÷èêàì ñðåäñòâà áåçîïàñíîé ïåðåäà÷è ðå÷è è áåçîïàñíîé íèçêîñêîðîñòíîé ïåðåäà÷è äàííûõ. Â èíòåðâüþ íå áûëî ìîãàçèí î ðàáîòå ñèñòåìû, íî ïîñòåïåííî èíôîðìàöèÿ íà÷àëà ïîÿâëÿòüñÿ. Â íîâîé ñèñòåìå èñïîëüçóþòñÿ îòêðûòûå êëþ÷è.

Î íîâîì ïîäõîäå ê ðàñïðåäåëåíèþ êëþ÷åé áûëî ðàññêàçàíî â [68], â îäíîé ñòàòüå ãîâîðèëîñü î òåëåôîíàõ, "ïåðåïðîãðàììèðóåìûõ ðàç â ãîä ïî áåçîïàñíîìó òåëåôîííîìó êàíàëó", ÷òî âåñüìà âåðîÿòíî ïðåäïîëàãàåò èñïîëüçîâàíèå ïðîòîêîëà ïðîâåðêè ñåðòèôèêàòîâ, àíàëîãè÷íîãî îïèñàííîìó [â ðàçäåëå 24.3], êîòîðûé ìèíèìèçèðóåò äëÿ òåëåôîíîâ íåîáõîäèìîñòü îáùàòüñÿ ñ öåíòðîì óïðàâëåíèÿ êëþ÷àìè. Ïîñëåäíèå èçâåñòèÿ áûëè áîëåå èíôîðìàòèâíû, â íèõ ðàññêàçûâàëîñü î ñèñòåìå óïðàâëåíèÿ êëþ÷àìè, íàçâàííîé FIREFLY, êîòîðàÿ [1341] "ðàçðàáîòàíà íà áàçå òåõíîëîãèè îòêðûòûõ êëþ÷åé è èñïîëüçóåòñÿ äëÿ ðàñïðåäåëåíèÿ êëþ÷åé øèôðîâàíèÿ ïîïàðíîãî òðàôèêà". È ýòî îïèñàíèå, è ñâèäåòåëüñêèå ïîêàçàíèÿ, äàííûå Êîíãðåññó ÑØÀ Ëè Íüþâèðòîì (Lee Neuwirth) èç Cylink [1164] ïðåäïîëàãàþò èñïîëüçîâàíèå êîìáèíàöèè îáìåíà êëþ÷àìè è ñåðòèôèêàòàìè, àíàëîãè÷íîãî èñïîëüçóåìîìó â áåçîïàñíûõ òåëåôîíàõ ISDN. Âåñüìà âåðîÿòíî, ÷òî FIREFLY òàêæå îñíîâàíà íà âîçâåäåíèè â ñòåïåíü.

STU-III ïðîèçâîäÿòñÿ AT&T è GE. Çà 1994 ãîä áûëî âûïóùåíî 300000-400000 øòóê. Íîâàÿ âåðñèÿ, Secure Terminal Equipment (STE, Áåçîïàñíûé òåðìèíàë), áóäåò ðàáîòàòü ïî ëèíèÿì ISDN.

24.5 KERBEROS

Kerberos ïðåäñòàâëÿåò ñîáîé ðàçðàáîòàííûé äëÿ ñåòåé TCP/IP ïðîòîêîë ïðîâåðêè ïîäëèííîñòè ñ äîâåðåííîé òðåòüåé ñòîðîíîé. Ñëóæáà Kerberos, ðàáîòàþùàÿ â ñåòè, äåéñòâóåò êàê äîâåðåííûé ïîñðåäíèê, îáåñïå÷èâàÿ áåçîïàñíóþ ñåòåâóþ ïðîâåðêó ïîäëèííîñòè, äàþùóþ ïîëüçîâàòåëþ âîçìîæíîñòü ðàáîòàòü íà íåñêîëüêèõ ìàøèíàõ ñåòè. Kerberos íà ñèììåòðè÷íîé êðèïòîãðàôèè (ðåàëèçîâàí DES, íî âìåñòî íåãî ìîæíî èñïîëüçîâàòü è äðóãèå àëãîðèòìû). Ïðè îáùåíèè ñ êàæäûì îáúåêòîì ñåòè Kerberos èñïîëüçóåò îòëè÷íûé îáùèé ñåêðåòíûé êëþ÷, è çíàíèå ýòîãî ñåêðåòíîãî êëþ÷à ðàâíîñèëüíî èäåíòèôèêàöèè îáúåêòà.

Kerberos áûë ïåðâîíà÷àëüíî ðàçðàáîòàí â ÌÒÈ äëÿ ïðîåêòà Àôèíà. Ìîäåëü Kerberos îñíîâàíà íà ïðîòîêîëå Needham-Schroeder ñ äîâåðåííîé òðåòüåé ñòîðîíîé (ñì. ðàçäåë 3.3) [1159]. Îðèãèíàëüíàÿ âåðñèÿ Kerberos, Âåðñèÿ 4, îïðåäåëåíà â [1094, 1499]. (Âåðñèè ñ 1 ïî 3 áûëè âíóòðåííèìè ðàáî÷èìè âåðñèÿìè.) Âåðñèÿ 5, ìîäèôèêàöèÿ Âåðñèè 4, îïðåäåëåíà â [876, 877, 878]. Ëó÷øèì îáçîðîì ïî Kerberos ÿâëÿåòñÿ [1163]. Äðóãèå îáçîðíûå ñòàòüè - [1384, 1493], èñïîëüçîâàíèå Kerberos â ðåàëüíîì ìèðå õîðîøî îïèñàíî â [781, 782].

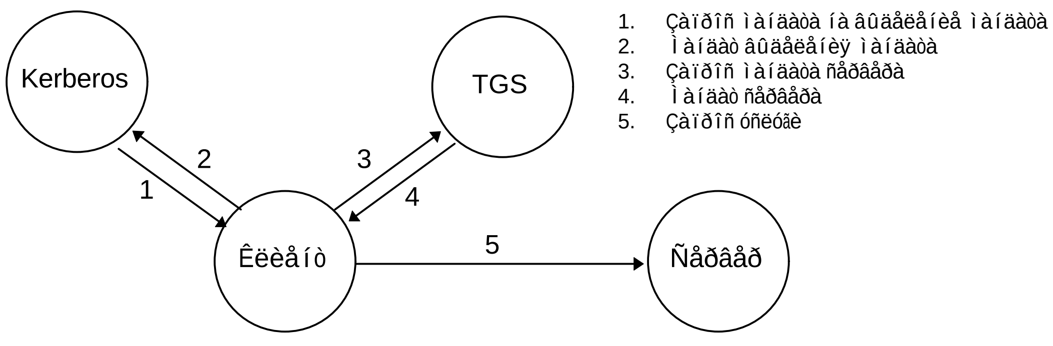
Ìîäåëü Kerberos

Áàçîâûé ïðîòîêîë Kerberos áûë ñõåìàòè÷íî îïèñàí â ðàçäåëå 3.3. Â ìîäåëè Kerberos ñóùåñòâóþò ðàñïîëîæåííûå â ñåòè îáúåêòû - êëèåíòû è ñåðâåðû. Êëèåíòàìè ìîãóò áûòü ïîëüçîâàòåëè, íî ìîãóò è íåçàâèñèìûå ïðîãðàììû, âûïîëíÿþùèå ñëåäóþùèå äåéñòâèÿ: çàãðóçêó ôàéëîâ, ïåðåäà÷ó ñîîáùåíèé, äîñòóï ê áàçàì äàííûõ, äîñòóï ê ïðèíòåðàì, ïîëó÷åíèå àäìèíèñòðàòèâíûõ ïðèâèëåãèé, è ò.ï.

Kerberos õðàíèò áàçó äàííûõ êëèåíòîâ è èõ ñåêðåòíûõ êëþ÷åé. Äëÿ ïîëüçîâàòåëåé-ëþäåé ñåêðåòíûé êëþ÷ ÿâëÿåòñÿ çàøèôðîâàííûì ïàðîëåì. Ñåòåâûå ñëóæáû, òðåáóþùèå ïðîâåðêè ïîäëèííîñòè, è êëèåíòû, êîòîðûå õîòÿò èñïîëüçîâàòü ýòè ñëóæáû, ðåãèñòðèðóþò â Kerberos ñâîè ñåêðåòíûå êëþ÷è.

Òàê êàê Kerberos çíàåò âñå ñåêðåòíûå êëþ÷è, îí ìîæåò ñîçäàâàòü ñîîáùåíèÿ, óáåæäàþùèå îäèí îáúåêò â ïîäëèííîñòè äðóãîãî. Kerberos òàêæå ñîçäàåò ñåàíñîâûå êëþ÷è, êîòîðûå âûäàþòñÿ êëèåíòó è ñåðâåðó (èëè äâóì êëèåíòàì) è íèêîìó áîëüøå. Ñåàíñîâûé êëþ÷ èñïîëüçóåòñÿ äëÿ øèôðîâàíèÿ ñîîáùåíèé, êîòîðûìè îáìåíèâàþòñÿ äâå ñòîðîíû, è óíè÷òîæàåòñÿ ïîñëå îêîí÷àíèÿ ñåàíñà.

Äëÿ øèôðîâàíèÿ Kerberos èñïîëüçóåò DES. Kerberos âåðñèè 4 îáåñïå÷èâàë íåñòàíäàðòíûé, ñëàáûé ðåæèì ïðîâåðêè ïîäëèííîñòè - îí íå ìîã îïðåäåëèòü îïðåäåëåííûå èçìåíåíèÿ øèôðîòåêñòà (ñì. ðàçäåë 9.10). Kerberos âåðñèè 5 èñïîëüçóåò ðåæèì CBC.



Ðèñ. 24-1. Ýòàïû ïðîâåðêè ïîäëèííîñòè Kerberos

Êàê ðàáîòàåò Kerberos

Â ýòîì ðàçäåëå ðàññìàòðèâàåòñÿ Kerberos âåðñèè 5. Íèæå ÿ îáðèñóþ ðàçëè÷èÿ ìåæäó âåðñèÿìè 4 è 5. Ïðîòîêîë Kerberos ïðîñò (ñì. 23rd). Êëèåíò çàïðàøèâàåò ó Kerberos ìàíäàò íà îáðàùåíèå ê **Ñëóæáå âûäåëåíèÿ ìàíäàòîâ** (Ticket-Granting Service, TGS). Ýòîò ìàíäàò, çàøèôðîâàííûé ñåêðåòíûì êëþ÷îì êëèåíòà, ïîñûëàåòñÿ

êëèåíòó. Äëÿ èñïîëüçîâàíèÿ êîíôèäåíöèàëüíîé ñåññèè êëèåíò çàïðàøèâàåò ó TGS ìàíäàò íà îáðàùåíèå ê ñåðâåðó. Åñëè âñå â ïîðÿäêå, TGS ïîñûëàåò ìàíäàò êëèåíòó. Çàòåì êëèåíò ïðåäúÿâëÿåò ñåðâåðó ýòîò ìàíäàò âìåñòî ñòàíäàðòíîãî ïàðîëÿ. È ñíîâà, åñëè àòðèáóòû êëèåíòà ïðàâèëüíû, ñåðâåð ïðåäîñòàâëÿåò êëèåíòó äîñòóï ê óñëóãå.

Òàáë. 24-1.
Òàáëèöà ñîêðàùåíèé Kerberos

c	= êëèåíò
s	= ñåðâåð
a	= ñåòåâîé àäðåñ êëèåíòà
v	= íà÷àëî è îêîí÷àíèå âðåìåíè äåéñòâèÿ ìàíäàòà
t	= ìåòêà âðåìåíè
K_x	= ñåêðåòíûé êëþ÷ *x*
$K_{x,y}$	= ñåàíñîâûé êëþ÷ äëÿ *x* è *y*
$(m)K_x$	= *m*, øèôðîâàííîå ñåêðåòíûì êëþ÷îì *x*
$T_{x,y}$	= ìàíäàò *x* íà èñïîëüçîâàíèå *y*
$A_{x,y}$	= óäîñòîâåðåíèå *x* äëÿ *y*

Àòðèáóòû

Kerberos èñïîëüçóåò äâà òèïà àòðèáóòîâ: **ìàíäàòû** è **óäîñòîâåðåíèÿ**. (Â äàëüíåéøåì â ýòîì ðàçäåëå áóäåò èñïîëüçîâàòüñÿ íîòàöèÿ, èñïîëüçóåìàÿ â äîêóìåíòàõ Kerberos - ñì. 23-é.) Ìàíäàò èñïîëüçóåòñÿ äëÿ áåçîïàñíîé ïåðåäà÷è ñåðâåðó ëè÷íîñòè êëèåíòà, êîòîðîìó âûäàí ýòîò ìàíäàò. Â íåì òàêæå ñîäåðæèòñÿ èíôîðìàöèÿ, êîòîðóþ ñåðâåð ìîæåò èñïîëüçîâàòü äëÿ ïðîâåðêè òîãî, ÷òî êëèåíò, èñïîëüçóþùèé ìàíäàò, - ýòî èìåííî òîò êëèåíò, êîòîðîìó ýòîò ìàíäàò áûë âûäàí. Óäîñòîâåðåíèå - ýòî äîïîëíèòåëüíûé àòðèáóò, ïðåäúÿâëÿåìûé âìåñòå ñ ìàíäàòîì. Ìàíäàò Kerberos èìåò ñëåäóþùóþ ôîðìó:

$T_{c,s} = s, \{c, a, v, K_{c,s}\}K_s$.

Ìàíäàò õîðîø äëÿ îäíîãî ñåðâåðà è îäíîãî êëèåíòà. Î í ñîäåðæèò èìÿ êëèåíòà, åãî ñåòåâîé àäðåñ, èìÿ ñåðâåðà, ìåòêó âðåìåíè è ñåàíñîâûé êëþ÷. Ýòà èíôîðìàöèÿ øèôðóåòñÿ ñåêðåòíûì êëþ÷îì ñåðâåðà. Åñëè êëèåíò ïîëó÷èë ìàíäàò, îí ìîæåò èñïîëüçîâàòü åãî äëÿ äîñòóïà ê ñåðâåðó ìíîãî ðàç - ïîêà íå èñòå÷åò ñðîê äåéñòâèÿ ìàíäàòà. Íå ìîæåò ðàñøèôðîâàòü ìàíäàò (îí íå çíàåò ñåêðåòíîãî êëþ÷à ñåðâåðà), íî îí ìîæåò ïðåäúÿâèòü åãî ñåðâåðó â çàøèôðîâàííîé ôîðìå. Ïðî÷èòàòü èëè èçìåíèòü ìàíäàò ïðè ïåðåäà÷å åãî ïî ñåòè íåâîçìîæíî. Óäîñòîâåðåíèå Kerberos èìåò ñëåäóþùóþ ôîðìó:

$A_{c,s} = \{c, t, êëþ÷\}K_{c,s}$

Êëèåíò ñîçäàåò åãî êàæäûé ðàç, êîãäà åìó íóæíî âîñïîëüçîâàòüñÿ óñëóãàìè ñåðâåðà. Óäîñòîâåðåíèå ñîäåðæèò ëèñòèíã, ìàòêó âðåìåíè è íåîáÿçàòåëüíûé äîïîëíèòåëüíûé ñåàíñîâûé êëþ÷, âñå ýòè äàííûå øèôðóþòñÿ ñåàíñîâûì êëþ÷îì, îáùèì äëÿ êëèåíòà è ñåðâåðà. Â îòëè÷èå îò ìàíäàòà óäîñòîâåðåíèå èñïîëüçóåòñÿ òîëüêî îäèí ðàç. Îáíàêî ýòî íå ïðîáëåìà, òàê êàê êëèåíò ìîæåò ãåíåðèðîâàòü óäîñòîâåðåíèÿ ïî ìåðå íàäîáíîñòè (åìó èçâåñòåí îáùèé ñåêðåòíûé êëþ÷).

Èñïîëüçîâàíèå óäîñòîâåðåíèÿ ïðåñëåäóåò äâå öåëè. Âî ïåðâûõ, îíî ñîäåðæèò íåêîòîðûé òèêåò, çàøèôðîâàííûé ñåàíñîâûì êëþ÷îì. Ýòî äîêàçûâàåò, ÷òî êëèåíò èçâåñòåí êëþ÷. ×òî íå ìåíåå âàæíî, çàøèôðîâàííûé îêðûòûé òåêñò âêëþ÷àåò ìàòêó âðåìåíè. Çëîóìûøëåííèê, êîòîðîìó óäàëîñü çàïèñàòü è ìàíäàò, è óäîñòîâåðåíèå, íå ñìîæåò èñïîëüçîâàòü èõ ïîñòóïàÿ âäà äíÿ.

Ñîâìåùåíèå Kerberos âåðñèè 5

Â Kerberos âåðñèè 5 èñïîëüçóåòñÿ ïÿòü ñîîáùåíèé (ñì. 23-é):

1. Êëèåíò-Kerberos: *c,tgs*
2. Kerberos-êëèåíò: $\{K_{c,tgs}\}K_c$, $\{T_{c,tgs}\}K_{tgs}$
3. Êëèåíò-TGS: $\{A_{c,s}\}K_{c,tgs}\{T_{c,tgs}\}\ K_{tgs,s}$
4. TGS-êëèåíò: $\{K_{c,s}\}K_{c,tgs}\{T_{c,s}\}K_s$
5. Êëèåíò-ñåðâåð: $\{A_{c,s}\}K_{c,s}\ \{T_{c,s}\}K_s$

Òåïåðü ðàññìîòðèì èñïîëüçîâàíèå ýòèõ ñîîáùåíèé ïîäðîáíî.

Ïîëó÷åíèå ïåðâîíà÷àëüíîãî ìàíäàòà

Ó êëèåíòà åñòü ÷ñòü èíôîðìàöèè, äîêàçûâàþùåé åãî ëè÷íîñòü - åãî ïàðîëü. Ïîíÿòíî, ÷òî íå õî÷åòñÿ çàñòàâëÿòü êëèåíòà ïåðèîäè÷åñêè ïàðîëü ïî ñåòè. Ïðîòîêîë Kerberos ìèíèìèçèðóåò âðåìÿ÷íîñòü ïîäñëóøèâàíèÿ ïàðîëÿ, íî ïðè ýòîì íå ïîçâîëÿåò ïîëüçîâàòåëþ ïðàâèëüíî èäåíòèôèöèðîâàòüñÿ èíà÷å, åñëè îí íå çíàåò ïàðîëÿ.

Êëèåíò ïîñûëàåò ñîîáùåíèå, ñîäåðæàùåå åãî èìÿ è èìÿ åãî ñåðâåðà TGS íà ñåðâåð ïðîâåðêè ïîäëèííîñòè Kerberos. (ìîæåò áûòü íåñêîëüêî ñåðâåðîâ TGS.) Íà ïðàêòèêå ïîëüçîâàòåëü, ñêîðåå âñåãî, ïðîñòî ââîäèò ñâîå èìÿ è ïðîãðàììà âõîäà â ñèñòåìó ïîñûëàåò çàïðîñ.

Ñåðâåð ïðîâåðêè ïîäëèííîñòè Kerberos èùåò äàííûå î êëèåíòå â ñâîåé áàçå äàííûõ. Åñëè èíôîðìàöèÿ î êëèåíòå åñòü â áàçå äàííûõ, Kerberos ãåíåðèðóåò ñåàíñîâûé êëþ÷, êîòîðûé áóäåò èñïîëüçîâàòüñÿ äëÿ îáìåíà äàííûìè ìåæäó êëèåíòîì è TGS. Îí íàçûâàåòñÿ **Ìàíäàòîì íà âûäåëåíèå ìàíäàòà** (Ticket Granting Ticket, TGT). Kerberos øèôðóåò ýòîò ñåàíñîâûé êëþ÷ ñåêðåòíûì êëþ÷îì êëèåíòà. Çàòåì îí ñîçäàåò äëÿ êëèåíòà TGT, äîêàçûâàþùèé ïîäëèííîñòü êëèåíòà TGS, è øèôðóåò åãî ñåêðåòíûì êëþ÷îì TGS. Ñåðâåð ïðîâåðêè ïîäëèííîñòè ïîñûëàåò ýòè äâà çàøèôðîâàííûõ ñîîáùåíèÿ êëèåíòó.

Òåïåðü êëèåíò ðàñøèôðîâûâàåò ïåðâîå ñîîáùåíèå è ïîëó÷àåò ñåàíñîâûé êëþ÷. Ñåêðåòíûé êëþ÷ ÿâëÿåòñÿ îäíîíàïðàâëåííîé õýø-ôóíêöèåé êëèåíòñêîãî ïàðîëÿ, ïîýòîìó ó çàêîííîãî ïîëüçîâàòåëÿ íå áóäåò íèêàêèõ ïðîáëåì. Ñàìîçâàíåö íå çíàåò ïðàâèëüíîãî ïàðîëÿ è, ñëåäîâàòåëüíî, íå ìîæåò ðàñøèôðîâàòü îòâåò ñåðâåðà ïðîâåðêè ïîäëèííîñòè. Äîñòóï çàïðåùàåòñÿ, è ñàìîçâàííûé êëèåíò íå ìîæåò ïîëó÷èòü ìàíäàò èëè ñåàíñîâûé êëþ÷.

Êëèåíò ñîõðàíÿåò TGT è ñåàíñîâûé êëþ÷, ñòèðàÿ ïàðîëü è õýø-çíà÷åíèå. Ýòà èíôîðìàöèÿ óíè÷òîæàåòñÿ äëÿ óìåíüøåíèÿ âåðîÿòíîñòè êîìïðîìåòàöèè. Åñëè âðàã ïîïûòàåòñÿ ñêîïèðîâàòü ïàìÿòü êëèåíòà, îí ïîëó÷èò òîëüêî TGT è ñåàíñîâûé êëþ÷. Ýòè äàííûå âàæíû, íî òîëüêî íà âðåìÿ æèçíè TGT. Êîãäà ñðîê äåéñòâèÿ TGT èñòå÷åò, ýòè ñâåäåíèÿ ñòàíóò áåññìûñëåííûìè. Òåïåðü â òå÷åíèå âðåìåíè æèçíè TGT êëèåíò ìîæåò äîêàçûâàòü TGS ñâîþ ïîäëèííîñòü.

Ïîëó÷åíèå ñåðâåðíûõ ìàíäàòîâ

Êëèåíòó òðåáóåòñÿ ïîëó÷àòü îòäåëüíûé ìàíäàò äëÿ êàæäîé íóæíîé åìó óñëóãè. TGS âûäåëÿåò ìàíäàòû äëÿ îòäåëüíûõ ñåðâåðîâ.

Êîãäà êëèåíòó íóæåí ìàíäàò, êîòîðîãî ó íåãî ïîêà íåò, îí ïîñûëàåò çàïðîñ ê TGS. (Íà ïðàêòèêå ïðîãðàììà, ñêîðåå âñåãî, äåëàåò ýòî àâòîìàòè÷åñêè è íåçàìåòíî äëÿ ïîëüçîâàòåëÿ.)

TGS, ïîëó÷èâ çàïðîñ, ðàñøèôðîâûâàåò TGT ñâîèì ñåêðåòíûì êëþ÷îì. Çàòåì TGS èñïîëüçóåò âêëþ÷åííûé â TGT ñåàíñîâûé êëþ÷, ÷òîáû ðàñøèôðîâàòü óäîñòîâåðåíèå. Íàêîíåö TGS ñðàâíèâàåò èíôîðìàöèþ óäîñòîâåðåíèÿ ñ èíôîðìàöèåé ìàíäàòà, ñåòåâîé àäðåñ êëèåíòà ñ àäðåñîì îòïðàâèòåëÿ çàïðîñà è ìåòêó âðåìåíè ñ òåêóùèì âðåìåíåì. Åñëè âñå ñîâïàäàåò, TGS ðàçðåøàåò âûïîëíåíèå çàïðîñà.

Ïðîâåðêà ìåòîê âðåìåíè ïðåäïîëàãàåò, ÷òî ÷àñû âñåõ êîìïüþòåðîâ ñèíõðîíèçèðîâàíû, ïî êðàéíåé ìåðå ñ òî÷íîñòüþ äî íåñêîëüêèõ ìèíóò. Åñëè âðåìÿ, óêàçàííîå â çàïðîñå, îòñòîèò îò òåêóùåãî ìîìåíòà ñëèøêîì äàëåêî â ïðîøëîå èëè â áóäóùåå, TGS ñ÷èòàåò çàïðîñ ïîïûòêîé ïîâòîðåíèÿ ïðåäûäóùåãî çàïðîñà. TGS äîëæíà òàêæå îòñëåæèâàòü ïðàâèëüíîñòü ñðîêîâ äåéñòâèÿ óäîñòîâåðåíèé, òàê êàê óñëóãè ñåðâåðà ìîãóò çàïðàøèâàòüñÿ íåñêîëüêî ðàç ïîñëåäîâàòåëüíî ñ îäíèì ìàíäàòîì, íî ðàçíûìè óäîñòîâåðåíèÿìè. Äðóãîé çàïðîñ ñ òåì æå ìàíäàòîì è óæå èñïîëüçîâàííîé ìåòêîé âðåìåíè óäîñòîâåðåíèÿ áóäåò îòâåðãíóò.

Â îòâåò íà ïðàâèëüíûé çàïðîñ TGS âîçâðàùàåò ïðàâèëüíûé ìàíäàò, êîòîðûé êëèåíò ìîæåò ïðåäúÿâèòü ñåðâåðó. TGS òàêæå ñîçäàåò íîâûé ñåàíñîâûé êëþ÷ äëÿ êëèåíòà è ñåðâåðà, çàøèôðîâàííûé ñåàíñîâûì êëþ÷îì, îáùèì äëÿ êëèåíòà è TGS. Îáà ýòèõ ñîîáùåíèÿ îòïðàâëÿþòñÿ êëèåíòó. Êëèåíò ðàñøèôðîâûâàåò ñîîáùåíèå è èçâëåêàåò ñåàíñîâûé êëþ÷.

Çàïðîñ óñëóãè

Òåïåðü êëèåíò ìîæåò äîêàçàòü ñâîþ ïîäëèííîñòü ñåðâåðó. Îí ñîçäàåò ñîîáùåíèå, î÷åíü ïîõîæåå íà òî, êîòîðîå ïîñûëàëîñü TGS (è ýòî ïîíÿòíî, òàê êàê TGS - òîæå óñëóãà).

Êëèåíò ñîçäàåò óäîñòîâåðåíèå, ñîñòîÿùåå èç åãî èìåíè, ñåòåâîãî àäðåñà è ìåòêè âðåìåíè, çàøèôðîâàííîå ñåàíñîâûì êëþ÷îì, êîòîðûé áûë ãåíåðèðîâàí TGS äëÿ ñåàíñà êëèåíòà è ñåðâåðà. Çàïðîñ ñîñòîèò èç ìàíäàòà, ïîëó÷åííîãî îò Kerberos (óæå çàøèôðîâàííîãî ñåêðåòíûì êëþ÷îì ñåðâåðà) è çàøèôðîâàííîãî èäåíòèôèêàòîðà.

Ñåðâåð ðàñøèôðîâûâàåò è ïðîâåðÿåò ìàíäàò è óäîñòîâåðåíèå, êàê óæå îòìå÷àëîñü, à òàêæå ïðîâåðÿåò àäðåñ êëèåíòà è ìåòêó âðåìåíè. Åñëè âñå â ïîðÿäêå, òî ñåðâåð óçíàåò, ÷òî, ñîãëàñíî Kerberos, êëèåíò - èìåííî òîò, çà êîãî îí ñåáÿ âûäàåò.

Åñëè ïðèëîæåíèå òðåáóåò âçàèìíîé ïðîâåðêè ïîäëèííîñòè, ñåðâåð ïîñûëàåò êëèåíòó ñîîáùåíèå, ñîñòîÿùåå èç ìåòêè âðåìåíè, çàøèôðîâàííîé ñåàíñîâûì êëþ÷îì. Ýòî äîêàçûâàåò, ÷òî ñåðâåðó èçâåñòåí ïðàâèëüíûé ñåêðåòíûé êëþ÷, è îí ìîæåò ðàñøèôðîâàòü ìàíäàò è óäîñòîâåðåíèå.

Ïðè íåîáõîäèìîñòè êëèåíò è ñåðâåð ìîãóò øèôðîâàòü äàëüíåéøèå ñîîáùåíèÿ îáùèì êëþ÷îì. Òàê êàê ýòîò êëþ÷ èçâåñòåí òîëüêî èì, îíè îáà ìîãóò áûòü óâåðåíû, ÷òî ïîñëåäíåå ñîîáùåíèå, çàøèôðîâàííîå ýòèì êëþ÷îì, îòïðàâëåíî äðóãîé ñòîðîíîé.

Kerberos âåðñèè 4

Â ïðåäûäóùèõ ðàçäåëàõ ðàññìàòðèâàëñÿ Kerberos âåðñèè 5. Âåðñèÿ 4 íåìíîãî îòëè÷àåòñÿ ñîîáùåíèÿìè è êîíñòðóêöèåé ìàíäàòîâ è óäîñòîâåðåíèé. Â Kerberos âåðñèè 4 èñïîëüçóþòñÿ ñëåäóþùèå ïÿòü ñîîáùåíèé:

1. Êëèåíò-Kerberos: c,tgs
2. Kerberos-êëèåíò: $\{K_{c,tgs}\{T_{c,tgs}\}K_{tgs}\}K_c$,
3. Êëèåíò-TGS: $\{A_{c,s}\}K_{c,tgs}\{T_{c,tgs}\}\ K_{tgs,s}$
4. TGS-êëèåíò: $\{K_{c,s}\{T_{c,s}\}K_s\}K_{c,tgs}$
5. Êëèåíò-ñåðâåð: $\{A_{c,s}\}K_{c,s}\ \{T_{c,s}\}K_s$

$$T_{c,s} = \{s, c, a, v, l, K_{c,s}\}K_s$$

$$A_{c,s} = \{c, a, t\}\ K_{c,s}$$

Ñîîáùåíèÿ 1,3 è 5 íå èçìåíèëèñü. Äâîéíîå øèôðîâàíèå ìàíäàòà íà ýòàïàõ 2 è 4 â âåðñèè 5 áûëî óñòðàíåíî. Ìàíäàòû âåðñèè 5 äîïîëíèòåëüíî âêëþ÷àþò âîçìîæíîñòü èñïîëüçîâàòü íåñêîëüêî àäðåñîâ, à ïîëå "âðåìÿ æèçíè", l, çàìåíåíî âðåìåíåì íà÷àëà è îêîí÷àíèÿ. Â óäîñòîâåðåíèå âåðñèè ïÿòü äîáàâëåíà âîçìîæíîñòü âêëþ÷åíèÿ äîïîëíèòåëüíîãî êëþ÷à.

Áåçîïàñíîñòü Kerberos

Ñòèâ Áåëëîâèí (Steve Bellovin) è Ìàéêë Ìåððèòò (Michael Merritt) ïðîàíàëèçèðîâàëè íåêîòîðûå ïðîáëåìû óÿçâèìûå ìåñòà Kerberos [108]. Õîòÿ ýòà ðàáîòà áûëà íàïèñàíà ïðî ïðîòîêîëû âåðñèè 4, ìíîãèå åå çàìå÷àíèÿ ïðèìåíèìû è ê âåðñèè 5.

Âîçìîæíî êýøèðîâàíèå è ïîâòîðíîå èñïîëüçîâàíèå ñòàðûõ óäîñòîâåðåíèé. Õîòÿ ìåòêè äîëæíû ïðåäîòâðàòèòü èàêóþ âîçìîæíîñòü, óäîñòîâåðåíèÿ ìîãóò èñïîëüçîâàòüñÿ ïîâòîðíî â òå÷åíèå âðåìåíè æèçíè ìàíäàòà. Ïðåäïîëàãàåòñÿ, ÷òî ñåðâåðû õðàíÿò âñå ïðàâèëüíûå ìàíäàòû, ÷òîáû îáíàðóæèòü ïîâòîðû, íî ýòî íå âñåãäà âîçìîæíî. Êðîìå òîãî, âðåìÿ æèçíè áûâàåò äîñòàòî÷íî áîëüøèì, ÷àñòî äî âîñüìè ÷àñîâ.

Èñïîëüçîâàíèå óäîñòîâåðåíèé îñíîâàíû íà òîì, ÷òî âñå ÷àñû ñåòè áîëåå èëè ìåíåå ñèíõðîíèçèðîâàíû. Åñëè âðåìÿ êîìïüþòåðà áóäåò óñòàíîâëåíî, òî ñòàðûå óäîñòîâåðåíèå ìîæåò áûòü èñïîëüçîâàíî áåç ïðîáëåì. Áîëüøèíñòâî ñåòåâûõ ïðîòîêîëîâ ïîääåðæèâàþò íåêîòîðóþ ìåðó ñèíõðîíèçàöèè âðåìåíè íåáîëüøèõ ðàñõîæäåíèé. Áîëåå ñëîæíûå ñåòåâûå ïðîòîêîëû, íàïðèìåð, ïðåäíàçíà÷åííûå äëÿ ðàñïðåäåëåííûõ áàç äàííûõ, ìîãóò ïîòðåáîâàòü áîëåå òî÷íîé ñèíõðîíèçàöèè âðåìåíè. Ýòî ïðèâîäèò ê íåîáõîäèìîñòè ðåàëèçàöèè ïðîòîêîëîâ ïîääåðæêè âðåìåíè íåáîëüøèõ ðàñõîæäåíèé ìåæäó ñåðâåðàìè Kerberos.

Kerberos òàêæå ÷óâñòâèòåëåí ê âñêðûòèþ ñóãàäûâàíèåì ïàðîëÿ. Çëîóìûøëåííèê ìîæåò çàïèñàòü ìàíäàòû è çàòåì ïîâòîðíî èõ ðàñøèôðîâàòü. Íå çàáóäåì, ÷òî ñðåäíèé ïîëüçîâàòåëü ðåãóëÿðíî ìåíÿåò ïàðîëü. Åñëè Ìýëîðè äîáóäåò äîñòàòî÷íî ìàíäàòîâ, ó íåãî ïîÿâÿòñÿ íåïîñòè øàíñû ðàñêðûòü ïàðîëü.

Âîçìîæíî ñàìûì îïàñíûì ÿâëÿåòñÿ âñêðûòèå, èñïîëüçóþùåå ñïåöèàëüíîå ïðîãðàììíîå îáåñïå÷åíèå. Ïðîòîêîë Kerberos ïîäâåðãëòñÿ, ÷òî ïðîãðàììíîìó îáåñïå÷åíèþ ìîæíî äîâåðÿòü. Íåò ñïîñîáà ïîìåøàòü Ìýëîðè èñïîëüçîâàòü Kerberos òàêîé âåðñèåé, êîòîðàÿ ïîìîæåò çàìåíèòü âñå êëèåíòñêîå ïðîãðàììíîå îáåñïå÷åíèå Kerberos çàïèñûâàò ïàðîëè. Ýòî ÿâëÿåòñÿ ïðîáëåìîé äëÿ ëþáîãî êðèòè÷åñêîãî ïðîãðàììíîãî ïàêåòà, ðàáîòàþùåãî íà íåáåçîïàñíîì êîìüòåðå, íî øèðîêî ðàñïðîñòðàíåííîå èñïîëüçîâàíèå Kerberos â ïîäîáíûõ ñðåäàõ äåëàåò åãî ÷ñîáåííî ïðèâëåêàòåëüíîé ìèøåíüþ.

Âåäóòñÿ ðàáîòû íàä óëó÷øåíèåì Kerberos, âêëþ÷àÿ ìîäóëèçàöèþ óïðàâëåíèÿ êëþ÷àìè ñ ïîìîùüþ êðèïòîãðàôèè ñ îòêðûòûì êëþ÷îì è èíòåðôåéñà èíòåëëåêòóàëüíûõ êàðòî÷åê.

Ëèöåíçèè

Kerberos íå ÿâëÿåòñÿ îáùåäîñòóïíûì, íî êîä ÌÒÈ äîñòóïåí ñâîáîäíî. Äåéñòâèòåëüíàÿ ðåãèñòðàöèÿ â ðàáîòàþùèõ ñèñòåìàõ UNIX - ýòî ñîâñåì äðóãàÿ èñòîðèÿ. Ðÿä êîìïàíèé ïðîäàåò âåðñèè Kerberos, íî ìîæíî ïîëó÷èòü õîðîøóþ âåðñèþ áåñïëàòíî îò Cygnus Support, 814 University Ave., Pale Alto, CA, 94301; (415) 32,2.-3811; fax: (415) 32.2.-3270.

24.6 KRYPTOKNIGHT

KryptoKnight (ÊðèïòîÐûöàðü) ÿâëÿåòñÿ ñèñòåìîé ïðîâåðêè ïîäëèííîñòè è ðàñïðåäåëåíèÿ êëþ÷åé, ðàçðàáîòàííîé â IBM. Ýòî ïðîòîêîë ñ ñâîéſòâåííûì êëþ÷îì, èñïîëüçóþùèé ëèáî DES â ðåæèìå CBC (ñì. ðàçäåë 9.3) èëè ìîäèôèöèðîâàííóþ âåðñèþ MD5 (ñì. ðàçäåë 18.5). KryptoKnight ïîääåðæèâàåò ÷åòûðå ñâîéſòâà áåçîïàñíîñòè:

— Ïðîâåðêà ïîäëèííîñòè ïîëüçîâàòåëÿ (íàçûâàåìàÿ åäèíîâðåìåííîé ïîäïèñüþ - single sign-on)

— Äâóñòîðîííÿÿ ïðîâåðêà ïîäëèííîñòè

— Ðàñïðåäåëåíèå êëþ÷åé

— Ïðîâåðêà ïîäëèííîñòè ñîäåðæàíèÿ è ïðîèñõîæäåíèÿ äàííûõ

Ñòî÷êè çðåíèÿ ïîëüçîâàòåëÿ, KryptoKnight ïîõîæ íà Kerberos. Âîò íåêîòîðûå îòëè÷èÿ:

— Äëÿ ïðîâåðêè ïîäëèííîñòè è øèôðîâàíèÿ ìàíäàòîâ KryptoKnight èñïîëüçóåò õýø-ôóíêöèþ.

— KryptoKnight íå èñïîëüçóåò ñèíõðîíèçèðîâàííûõ ÷àñîâ, èñïîëüçóþòñÿ òîëüêî òåêóùèå çàïðîñû (ñì. ðàçäåë 3.3).

— Åñëè Àëèñà íóæíî ñâÿçàòüñÿ ñ Áîáîì, îäíà èç îïöèé KryptoKnight ïîçâîëÿåò Àëèñå ïîñëàòü ñîîáùåíèå Áîáó, à çàòåì ïîçâîëÿåò Áîáó íà÷àòü ïðîòîêîë îáìåíà êëþ÷àìè.

KryptoKnight, êàê è Kerberos, èñïîëüçóåò ìàíäàòû è óäîñòîâåðåíèÿ. Î í ñîäåðæèò è TGS, íî â KryptoKnight íàçûâàþòñÿ ñåðâåðàìè ïðîâåðêè ïîäëèííîñòè. Ðàçðàáîò÷èêè KryptoKnight ïîðàçëè íåìåöêîãî óñëóæíîãî, èñïîëüçîâàíèå, èõ ðàçìåð è îáúåì øèôðîâàíèÿ. Î KryptoKnight ÷èòàéòå â [1110, 173, 174, 175].

24.7 SESAME

SESAME îçíà÷àåò Secure European System for Applications in a Multivendor Environment - Áåçîïàñíàÿ åâðîïåéñêàÿ ñèñòåìà äëÿ ïðèëîæåíèé â íåîäíîðîäíûõ ñðåäàõ. Ýòî ïðîåêò Åâðîïåéñêîãî ñîþçà, íà 50 ïðîöåíòîâ ôèíàíñèðóåìûé RACE (ñì. ðàçäåë 25.7), ãëàâíîé öåëüþ êîòîðîé ÿâëÿåòñÿ ðàçðàáîòêà òåõíîëîãèè äëÿ ïðîâåðêè ïîäëèííîñòè ïîëüçîâàòåëÿ ïðè ðàñïðåäåëåííîì êîíòðîëå äîñòóïà. Ýòó ñèñòåìó ìîæíî ðàññìàòðèâàòü êàê åâðîïåéñêèé âàðèàíò Kerberos. Ïðîåêò ñîñòîèò èç äâóõ ÷àñòåé: íà ïåðâîé ñòàäèè ðàçðàáàòûâàåòñÿ áàçîâàÿ àðõèòåêòóðà, à âòîðàÿ ñòàäèÿ ïðåäïîëàãàåò ñîçäàíèå ïðîòîòèïîâ è ïîëíîìàñøòàáíóþ ðåàëèçàöèþ. Ñëåäóþùèå òðè êîìïàíèè ïðèíèìàþò íàèáîëüøåå ó÷àñòèå â ðàçðàáîòêå ñèñòåìû - ICL â Åâðîïåéñêîì Ñîþçå, Siemens â Ãåðìàíèè è Bull âî Ôðàíöèè.

SESAME ïðåäñòàâëÿåò ñîáîé ñèñòåìó ïðîòîêîëîâ è îáìåíà êëþ÷àìè [361, 1248, 797, 1043]. Î íà èñïîëüçóåò ïðîòîêîë Needham-Schroeder, ïðèìåíÿÿ êðèïòîãðàôèþ ñ îòêðûòûìè êëþ÷àìè äëÿ ñâÿçè ìåæäó ðàçëè÷íûìè áåçîïàñíûìè äîìåíàìè. Â ñèñòåìå åñòü ñåðüåçíûõ èçúÿíîâ. Âìåñòî èñïîëüçîâàíèÿ íàñòîÿùåãî ìàñòåðêëþ÷à øèôðîâàíèÿ â ýòîé ñèñòåìå ïðèìåíÿåòñÿ XOR ñ 64-áèòîâûì êëþ÷îì. ×òî åùå õóæå, â SESAME èñïîëüçóåòñÿ XOR â ðåæèìå CBC, êîòîðûé îñòàâëÿåò íåçàøèôðîâàííûì ïîëîâèíó îòêðûòîãî òåêñòà. Â çàùèòó ðàçðàáîò÷èêîâ íàäî ñêàçàòü, ÷òî îíè ñîáèðàëèñü èñïîëüçîâàòü DES, íî ôðàíöóçñêîå ïðàâèòåëüñòâî âûðàçèëî íåóäîâîëüñòâèå ïî ýòîìó ïîâîäó. Îíè óòâåðäèëè êîä ñ DES, íî çàòåì óáðàëè åãî. Ýòà ñèñòåìà ìåíÿ íå âïå÷àòëåíà.

Îòæäåñòâëåíèå â SESAME ÿâëÿåòñÿ ôóíêöèå ïåðâîãî áëîêà, à íå âñåãî ñîîáùåíèÿ. Â ðåçóëüòàòå ýòîãî òîæäåñòâëåííûì ñîîáùåíèé áóäåò ïðîâåðåíà ïî ñëîâàì "Dear Sir", à íå ïî âñåìó ñîäåðæèìó ñîîáùåíèé. Åùå îäíà öèôðà êëþ÷åé ñîñòîèò èç äâóõ âûçîâîâ ôóíêöèè rand îïåðàöèîííîé ñèñòåìû UNIX, êîòîðàÿ ñîâñåì íå ñëó÷àéíà. Â êà÷åñòâå îñíîâíîãî àëãîðèòìà øèôðîâàíèÿ SESAME èñïîëüçóåò crc32 è MD5. È êîíå÷íî, SESAME ïîääåðæèâàåò Kerberos ÷óâñòâèòåëüíà ê óãàäûâàíèþ ïàðîëåé.

24.8 Îáùàÿ êðèïòîãðàô è÷åñêàÿ àðõèòåêòóðà IBM

Îáùàÿ êðèïòîãðàôè÷åñêàÿ àðõèòåêòóðà (Common Cryptographic Architecture, CCA) áûëà ðàçðàáîòàíà êîìïàíèåé IBM, ÷òîáû îáåñïå÷èòü êðèïòîãðàôè÷åñêèå ïðèìèòèâû äëÿ êîíôèäåíöèàëüíîñòè, öåëîñòíîñòè, óïðàâëåíèÿ êëþ÷àìè è îáðàáîòêè ïåðñîíàëüíîãî èäåíòèôèêàöèîííîãî êîäà (PIN) [751, 784, 1025, 1026, 940, 752]. Óïðàâëåíèå êëþ÷àìè ïðîèñõîäèò ñ ïîìîùüþ âåêòîðîâ óïðàâëåíèÿ (control vector, CV) (ñì. ðàçäåë 8.5). Êàæäîìó êëþ÷ó ñîîòâåòñòâóåò CV, ñ êîòîðûì êëþ÷ îáúåäèíåí îïåðàöèîííûé XOR. Êëþ÷ è CV ðàçäåëÿþòñÿ òîëüêî â áåçîïàñíîì àïïàðàòíîì ìîäóëå. CV ïðåäñòàâëÿåò ñòðóêòóðó äàííûõ, îáðïå÷èâàþùóþ èíòåãðèòåòíîñòü ïîíèìàíèå ïðèâèëåãèé, ñâÿçàííûõ ñ êîíêðåòíûì êëþ÷îì.

Îòäåëüíûå áèòû CV îáëàäàþò êîíêðåòíûì ñìûñëîì ïðè èñïîëüçîâàíèè êàæäîãî êëþ÷à, ïðèìåíÿåìîãî â CGA. CV ïåðåäàþòñÿ âìåñòå ñ çàøèôðîâàííûì êëþ÷îì â ñòðóêòóðàõ äàííûõ, íàçûâàåìûõ êëþ÷åâûìè ïðèìèòèâàìè (key token). Âíóòðåíèå êëþ÷åâûå ìàòåðèè èñïîëüçóþòñÿ ëîêàëüíî è ñîäåðæàò êëþ÷è, øèôðîâàííûå ëîêàëüíûì ãëàâíûì êëþ÷îì (master key, MK). Âíåøíèå êëþ÷åâûå ìàòåðèè èñïîëüçóþòñÿ äëÿ øèôðîâàííûõ êëþ÷àìè ìåæäó ñèñòåìàìè. Êëþ÷è âî âíåøíåì êëþ÷åâûõ ìàòåðèàõ çàøèôðîâàíû êëþ÷àìè øèôðîâàíèÿ êëþ÷åé (key-encrypting key, KEK). Óïðàâëåíèå KEK îñóùåñòâëÿþòñÿ ñ ïîìîùüþ âíóòðåííèõ êëþ÷åâûõ ìàòåðèàëîâ. Êëþ÷è ðàçäåëÿþòñÿ íà ãðóïïû â ñîîòâåòñòâèè ñ èõ èñïîëüçîâàíèåì.

Äëèíà êëþ÷à òàêæå çàâèñèò ïðè ïîìîùè áèòîâ CV. Êëþ÷è îäíàðíîé äëèíû - 56-áèòîâûå - èñïîëüçóþòñÿ äëÿ òàêèõ ôóíêöèé, êàê îáåñïå÷åíèå êîíôèäåíöèàëüíîñòè è ñîâìåñòèìîñòü. Êëþ÷è äâîéíîé äëèíû - 112-áèòîâûå - ïðèìåíÿþòñÿ äëÿ óïðàâëåíèÿ êëþ÷àìè, ôóíêöèé PIN è äðóãèõ ñïåöèàëüíûõ öåëåé. Êëþ÷è ìîãóò áûòü DOUBLE-ONLY (òîëüêî äâîéíûå), ïðåäûå è ëåâûå ïîëîâèíû êîòîðûõ äîëæíû áûòü ðàçëè÷íû, DOUBLE (äâîéíûå) ïîëîâèíû êîòîðûõ ìîãóò ñëó÷àéíî ñîâïàñòü, SINGLE-REPLICATED (îäèíàðíûå-ïîâòîðåííûå), â êîòîðûõ ïðàâûå è ëåâûå ïîëîâèíû ðàâíû, èëè SINGLE (îäèíàðíûå), ñîäåðæàùèå òîëüêî 56 áèòîâ. CGA îïðåäåëÿåò àïïàðàòíóþ ðåàëèçàöèþ îïðåäåëåííûõ òèïîâ êëþ÷åé, èñïîëüçóåìûõ äëÿ íåêîòîðûõ îïåðàöèé.

CV ïðîâåðÿåòñÿ â áåçîïàñíîì àïïàðàòíîì ìîäóëå: äëÿ êàæäîé ôóíêöèè CGA âåêòîð äîëæåí ñîîòâåòñòâîâàòü îïðåäåëåííûì ïðàâèëàì. Åñëè CV óñïåøíî ïðîõîäèò ïðîâåðêó, òî ïðè ïîìîùè XOR KEK èëè MK ñ CV ïîëó÷àåòñÿ âàðèàíò KEK èëè MK, è èçâëå÷åíèé êëþ÷ äëÿ äåøèôðèðîâàíèÿ îòêðûòîãî òåêñòà ñîîáùåíèÿ èñïîëüçóåòñÿ òîëüêî ïðè âûïîëíåíèè ôóíêöèè CGA. Ïðè ãåíåðàöèè íîâûõ êëþ÷åé CV çàäàåò ñïîñîá èñïîëüçîâàíèÿ ñîçäàííîãî êëþ÷à. Êîìáèíàöèè òèïîâ êëþ÷åé, êîòîðûå ìîãóò áûòü èñïîëüçîâàíû äëÿ âñêðûòèÿ ñèñòåìû, íå ñîçäàþòñÿ â CGA-ñîâìåñòèìûõ ñèñòåìàõ è íå èìîðòèðóþòñÿ â íèõ.

Äëÿ ðàñïðåäåëåíèÿ êëþ÷åé CGA ïðèìåíÿåò êîìáèíàöèþ êðèïòîãðàôèè ñ îòêðûòûì êëþ÷àìè è êðèïòîãðàôèè ñ ñåêðåòíûì êëþ÷àìè. KDC øèôðóåò ñåàíñîâûé êëþ÷ äëÿ ïîëüçîâàòåëÿ ñåêðåòíûì ãëàâíûì êëþ÷îì, ðàçäåëÿåìûì ñ ýòèì ïîëüçîâàòåëåì. Ðàñïðåäåëåíèå ãëàâíûõ êëþ÷åé ïðîèñõîäèò ñ ïîìîùüþ êðèïòîãðàôèè ñ îòêðûòûì êëþ÷àìè.

Ðàçðàáîò÷èêè ñèñòåì âûáðàëè òàêîé ãèáðèäíûé ïîäõîä ïî ââóì ïðè÷èíàì. Ïåðâîé èç íèõ ÿâëÿåòñÿ ýôôåêòèâíîñòü. Êðèïòîãðàôèÿ ñ îòêðûòûì êëþ÷àìè òðåáóåò âû÷èñëèòåëüíûõ ðåñóðñîâ, åñëè ñåàíñîâûå êëþ÷è ðàñïðåäåëÿþòñÿ ñ ïîìîùüþ êðèïòîãðàôèè ñ îòêðûòûì êëþ÷àìè, ñèñòåìà ìîæåò ïîâòîðíî èñïîëüçîâàòü íåáîëüøîå êîëè÷åñòâî ñåàíñîâûõ êëþ÷åé, ïîëó÷åííûõ ïðè ïîìîùè îäíîãî îòêðûòîãî êëþ÷à. Òàêîé ïîäõîä ïîçâîëÿåò ñîõðàíèòü ïðåèìóùåñòâà ñèììåòðè÷íîãî øèôðîâàíèÿ, íå ïîæåðòâóÿ ïðåèìóùåñòâàìè îòêðûòîãî êëþ÷à. Ñèñòåìà ìîæåò èñïîëüçîâàòü ñèììåòðè÷íûé ñåàíñîâûé êëþ÷ äëÿ øèôðîâàíèÿ ñîîáùåíèé, à îòêðûòûé êëþ÷ — äëÿ ïåðåäà÷è ñåêðåòíîãî êëþ÷à.

CGA-ñèñòåìû ïðîåêòèðîâàëèñü òàê, ÷òîáû îíè ìîãëè âçàèìîäåéñòâîâàòü ñ ðàçëè÷íûìè äóãèìè ñèñòåìàìè. Ïðè êîíòàêòå ñ íåñîâìåñòèìûìè ñèñòåìàìè ôóíêöèÿ òðàíñëÿöèè äóãè (Control Vector Translate, CVXLT) ïîçâîëÿåò ñèñòåìàì îáìåíèâàòüñÿ êëþ÷àìè. Èíòåãðàöèÿ CVXLT òðåáóåò êîíòðîëÿ ñ îáåèõ ñòîðîí. Êàæäàÿ èç íèõ äîëæíà íåçàâèñèìî óñòàíîâèòü íóæíûå òàáëèöû òðàíñëÿöèè. Òàêîé ââîä íîâûõ êîíòðîëü îáåñïå÷èâàåò âûñîêóþ ñòåïåíü íàäåæíîñòè, êàñàþùåéñÿ öåëîñòíîñòè è ïðîèñõîæäåíèÿ êëþ÷åé, èìïîðòèðóåìûõ â ñèñòåìó.

Òèï êëþ÷à DATA ïîääåðæèâàåòñÿ äëÿ ñîâìåñòèìîñòè ñ äðóãèìè ñèñòåìàìè. Êëþ÷ òèïà DATA õðàíèòñÿ âìåñòå ñ ñîîòâåòñòâóþùèì CV, óêàçûâàþùèì, ÷òî ýòî êëþ÷ òèïà DATA. Êëþ÷è òèïà DATA ìîãóò èñïîëüçîâàòüñÿ äîñòàòî÷íî øèðîêî, è ïîýòîìó ê íèì íóæíî îòíîñèòüñÿ ñ ïîäîçðåíèåì è èñïîëüçîâàòü èõ ñ îñòîðîæíîñòüþ. Êëþ÷è òèïà DATA íåëüçÿ èñïîëüçîâàòü íè äëÿ êàêèõ ôóíêöèé óðàâëåíèÿ êëþ÷àìè.

Àïïàðàòóðà çàêðûòèÿ êîììåð÷åñêèõ äàííûõ (Commercial Data Masking Facility, CDMF) ïðåäñòàâëÿåò ñîáîé ýêñïîðòèðóåìóþ âåðñèþ CGA. Åå îñîáåííîñòüþ ÿâëÿåòñÿ óìåíüøåíèå ýôôåêòèâíîé äëèíû êëþ÷åé DES äî ðàçðåøåííûõ ê ýêñïîðòó 40 áèòîâ (ñì. ðàçäåë 15.5) [785].

24.9 Ñõåìà ïðîâåðêè ïîäëèííîñòè ISO

Äëÿ èñïîëüçîâàíèÿ â ñõåìå ïðîâåðêè ïîäëèííîñòè ISO, òàêæå èçâåñòíîé êàê ïðîòîêîë X.509, ðåêîìåíäóþò êðèïòîãðàôèÿ ñ îòêðûòûì êëþ÷àìè [304]. Ýòà ñõåìà îáåñïå÷èâàåò ïðîâåðêó ïîäëèííîñòè ïî ñåòè. Õîòÿ êîíêðåòíûé àëãîðèòì íå ïîðåäëåí íè äëÿ îáåñïå÷åíèÿ áåçîïàñíîñòè, íè äëÿ ïðîâåðêè ïîäëèííîñòè, ñïåöèôèêàöèÿ ðåêîìåíäóåò èñïîëüçîâàòü RSA. Îäíàêî âîçìîæíî èñïîëüçîâàíèå íåñêîëüêèõ àëãîðèòìîâ è õýø-ôóíêöèé. Ïåðâîíà÷àëüíûé âàðèàíò X.509 áûë âûïóùåí â 1988 ã. Ïîñëå òðåõëåòíåãî èçó÷åíèÿ è êîììåíòèðîâàíèÿ îí áûë ïåðåñìîòðåí â 1993 ãîäó, ÷òîáû èñïðàâèòü íåêîòîðûå èçúÿíû â áåçîïàñíîñòè [1100, 750].

Âåðñèÿ
Ïîñëåäîâàòåëüíûé íîìåð
Èäåíòèôèêàòîð àëãîðèòìà - Àëãîðèòì - Ïàðàìåòðû
Âûäâèãàþùàÿ îðãàíèçàöèÿ
Âðåìÿ äåéſòâèÿ - íà÷àëî äåéſòâèÿ - ãîíåö äåéſòâèÿ
Ñóáúåêò
Îòêðûòûé êëþ÷ ñóáúåêòà - Àëãîðèòì - Ïàðàìåòðû - Îòêðûòûé êëþ÷

Ïîäïèñü

Ðèñ. 24-2. Ñåðòèôèêàò X.509.

Ñåðòèôèêàòû

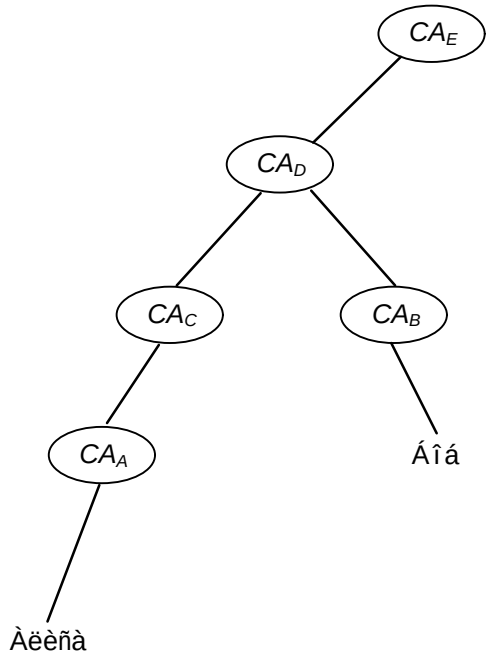
Íàèáîëåå âàæíîé ÷àñòüþ X.509 èñïîëüçóåìàÿ è ñòðóêòóðà ñåðòèôèêàòîâ îòêðûòûõ êëþ÷åé. Èìåíà âñåõ ïîëüçîâàòåëåé ðàçëè÷íû. Äîâåðåííûé Îðãàí ñåðòèôèêàöèè (Certification Authority, CA) ïðèñâàèâàåò êàæäîìó ïîëüçîâàòåëþ óíèêàëüíîå èìÿ è âûäàåò ïîäïèñàííûé ñåðòèôèêàò, ñîäåðæàùèé èìÿ è îòêðûòûé êëþ÷ ïîëüçîâàòåëÿ. Ñòðóêòóðà ñåðòèôèêàòà X.509 ïîêàçàíà íà 22-é [304].

Ïîêå âåðñèè îïðåäåëÿåò ôîðìàò ñåðòèôèêàòà. Ïîñëåäîâàòåëüíûé íîìåð óíèêàëåí äëÿ êîíêðåòíîãî CA. Ñëåäóþùåå ïîëå îïðåäåëÿåò àëãîðèòì, èñïîëüçîâàííûé äëÿ ïîäïèñè ñåðòèôèêàòà, âìåñòå ñî âñåìè íåîáõîäèìûìè ïàðàìåòðàìè. Âûäàâøåé îðãàíèçàöèåé ÿâëÿåòñÿ CA. Ñðîê äåéſòâèÿ ïðåäñòàâëÿåò ñîáîé ïàðó äàò, ñåðòèôèêàò äåéſòâèòåëåí â ïðîìåæóòêå ìåæäó ýòèìè äâóìÿ äàòàìè. Ñóáúåêò - ýòî èìÿ ïîëüçîâàòåëÿ. Èíôîðìàöèÿ îá îòêðûòîì êëþ÷å âêëþ÷àåò íàçâàíèå àëãîðèòìà, âñå íåîáõîäèìûå ïàðàìåòðû è îòêðûòûé êëþ÷. Ïîñëåäíèì ïîëåì ÿâëÿåòñÿ ïîäïèñü CA.

Åñëè Àëèñà õî÷åò ñâÿçàòüñÿ ñ Áîáîì, îíà ñíà÷àëà èçâëåêàåò èç áàçû äàííûõ åãî ñåðòèôèêàò è ïðîâåðÿåò åãî äîñòîâåðíîñòü. Åñëè ó íèõ îáùèé CA, òî âñå ïðîñòî. Àëèñà ïðîâåðÿåò ïîäïèñü CA íà ñåðòèôèêàòå Áîáà.

Åñëè îíè ïîëüçóþòñÿ ðàçëè÷íûìè CA, òî âñå ãîðàçäî ñëîæíåå. Ïðåäïîëàãàþò ñåáÿ äðåâîâèäíóþ ñòðóêòóðó, â êîòîðîé îäíè CA ñåðòèôèöèðóþò äðóãèå CA è ïîëüçîâàòåëè. Íà ñàìîì âåðõíåì óðîâíå íàõîäèòñÿ ãèàâíûé CA. Ó êàæäîãî CA åñòü ñåðòèôèêàòû, ïîäïèñàííûå âûøåñòîÿùèì CA è íèæåñòîÿùèì CA. Ïðè ïðîâåðêå ñåðòèôèêàòà Áîáà Àëèñà èñïîëüçóåò ýòè ñåðòèôèêàòû.

Òàêàÿ ñõåìà ïðîäåìîíſòðèðîâàíà íà 21-é. Ñåðòèôèêàò Àëèñû çàâåðåí CA_A, ñåðòèôèêàò Áîáà çàâåðåí $CA_Â$. Àëèñà çíàåò îòêðûòûé êëþ÷ CA_A. Ó CA_C åñòü ñåðòèôèêàò, ïîäïèñàííûé CA_A, ïîýòîìó Àëèñà ìîæåò ïðîâåðèòü ýòî. Ó $CA_Ñ$ åñòü ñåðòèôèêàò, ïîäïèñàííûé CA_D. È ñåðòèôèêàò Áîáà ïîäïèñàí CA_D. Ïîâòîðíûì ïî äðåâó ñåðòèôèêàöèè äî îáùåé òî÷êè, â äàííîì ñëó÷àå CA_D, Àëèñà ìîæåò ïðîâåðèòü ñåðòèôèêàò Áîáà.



Ðèñ. 24-3. Ïðèìåð èåðàðõèè ñåðòèôèêàöèè.

Ñåðòèôèêàòû ìîãóò õðàíèòüñÿ â áàçàõ äàííûõ íà ðàçëè÷íûõ óçëàõ ñåòè. Ïîëüçîâàòåëè ìîãóò ïîñûëàòü èõ äðóã äðóãó. Èñòå÷åíèè ñðîêà äåéſòâèÿ ñåðòèôèêàòà îí äîëæåí áûòü óäàëåí èç âñåõ îáùåäîſòóïíûõ êàòàëîãîâ. Îäíàêî CA, âûäàâøèé ñåðòèôèêàò, äîëæåí ïðîäîëæàòü õðàíèòü åãî îïèſ, êîòîðàÿ ìîæåò ïîòðåáîâàòüſÿ ïðè ðàçðåøåíèè âîçíèêíîõ ñïîðîâ.

Ñåðòèôèêàòû òàêæå ìîãóò áûòü îòîçâàíû, ëèáî èç-çà êîìïðîìåòàöèè êëþ÷à ïîëüçîâàòåëÿ, ëèáî èç-çà òîãî, ÷òî CA áîëüøå íå õî÷åò ïîääåðæàòü ñåðòèôèêàò ïîëüçîâàòåëÿ. Êàæäûé CA äîëæåí ïîääåðæèâàòü ñïèſîê âñåõ îòîçâàííûõ ñåðòèôèêàòîâ, ñðîê äåéſòâèÿ êîòîðûõ åùå íå çàêîí÷èëſ. Êîãäà Àëèſà ïîëó÷àåò íîâûé ſåðòèôèêàò, îíà äîëſíà ïðîâåðèòü, íå áûë ëè îí îòîçâàí. Îíà ìîſåò ïðîâåðèòü áàçó äàííûõ îòîçâàííûõ êëþ÷åé ïî ſàòå, íî ſêîðåé âſſãî îíà ïðîâåðèò ëîêàëüíî êýøèðóåìûé ïåðå÷åíü îòîçâàííûõ ſåðòèôèêàòîâ. Â òàêîé ſèſòåìå îïðåäåëåííî âåðîſòíû çëîíîòðåſëåſëü, îòçûâ ſåðòèôèêàòîâ âîçìîſíî ſâëſſåò ſàìîé ſëàáîé ſòîſüþ

ýòîé ñõåìû.

Ïðîòîêîëû ïðîâåðêè ïîäëèííîñòè

Àëèñå íóæíî ñâÿçàòüñÿ ñ Áîáîì. Ñíà÷àëà îíà èçâëåêàåò èç áàçû äàííûõ **ïîñëåäîâàòåëüíîñòü ñåðòèôèêàöèè** îò Àëèñû äî Áîáà è îòêðûòûé êëþ÷ Áîáà. Â ýòîò ìîìåíò Àëèñà ìîæåò èíèöèèðîâàòü îäíîïðîõîäíûé, äâóõïðîõîäíûé èëè òðåõïðîõîäíûé ïðîòîêîë ïðîâåðêè ïîäëèííîñòè.

Îäíîïðîõîäíûé ïðîòîêîë ïðåäñòàâëÿåò ñîáîé ïðîñòóþ ïåðåäà÷ó äàííûõ Áîáó Àëèñîé. Ïðîòîêîë óñòàíàâëèâàåò ëè÷íîñòè è Àëèñû, è Áîáà, à òàêæå öåëîñòíîñòü èíôîðìàöèè, ïåðåäàâàåìîé Áîáó Àëèñîé. Êðîìå òîãî, îí îáåñïå÷èâàåò çàùèòó îò âñêðûòèÿ ëèíèè ñâÿçè ñ ïîìîùüþ ïîâòîðà.

Â äâóõïðîõîäíîì ïðîòîêîëå äîáàâëåí îòâåò Áîáà. Ïðîòîêîë óñòàíàâëèâàåò, ÷òî èìåííî Áîá, à íå êàêîé-òî ñàìîçâàíåö, ïîñûëàåò îòâåò. Îí òàêæå îáåñïå÷èâàåò áåçîïàñíîñòü îáåèõ ïåðåäà÷ è çàùèùàåò îò âñêðûòèÿ ïîâòîðîì.

È â îäíîïðîõîäíûõ, è â äâóõïðîõîäíûõ àëãîðèòìàõ èñïîëüçóþòñÿ ìåòêè âðåìåíè. Â òðåõïðîõîäíîì ïðîòîêîëå äîáàâëÿåòñÿ åùå îäíî ñîîáùåíèå Àëèñû Áîáó è ïîçâîëÿåò èçáåæàòü ìåòîê âðåìåíè (è, ñëåäîâàòåëüíî, ïðàâèëüíîãî åäèíîãî âðåìåíè).

Îäíîïðîõîäíûé ïðîòîêîë:

(1) Àëèñà ãåíåðèðóåò ñëó÷àéíîå ÷èñëî R_A.

(2) Àëèñà ñîçäàåò ñîîáùåíèå, $M = (T_A, R_A, I_B, d)$, ãäå T_A - ìåòêà âðåìåíè Àëèñû, I_B - èäåíòèôèêàòîð Áîáà, d - ïðîèçâîëüíûå äàííûå. Äëÿ áåçîïàñíîñòè äàííûå ìîãóò áûòü çàøèôðîâàíû îòêðûòûì êëþ÷îì Áîáà E_B.

(3) Àëèñà ïîñûëàåò Áîáó $(C_A, D_A(M))$. (C_A - ýòî ñåðòèôèêàò Àëèñû, D_A - ýòî îáùèé óçåë äåðåâà ñåðòèôèêàöèè.)

(4) Áîá ïðîâåðÿåò C_A è ïîëó÷àåò E_A. Îí ïðîâåðÿåò, ÷òî ñðîê äåéñòâèÿ ýòèõ êëþ÷åé åùå íå èñòåê. (E_A - ýòî îòêðûòûé êëþ÷ Àëèñû.)

(5) Áîá èñïîëüçóåò E_A äëÿ äåøèôðèðîâàíèÿ $D_A(M)$. Ýòèì äåéñòâèåì îí ïðîâåðÿåò è ïîäïèñü Àëèñû, è öåëîñòíîñòü ïîäïèñàííîé èíôîðìàöèè.

(6) Áîá äëÿ òî÷íîñòè ïðîâåðÿåò I_B â M.

(7) Áîá ïðîâåðÿåò T_A â M è óáåæäàåòñÿ, ÷òî ñîîáùåíèå ÿâëÿåòñÿ òåêóùèì.

(8) Äîïîëíèòåëüíî Áîá ìîæåò ïðîâåðèòü R_A â M ïî áàçå äàííûõ ñòàðûõ íîìåðîâ, ÷òîáû óáåäèòüñÿ, ÷òî ñîîáùåíèå íå ÿâëÿåòñÿ ïîâòîðÿåìûì ñòàðûì ñîîáùåíèåì.

Äâóõïðîõîäíûé ïðîòîêîë ñîñòîèò èç îäíîïðîõîäíîãî ïðîòîêîëà è ïîñëåäóþùåãî àíàëîãè÷íîãî îäíîïðîõîäíîãî ïðîòîêîëà îò Áîáà ê Àëèñå. Ïîñëå âûïîëíåíèÿ ýòàïîâ (1)-(8) îäíîïðîõîäíîãî ïðîòîêîëà äâóõïðîõîäíûé ïðîòîêîë ïðîäîëæàåòñÿ ñëåäóþùèì îáðàçîì:

(9) Áîá ãåíåðèðóåò ñëó÷àéíîå ÷èñëî R_B.

(10) Áîá ñîçäàåò ñîîáùåíèå $M' = (T_B, R_B, I_A, R_A, d)$, ãäå T_B - ìåòêà âðåìåíè Áîáà, I_A- èäåíòèôèêàòîð Àëèñû, à d - ïðîèçâîëüíûå äàííûå. Äëÿ áåçîïàñíîñòè äàííûå ìîãóò áûòü çàøèôðîâàíû îòêðûòûì êëþ÷îì Àëèñû $E_{À}$. R_A - ñëó÷àéíîå ÷èñëî Àëèñû, ñîçäàííîå íà ýòàïå (1).

(11) Áîá ïîñûëàåò Àëèñå sends $D_{Â}(M')$.

(12) Àëèñà èñïîëüçóåò E_B, ÷òîáû ðàñøèôðîâàòü $D_{Â}(M')$. Òàêèì îáðàçîì îäíîâðåìåííî ïðîâåðÿþòñÿ ïîäïèñü Áîáà è öåëîñòíîñòü ïîäïèñàííîé èíôîðìàöèè.

(13) Àëèñà äëÿ òî÷íîñòè ïðîâåðÿåò I_A â M'.

(14) Àëèñà ïðîâåðÿåò $T_{Â}$ â M' è óáåæäàåòñÿ, ÷òî ñîîáùåíèå ÿâëÿåòñÿ òåêóùèì.

(15) Äîïîëíèòåëüíî Àëèñà ìîæåò ïðîâåðèòü $R_{Â}$ â M', ÷òîáû óáåäèòüñÿ, ÷òî ñîîáùåíèå íå ÿâëÿåòñÿ ïîâòîðÿìûì ñòàðûì ñîîáùåíèåì.

Òðåõïðîõîäíûé ïðîòîêîë ðåøàåò òó æå ñàìóþ çàäà÷ó, íî áåç ìåòîê âðåìåíè. Ýòàïû (1) - (15) òàêèå æå, êàê â äâóõïðîõîäíîì àëãîðèòìå, íî $T_A = T_{Â} = 0$.

(16) Àëèñà ñâåðÿåò ïîëó÷åííóþ âåðñèþ R_A ñ R_A, êîòîðîå áûëî îòïðàâëåíî Áîáó íà ýòàïå (3).

(17) Àëèñà ïîñûëàåò Áîáó $D_A(R_{Â})$.

(18) Áîá èñïîëüçóåò $E_{À}$, ÷òîáû ðàñøèôðîâàòü $D_{À}(R_{Â})$. Òàêèì îáðàçîì îäíîâðåìåííî ïðîâåðÿþòñÿ ïîäïèñü Àëèñû è öåëîñòíîñòü ïîäïèñàííîé èíôîðìàöèè.

(19) Àëèñà ñâåðÿåò ïîëó÷åííóþ âåðñèþ $R_{Â}$ ñ $R_{Â}$, êîòîðîå áûëî îòïðàâëåíî Àëèñå íà ýòàïå (10).

24.10 Ï î÷òà ñ ïîâûøåíí îé ñåêðåòí îñòüþ PRIVACY-ENHANCED MAIL (PEM)

Ï î÷òà ñ ïîâûøåíí îé ñåêðåòí îñòüþ (Privacy-Enhanced Mail, PEM) ïðåäñòàâëÿò ñîáî ñòàíäàðò Internet äëÿ ïî÷òû ñ ïîâûøåíí îé ñåêðåòí îñòüþ, îäîáðåí Ñîâåòîì ïî àðõèòåêòóðå Internet (Internet Architecture Board, IAB) äëÿ îáåñïå÷åíèÿ áåçîïàñí îñòè ýëåêòðîí íîé ïî÷òû â Internet. Ïðåäâ íà÷àëüíûé âàðèàíò áûë ðàçðàáîòàí Ãðóïïîé ñåêðåòí îñòè è áåçîïàñí îñòè (Privacy and Security Research Group, PSRG) Internet Resources Task Force (IRTF), à çàòåì èõ ðàçðàáîòêà áûëà ïðåäàíà â Ðàáî÷óþ ãðóïïó PEM Internet Engineering Task Force (IETF) PEM Working Group. Ïðîòîêîëû PEM ïðåäíàçíà÷åíû äëÿ øèôðîâàíèÿ, ïðîâåðêè ïîäëèííîñòè, ïðîâåðêè öåëî-ñòí îñòè ñîîáùåíèÿ è óïðàâëåíèÿ êëþ÷àìè.

Ï îëí îñòüþ ïðîòîêîëû PEM ñíà÷àëà áûëè äåòàëüíî îïèñàí û â ðÿäå RFC (Requests for Comment, Çàïðîñû êî ì åíòàðèåâ) â [977] è çàòåì ïåðåñì îòðåí û â [978]. Òðåòüÿ èòåðàöèÿ ïðîòîêîëîâ [979, 827, 980] ñâÿçàíà â [177, 178]. Ïðîòîêîëû áûëè èçìåíåí û è óëó÷øåí û, è îêî í÷àòåëüíûå ïðîòîêîëû äåòàëüíî îïèñûâàþñÿ â äðóãî ì íàáîðå RFC [981, 825, 76, 802]. Â äðóãîé ñòàòüå Ì ýòüþ Áèøîïà (Matthew Bishop) [179] ïîäðîáí î îïèñàí û âñå èçìåíåíèÿ. Ï îïûòíè ðàëëèçàöèè PEM ðàññì àòðèâàþòñÿ â [602, 1505, 1522, 74, 351, 1366, 1367]. Ñì. òàêæå [1394].

PEM ÿâëÿåòñÿ ðàñøèðÿåì û ñòàíäàðòî ì. Ïðîòîêîëû PEM ðàçðàáîòàí û òàê, ÷òîáû áûòü ñî-âì åñòèì û ì ì íîæåñòâî ì ïîäõîäîâ ê óïðàâëåíèþ êëþ÷àì è, âêëþ÷àÿ ñèì åòðè÷íó ñõåì ó è ñìåøàííûå ñõåì û. Ñèì åòðè÷íàÿ êðèïòîãðàôèÿ ïðèìåíÿåòñÿ äëÿ øèôðîâàíèÿ òåêñòà ñîîáùåíèé. Äëÿ êîíôèãóðàöèè ñîîáùåíèé èñïîëüçóþòñÿ êðèïòîãðàô÷åñêèå ñîîáùåíèÿ, ïîääåðæèâàþò ìåõàíèçì óïðàâëåíèÿ êëþ÷àìè ñ ïîì ùüþ ñåðòèôèêàòîâ îêðûòûõ êëþ÷åé, äëãîâðåì åííûõ, ðåæèì îâ è ñâÿçàíí ûõ èäåíòè÷íîñòåé, à òàêæå è ýëåòðîííûå ïîäïèñè, èíôðàñòðóêòóð è ïðîöåäóð óïðàâëåíèÿ êëþ÷àìè.

PEM ïîääåðæèâàåò òîëüêî îòêðûòûé äëãîðèòì, íî ïîçâîëÿåò äîáàâëÿòü è áîëåå ïîçäíèå äëãîðèòì û. Ñîîáùåíèÿ øèôðóþñÿ äëãîðèòì îì DES â ðåæèìå CBC. Ïðîâåðêà ïîäëèííîñòè, îáåñïå÷èâàåì ñðåäñòâîì **Ï ðîâåðêè öåëîñòíîñòè ñîîáùåíèÿ** (Message Integrity Check, MIC), èñïîëüçóåò MD2 èëè MD5. Ñèì åòðè÷íûå óïðàâëåíèå êëþ÷àìè ïðèìåíÿþò DES â ðåæèìå , ëèáî òðîéíîé DES ñ äâóì÷ êëþ÷àìè (òàê íàçûâàåì ûé ðåæèì EDE). Äëÿ óïðàâëåíèÿ êëþ÷àìè PEM òàêæå ïîääåðæèâàþò ñåðòèôèêàòû îêðûòûõ êëþ÷åé, èñïîëüçóÿ RSA (äëèíà êëþ÷à äî 1024 áèòîâ) è ñòàíäàðò X.509 äëÿ ñòðóêòóðû ñåðòèôèêàòîâ.

PEM îáåñïå÷èâàåò òðè ñåðâèñà ïîâûøåíèÿ ñåêðåòí îñòè: êîíôèäåíöèàëüí îñòü, ïðîâåðêà ïîäëèííîñòè è êîí-òðîëü öåëîñòíîñòè ñîîáùåíèé. Ê ýëåìåíòàðí îìó ñëó÷àþ ñèñòåìà íå ïðåäúÿâëÿåòñÿ íèêàêèõ ñïåöèàëüíûõ òðåá-âàíèé. PEM ì îæåò áûòü âñòðîåí â âûñîêîóðîâíåâûå óçëû è ïîääåðæèâàþò ïîëüçîâàòåëé, íå âëèÿÿ íà ðàáîò îñòàëüíîé ñåòè.

Äîêóìåíòû PEM

PEM îïðåäåëÿåòñÿ â ñëåäóþ ùèõ ÷åòûðåõ äîêóìåíòàõ:

— RFC 1421: ×àñòü I, Ïðîöåäóðû øèôðîâàíèÿ è ïðîâåðêè ïîäëèííîñòè ñîîáùåíèé. Â ýòî ì äîêóìåíòå îïðåäåëÿþòñÿ ïðîöåäóðû øèôðîâàíèÿ è ïðîâåðêè ïîäëèííîñòè ñîîáùåíèé, êîòîðûå äîëæíû îáíîâëÿòüñÿ ïî÷òû ñ ïîâûøåííîé ñåêðåòíîñòüþ äëÿ ïåðåäà÷è ýëåêòðîííîé ïî÷òû â Internet.

— RFC 1422: ×àñòü II, Óïðàâëåíèå êëþ÷àìè ñ ïîìîùüþ ñåðòèôèêàòîâ. Â ýòî ì äîêóìåíòå îïðåäåëÿþòñÿ àðõèòåêòóðà è èíôðàñòðóêòóðà óïðàâëåíèÿ êëþ÷àìè, êîòîðûå îñíîâàíû íà ìåòîäå ñåðòèôèêàòîâ îêðûòûõ êëþ÷åé, ïðåäîñòàâëÿþùèõ èíôîðìàöèþ î êëþ÷àõ îïðåäåëåííûõ ïîëüçîâàòåëåé, íå âëèÿÿ íà ðàáîòó îñòàëüíîé ñåòè.

— RFC 1423: ×àñòü III, Àëãîðèòì û, ðåæèì è èäåíòèôèêàòîðû. Ýòîò äîêóìåíò ñîäåðæèò îïðåäåëåíèÿ, ôîðìàòû, ññûëêè è öèòàòû äëÿ êðèïòîãðàôè÷åñêèõ àëãîðèòì îâ, ðåæèì îâ èñïîëüçîâàíèÿ è ñâÿçàííûõ èäåíòèôèêàòîðîâ è ïàðàìåòðîâ.

— RFC 1424: ×àñòü IV, Ñåðòèôèêàöèÿ êëþ÷åé è ðîäñòâåííûå ôóíêöèè. Â ýòî ì äîêóìåíòå îïèñûâàþñÿ òðè òèïà ôóíêöèé, ïîääåðæèâàåì ûõ PEM: ñåðòèôèêàöèÿ êëþ÷åé, õðàíåíèå è èçâëå÷åíèå ñïèñêà îòîçâàííûõ ñåðòèôèêàòîâ (certificate revocation list, CRL).

Ñåðòèôèêàòû

PEM ñîâì åñòèì ñî ñõåìîé ïðîâåðêè ïîäëèííîñòè, îïèñàííóé â [304], ñì. òàêæå [826]. PEM ïðåäñòàâëÿåò ñîáîé íàäì íîæåñòâî X.509, îïðåäåëÿÿ ïðîöåäóðû è ñîãëàøåíèÿ äëÿ èíôðàñòðóêòóðû óïðàâëåíèÿ êëþ÷àìè, èñïîëüçóåìîé ñ PEM è â áóäóùåì äðóãèõ ïðîòîêîëàìè (âêëþ÷àÿ ñòåê TCP/IP è OSI).

Èíôðàñòðóêòóðà óïðàâëåíèÿ êëþ÷àìè èñïîëüçóåò îáùèé êîðåíü äëÿ âñåé ñåðòèôèêàöèè Internet. Öåíòð ðåãè-ñòðàöèîííûé ïîëèòèêè (Internet Policy Registration Authority, IPRA) îïðåäåëÿåò äëîáàëüíóþ ñòðàòåãèþ, ïðèì åíÿþ êî âñåé èåðàðõèè. Íèæå êîðíÿ - IPRA - íàõîäÿòñÿ Öåíòðû ñåðòèôèêàöèîííûé ïîëèòèêè (Policy Certification Authorities, PCA), êàæäûé èç êîòîðûõ îïðåäåëÿåò è îóáëèêîâûâàåò ñâîþ ñòðàòåãèþ ðåãèñòðàöèè ïîëüçîâà-òåëåé è îðãàíèçàöèé. Êàæäûé PCA ñåðòèôèöèðîâàí IPRA. Ñëåäîì çà PCA èäóò CA, ñåðòèôèöèðóþùèå ïîëüçî-

âàòåëåé è è óïðàâëÿþùèå îðãàíèçàöèîííûìè ïîäðàçäåëåíèÿìè (äåïàðòàìåíòàìè, îôèñàìè, äî÷åðíèìè êîìïàíèÿìè). Ïåðâîíà÷àëüíî ïðåäïîëàãàëîñü, ÷òî áîëüøèíñòâî ïîëüçîâàòåëåé áóäåò ðåãèñòðèðîâàòüñÿ â êà÷åñòâå ÷ëåíîâ îðãàíèçàöèé.

Êàê îæèäàëîñü, ðÿä PCA áóäåò îáñëóæèâàòü ñåðòèôèêàöèþ ïîëüçîâàòåëåé, íå âõîäÿùèõ íè â îäíó îðãàíèçàöèþ. Ïðåäïîëàãàåòñÿ âûäåëèòü îäèí èëè íåñêîëüêî PCA äëÿ ðåãèñòðàöèè ïîëüçîâàòåëåé, æåëàþùèõ âîñïîëüçîâàòüñÿ ïðåèìóùåñòâàìè ñåêðåòíîãî PEM è ñîõðàíèòü ñîîòâåòñòâèå ìåæäó PCA áóäåò ïîçâîëÿòü ðåãèñòðèðîâàòü ïîëüçîâàòåëåé, íå æåëàþùèõ ðàñêðûâàòü ñâîè ëè÷íîñòè.

Ñîîáùåíèÿ PEM

Ñåðâåðå PEM ÿâëÿåòñÿ ôîðìàò ñîîáùåíèé. Íà 20-é ïîêàçàíî çàãîëîâî÷íûå ñîîáùåíèå ïðè ñèìâîëüíîì óïðàâëåíèè êëþ÷àìè. Íà 19-é ïîêàçàíî ïîäïèñàííûå è çàøèôðîâàííûå ñîîáùåíèå ïðè óïðàâëåíèè êëþ÷àìè íà áàçå îòêðûòîãî êëþ÷åé, è íà Figure 24.6 ïîêàçàíî ïîäïèñàííîå (íî íåçàøèôðîâàííîå) ñîîáùåíèå ïðè óïðàâëåíèè êëþ÷àìè íà áàçå îòêðûòîãî êëþ÷åé.

```
   -----BEGIN PRIVACY-ENHANCED MESSAGE-----
   Proc-Type: 4,ENCRYPTED
   Content-Domain: RFC822
   DEK-Info: DES-CBC,F8143EDE5960C597
   Originator-ID-Symmetric: schneler@counterpane.com,,
   Recipient-ID-Symmetric: schneler@chinet.com,ptf-kmc,3
   Key-Info                                                                :
DES-ECB,RSA-MD2,9FD3AAD2F2691B9A,B70665BB9BF7CBCDA60195DB94F727D3
   Recipient-lD-Symmetric: penl-dev@tis.com,ptf-kmc,4
   Key-Info :
DES-ECB,RSA-MD2,161A3F75DC82EF26,E2EF532C65CBCFF79F83A2658132DB47
LLrHBOeJzyhP+/fSStdH8okeEnv47jxe7SJ/iN72ohNcUk2jHEUSoHlnvNSIHE9M
8tEjmF/zxB+bATMtPjCUHbz8Er9wloxIkjHUlBEpvXROUrUzYbkNpkOagV2IzUpk
J6UiRRGcDSvzrsoK+oNvqu6z7Xs5Xfz5rDqUcMlKlZ6720dcBHGGsDLpTpSCnpot
   dXd/H5LMDHnonNvPCmQUHt==
   -----END PRIVACY ENHANCED MESSAGE-----
```

Ðèñ. 24-4. Ïðèìåð âñòðîåííîãî ñîîáùåíèÿ (ñèìâîëè÷íûé ñëó÷àé)

```
   -----BEGIN PRIVACY-ENHANCED MESSAGE-----
   Proc-Type: 4,ENCRYPTED
   ContentDomain: RFC822
   DEK-Info: DESCBC,BFF968AA74691AC1
   0riginator - Certificate :
MIIBlTCCAScCAWuwDQYJKoZIhvcNAQECBQAwUTELMAkGAlUEBhMCVVMxIDAeBgNV
BAoTFIJTQSBEYXRhIFNIY3VyaXR5LCBJbmMuMQ8wDQYDVQQLEmZCZXRhIDExDzAN
BgNVBAsTBk5PVEESWTAeFw05MTA5MDQxODM4MTdaFmO5MzA5MDMxODM4MTZaMEUx
CzAJBgNVBAYTAlVTMSAmHgYDVQQKExdSUOEgRGFOYSBTZWNlcmlOeSwgSW5jLjEU
MBIGAIUEAxMLVGVzdCBVc2VyIDEmHTAKBgRVCAEBAglCAANLADBIAkEAwHZHI7i+
yJcqDtjJComzTdBJrdAiLAnSC+CnnjOJEEyuQiBgkGrgIh3j8/xOfM+YrsyFlu3F
LZPVtzlrldhYFJQI DAQABMAOGCSqGSIb3DQEBAgUAAIkACKrOPqphJYwlj+YPtc
iWlFPuN5jJ79Khfg7ASFxskYkEMjRNZV/HZDZQEhtVaU7Jxfzs2mfX5byMp2X3U/
   5XIJXGx7qlJsDgHQGs7Jk9H8CHlfuSHUgN4w==
   Key-Info: RSA,
I3rRIGXUGWAF8js5wCzRTkdh034PTHdRZY9Tuvm03M+NM7fx6qc5uIxps2LrlgO+
   wGrtiUm/ovtKdlnzeZQ/aQ==
   Issuer-Certificate:
MIIB3DCCAUgCAQowDQYJKoZIhvcNAQECBQAwTzELMAkGAIUEBhMCVVMxIDAeBgNV
BAoTFIJTQSBEYXRhIFNIY3VyaXR5LCBJbmMuMQ8mDQYDVQQEEwZCZXRhIDExDTAE
BgNVBAsTBFRMQOEwHhcNOTEmOTAxMDgwMDAwWhcNOTlwOTAxMDclOTU5HjBRMQsw
CQYDVQQGEwJVUzEgMB4GAIUEChMXUINBIERhdGEgU2VjdXJpdHksIEIuYy4xDzAN
BgNVBAsTBkJIdGEgMTEPMAOGAIUECxMGTk9UQVJZMHAmCgYEVQgBAQICArmDYgAm
XwJYCsnp61QCxYykNIODwutF7jMJ3kE+3PjYyHOwk+79rLg6X65B/ED4bJHt05XH
cqAz/7R7XhjYCmOPcqbdzoACZtIIETrKrcJiDYoP+DkZ8klgCk7hQHpbImIDAQAB
MAOGCSqGSIb3DQEBAgUAA38AAICPv4f9Gx/tY4+p+4DB7MV+tKZnvBoy8zgoMGOx
dD2jMZ/3HsyWKHgSFOeH7AJB3qr9zosG47pyMnTf3aSy2nBO7CMxpUHRBcXUpE+x
EREZd9++32ofGBIXaIaInOgVUnOOzSYgugiQO77nJLDUjOhQehCizEs5wUJ35a5h
   MIC-Info: RSA-MD5,RSA,
UdFJR8u/TIGhfH651eeme210H4tooa3vZCvVNGBZirf/7nrgzHDABz8m9NsXSexv
   AjRFbHoNPzBuxwnlOAFeAOHJszE4yBvhG
   Recipient-ID-Asymmetric :
MFExCzAJBgNVBAYTAIVTMSAmHgYDVQQKExdSUOEgRGFOYSBTZHNlcmIOeSwgSH5j
   LjEPMAOGAIUECxMGQftiVOYSAxMQ81tfDQYDVQQLEwZOTIRBUIk=,
   66
   Key-Info: RSA,
06BSIww9CTyHPtS3bMLD+EOhejdvX6QvlHK2ds2sQPEaXhX8EhvVphHYTjmekdHv
   7xOZ3Jx2vTAhOYHMcqqCjA==
qeWlj/YJ2Uf5ng9yznPbtDOmYloSwIuV9FRYx+gzY+81Xd/NQrXHfi6/MhPfPF3d
   jIqCJAxvld2xgqQimUzoSla4r7kQQ5c/Iua4LqKeq3clFzEv7MbZhA==
   -----END PRIVACY ENHANCED MESSAGE-----
```

Ðèñ. 24-5. Ïðèìåð âñòðîåííîãî øèôðîâàííîãî (ENCRYPTED) ñîîáùåíèÿ (àñèììåòðè÷íûé ñëó÷àé).

Ïåðâûì ïîëåì ÿâëÿåòñÿ "Proc-Type", èäåíòèôèêàòîð òèïà îáðàáîòêè, êîòîðîé ïîäâåðãëèñü ñîîáùåíèå. Ñóùåñòâóåò òðè âîçìîæíûõ òèïà ñîîáùåíèé. Ñïåöèôèêàòîð "ENCRYPTED" îáîçíà÷àåò, ÷òî ñîîáùåíèå çàøèôðî-

âàíî è ïîäïèñàíî. Ñïåöèôèêàòîð "MIC-ONLY" è "MIC-CLEAR" óêàçûâàþò, ÷òî ñîîáùåíèå ïîäïèñàíî, íî íå çàøèôðîâàíî. Ñîîáùåíèÿ MIC-CLEAR íå êîäèðóþòñÿ è ìîãóò áûòü ïðî÷èòàíû ñ ïîìîùüþ äðóãîãî, íå âõîäÿùåãî â PEM ïðîãðàììíîãî îáåñïå÷åíèÿ. Äëÿ ïðåîáðàçîâàíèÿ ñîîáùåíèé MIC-ONLY â óäîáî÷èòàåìóþ ôîðìó íåîáõîäèìî ïðîãðàììíîå îáåñïå÷åíèå PEM. Ñîîáùåíèå PEM ïîäïèñûâàåòñÿ âñåãäà, à øèôðîâàíèå íå ÿâëÿåòñÿ îáÿçàòåëüíûì.

Ñëåäóþùåå ïîëå, "Content-Domain", çàäàåò òèï ïî÷òîâîãî ñîîáùåíèÿ. Îíî íå âëèÿåò íà áåçîïàñíîñòü. Ïîëå "DEK-Info" ñîäåðæèò èíôîðìàöèþ î **êëþ÷å îáìåíà äàííûìè** (Data Exchange Key, DEK), äëÿ îïèñàíèÿ êîíêðåòíîãî äëÿ øèôðîâàíèÿ òåêñòà, è ïàðàìåòðàõ, ñâÿçàííûõ ñ äëîðèòìîì øèôðîâàíèÿ. Â íàñòîÿùåå âðåìÿ îïðåäåëåí åäèíñòâåííûé äëîðèòì - DES â ðåæèìå CBC, "DES-CBC" Âòîðîå ïîäïîëå ñîäåðæèò IV. Â áóäóùåì äëÿ PEM ìîãóò áûòü îïðåäåëåíû è äðóãèå äëîðèòìû, èõ èñïîëüçîâàíèå áóäåò çàðåãèñòðèðîâàíî â ïîëå DEK-Info è äðóãèõ ïîëÿõ, îïðåäåëÿþùèõ äëîðèòì.

Â ñîîáùåíèÿõ ñ ñèììåòðè÷íûì óïðàâëåíèåì êëþ÷àìè (ñì. 20th) ñëåäóþùèì ïîëåì áóäåò "Originator-ID-Symmetric" ñ òðåìÿ ïîäïîëÿìè. Ïðåîá ïîäïîëå ñ ïîìîùüþ óíèêàëüíîãî àäðåñà ýëåêòðîííîé ïî÷òû îïðåäåëÿåò îòïðàâèòåëÿ. Âòîðîå ïîëå íå ÿâëÿåòñÿ îáÿçàòåëüíûì è îïðåäåëÿåò îðãàí, âûäàâøèé çàìåíÿåìûé êëþ÷. Òðåòüèì ÿâëÿåòñÿ íåîáÿçàòåëüíîå ïîäïîëå Âåðñèÿ/Îêî÷àíèå ñðîêà.

Äàëåå, ïðè èñïîëüçîâàíèè ñèììåòðè÷íîãî óïðàâëåíèÿ êëþ÷àìè, ó êàæäîãî ïîëó÷àòåëÿ åñòü äâà ïîëÿ: "Recipient-ID-Symmetric" è "Key-Info." Ïîëå "Recipient-ID-Symmetric" ñîäåðæèò òðè ïîäïîëÿ, êîòîðûå îïðåäåëÿþò ïîëó÷àòåëÿ òàêæå, êàê ïîäïîëÿ ïîëÿ "Originator- ID-Symmetric" îïðåäåëÿþò îòïðàâèòåëÿ.

Ïîëå "Key-Info" çàäàåò ïàðàìåòðû óïðàâëåíèÿ êëþ÷àìè. Ó ýòîãî ïîëÿ ÷åòûðå ïîäïîëÿ. Ïåðâîå îïðåäåëÿåò àëãîðèòì, èñïîëüçîâàííûé äëÿ øèôðîâàíèÿ DEK. Òàê êàê â ðàññìàòðèâàåìîì ñîîáùåíèè ïðèìåíÿåòñÿ ñèììåòðè÷íîå óïðàâëåíèå êëþ÷àìè, òî îòïðàâèòåëü è ïîëó÷àòåëü èñïîëüçóþò îäèí è òîò æå êëþ÷. Îí íàçûâàåòñÿ **çàìåíÿåìûì êëþ÷îì** (Interchange Key, IK) è èñïîëüçóåòñÿ äëÿ øèôðîâàíèÿ DEK. DEK ìîæåò áûòü çàøèôðîâàí ëèáî ñ ïîìîùüþ DES â ðåæèìå ECB (ýòî ñïîñîá îáîçíà÷àåòñÿ "DES-ECB"), ëèáî òðîéíûì DES ("DES-EDE"). Âòîðîå ïîäïîëå îïðåäåëÿåò àëãîðèòì MIC. Ìîæåò èñïîëüçîâàòüñÿ MD2 (îáîçíà÷åíî "RSA-MD2") èëè MD5 ("RSA-MD5"). Òðåòüå ïîäïîëå, DEK, è ÷åòâåðòîå ïîäïîëå, MIC, øèôðóþòñÿ ñ ïîìîùüþ IK.

Íà 19-é è 18-é ïîêàçàíû ñîîáùåíèÿ, â êîòîðûõ èñïîëüçóåòñÿ óïðàâëåíèå êëþ÷àìè ñ ïîìîùüþ îòêðûòûõ êëþ÷åé (â ïððå÷íå PEM òàêîé ñïîñîá íàçûâàåòñÿ àñèììåòðè÷íûì). Çàãîëîâêè èçìåíÿþòñÿ. Â ñîîáùåíèÿõ ENCRYPTED ïîñëå ïîëÿ "DEK-Info" èäåò ïîëå "Originator-Certificate". Ôîðìà ñåðòèôèêàòà ñîîòâåòñòâóåò ñòàíäàðòó X.509 (ñì. ðàçäåë 24.9). Ñëåäóþùèì ïîëåì ÿâëÿþòñÿ "Key-Info" ñ äâóìÿ ïîäïîëÿìè. Ïåðâîå ïîäïîëå îòêðûâàåò äëÿ îòïðàâèòåëÿ ñ îòêðûòûì êëþ÷îì, èñïîëüçîâàííûé äëÿ øèôðîâàíèÿ DEK, â íàñòîÿùåå âðåìÿ ïîääåðæèâàåòñÿ òîëüêî RSA. Ñëåäóþùåå ïîäïîëå - DEK, çàøèôðîâàííûé îòêðûòûì êëþ÷îì îòïðàâèòåëÿ. Ýòî íåîáÿçàòåëüíîå ïîëå, êîòîðîå ïîçâîëÿåò îòïðàâèòåëþ ðàñøèôðîâàòü ñâîå ñîáñòâåííîå ïîòîâîå ñèñòåìíîé. Ñëåäóþùèì ïîëåì ÿâëÿåòñÿ "Issuer-Certificate", ñåðòèôèêàò îðãàíèçàöèè, ïîäïèñàâøåé ñåðòèôèêàò îòïðàâèòåëÿ ("Originator-Certificate").

Äàëåå ïðè àñèììåòðè÷íîì óïðàâëåíèè êëþ÷àìè ñëåäóåò ïîëå "MIC-Info". Ïåðâîå ïîäïîëå çàäàåò àëãîðèòì âû÷èñëåíèÿ MIC, à âòîðîå - àëãîðèòì, èñïîëüçîâàííûé äëÿ ïîäïèñè MIC. Òðåòüå ïîäïîëå ñîäåðæèò MIC, ïîäïèñàííûé çàêðûòûì êëþ÷îì îòïðàâèòåëÿ.

```
   -----BEGIN PRIVACY-ENHANCED MESSAGE-----
   Proc-Type: 4,MIC-ONLY
   Content-Domain: RFC822
   Originator - Certificate :
MIIBITCCAScCAHUwDQYJKoZIhvcNAQECBQAwTzELMAkGAIUEBhMCVVMxlDAeBgNV
BAoTFIJTQSBEYXRhIFNIY3VyaXR5LCBJbmMuMQ8wDQYDVQQLEwZCZXRhIDExDzAN
BgNVBAsTBk5PVEFSHTAeEw05MTA5MDQxODM4MTdaFw05MzA5MDMxODM4MTZaMEUx
CzAJBgNVBAYTAIVTMSAwHgYDVQQKExdSUOEgRGFOYSBTZMNlcmlOeSwgSW5jLjEU
MEIGAIUEAxMLVGVzdCBVc2VylDEwHTAKBgRVCAEBAgICAANLADBIAkEAmHZHI71+
yJcqDtjJCowzTdBJrdAiLAnSC+CnnjOJELyuQiBgkGrgIh3j8/xOfM+YrsyFlu3F
LZPVtzlndhYFJQIDAQABMAOGCSqGSIb3DQEBAgUAAIkACKrOPqphJYwlj+YPtcIq
ItJIFPuN5jJ79Khfg7ASFxskYkEMjRNZV/HZDZQEhtVaU7Jxfzs2mfX5bMp2X3U/
   5XUXGx7qusDgHQGs7Jk9W8CW1fuSI4UgN4w==
   Issuer-Certificate:
MIIB3DCCAUgCAQowDQYJKoZIhvcNAQECBQAkTzELMAkGAIUEBhMCVVMxlDAeBgNV
BAoTFIJTQSBEYXRhIFNIY3VyaXR5LCBJbmMuMQ8wDQYDVQQLEIZCZXRhIDExDTAE
BgNVBAsTBFRMQOEwHhcNOTEwOTAxMDgwMDAmkmcNOTImOTAxMDclOTU5HjBRMQsw
CQYDVQQGEwJVUzEgMB4GAIUEChMXUINBIERhdGEgU2VjdXJpdHksIEIuYywxDzAN
BgNVBAsTBkJIdGEgMTEPMAOGAIUECxMGTk9UQVJZMHAwCgYEVQgBAQICArwDYgAw
XwJYCsnpelQCxYkNIODwlltF/jMJ3kE+3PjYjHOwk+/9rEg6X65B7LD4bJHt05XH
cqAz77R7XhjYCmOPcqbdzoACZIlETrKrcJIDYoP+DkZ8klgCk7hQHpbltflDAQAB
MAOGCSqGSIb3DQEBAgUAA38AAICPv4f9Gx7tY4+p+4DB7MV+tKZrlvBo8zgoMGOx
dD2jMZ73Hs*kl4gSFOeH7AJB3qr9zosG47pyMnTf3aS2nBO7CMxpUkfRBcXUpE+x
EREZd9++32otGBIXaIalnOgVUnOOzSYgljglQO77nJEDUOhQehCizEs5mUJ35a5h
   MIC-Info: RSA-MD5,RSA,
jV20fH+nnXHU8bnE8kPAad7mSQITDZIbVuxvZAOVRZ5q5+EjI5bQvqNeqOUNQjr6
   EtE7K2QDeVMCj/XsdJIA8fA==
LSBBIGIIc3NhZ2UgZrti9lHVzZSBpbBOZXNOaH5nLgOKESBGb2xsb3dpbmcgaXMg
   YSBibGFuaj/Bsakf51OgOKDQpUaGIzIGIzIHRoZSBIbrnQuDQo=
   -----END PRIVACY-ENHANCED MESSAGE-----
```

Ðèñ. 24-6. Ïðèìåð âñòðîåííîãî MIC-ONLY ñîîáùåíèÿ (àñèììåòðè÷íûé ñëó÷àé).

Ñëåäóþùèå ïîëÿ ñâÿçàíû ñ ïîëó÷àòåëåì. Êàæäîìó ïîëó÷àòåëþ ñîîòâåòñòâóþò äâà ïîëÿ: "Recipient-ID-Asymmetric" è "Key-Info". Ó ïîëÿ"Recipient-ID-Asymmetric" äâà ïîäïîëÿ. Ïåðâîå îïðåäåëÿåò îðãàí, âûäàâøèé îòêðûòûé êëþ÷ ïîëó÷àòåëÿ, à âòîðûì ÿâëÿåòñÿ íåîáÿçàòåëüíîå ïîäïîëå Âåðñèÿ/Îêîí÷àíèå ñðîêà. Ïîëå "Key-Info" çàäàåò ïðàâèëüíóþ èíôîðìàöèþ, íåîáõîäèìóþ äëÿ øèôðîâàíèÿ ñîîáùåíèÿ, à âòîðûì ïîäïîëåì ñëóæèò DEK, çàøèôðîâàííûé îòêðûòûì êëþ÷îì ïîëó÷àòåëÿ.

Áåçîïàñíîñòü PEM

Äëèíà êëþ÷åé RSA, èñïîëüçóåìûõ â PEM, ìîæåò ìåíÿòüñÿ â äèàïàçîíå îò 508 äî 1024 áèòîâ. Ýòîãî äîñòàòî÷íî ïðàêòè÷åñêè äëÿ ëþáîãî óðîâíÿ áåçîïàñíîñòè. Áîëåå âåðîÿòíî, ÷òî âñêðûòèå áóäåò íàïðàâëåíî ïðîòèâ ïîäáîðà ïàðîëåé ïî îòêðûòîìó êëþ÷ - íå çàïèñûâàéòå åãî íèãäå - èëè ïîïûòàòüñÿ ïîäñóíóòü âàì ôàëüøèâûé îôèöèàëüíûé êëþ÷. Ïðîöåäóðû ñåðòèôèêàöèè êëþ÷åé â PEM äëèíàþò ýòî íåâîçìîæíû, åñëè âñå ïîëüçîâàòåëè ñòðîãî ñëåäóþ ñîîòâåòñòâóþùèì ïðîöåäóðàì, íî, êàê èçâåñòíî, ëþäè ÷àñòî íåâíèìàòåëüíû.

Ìýëîðè ìîæåò ïîñòóïèòü õèððåå è ìîäèôèöèðîâàòü ðåàëèçàöèþ PEM, ðàáîòàþùóþ â âàøåé ñèñòåìå. Ýòà èçìåíåííàÿ âåðñèÿ ìîæåò òàéíî ïåðåíîñèòü Ìýëîðè âñþ âàøó ïî÷òó, çàøèôðîâàâ åå åãî îòêðûòûì êëþ÷îì. Åìó ìîæåò áûòü ïîñëàíà äàæå êîïèÿ âàøåãî çàêðûòîãî êëþ÷à. Åñëè èçìåíåííàÿ ðåàëèçàöèÿ áóäåò ðàíòàöèè õîðîøî, òî âû íèêîãäà íå óçíàåòå, ÷òî ñëó÷èëîñü.

Ðåàëüíîãî ñïîñîáà ïðåäîòâðàòèòü òàêîå âñêðûòèå íå ñóùåñòâóåò. Âû ìîæåòå èñïîëüçîâàòü îäíîíàïðàâëåííóþ õýø-ôóíêöèþ è ïîëó÷èòü êîíòðîëüíóþ ñóììó èñïîëíÿåìîãî êîäà PEM. Çàòåì, ïðè êàæäîì çàïóñêå ïðîãðàììíîãî îáåñïå÷åíèÿ âû ìîæåòå ïðîâåðÿòü êîíòðîëüíóþ ñóììó, ÷òîáû âîâðåìÿ îáíàðóæèòü èçìåíåíèÿ. Íî Ìýëîðè òî÷íî òàêæå ìîæåò èçìåíèòü è êîä êîíòðîëüíîé ñóììû ïðè èçìåíåíèè êîäà PEM. Ìîæíî ñîõðàíèòü êîíòðîëüíóþ ñóììó êîíòðîëüíîé ñóììû, íî Ìýëîðè ìîæåò èçìåíèòü è åå. Åñëè ó Ìýëîðè åñòü äîñòóï ê âàøåìó êîìïüþòåðó, îí ìîæåò ðàçðóøèòü áåçîïàñíîñòü PEM.

Ìîðàëüíî âòîì, ÷òî âû íå äîëæíû äîâåðÿòü íèêàêîìó ýëåìåíòó ïðîãðàììíîãî îáåñïå÷åíèÿ, åñëè âû íå ìîæåòå äîâåðÿòü àïïàðàòóðå, íà êîòîðîé ðàáîòàåò ýòî ïðîãðàììíîå îáåñïå÷åíèå. Äëÿ áîëüøèíñòâà òàêèå îïàñåíèÿ íåîáîñíîâàííûì. Íî äëÿ íåêîòîðûõ ëþäåé îíè âïîëíå ðåàëüíû.

TIS/PEM

Äîâåðåííûå èíôîðìàöèîííûå ñèñòåìû (TIS, Trusted Information Systems), ÷àñòè÷íî ïîääåðæèâàþò Óïðàâëåíèå ïî ïðåäâû íàó÷íûì ïðîåêòàì ïðàêòè÷åñêîãî Ñîâåòíîãî Øòàòîâ, âêëþ÷àþò ðåàëèçàöèþ PEM (TIS/PEM). Ðàçðàáîòàííûå äëÿ ïëàòôîðì UNIX, îíè áûëè òàêæå ïåðåíåñåíû íà VMS, DOS è Windows.

Õîòÿ ñïåöèôèêàöèè PEM îïðåäåëÿþò äëÿ Internet îäèí ãëàâíûé ñåðòèôèêàöèîííûé öåíòð, TIS/PEM ïîääåðæèâàþò ñóùåñòâîâàíèå íåñêîëüêèõ èåðàðõèé ñåðòèôèêàöèè. Óçëû ìîãóò îïðåäåëèòü íàáîð ñåðòèôèêàòîâ, êîòîðûå áóäóò ñ÷èòàòüñÿ äåéñòâèòåëüíûìè, âêëþ÷àÿ ðåãèñòðàöèîííûå óçëû òîãî, ÷òîáû ïîëüçîâàòåëè TIS/PEM óçëó íå íóæíî ïðèñûëàòü ê èåðàðõèè Internet.

Âñå îðãàíèçàöèè è ãðàæäàíå ÑØÀ è Êàíàäû ïðè æåëàíèè ìîãóò ïîëó÷èòü äîñòóï ê TIS/PEM, êîòîðàÿ ðàñïðîñòðàíÿåòñÿ â âèäå èñõîäíîãî êîäà. Çàèíòåðåñîâàííûå ëèöà äîëæíû îáðàùàòüñÿ ïî ñëåäóþùåìó àäðåñó: Privacy-Enhanced Mail, Trusted Information Systems, Inc., 3060 Washington Road IRte. 97), Glenwood, MD 2,1738; (301) 854-6889; fax: (301) 854-5363; Internet: pern-info@tis.com.

RIPEM

RIPEM - ýòî ïðîãðàììà, íàïèñàííàÿ Ìàðêîì Ðèîðäàíîì (Mark Riordan) è ðåàëèçóþùàÿ ïðîòîêîëû PEM. Õîòÿ ýòà ïðîãðàììà íå ÿâëÿåòñÿ ñâîáîäíî äîñòóïíîé, åé ìîæíî âîñïîëüçîâàòüñÿ áåñïëàòíî äëÿ ÷àñòíîãî, íåêîììåð÷åñêîãî èñïîëüçîâàíèÿ. Ëèöåíçèÿ íà åå èñïîëüçîâàíèå âõîäèò â äîêóìåíòàöèþ.

Êîä íå ìîæåò áûòü ýêñïîðòèðîâàí. Êîíå÷íî, çàêîíû ïðàâèòåëüñòâà ÑØÀ íå äåéñòâóþò çà ïðåäåëàìè Ñîåäèíåííûõ Øòàòîâ, è ðÿä ëþäåé èãíîðèðóåò ýêñïîðòíûå ïðàâèëà. Êîä RIPEM äîñòóïåí ïî âñåìó ìèðó íà ýëåêòðîííûõ äîñêàõ îáúÿâëåíèé. Ðàçðåøåíà äëÿ ýêñïîðòà âåðñèÿ, íàçûâàåìàÿ RIPEM/SIC, ðåàëèçóþùàÿ òîëüêî öèôðîâûå ïîäïèñè.

Ê ìîìåíòó íàïèñàíèÿ ýòèõ ñòðîê RIPEM íå ïîëíîñòüþ ðåàëèçîâàëà ïðîòîêîëû PEM, â íåé íåò âîçìîæíîñòè èñïîëüçîâàòü ñåðòèôèêàòû ïðîâåðêè ïîäëèííîñòè êëþ÷åé.

Äî RIPEM Ðèîðäàí íàïèñàë ïîõîæóþ ïðîãðàììó RPEM. Ïîäðàçóìåâàëîñü, ÷òî ýòî áóäåò îáùåäîñòóïíàÿ ïðîãðàììà ýëåêòðîííîé ïî÷òû. Ïûòàÿñü îáîéòè ïàòåíòíûå ïðîáëåìû, Ðèîðäàí èñïîëüçîâàë àëãîðèòì Rabin (ñì. ðàçäåë 19.5). Public Key Partners çàÿâèëà, ÷òî èõ ïàòåíòû ðàñïðîñòðàíÿþòñÿ íà âñþ êðèïòîãðàôèþ ñ îòêðûòûìè êëþ÷àìè. Ïîä óãðîçîé ñóäåáíîãî ïðîöåññà Ðèîðäàí ïðåêðàòèë ðàñïðîñòðàíåíèå ïðîãðàììû.

Ñåé÷àñ RPEM íå èñïîëüçóåòñÿ. Îíà íå ñîâìåñòèìà ñ RIPEM. Òàê êàê ìîæíî èñïîëüçîâàòü RIPEM, íå âñòðå÷àÿ ïðåïÿòñòâèé ñî ñòîðîíû Public Key Partners, íåò ïîâîäà âîçâðàùàòüñÿ ê RPEM.

24.11 Ïðîòîêîë áåçîïàñíîñòè ñîîáùåíèé

Ïðîòîêîë áåçîïàñíîñòè ñîîáùåíèé (Message Security Protocol, MSP) - ýòî âîåííûé ýêâèâàëåíò PEM. Îí áûë ðàçðàáîòàí NSA â êîíöå 80-õ ãîäîâ ïðè ðàáîòå ïî ïðîãðàììå ñîçäàíèÿ Áåçîïàñíîé ñèñòåìû ïåðåäà÷è äàííûõ ïî ñåòè (Secure Data Network System, SDNS) program. Ýòî ñîâìåñòèìûé ñ X.400 ïðîòîêîë óðîâíÿ ïðèëîæåíèÿ äëÿ çàêðûòèÿ ýëåêòðîííîé ïî÷òû. MSP ïëàíèðóåòñÿ èñïîëüçîâàòü â ðàçðàáàòûâàåìîé ñåòè îáîðîííûõ ñîîáùåíèé (Defense Message System, DMS) Ìèíèñòåðñòâà îáîðîíû.

Ïðåäâàðèòåëüíûé ïðîòîêîë áåçîïàñíîñòè ñîîáùåíèé (Preliminary Message Security Protocol, PMSP), êîòîðûé ïðåäïîëàãàåòñÿ èñïîëüçîâàòü äëÿ "íåñåêðåòíûõ, íî âàæíûõ" ñîîáùåíèé, ïðåäñòàâëÿåò ñîáîé àäàïòèðîâàííóþ äëÿ èñïîëüçîâàíèÿ ñ X.400 è TCP/IP âåðñèþ MSP. Ýòîò ïðîòîêîë òàêæå íàçûâàþò Mosaic.

Êàê è PEM, ïðîãðàììíûå ðåàëèçàöèè MSP è PMSP äîñòàòî÷íî ãèáêè, èõ êîíñòðóêöèÿ ïîçâîëÿåò ïîäñòðîèòüñÿ ïîä èñïîëüçîâàíèå ðàçëè÷íûõ àëãîðèòìîâ äëÿ îñóùåñòâëåíèÿ ôóíêöèé áåçîïàñíîñòè, òàêèõ êàê ïîäïèñü, õýøèðîâàíèå è øèôðîâàíèå. PSMP áóäåò ðàáîòàòü ñ ìèêðîñõåìîé Capstone (ñì. ðàçäåë 24.17).

24.12 PRETTY GOOD PRIVACY (PGP)

Pretty Good Privacy (PGP, âåñüìà õîðîøàÿ ñåêðåòíîñòü) - ýòî ñâîáîäíî ðàñïðîñòðàíÿåìàÿ ïðîãðàììà áåçîïàñíîé ýëåêòðîííîé ïî÷òû, ðàçðàáîòàííàÿ Ôèëèïïîì Öèììåðìàííîì (Philip Zimmermann) [1652]. Äëÿ øèôðîâàíèÿ äàííûõ îíà èñïîëüçóåò IDEA, äëÿ óïðàâëåíèÿ êëþ÷àìè è öèôðîâîé ïîäïèñè - RSA (äëèíà êëþ÷à äî 2047 áèòîâ), à äëÿ îäíîíàïðàâëåííîãî õýøèðîâàíèÿ - MD5.

Äëÿ ïîëó÷åíèÿ ñëó÷àéíûõ îòêðûòûõ êëþ÷åé PGP èñïîëüçóåò âåðîÿòíîñòíóþ ïðîâåðêó ÷èñåë íà ïðîñòîòó, èñïîëüçóÿ äëÿ ïîëó÷åíèÿ ñòàðòîâûõ ïîñëåäîâàòåëüíîñòåé èíòåðâàëû ìåæäó íàæàòèÿìè ïîëüçîâàòåëåì êëàâèø íà êëàâèàòóðå. PGP ãåíåðèðóåò ñëó÷àéíûå êëþ÷è IDEA ñ ïîìîùüþ ìåòîäà, â ANSI X9.17, Appendix C (ñì. ðàçäåë 8.1) [55], èñïîëüçóÿ âìåñòî DES â êà÷åñòâå ñèììåòðè÷íîãî àëãîðèòìà IDEA. PGP òàêæå øèôðóåò çàêðûòûé êëþ÷ ïîëüçîâàòåëÿ ñ ïîìîùüþ õýøèðîâàííîé ïàðîëüíîé ôðàçû, à íå ïàðîëÿ íåïîñðåäñòâåííî.

Ñîîáùåíèÿ, çàøèôðîâàííûå PGP, èìåþò íåñêîëüêî óðîâíåé áåçîïàñíîñòè. Åäèíñòâåííàÿ âåùü, èçâåñòíàÿ êðèïòîàíàëèòèêó î çàøèôðîâàííîì ñîîáùåíèè, - ýòî ïîëó÷àòåëü ñîîáùåíèÿ ïðè óñëîâèè, ÷òî êðèïòîàíàëèòèêó èçâåñòåí ID êëþ÷à ïîëó÷àòåëÿ. Òîëüêî ðàñøèôðîâàâ ñîîáùåíèå, ïîëó÷àòåëü óçíàåò, êåì îíî ïîäïèñàíî, åñëè îíî ïîäïèñàíî. Ýòî ðåçêî îòëè÷àåòñÿ îò ñîîáùåíèÿ PEM, â çàãîëîâêå êîòîðîãî íåìàëî èíôîðìàöèè îá îòïðàâèòåëå, ïîëó÷àòåëå è ñàìîì ñîîáùåíèè õðàíèòñÿ â íåçàøèôðîâàííîì âèäå.

Ñàìîé èíòåðåñíîé îñîáåííîñòüþ PGP ÿâëÿåòñÿ ðàñïðåäåëåííûé ïîäõîä ê óïðàâëåíèþ êëþ÷àìè (ñì. ðàçäåë 8.12). Öåíòðîâ ñåðòèôèêàöèè êëþ÷åé íåò, âìåñòî ýòîãî â PGP ïîääåðæèâàåòñÿ "ñåòü äîâåðèÿ". Êàæäûé ïîëüçîâàòåëü ñàì ñîçäàåò è ðàñïðîñòðàíÿåò ñâîé îòêðûòûé êëþ÷. Ïîëüçîâàòåëè ïîäïèñûâàþò êëþ÷è äðóã äðóãà, ñîçäàâàÿ âçàèìîñâÿçàííîå ñîîáùåñòâî ïîëüçîâàòåëåé PGP.

Íàïðèìåð, Àëèñà ìîæåò ôèçè÷åñêè ïåðåäàâàòü Áîáó ñâîé îòêðûòûé êëþ÷. Áîá ëè÷íî çíàåò Àëèñó, ïîýòîìó îí

ïîäïèñûâàåò åå îòêðûòûé êëþ÷. Îäíó ïîäïèñàíóþ êîïèþ îí âîçâðàùàåò Àëèñå, à äðóãóþ îñòàâëÿåò. Êîãäà Àëèñå íóæíî ñâÿçàòüñÿ ñ Êýðîë, îíà ïîñûëàåò Êýðîë ïîäïèñàíóþ Áîì êîïèþ êëþ÷à. Êýðîë, ó êîòîðîé êàêèì-òî îáðàçîì óæå åñòü êëþ÷ Áîáà (îíà ïîëó÷èëà åãî ðàíüøå), è êîòîðàÿ äîâåðÿåò Áîáó çàâåðèò êëþ÷ äðóãîãî ÷åëîâåêà, ïðîâåðÿåò åãî ïîäïèñü ïîä êëþ÷îì Àëèñû è óâåæäàåòñÿ, ÷òî îíà ïðàâèëüíà. Òàêèì îáðàçîì, Áîá çíàêîìèò Àëèñó è Êýðîë.

PGP íå îïðåäåëÿåò ñòðàòåãèþ óñòàíîâêè äîâåðèòåëüíûõ ñâÿçåé, ïîëüçîâàòåëè ñàìè ðåøàþò, êîìó âåðèòü, à êîìó íåò. PGP îáåñïå÷èâàåò ìåõàíèçìû äëÿ ïîääåðæêè àññîöèàòèâíîãî äîâåðèÿ îòêðûòûì êëþ÷àì è äëÿ èñïîëüçîâàíèÿ äîâåðèÿ. Êàæäûé ïîëüçîâàòåëü õðàíèò íàáîð ïîäïèñàííûõ îòêðûòûõ êëþ÷åé â âèäå ôàéëà **êîëüöà îòêðûòûõ êëþ÷åé** (public-key ring). Êàæäûé êëþ÷ êîëüöà îáëàäàåò ïîëåì çàêîíîííîñòè êëþ÷à, îïðåäåëÿþùèì óðîâíåì äîâåðèÿ ê êëþ÷ó êîíêðåòíîãî ïîëüçîâàòåëÿ. ×åì áîëüøå óðîâíåì äîâåðèÿ, òåì áîëüøå ïîëüçîâàòåëü óâåðåí â çàêîííîñòè êëþ÷à. Ïîëå äîâåðèÿ ê ïîäïèñè èçìåðÿò, íàñêîëüêî ïîëüçîâàòåëü âåðèòî÷íî, êòî ïîäïèñàë îòêðûòûå êëþ÷è äðóãèõ ïîëüçîâàòåëåé. È íàêîíåö ïîëå äîâåðèÿ ê âëàäåëüöó êëþ÷à çàäàåò óðîâåíü, îïðåäåëÿþùèé, íàñêîëüêî êîíêðåòíûé ïîëüçîâàòåëü âåðèò âëàäåëüöó êëþ÷à, ïîäïèñàâøåìó äðóãèå îòêðûòûå êëþ÷è. Ýòî ïîëå âðó÷íóþ óñòàíàâëèâàåòñÿ ïîëüçîâàòåëåì. PGP íåïðåðûâíî îáíîâëÿåò ýòè ïîëÿ ïî ìåðå ïîÿâëåíèÿ íîâîé èíôîðìàöèè.

Íà 17-é ïîêàçàíî, êàê âûãëÿäèò ýòà ìîäåëü äëÿ êîíêðåòíîãî ïîëüçîâàòåëÿ, Àëèñû. Êëþ÷ Àëèñû íàõîäèòñÿ â ñàìîì âåðõó èåðàðõèè, âëàäåëåö êëþ÷à àáñîëþòíî íàäåæåí. Àëèñà ïîäïèñûâàåò êëþ÷è Áîáà, Êýðîë, Äýéâà, Ýëåí è Ôðýíêà. Îíà äîâåðÿåò Áîáó è Êýðîë ïîäïèñûâàòü îòêðûòûå êëþ÷è äðóãèõ ëþäåé, êðîìå òîãî, îíà ÷àñòè÷íî äîâåðÿåò Äýéâó è Ýëåí ïîäïèñûâàòü îòêðûòûå êëþ÷è äðóãèõ ëþäåé. È îíà äîâåðÿåò Ãåéë ïîäïèñûâàòü îòêðûòûå êëþ÷è äðóãèõ ëþäåé, õîòÿ ñàìà íå ïîäïèñûâàëà êëþ÷ Ãåéë.

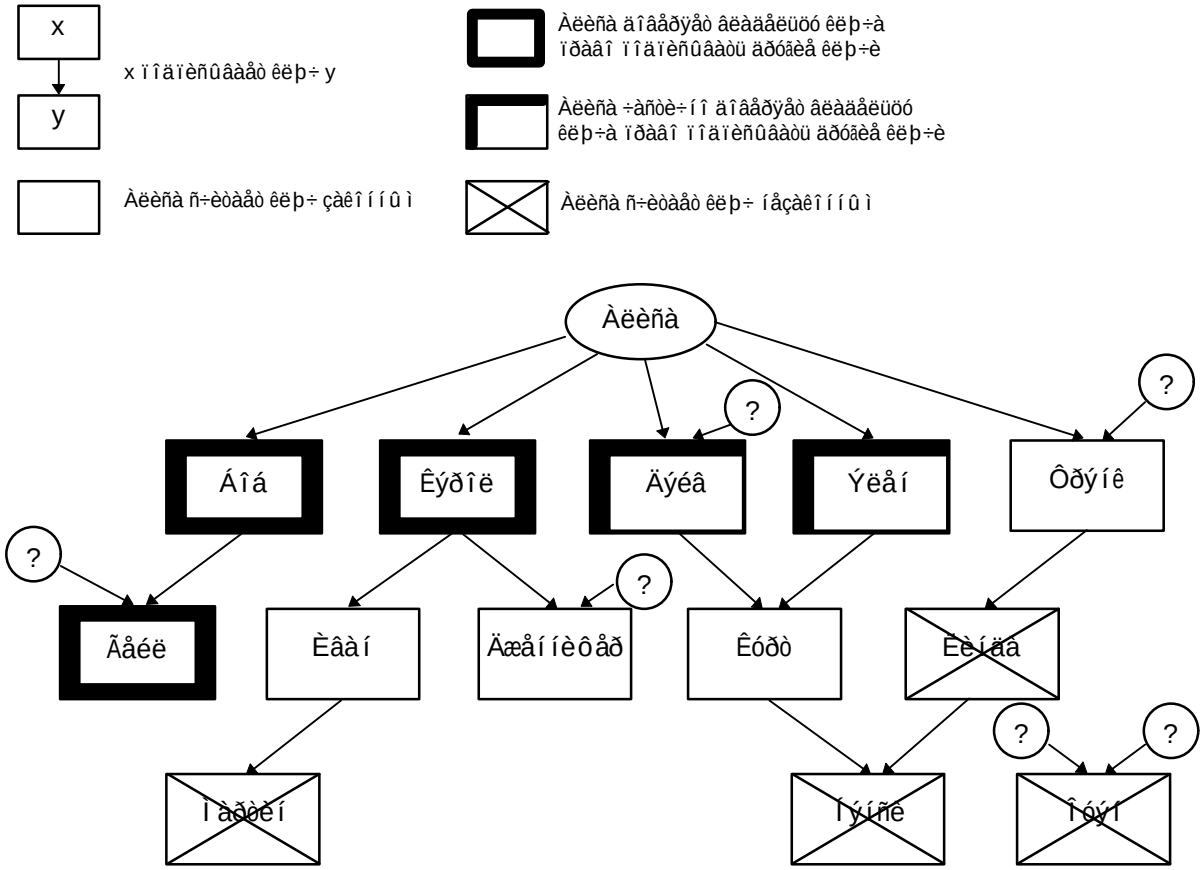
Äâóõ ÷àñòè÷íî äîâåðÿåìûõ ïîäïèñåé ìîæåò îêàçàòüñÿ äîñòàòî÷íûì äëÿ ñðåäíèõ êëþ÷à. Àëèñà ñ÷èòàåò, ÷òî êëþ÷ Êðóòà çàêîíåí, òàê êàê Äýéâ è Ýëåí ïîäïèñàëè åãî. Óðîâåíü äîâåðèÿ óñòàíàâëèâàåòñÿ â PGP âðó÷íóþ, Àëèñà ìîæåò âûáðàòü óñòðàíèòü ïðàêòè÷åñêè ëþáóþ åå ñòåïåíü ïàðàíîéè.

Àëèñà íå äîëæíà àâòîìàòè÷åñêè äîâåðÿòü êëþ÷àì äóãèõ ëþäåé òîëüêî ïîòîìó, ÷òî îíè ïîäïèñàíû êëþ÷îì, êîòîðûé íà÷èòàò ïîäâåëüíûì. Àëèñà Îíà íå äîâåðÿåò Ôðýíêó Îíà ïîäïèñûâàòü äðóãèå êëþ÷è, õîòÿ îíà ñîáñòâåííîðó÷íî ïîäïèñûâàëà åãî êëþ÷. Êðîìå òîãî, îíà íå äîâåðÿåò ïîäïèñè Èâàíà ïîä êëþ÷îì Ìàðèíà èëè ïîäïèñè Êóðòà ïîä êëþ÷îì.

Êëþ÷ Îóíà âîîáùå íà âõîäè â ñåòü, ìîæåò áûòü, Àëèñà ïîëó÷èëà åãî òò ñåðâåðà. PGP íå ñ÷èòàåò êëþ÷ àâòîìàòè÷åñêè ïðàâèëüíûì, Àëèñà äîëæíà ëèíî îáúÿâèòü î ïðàâèëüíîñòè êëþ÷à, ëèíî ðåøèòüñÿ ïîâåðèòü îäíîìó èç òåõ, êòî ïîäïèñàë êëþ÷.

Êîíå÷íî, íè÷òî íå ìåøàåò Àëèñå èñïîëüçîâàòü êëþ÷è, êîòîðûì îíà íå äîâåðÿåò. Çàäà÷à PGP - ïðåäóïðåäèòü Àëèñó î ïîäîçðèòåëüíîñòè êëþ÷à, à íå ïîìåøàòü åé óñòàíàâëèâàòü ñîâåðøåííóþ.

Ñàìûì ñëàáûì çâåíîì ýòîé ñèñòåìû ÿâëÿåòñÿ îòçûâ êëþ÷åé: ãàðàíòèðîâàòü, ÷òî êòî-íèáóäü íå âîñïîëüçóåòñÿ ñêîìïðîìåòèðîâàííûì êëþ÷îì, íåâîçìîæíî. Åñëè çàêðûòûé êëþ÷ Àëèñû óêðàäåí, îíà ìîæåò ïîñëàòü **ñåðòèôèêàò îòçûâà êëþ÷à** (key revocation certificate), íî, òàê êàê íåò ðàñïðåäåëåíèÿ êëþ÷åé óæå ïðîçîøëî, íåëüçÿ ãàðàíòèðîâàòü, ÷òî ýòî ñîîáùåíèå áóäåò ïîëó÷åíî âñåìè, èñïîëüçóþùèìè åå òêðûòûé êëþ÷ â ñâîåì êîëüöå êëþ÷åé. È òàê êàê Àëèñà äîëæíà áóäåò ïîäïèñàòü ñâîé ñåðòèôèêàò îòçûâà êëþ÷à ñâîèì çàêðûòûì êëþ÷îì, òî åñëè îíà ïîòåðÿåò êëþ÷, îíà íå ñìîæåò è îòîçâàòü åãî.



Ðèñ. 24-7. Ì îäåëü äîâåðèÿ â PGP.

Òåêóùåé âåðñèåé PGP ÿâëÿåòñÿ 2.6.2. Ï îÿâëåíèå íîâîé âåðñèè, PGP 3.0, îæèäàåòñÿ ê êîíöó 1995 ãîäà. Â 3.0 âêëþ÷åíû îïöèè òðîéíîãî DES, SHA, äðóãèå àëãîðèòìû ñ îòêðûòûì êëþ÷àìè, ðàçäåëåíèå ïàð "îòêðûòûé êëþ÷/çàêðûòûé êëþ÷" äëÿ øèôðîâàíèÿ è äëÿ ïîäïèñè, ðàñøèðåíèå ïðîòîêîëà îáìåíà êëþ÷åé, óëó÷øåíèå óïðàâëåíèÿ êîëüöîì êëþ÷åé, API äëÿ èíòåãðèðîâàíèÿ PGP â äðóãèå ïðîãðàììû è ïîëíîöåííàíûå èñïîëíÿåìûå ìîäóëè.

PGP äîñòóïíà äëÿ MS-DOS, UNIX, Macintosh, Amiga è Atari. Â ëè÷íûõ íåêîìåð÷åñêèõ öåëÿõ åå ìîæíî èñïîëüçîâàòü ñâîáîäíî, ñêà÷àâ ñî ìíîãèõ óçëîâ ftp â Internet. ×òîáû ñêîïèðîâàòü PGP ñ óçëà MIT ñ ïîìîùüþ telnet ïîäêëþ÷èòåñü ê net-dist.mit.edu, âîéäèòå â ñèñòåìó êàê getpgp, îòâåòüòå íà âîïðîñû, çàéäèòå â êàòàëîã, óêàçàííûé â ñåññèè telnet. Ýòó ïðîãðàììó òàêæå ìîæíî ïîëó÷èòü ftp.ox.ac.uk, ftp.dsi.unimi.it, ftp.funet.fi, ftp.demon.co.uk, CompuServe, AOL, è ò.ï. Äëÿ êîìåð÷åñêîãî èñïîëüçîâàíèÿ â ÑØÀ PGP ìîæíî ïðèîáðåñòè - ïîëíîñòüþ, âìåñòå ñ ëèöåíçèåé - ïðèìåðíî çà 100 äîëëàðîâ â êîìïàíèè ViaCrypt, 9033 N 24th Ave., Phoenix, AZ, 85021; (602) 944-0773; viacrypt@acm.org. Ñóùåñòâóþò ðàçëè÷íûå ñðåäñòâà, ïîìîãàþùèå èíòåãðèðîâàòü PGP â MS-DOS, Microsoft Windows, Macintosh è UNIX.

Î PGP íàïèñàíî íåñêîëüêî êíèã [601,1394,1495]. Èñõîäíûé êîä áûë äàæå îïóáëèêîâàí â ïå÷àòíîì âèäå â [1653] ïðè ïîìîùè îáû÷íîãî ÑØÀ, êîòîðûé ïðîäëæàåò ñ÷èòàòü, ÷òî èñõîäíûé êîä ìîæíî ýêñïîðòèðîâàòü òîëüêî â áóìàæíîì, à íå â ýëåêòðîííîì âèäå. Åñëè âû äîâåðÿåòå IDEA, PGP ïîçâîëèò âàì ïðèáëèçèòüñÿ ê âîâëå÷åííîìó óðîâíþ øèôðîâàíèÿ.

24.13 Èíòåëëåêòóàëüíûå êàðòî÷êè

Èíòåëëåêòóàëüíàÿ êàðòî÷êà ïðåäñòàâëÿåò ñîáîé ïëàñòèêîâóþ êàðòî÷êó, ïî ðàçìåðó è ôîðìå êàê êðåäèòíàÿ êàðòî÷êà, ñ âñòðîåííîé êîìïüþòåðíîé ìèêðîñõåìîé. Èäåÿ ñòàðà - ïðåâûå ïàðîëüíûå äëÿ 20 òîìó íàçàä - íî èç-çà ïðàêòè÷åñêèõ îãðàíè÷åíèé âîçìîæíîñòü ðåàëèçîâàòü òàêèå êàðòî÷êè ïîÿâèëàñü òîëüêî ïðèìåíî íåäàâíî. Ñ òåõ ïîð íèêòî ñòàëè ïîïóëÿðíû, ãëàâíûì îáðàçîì â Åâðîïå. Âî ìíîãèõ ñòðàíàõ èíòåëëåêòóàëüíûå êàðòî÷êè èñïîëüçóþòñÿ äëÿ îïëàòû çà òåëåôîí. Ñóùåñòâóþò èíòåëëåêòóàëüíûå êðåäèòíûå êàðòî÷êè, èíòåëëåêòóàëüíûå äåáåòíûå êàðòî÷êè, èíòåëëåêòóàëüíûå êàðòî÷êè äëÿ ÷åî óãîäíî. Àìåðèêàíñêèå êîìïàíèè îïâûñèëè êðåäèòíûõ êàðòî÷åê ðàáîòàþò íàä òåõíîëîãèåé, è ÷åðåç íåñêîëüêî ëåò äàæå çàõâàòèëè àìåðèêàíñêèé óðûíîê èíòåëëåêòóàëüíûå êàðòî÷êè â ñâîèõ óìàæíèêàõ.

Èíòåëëåêòóàëüíàÿ êàðòî÷êà ñîäåðæèò ìèêðîïðîöåññîð (îáû÷íî 8-áèòîâûé ìèêðîïðîöåññîð), ÎÇÓ (÷åòâåðòè êèëîáàéòà), ÏÇÓ (ïðîãðàììèðóåìîå 6-8 êèëîáàéò), è íåñêîëüêî êèëîáàéò ëèáî EPROM (ñòèðàåìîå ïðîãðàììèðóåìîå ÏÇÓ) èëè EEPROM (ýëåêòðîííî ñòèðàåìîå ïðîãðàììèðóåìîå ÏÇÓ). Îáû÷íà ïàìÿòè â èíòåëëåêòóàëü-

íûõ êàðòî÷êàõ ñëåäóþùåãî ïîêîëåíèÿ íàâåðíÿêà âîçðàñòåò, íî îïðåäåëåííûå ôèçè÷åñêèå îãðàíè÷åíèÿ çàòðóäíÿò òàêèå ðàñøèðåíèÿ. Êàðòî÷êà èñïîëüçóåò ñâîþ îïåðàöèîííóþ ñèñòåìó, ïðîãðàììû è äàííûå. (×åãî â íåé íåò, òàê ýòî èñòî÷íèêà ïèòàíèÿ, ýëåêòðîýíåðãèÿ ïîäàåòñÿ, êîãäà êàðòî÷êó âñòàâëÿþò â ñ÷èòûâàòåëü.) Êàðòî÷êà áåçîïàñíà. Â íàøåì ìåíÿþùåìñÿ ìèðå, êîãäà íåëüçÿ äîâåðÿòü ÷óæîìó êîìïüþòåðó, òåëåôîíó, äà ÷åìó óãîäíî, âû ìîæåòå áûòü óâåðåíû â ñâîåé êàðòî÷êå, êîòîðàÿ õðàíèòñÿ â âàøåì áóìàæíèêå.

Â èíòåëëåêòóàëüíûõ êàðòî÷êàõ ìîãóò èñïîëüçîâàòüñÿ ðàçëè÷íûå êðèïòîãðàôè÷åñêèå ïðîòîêîëû è àëãîðèòìû. Îíè ìîãóò áûòü ýëåêòðîííûì êîøåëüêîì, äàâàÿ âîçìîæíîñòü òðàòèòü è ïîëó÷àòü ýëåêòðîííûå íàëè÷íûå. Êàðòî÷êè ìîãóò èñïîëüçîâàòüñÿ â ïðîòîêîëàõ ïðîâåðêè ïîäëèííîñòè ñ íóëåâûì çíàíèåì, îíè ìîãóò îáëàäàòü ñîáñòâåííûìè êëþ÷àìè øèôðîâàíèÿ. Âîçìîæíî, îíè ïîçâîëÿþò ïîäïèñûâàòü äîêóìåíòû èëè ñíèìàòü áëîêèðîâêó ñ êîìïüþòåðíûõ ïðîãðàìì.

Íåêîòîðûå èíòåëëåêòóàëüíûå êàðòî÷êè ñ÷èòàþòñÿ óñòîé÷èâûìè ê âçëîìó, òàêèì îáðàçîì ñåáÿ ÷àñòî çàùèùàþò îðãàíèçàöèè, ýìèòèðîâàâøèå êàðòî÷êè. Áàíê âîâñå íå õî÷åò, ÷òîáû âû ìîãëè âëåçòü â èõ èíòåëëåêòóàëüíóþ êàðòî÷êó è íà÷èñëèòü ñåáå ïîáîëüøå äåíåã.

Èíòåëëåêòóàëüíûå êàðòî÷êè - ýòî î÷åíü èíòåðåñíàÿ òåìà, íà êîòîðóþ íàïèñàíî ìíîæåñòâî ëèòåðàòóðû. Õîðîøåé îáçîðíîé ñòàòüåé ïî êðèïòîãðàôèè â èíòåëëåêòóàëüíûõ êàðòî÷êàõ ìîæåò ñëóæèòü [672]. Åæåãîäíî ïðîâîäÿòñÿ êîíôåðåíöèè: CARTES â îêòÿáðå â Ïàðèæå è CardTech â àïðåëå â Âàøèíãòîíå, îêðóã Êîëóìáèÿ. Òðóäû äâóõ äðóãèõ êîíôåðåíöèé ïî èíòåëëåêòóàëüíûì êàðòî÷êàì ìîæíî íàéòè â [342, 382]. Â îáëàñòè èíòåëëåêòóàëüíûõ êàðòî÷åê ñóùåñòâóþò ñîòíè ïàòåíòîâ, ÷àñòüþ ïðèíàäëåæàùèå åâðîïåéñêèì êîìïàíèÿì. Èíòåðåñíûå âîïðîñû áóäóùåãî èñïîëüçîâàíèÿ èíòåëëåêòóàëüíûõ êàðòî÷åê - ïðîâåðêà öåëîñòíîñòè, àóäèòîðñêèé êîíòðîëü, çàùèòà îò êîïèðîâàíèÿ, ýëåêòðîííûå íàëè÷íûå, îïëàòà ïî÷òîâûõ ðàñõîäîâ - îïèñàíû â [1628].

24.14 Ñòàíäàðòû êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè

Ñòàíäàðòû êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè (Public-Key Cryptography Standards, PKCS) - ýòî ïîïûòêà êîìïàíèè RSA Data Security, Inc îáåñïå÷èòü ïðîìûøëåííûé ñòàíäàðò äëÿ êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè. Ïî òðàäèöèè òàêèìè äåëàìè çàíèìàëñÿ ANSI, íî, ó÷èòûâàÿ òåêóùóþ ñèòóàöèþ â êðèïòîãðàôè÷åñêîé ïîëèòèêå, RSADSI ðåøèëà, ÷òî ëó÷øå îíè âñå ñäåëàþò ñàìè. Ðàáîòàÿ ñî ìíîæåñòâîì êîìïàíèé, RSADSI ðàçðàáîòàëà íàáîð ñòàíäàðòîâ. Íåêîòîðûå èç íèõ ñîâìåñòèìû ñ äðóãèìè ñòàíäàðòàìè, à íåêîòîðûå - íåò.

Ýòè ñòàíäàðòû íå ÿâëÿþòñÿ ñòàíäàðòàìè â îáùåïðèíÿòîì ñìûñëå ýòîãî ñëîâà, íèêòî íå ñîáèðàëñÿ è íå ãîëîñîâàë çà PKCS. Ïî ñâîèì ñîáñòâåííûì ñëîâàì RSADSI "áóäåò åäèíñòâåííîé îðãàíèçàöèåé, ïðàâîìî÷íîé ïðèíèìàòü ðåøåíèÿ î êàæäîì ñòàíäàðòå, è áóäåò ïåðåñìàòðèâàòü ýòè ñòàíäàðòû ïî ìåðå íåîáõîäèìîñòè " [803].

Äàæå ýòî óæå ñîâñåì. Åñëè âû íåóâåðåíû, êàêèå ñòðóêòóðû äàííûõ è ñèíòàêñèñ èñïîëüçîâàòü ïðè ïðîãðàììèðîâàíèè êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè, ýòè ñòàíäàðòû íå õóæå êàêèõ-ëèáî äðóãèõ. Ê òîìó æå, òàê êàê ýòî íå íàñòîÿùèå ñòàíäàðòû, âû ìîæåòå ïîäñòðîèòü èõ ïîä ñâîè íóæäû.

Äàëåå ïðèâåäåíî êðàòêîå îïèñàíèå êàæäîãî PKCS (PKCS #2 è PKCS #4 áûëè âêëþ÷åíû â PKCS #l).

PKCS #l [1345] îïèñûâàåò ñïîñîá øèôðîâàíèÿ è äåøèôðèðîâàíèÿ RSA, ãëàâíûì îáðàçîì äëÿ ñîçäàíèÿ öèôðîâûõ ïîäïèñåé è öèôðîâûõ êîíâåðòîâ, îïèñàííûõ â PKCS #7. Äëÿ öèôðîâûõ ïîäïèñåé ñîîáùåíèå õýøèðóåòñÿ, à çàòåì õýø-çíà÷åíèå øèôðóåòñÿ çàêðûòûì êëþ÷îì ïîäïèñûâàþùåãî. Ñîâìåñòíîå ïðåäñòàâëåíèå ñîîáùåíèÿ è õýø-çíà÷åíèÿ ïîäðîáíî îïèñàíî â in PKCS #7. Äëÿ öèôðîâûõ êîíâåðòîâ (øèôðîâàííûå ñîîáùåíèÿ) ñîîáùåíèå ñíà÷àëà øèôðóåòñÿ ñèììåòðè÷íûì àëãîðèòìîì, à çàòåì êëþ÷ ñîîáùåíèé øèôðóåòñÿ îòêðûòûì êëþ÷îì ïîëó÷àòåëÿ. Ñîâìåñòíîå ïðåäñòàâëåíèå øèôðîâàííîãî ñîîáùåíèÿ è øèôðîâàííîãî êëþ÷à äîëæíî ñîîòâåòñòâîâàòü PKCS #7. Ýòè äâà ìåòîäà ñîâìåñòèìû ñî ñòàíäàðòàìè PEM. Äëÿ ñòðóêòóðû ñåðòèôèêàòîâ (èëè èõ ïîäîáèÿ) îòêðûòûõ è çàêðûòûõ êëþ÷åé RSA è òðåõ àëãîðèòìîâ ïîäïèñè - MD2 è RSA, MD4 è RSA, MD5 è RSA - PKCS #l òàêæå îïèñûâàåò ñèíòàêñèñ, èäåíòè÷íûé ñèíòàêñèñó X.509 è PEM.

PKCS #3 [1346] îïèñûâàåò ñïîñîá ðåàëèçàöèè îáìåíà êëþ÷àìè ïî ñõåìå Diffie-Hellman.

PKCS #5 [1347) îïèñûâàåò ñïîñîá øèôðîâàíèÿ ñîîáùåíèé ñåêðåòíûì êëþ÷îì, ïîëó÷åííûì èç ïàðîëÿ. Ñòàíäàðò èñïîëüçóåò MD2 èëè MD5 äëÿ ïîëó÷åíèÿ êëþ÷à èç ïàðîëÿ è øèôðóåò ñîîáùåíèÿ ñ ïîìîùüþ DES â ðåæèìå CBC. Ýòîò ìåòîä ïðåäíàçíà÷åí ãëàâíûì îáðàçîì äëÿ øèôðîâàíèÿ çàêðûòûõ êëþ÷åé ïðè èõ ïåðåäà÷å îò îäíîé êîìïüþòåðíîé ñèñòåìû äðóãîé, íî ìîæåò áûòü èñïîëüçîâàí è äëÿ øèôðîâàíèÿ ñîîáùåíèé.

PKCS #6 [1348] îïèñûâàåò ñòàíäàðòíûé ñèíòàêñèñ ñåðòèôèêàòîâ îòêðûòûõ êëþ÷åé. Ñèíòàêñèñ ÿâëÿåòñÿ íàäìíîæåñòâîì ñåðòèôèêàòà X.509, ïðè íåîáõîäèìîñòè ìîæíî èçâëå÷ü è ñåðòèôèêàò X.509. Äîïîëíèòåëüíûå àòðèáóòû íå îãðàíè÷èâàþò ïðîöåññ ñåðòèôèêàöèè òîëüêî îòêðûòûì êëþ÷îì. Îíè ñîäåðæàò è äðóãóþ èíôîðìàöèþ, íàïðèìåð, àäðåñ ýëåêòðîííîé ïî÷òû.

PKCS # 7 [1349] ïðåäñòàâëÿåò ñîáîé îáùèé ñèíòàêñèñ äëÿ ïîäïèñûâàåìûõ èëè øèôðóåìûõ äàííûõ, íàïðèìåð, öèôðîâûõ ïîäïèñåé èëè öèôðîâûõ êîíâåðòîâ. Ñèíòàêñèñ ÿâëÿåòñÿ ðåêóðñèâíûì, ïîýòîìó ìîæíî îðãàíèçîâàòü âëîæåííîñòü êîíâåðòîâ èëè ïîñòàâèòü ÷üþ-òî ïîäïèñü ïîä ðàíåå çàøèôðîâàííûìè äàííûìè. Ñèíòàêñèñ òàêæå ðàçðåøàåò âìåñòå ñ ñîäåðæàíèåì ñîîáùåíèÿ ïðîâåðêó ïîäëèííîñòè äðóãèõ àòðèáóòîâ, íàïðèìåð, ìåòîê

âðåìåíè. PKCS #7 ñ PEM, ïîýòîìó ïîäïèñàííûå è çàøèôðîâàííûå ñîîáùåíèÿ ìîãóò áûòü ïðåîáðàçîâàíû â ñîîáùåíèÿ PEM, è íàîáîðîò, áåç äîïîëíèòåëüíûõ êðèïòîãðàôè÷åñêèõ îïåðàöèé. Äëÿ óïðàâëåíèÿ êëþ÷àìè ñ ïîìîùüþ ñåðòèôèêàòîâ PKCS #7 ìîæåò ïîääåðæèâàòü ìíîæåñòâî àðõèòåêòóð - îäíîé èç íèõ ÿâëÿåòñÿ PEM.

PKCS #8 [1350] îïèñûâàåò ñèíòàêñèñ èíôîðìàöèè î çàêðûòûõ êëþ÷àõ, âêëþ÷àÿ çàêðûòûé êëþ÷ è íàáîð àòðèáóòîâ, è ñèíòàêñèñ øèôðîâàííûõ çàêðûòûõ êëþ÷åé. Äëÿ øèôðîâàíèÿ èíôîðìàöèè î çàêðûòûõ êëþ÷àõ ìîæíî èñïîëüçîâàòü PKCS #5.

PKCS #9 [1351] îïðåäåëÿåò èçáðàííûå òèïû àòðèáóòîâ äëÿ ðàñøèðåííûõ ñåðòèôèêàòîâ PKCS #6, ñîîáùåíèé ñ öèôðîâîé ïîäïèñüþ PKCS #7 è èíôîðìàöèè î çàêðûòûõ êëþ÷àõ PKCS #8.

PKCS #10 [1352,] îïèñûâàåò ñòàíäàðòíûé ñèíòàêñèñ çàïðîñà ñåðòèôèêàöèè. Ñåðòèôèêàöèÿ âêëþ÷àåò èíäèâèäóàëüíîå èìÿ, îòêðûòûé êëþ÷ è (íåîáÿçàòåëüíî) íàáîð àòðèáóòîâ, êîòîðûå ïîäïèñàíû ëèöîì, ïðèñûëàþùèì çàïðîñ. Çàïðîñû ñåðòèôèêàöèè ïðèñûëàþòñÿ â ñåðòèôèöèðóþùèé îðãàí, êîòîðûé ïðåîáðàçóåò çàïðîñ ëèáî â ñåðòèôèêàò îòêðûòîãî êëþ÷à X.509, ëèáî â ñåðòèôèêàò PKCS #6.

PKCS #11 [1353], Ñòàíäàðò API êðèïòîãðàôè÷åñêîé ìåòêè (Cryptographic Token API Standard) , îïðåäåëÿåò èíòåðôåéñ ïðîãðàììèðîâàíèÿ, íàçûâàåìûé "Cryptoki", äëÿ ïîðòàòèâíûõ êðèïòîãðàôè÷åñêèõ óñòðîéñòâ âñåõ òèïîâ. Cryptoki ïðåäñòàâëÿåò ñîáîé îáîáùåííóþ ëîãè÷åñêóþ ìîäåëü, ïîçâîëÿþùóþ ïðèëîæåíèÿì âûïîëíÿòü êðèïòîãðàôè÷åñêèå îïåðàöèè íà ïîðòàòèâíûõ óñòðîéñòâàõ, íå çíàÿ äåòàëåé èñïîëüçóåìîé òåõíîëîãèè. Ýòîò ñòàíäàðò òàêæå îïðåäåëÿåò ïðîôèëè ïðèëîæåíèÿ: íàáîðû àëãîðèòìîâ, êîòîðûå ìîæåò ïîääåðæèâàòü óñòðîéñòâî.

PKCS #12 [1354] îïèñûâàåò ñèíòàêñèñ õðàíåíèÿ â ïðîãðàììíîì îáåñïå÷åíèè îòêðûòûõ êëþ÷åé ïîëüçîâàòåëåé, çàùèùåííûõ çàêðûòûõ êëþ÷åé, ñåðòèôèêàòîâ è äðóãîé ñâÿçàííîé êðèïòîãðàôè÷åñêîé èíôîðìàöèè. Öåëüþ ýòîãî ÿâëÿåòñÿ ñòàíäàðòèçàöèÿ åäèíîãî ôàéëà êëþ÷åé, èñïîëüçóåìîãî ìíîãèìè ïðèëîæåíèÿìè.

Ýòè ñòàíäàðòû âñåñòîðîííè, íî íå âñåîáúåìëþùè. Ìíîãèå âîïðîñû îñòàëèñü çà ïðåäåëàìè ýòèõ ñòàíäàðòîâ: ïðîáëåìà ïðèñâîåíèÿ èìåí, íåêðèïòîãðàôè÷åñêèå âîïðîñû, êàñàþùèåñÿ ñåðòèôèêàöèè, äëèíû êëþ÷åé è óñëîâèÿ äëÿ ðàçëè÷íûõ ïàðàìåòðîâ. PKCS ïðèçâàíû îáåñïå÷èòü ôîðìàò ïåðåäà÷è äàííûõ, îñíîâàííîé íà êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè, è èíôðàñòðóêòóðó, ïîääåðæèâàþùóþ òàêóþ ïåðåäà÷ó.

24.15 Óíèâåðñàëüíàÿ ñèñòåìà ýëåêòðîííûõ ïëàòåæåé

Óíèâåðñàëüíàÿ ñèñòåìà ýëåêòðîííûõ ïëàòåæåé (Universal Electronic Payment System, UEPS) ïðåäñòàâëÿåò ñîáîé áàíêîâñêîå ïðèëîæåíèå, èñïîëüçóþùåå èíòåëëåêòóàëüíûå êàðòî÷êè, ïåðâîíà÷àëüíî ðàçðàáîòàííîå äëÿ ñåëüñêîé Þæíîé Àôðèêè, íî ïîçäíåå ïðèíÿòîå îñíîâíûìè áàíêîâñêèìè ãðóïïàìè ýòîé ñòðàíû. Ê íà÷àëó 1995 ãîäà â ÞÀÐ áûëî âûïóùåíî îêîëî 2 ìèëëèîíîâ êàðòî÷åê. Ýòà ñèñòåìà òàêæå ïðèíÿòà â Íàìèáèè, è ðàçâåðòûâàåòñÿ ïî êðàéíåé ìåðå îäíèì ðîññèéñêèì áàíêîì.

Ñèñòåìà ïîçâîëÿåò èñïîëüçîâàòü áåçîïàñíûå äåáèòíûå êàðòî÷êè, ïîäõîäÿùèå äëÿ ðåãèîíîâ, â êîòîðûõ ïëîõàÿ òåëåôîííàÿ ñåòü äåëàåò íåâîçìîæíîé äèàëîãîâóþ ïðîâåðêó. Êàðòî÷êè åñòü è ó ïîêóïàòåëåé, è ó ïðîäàâöîâ, ïîêóïàòåëè ìîãóò èñïîëüçîâàòü ñâîè êàðòî÷êè äëÿ ïåðåâîäà äåíåã ïðîäàâöàì. Ïðîäàâåö ìîæåò âîñïîëüçîâàòüñÿ ñâîåé êàðòî÷êîé, ÷òîáû ïîçâîíèòü â áàíê è ïîìåñòèòü äåíüãè íà ñâîé áàíêîâñêèé ñ÷åò, ïîêóïàòåëü ìîæåò âîñïîëüçîâàòüñÿ ñâîåé êàðòî÷êîé, ÷òîáû ïîçâîíèòü â áàíê è ïåðåâåñòè äåíüãè íà ñâîþ êàðòî÷êó. Íåò íåîáõîäèìîñòè çàáîòèòüñÿ îá àíîíèìíîñòè, íóæíî îáåñïå÷èòü òîëüêî çàùèòó îò ìîøåííè÷åñòâà.

Âîò êàê âûãëÿäèò ïðîòîêîë ñâÿçè ìåæäó ïîêóïàòåëåì Àëèñîé è ïðîäàâöîì Áîáîì (Â äåéñòâèòåëüíîñòè, Àëèñà è Áîá ïðîñòî âñòàâëÿþò ñâîè êàðòî÷êè â ìàøèíó è îæèäàþò âûïîëíåíèÿ òðàíçàêöèè.) Êîãäà Àëèñà âïåðâûå ïîëó÷àåò ñâîþ êàðòî÷êó, îíà ïîëó÷àåò è ïàðó êëþ÷åé, K_1 è K_2, áàíê âû÷èñëÿåò èõ, èñïîëüçóÿ åå èìÿ è íåêîòîðóþ ñåêðåòíóþ ôóíêöèþ. Òîëüêî â êàðòî÷êè ïðîäàâöîâ âñòðîåíû ñåêðåòíûå ñðåäñòâà, íåîáõîäèìûå äëÿ âû÷èñëåíèÿ êëþ÷åé ïîëüçîâàòåëåé.

(1) Àëèñà ïîñûëàåò Áîáó ñâîå èìÿ, A, åãî èìÿ, B, è ñëó÷àéíîå ÷èñëî R_A, øèôðóÿ èõ ñ ïîìîùüþ DES: ñíà÷àëà êëþ÷îì K_2, çàòåì K_1. Îíà òàêæå ïîñûëàåò ñâîå èìÿ îòêðûòûì òåêñòîì.

$$A, E_{K_1}(E_{K_2}(A,B,R_A))$$

(2) Áîá âû÷èñëÿåò K_1 è K_2 ïî èìåíè Àëèñû. Îí ðàñøèôðîâûâàåò ñîîáùåíèå, óáåæäàåòñÿ, ÷òî A è B ïðàâèëüíû, çàòåì øèôðóåò íåçàøèôðîâàííóþ âòîðóþ ïîëîâèíó ñîîáùåíèÿ Àëèñû êëþ÷îì K_2.

$$E_{K_2}(A,B,R_A)$$

Áîá íå ïîñûëàåò ýòî ñîîáùåíèå Àëèñå, 56 áèòîâ øèôðîòåêñòà ñòàíîâÿòñÿ êëþ÷îì K_3. Áîá ïîñûëàåò Àëèñå ñâîå èìÿ, åå èìÿ è ñëó÷àéíîå ÷èñëî, R_B, øèôðóÿ èõ ñ ïîìîùüþ DES: ñíà÷àëà êëþ÷îì K_3, çàòåì K_1.

$$E_{K_1}(E_{K_3}(B,A,R_{\hat{A}}))$$

(3) Àëèñà àíàëîãè÷íûì îáðàçîì âû÷èñëÿåò K_3 è ðàñøèôðîâûâàåò ñîîáùåíèå Áîáà, óáåæäàÿñü, ÷òî A è B ïðà-

âèëüíû, çàòåì øèôðóåò íåçàøèôðîâàííóþ âòîðóþ ïîëîâèíó ñîîáùåíèÿ ÁÎáà êëþ÷îì K_3.

$$E_{K_3}(B,A,R_A)$$

Àëèñà íå ïîñûëàåò ýòî ñîîáùåíèå ÁÎáó, 56 áèòîâ øèôðîâàííîñòè ñòàíäàðòíûì êëþ÷îì K_4. Çàòåì Àëèñà ïîñûëàåò ÁÎáó ñâîå èìÿ, åãî èìÿ ïðîâåðî÷íîå çíà÷åíèå C. Ýòî ïðîâåðî÷íîå çíà÷åíèå ñîäåðæèò èìåíà îòïðàâèòåëÿ è ïîëó÷àòåëÿ, äàòó, êîíòðîëüíóþ ñóììó, êîëè÷åñòâî è äâà MAC. Âñå ýòî øèôðóåòñÿ DES: ñíà÷àëà êëþ÷îì K_4, çàòåì K_1. Îäèí èç MAC ìîæåò áûòü ïðîâåðåí áàíêîì Àëèñû, à âòîðîé ìîæåò áûòü ïðîâåðåí òîëüêî ðàñ÷åòíî-êàññîâûì öåíòðîì. Àëèñà óìåíüøàåò ñâîé ñ÷åò íà ñîòâåòñòâóþùåå çíà÷åíèå.

$$E_{K_1}(E_{K_4}(A,B,\tilde{N}))$$

(4) Áîá àíàëîãè÷íûì îáðàçîì âû÷èñëÿåò K_4. Ïðè óñïåøíîì ñîâïàäåíèè, ÷òî âñå èìåíà ñîâïàäàþò, è ïðàâèëüíî âûïîëíåíà ïðîâåðêà, îí ïðèíèìàåò ïëàòåæ.

Âåëèêîëåïíûì íîâîââåäåíèåì â ýòîì ïðîòîêîëå ÿâëÿåòñÿ òî, ÷òî êàæäîå ñîîáùåíèå çàâèñèò îò ïðåäûäóùåãî. Êàæäîå ñîîáùåíèå âûñòóïàåò óâåëè÷åíèåì *âñåõ* ïðåäûäóùèõ ñîîáùåíèé. Ýòî îçíà÷àåò, ÷òî ïîâòîðèòü ñòàðîå ñîîáùåíèå íèêîìó íå óäàñòñÿ, ïîëó÷àòåëü ïðîñòî íèêîãäà íå ðàñøèôðóåò åãî. Ì íå íðàâèòñÿ ýòà èäåÿ, è ÿ óâåðåí, ÷òî îíà ïîëó÷èò øèðîêîå ïðèìåíåíèå, êàê òîëüêî ñòàíåò øèðîêî èçâåñòíà.

Äðóãîé ðàçíîíé âåùüþ â ýòîì ïðîòîêîëå - íàâÿçûâàíèå ïðàâèëüíîé ðåëèçàöèè. Åñëè ðàçðàáîò÷èê ïðèëîæåíèÿ íåïðàâèëüíî ðåàëèçóåò ïðîòîêîë, îí ïðîñòî íå áóäåò ðàáîòàòü.

Îáå êàðòî÷êè ñîõðàíÿþò çàïèñè êàæäîé òðàíçàêöèè. Êîãäà êàðòî÷êè ðàíî èëè ïîçäíî óñòàíîâÿò äèàëîãîâîå ñîåäèíåíèå ñ áàíêîì (ïðîãðàììà - ïîëíæèòü äåíüãè íà ñ÷åò, à ïîêóïàòåëü - ñíÿòü ñî ñ÷åòà), áàíê èçâëå÷åò ýòè çàïèñè äëÿ ïîñëåäóþùåãî êîíòðîëÿ.

Àïïàðàòóðà èçãîòàâëèâàåòñÿ óñòîé÷èâîé ê âçëîìó, ÷òîáû ïîìåøàòü ëþáîìó èç ó÷àñòíèêîâ èñïîðòèòü äàííûå. Àëèñà íå ñìîæåò èçìåíèòü çíà÷åíèå ñâîåé êàðòî÷êè. Ï îäîáíàÿ çàïèñü çàùèùàåòñÿ è çàïå÷àòûâàåòñÿ ñâîåé ïîäïèñüþ - êëþ÷è MAC â êàðòî÷êàõ ïîêóïàòåëåé, ôóíêöèè äëÿ ïðîâåðçîâàíèÿ èìåí ïîëüçîâàòåëåé â K_1 è K_2 - íî ñ÷èòàòñÿ, ÷òî ðåøåíèå îáðàòíîé çàäà÷è äëÿ ýòèõ ñåêðåòîâ äîñòàòî÷íî òðóäíî.

Ýòà ñõåìà, êîíå÷íî æå, íåñîâåðøåííà, íî îíà áåçîïàñíåå áóìàæíûõ ÷åêîâ è îáû÷íûõ äåíåæíûõ êàðòî÷åê. Èñòî÷íèêîì óãðîçû ìîøåííè÷åñòâà ÿâëÿþòñÿ íå âîâíóå ðàäè, à ïîêóïàòåëè è ïðîäàâöû. UEPS ïðåäîñòàâëÿåò çàùèòó îò òàêèõ çëîóïîòðåáëåíèé.

Îáìåí ñîîáùåíèÿ ÿâëÿåòñÿ ïðåêðàñíûì ïðèìåðîì óñòîé÷èâîãî ïðîòîêîëà: Â êàæäîì ñîîáùåíèè ïðèñóòñòâóþò èìåíà îáåèõ ñòîðîí, âêëþ÷àÿ èíôîðìàöèþ, óíèêàëüíóþ äëÿ ñîîáùåíèÿ, êàæäîå ñîîáùåíèå ÿâíûì îáðàçîì çàâèñèò îò âñåõ ïðåäûäóùèõ.

24.16 CLIPPER

Ìèêðîñõåìà Clipper (èçâåñòíàÿ òàêæå êàê MYK-78T) - ýòî ðàçðàáîòàííàÿ â NSA, óñòîé÷èâàÿ ê âçëîìó ìèêðîñõåìà, ïðåäíàçíà÷åííàÿ äëÿ øèôðîâàíèÿ ïåðåãîâîðíûõ ãîëîñîâ. Ýòî îäíà èç äâóõ ñõåì, ðàâèëçóþùèõ ïðàâèòåëüñòâåííûé Ñòàíäàðò óñëîâíîãî øèôðîâàíèÿ (Escrowed Encryption Standard, EES) [1153]. VLSI Technologies, Inc. èçãîòîâëåíà ìèêðîñõåìó, à Mykotronx, Inc. çàïðîãðàììèðîâàëà åå. Ñíà÷àëà âñå ìèêðîñõåìû Clipper áóäóò âõîäèòü â Ååçîïàñíîå òåëåôîííîå óñòðîéñòâî Model 3600 AT&T (ñì. ðàçäåë 24.18). Ì èêðîñõåìà ðåàëèçóåò äëîðèì øèôðîâàíèÿ Skipjack (ñì. ðàçäåë 13.12,), ðàçðàáîòàííûé NSA ñåêðåòíûé àëãîðèòì ñ øèôðîâàíèåì ñåêðåòíûì êëþ÷îì, òîëüêî â ðåæèìå OFB.

Ñàìûì ïðîòèâîðå÷èâûì ìîìåíòîì ìèêðîñõåìû Clipper, è EES â öåëîì, ÿâëÿåòñÿ ïðîòèâîðå÷èâîñòü êëþ÷åé (ñì. ðàçäåë 4.14). Ó êàæäîé ìèêðîñõåìû åñòü ñïåöèàëüíûé, íåíóæíûé äëÿ ñîîáùåíèé, êëþ÷. Ýòîò êëþ÷ èñïîëüçóåòñÿ äëÿ øèôðîâàíèÿ êîíöà ñîîáùåíèé êàæäîãî ïîëüçîâàòåëÿ. Â õîäå ïðîöåññà ñèíõðîíèçàöèè ïðåäàþùàÿ ìèêðîñõåìà Clipper ãåíåðèðóåò è ïîñûëàåò ïðèíèìàþùåé Ïîëå äîñòóïà äëÿ âûïîëíåíèÿ çàêîíà (Law Enforcement Access Field, LEAF). LEAF ñîäåðæèò êîíåö òåêóùåãî ñåàíñîâîãî êëþ÷à, çàøèôðîâàííîãî ñïåöèàëüíûì êëþ÷îì (íàçûâàåìûì **êëþ÷îì ìîäóëÿ**). Ýòî ïîçâîëÿåò ïðàâèòåëüñòâåííûì ïîñëóøèâàòåëüíûì ïðîñëóøèâàíèåì ïîëó÷èòü ñâîé êëþ÷ è ðàñøèôðîâàòü îòêðûòûé òåêſò ðàçãîâîðà.

Ï î ñëîâàì äèðåêòîðà NIST [812]:

Ïðåäóñìàòðèâàåòñÿ, ÷òî ñèſòåìà "ñ óſëîâíî âðó÷åííûì êëþ÷îì" îáåſïå÷èò èſïîëüçîâàíèå ìèêðîſõåìû Clipper äëÿ çàùèſòû çàêîííſïſñëóſíûõ àìåðèêàíöåâ. Â êàæäîì óſòðîſñòâå, ſïäðæàùåì ìèêðîſõåìó áóäåò ââà óſíèêàëüſûõ "êëþ÷à", äâà ſ÷ſëà, êſòîðûå ſſſàâſáſÿſſſ óſſëſſſſſ÷åſſûſ ſðàâèòåëſſòâåſſſûſ îðãàíàì äëÿ åſøèſðèſðîâàſíèÿ ſſſáſùåſíèé, çàøſſðſſâàſſſûſ óſòðſſéſòâſ. Sðſ èçãſòſâëſíèſ óſòðſſéſòâà îáà êëþ÷à áóäóò ſſſåſùåſûſ ſſðſçſſ â ââóſ áàçàſ äàſſſûſ " óſſëſâſſ âðó÷åſſûſ êëþ÷åé", êſſòſſſèëðóåſſûſ Ååſåðàëſûſ ſðſêſðſſſ. Äſſòóſ ê ýòſſ êëþ÷àſ áóäåò ðàçðåøåſ òſſëſêſ ſðàâſòåëſſòâſſſûſ ÷ſſſâſêàſ ſ çàſſſſûſ ðàçðåøåſſſſ ſſäêſëþ÷ſòſſ ſſäſëſøſſâàþ ùåå óſòðſſéſòâſ.

Ïðàâèòåëüñòâî òàêæå ñîáèðàåòñÿ ïîîùðÿòü øèðîêîå ðàñïðîñòðàíåíèå òàêèõ òåëåôîííûõ àïïàðàòîâ, íî íèêòî íå çíàåò, ÷òî ìîæåò ïðîèçîéòè ñ áàçàìè äàííûõ óñëîâíî âðó÷åííûõ êëþ÷åé.

Ïîìèìî ïîëèòè÷åñêèõ àñïåêòîâ, ñòîèò ïîãîâîðèòü è î âíóòðåííåé ñòðóêòóðå LEAF [812, 1154, 1594, 459, 107, 462]. LEAF - ýòî ñòðîêà, âêëþ÷àþùàÿ äîñòàòî÷íî èíôîðìàöèè, ÷òîáû ïðè îáåñïå÷åíèè ïðàâîïîðÿäêà ìîæíî áûëî ðàñêðûòü ñåàíñîâûé êëþ÷ K_s ïðè óñëîâèè, ÷òî äâà **óñëîâíî ïîëó÷èâøèõ êëþ÷è ó÷ðåæäåíèÿ** áóäóò äåéñòâîâàòü ñîîáùà. LEAF ñîäåðæèò 32-áèòîâûé èäåíòèôèêàòîð ìîäóëÿ U, óíèêàëüíûé äëÿ êàæäîé ìèêðîñõåìû Clipper. Îíî òàêæå ñîäåðæèò òåêóùèé 80-áèòîâûé ñåàíñîâûé êëþ÷, çàøèôðîâàííûé óíèêàëüíûì êëþ÷îì ìîäóëÿ ìèêðîñõåìû K_U, è 16-áèòîâóþ êîíòðîëüíóþ ñóììó C, íàçûâàåìóþ èäåíòèôèêàòîðîì óñëîâíîãî âðó÷åíèÿ. Êîíòðîëüíàÿ ñóììà ïðåäñòàâëÿåò ñîáîé ôóíêöèþ ñåàíñîâîãî êëþ÷à, IV è âîçìîæíî äðóãîé èíôîðìàöèè. Ýòè òðè ïîëÿ øèôðóþòñÿ ôèêñèðîâàííûì îáùèì êëþ÷îì K_F, îáùèì äëÿ âñåõ âçàèìîäåéñòâóþùèõ ìèêðîñõåì Clipper. Îáùèé êëþ÷, èñïîëüçóåìûå ðåæèìû øèôðîâàíèÿ, äåòàëè êîíòðîëüíîé ñóììû è òî÷íàÿ ñòðóêòóðà LEAF çàñåêðå÷åíû. Âîçìîæíî ýòî ïîëå ïîõîæå íà ÷òî-òî ïîäîáíîå:

$$E_{K_F}(E_{K_U}(K_s,U,C))$$

K_U ââîäèòñÿ â ìèêðîñõåìû Clipper ïðè èçãîòîâëåíèè. Ýòîò êëþ÷ çàòåì ðàçäåëÿåòñÿ (ñì. ðàçäåë 3.5) è õðàíèòñÿ â äâóõ áàçàõ äàííûõ óñëîâíî âðó÷åííûõ êëþ÷åé, îõðàíÿåìûõ äâóìÿ ðàçëè÷íûìè ó÷ðåæäåíèÿìè.

×òîáû Åâà ìîãëà èçâëå÷ü K_s èç LEAF, îíà äîëæíà ñíà÷àëà ðàñøèôðîâàòü LEAF êëþ÷îì K_F è ïîëó÷èòü U. Çàòåì îíà äîëæíà ïîëó÷èòü ïîñòàíîâëåíèå ñóäà äëÿ êàæäîãî èç ó÷ðåæäåíèé óñëîâíîãî âðó÷åíèÿ, êàæäîå èç êîòîðûõ âîçâðàùàåò ïîëîâèíó K_U äëÿ äàííîãî U. Åâà âûïîëíÿåò XOR îáåèõ ïîëîâèí è ïîëó÷àåò K_U, çàòåì îíà èñïîëüçóåò K_U äëÿ ïîëó÷åíèÿ K_s, è K_s - äëÿ ïîäñëóøèâàíèÿ ðàçãîâîðà.

Êîíòðîëüíàÿ ñóììà äîëæíà ïîìåøàòü íàðóøåíèþ ýòîé ñõåìû, ïðèíèìàþùàÿ ìèêðîñõåìà Clipper íå ìîæåò âûïîëíèòü äåøèôðèðîâàíèå, åñëè êîíòðîëüíàÿ ñóììà íåïðàâèëüíà. Îäíàêî ñóùåñòâóåò ëèøü 2^{16} âîçìîæíûõ çíà÷åíèé êîíòðîëüíîé ñóììû, è ôàëüøèâîå LEAF ñ ïðàâèëüíîé êîíòðîëüíîé ñóììîé, íî íåïðàâèëüíûì êëþ÷îì, ìîæåò áûòü íàéäåíî ïðèìåðíî çà 42 ìèíóòû [187]. Íî ýòî íå î÷åíü ïîìîæåò ïîäñëóøàòü ðàçãîâîð, âåäóùèéñÿ ñ ïîìîùüþ Clipper. Òàê êàê ïðîòîêîë îáìåíà êëþ÷àìè íå ÿâëÿåòñÿ ÷àñòüþ ìèêðîñõåìû Clipper, 42-ìèíóòíîå âñêðûòèå ãðóáîé ñèëîé äîëæíî áûòü âûïîëíåíî ïîñëå îáìåíà êëþ÷àìè, îíî íå ìîæåò áûòü âûïîëíåíî äî òåëåôîííîãî çâîíêà. Òàêîå âñêðûòèå ìîæåò ðàáîòàòü ïðè ïåðåäà÷å ôàêñîâ èëè ïðè èñïîëüçîâàíèè êàðòî÷êè Fortezza (ñì. ðàçäåë 24.17).

Ïðåäïîëîæèòåëüíî ìèêðîñõåìà Clipper äîëæíà ïðîòèâîñòîÿòü èíæåíåðíîìó âñêðûòèþ, âûïîëíåííîìó "èçîùðåííûì, õîðîøî" [1154], íî ïî ñëóõàì â Sandia National Laboratories óñïåøíî ïðîâåëè èññëåäîâàíèå îäíîé èç ìèêðîñõåì. Äàæå åñëè ýòè ñëóõè ëîæíû, ÿ ïîäîçðåâàþ, ÷òî ñàìûì êðóïíûì ìèðîâûì ïðîèçâîäèòåëÿì òàêîå èíæåíåðíîå âñêðûòèå âïîëíå ïî ñèëàì, è åãî ñðîê ÿâëÿåòñÿ òîëüêî âîïðîñîì ðåñóðñîâ è ìîðàëè.

Ñ ýòîé òåìîé ñâÿçàíî ìíîæåñòâî âîïðîñîâ î òàéíå ëè÷íîñòè. Ìíîãî÷èñëåííûå ãðóïïû çàùèòû ãðàæäàíñêèõ ñâîáîä âåäóò àêòèâíóþ êîìïàíèþ ïðîòèâ ëþáîãî ìåõàíèçìà óñëîâíîãî âðó÷åíèÿ êëþ÷åé, êîòîðûé äàñò ïðàâèòåëüñòâó ïðàâî ïîäñëóøèâàòü ãðàæäàí. Âñÿ ïîäëîñòü â òîì, ÷òî, õîòÿ ýòà ñõåìà íèêîãäà íå ïðîõîäèëà ÷åðåç Êîíãðåññ, NIST îïóáëèêîâàë EES â êà÷åñòâå FIPS [1153], îáîéäÿ áîëåçíåííûé çàêîíîäàòåëüíûé ïðîöåññ. Ñåé÷àñ âñå âûãëÿäèò, êàê åñëè áû EES òèõî è ìåäëåííî óìèðàë, íî ñòàíäàðòû ñïîñîáíû ïðîäîëæàòü ñâîþ ïîëçó÷óþ äåÿòåëüíîñòü.

Â 22-é ïåðå÷èñëåíû ðàçëè÷íûå îðãàíèçàöèè, ó÷àñòâóþùèå â ýòîé ïðîãðàììå. Êàê íàñ÷åò èäåè, ÷òîáû îáà ó÷ðåæäåíèÿ óñëîâíîãî âðó÷åíèÿ îòíîñèëèñü òîëüêî ê èñïîëíèòåëüíîé âåòâè âëàñòè? ×òî âû ñêàæåòå îá ó÷ðåæäåíèÿõ óñëîâíîãî âðó÷åíèÿ, êîòîðûå ïî ñóòè íè÷åãî íå çíàþò î çàÿâêàõ íà ïîäñëóøèâàíèå è ìîãóò òîëüêî ñëåïî îäîáðÿòü èõ? È ÷òî íàñ÷åò èäåè î ïðèíÿòèè ïðàâèòåëüñòâîì ñåêðåòíîãî àëãîðèòìà â êà÷åñòâå êîììåð÷åñêîãî ñòàíäàðòà?

Òàáë. 24-2.
Îðãàíèçàöèè, ó÷àñòâóþùèå â EES.

Ìèíèñòåðñòâî þñòèöèè - Ñïîíñîð ñèñòåìû, âëàäåëåö îáùåãî êëþ÷à
NIST - Ðóêîâîäñòâî ïðîãðàììîé, õðàíèòåëü óñëîâíî âðó÷åííîé ÷àñòè êëþ÷à
FBI - Ïîëüçîâàòåëü-äåøèôðîâùèê, âëàäåëåö îáùåãî êëþ÷à
Ìèíèñòåðñòâî ôèíàíñîâ - Õðàíèòåëü óñëîâíî âðó÷åííîé ÷àñòè êëþ÷à
NSA - Ðàçðàáîò÷èê ïðîãðàììû

Â ëþáîì ñëó÷àå, èñïîëüçîâàíèå Clipper ïîðîäèò íåìàëî ïðîáëåì ïðè îáðàùåíèè â ñóä. Íå çàáûâàéòå, Clipper ðàáîòàåò òîëüêî â ðåæèìå OFB. ×òî áû âàì èíîå íå ãîâîðèëè, ýòîò ðåæèì íå îáåñïå÷èâàåò öåëîñòíîñòè èëè ïðîâåðêè ïîäëèííîñòè. Ïðåäïîëîæèì, ÷òî Àëèñà ïðåäñòàëà ïåðåä ñóäîì, è ÷àñòüþ äîêàçàòåëüñòâ ÿâëÿåòñÿ òåëåôîííûé ðàçãîâîð, çàøèôðîâàííûé ìèêðîñõåìîé Clipper. Àëèñà óòâåðæäàåò, ÷òî îíà íèêîãäà íå çâîíèëà, è ãîëîñ - íå åå. Àëãîðèòì ñæàòèÿ ðå÷è íàñòîëüêî ïëîõ, ÷òî îïîçíàòü ãîëîñ Àëèñû òðóäíî, íî îáâèíåíèå óòâåðæäàåò, ÷òî, òàê êàê ðàñøèôðîâàòü ðàçãîâîð ìîæíî òîëüêî ñ ïîìîùüþ óñëîâíî âðó÷åííîãî êëþ÷à Àëèñû, ýòîò çâîíîê áûë

ñäåëàí ñ åå òåëåôîíà.

Àëèñà çàÿâëÿåò, ÷òî ðàçãîâîð áûë ïîäâåðãíóò àòàêå ñ [984, 1339]: äâîû øèôðîâàëüùèê XOR, ìîæíî ïîëó÷èòü êëþ÷åâîé ïîòîê. Çàòåì ýòîò êëþ÷åâîé ïîòîê ìîæíî íàêëàäûâàòü íà äâîè÷íîå ïðåäñòàâëåíèå îòêðûòîãî òåêñòà, ïîëó÷àÿ òàêîâûì øèôðîâàëüùèê XOR ñ àáñîëþòíî äóãèì îòêðûòûì òåêñòîì, ïîëó÷åííûì íà äâîè÷íîì ïðåäñòàâëåíèè. Ïðè óñòàíîâêå êëþ÷à Àëèñà äåëàåò ñåàíñîâûé êëþ÷ èäåíòè÷íûì òîì, êîòîðûé íà èñïîëüçîâàëà äëÿ ðàçãîâîðà ñ Áîáîì. Äëÿ ýòîãî ïîòðåáóåòñÿ âçëîìàòü òåëåôîí, íî ýòî íåòðóäíî. Çàòåì âìåñòî òîãî, ÷òîáû ïîñëàòü ñâîé LEAF, îíà ïîñûëàåò LEAF Áîáà. Ýòî ïðàâèëüíûå LEAF, ïîýòîìó òåëåôîí Êýðîë íè÷åãî íå çàìåòèò. Òåïåðü îíà ìîæåò ãîâîðèòü Êýðîë âñå, ÷òî çàõ÷åò - êîãäà ïîëüçîâàòåëü ðàñøèôðóåò LEAF, îíà îáíàðóæèò, ÷òî íîí ïðîäóêòèâíà, è ïîñûëàåò Áîáó. Äàæå åñëè Àëèñà íå óâåðåííà âûäàòü ñåãî Áîáà, åìó ïðèäåòñÿ âîâðåìÿ âûáðàòü ìåæäó Áîáîì è Äæîíîì. Äëÿ åñëè Àëèñà íå óâåðåíà, ÷òî ïîëó÷èëà ïîäëèííûé îòêðûòûé òåêñò, îíà íèêîãäà íå ñìîæåò îïðåäåëèòü ïîäëèííûé ñîîáùåíèå.

Îðãàíû îõðàíû ïðàâîïîðÿäêà Ñîâåòíåíûõ Øòàòîâ íà äîëæíû òðàíñëèðîâàòü, çàíèìàÿñü ñáîðîì èíôîðìàöèè â óãîëîâíûõ ðàññëåäîâàíèÿõ, êîòîðûå íåëüçÿ èñïîëüçîâàòü â ñóäå. Äàæå åñëè óñëîâíûå âðó÷åíèå è ÿâëÿëîñü áû íåïîíÿòíûé èäåé, Clipper - ýòî íå ëó÷øèé ñïîñîá ðàçëèçàòèè ýòîé èäåè.

24.17 CAPSTONE

Capstone (èçâåñòíûé òàêæå êàê MYK-80) - ýòî äóãàÿ ðàçðàáîòàííàÿ NSA ÑÁÈÑ, ðåàëèçóþùàÿ Ñòàíäàðò óñëîâíîãî øèôðîâàíèÿ ïðàâèòåëüñòâà ÑØÀ [1153]. Capstone ðåàëèçóåò ñëåäóþùèå ôóíêöèè [1155, 462]:

— Àëãîðèòì Skipjack â ëþáîì èç ÷åòûðåõ îñíîâíûõ ðåæèìîâ: ECB, CBC, CFB è OFB.

— Àëãîðèòì îáìåíà êëþ÷àìè (Key Exchange Algorithm, KEA) íà áàçå îòêðûòûõ êëþ÷åé, ñêîðåå âñåãî Diffie-Hellman.

— Àëãîðèòì öèôðîâîé ïîäïèñè (Digital Signature Algorithm, DSA). *

— Àëãîðèòì áåçîïàñíîãî õýøèðîâàíèÿ (Secure Hash Algorithm, SHA). j

— Àëãîðèòì âîçâðàùåíèÿ â ñòàíäàðòíûé äëÿ îáùåãî íàçíà÷åíèÿ.

— Åíåðàòîð ñëó÷àéíûõ ÷èñåë ñ èñïîëüçîâàíèåì èñòèííî øóìîâîãî èñòî÷íèêà.

Capstone îáåñïå÷èâàåò êðèïòîãðàôè÷åñêèå âîçìîæíîñòè, íåîáõîäèìûå äëÿ áåçîïàñíîé ýëåêòðîííîé òîðãîâëè è äðóãèõ êîììåðöèàëüíûõ ïðèëîæåíèé. Ïðåäûì ïðèíåíèåì Capstone ÿâëÿåòñÿ êàðòî÷êà PCMCIA, íàçâàííàÿ Fortezza. (Ñíà÷àëà îíà íàçûâàëàñü Tessera, ïîêà íà ýòî íå ïîæàëîâàëàñü êîìïàíèÿ Tessera, Inc..)

NSA èçó÷èëî âîçìîæíîñòü óäëèíåíèÿ êîòðîëüíîé ñóììû LEAF â Capstone â âåðñèÿõ äëÿ êàðòî÷åê äëÿ òîãî, ÷òîáû ïîìåøàòü ðàíåå ðàñïîòðåíèþ âñêðûòèþ LEAF. Âìåñòî ýòîãî áûëà äîáàâëåíà âîçìîæíîñòü âûïîëíÿòü ïåðåçàïóñê êàðòî÷êè ïîñëå 10 íåïðàâèëüíûõ LEAF. Ìåíÿ ýòî íå âïå÷àòëèëî - âðåìÿ ïîêàçàëî ïðàâèëüíîãî LEAF òîëüêî íà 10 ïðîöåíòîâ, äî 46 ìèíóò.

24.18 Áåçîïàñíûé òåëåôîí AT&T MODEL 3600 TELEPHONE SECURITY DEVICE (TSD)

Áåçîïàñíûé òåëåôîí AT&T (Telephone Security Device, TSD) - ýòî òåëåôîí ñ ìèêðîñõåìîé Clipper. Íà ñàìîì äåëå ñóùåñòâóåò ÷åòûðå ìîäåëè TSD. Îäíà ñîäåðæèò ìèêðîñõåìó Clipper, äóãàÿ - ýêñïîðòèðóåìûé êëþ÷åâîé àëãîðèòì øèôðîâàíèÿ AT&T òðåüÿ - êëþ÷åâîé àëãîðèòì äëÿ ñîîòâåòñòâèÿ âíóòðè ñòðàíû ïëþñ ýêñïîðòèðóåìûé àëãîðèòì, à ÷åòâåðòàÿ âêëþ÷àåò Clipper, âíóòðåííèé è ýêñïîðòèðóåìûé àëãîðèòì.

Äëÿ êàæäîãî òåëåôîííîãî çâîíêà TSD èñïîëüçóþò îòëè÷íûé ñåàíñîâûé êëþ÷. Ïàðà TSD ãåíåðèðóåò ñåàíñîâûé êëþ÷ ñ ïîìîùüþ ñõåìû îáìåíà êëþ÷àìè Diffie-Hellman, íåçàâèñèìî îò ìèêðîñõåìû Clipper. Òàê êàê Diffie-Hellman íå âêëþ÷àåò ïðîâåðêè ïîäëèííîñòè, TSD èñïîëüçóåò äâà ìåòîäà äëÿ ïðåäîòâðàùåíèÿ âñêðûòèÿ "÷åëîâåê â ñåðåäèíå".

Ïåðâûì ÿâëÿåòñÿ ýêðàí. TSD õýøèðóåò ñåàíñîâûé êëþ÷ è âûâîäèò õýø-çíà÷åíèå íà ìàëåíüêîì ýêðàíå â âèäå ÷åòûðåõ øåñòíàäöàòèðè÷íûõ öèôð. Ñîáåñåäíèêè ïðîâåðÿþò, ÷òî íà èõ ýêðàíå âûâåäåíû îäèíàêîâûå öèôðû. Êà÷åñòâî ãîëîñà äîñòàòî÷íî õîðîøî, ÷òîáû îíè ìîãëè óçíàòü äðóã äðóãà ïî ãîëîñó.

Âñå æå Åâà ìîæåò âñêðûòü ýòó ñõåìó. Ïóñòü åé óäàëîñü âêëèíèòüñÿ â ëèíèþ ìåæäó Áîáîì è Àëèñîé. Îíà èñïîëüçóåò TSD íà ëèíèè ñ Àëèñîé è ìîäèôèöèðîâàííûé TSD íà ëèíèè ñ Áîáîì. Ïîñêîëüêó îíà ñîïðÿãàåò äâà

òåëåôîííûõ çâîíêà. Àëèñà ïûòàåòñÿ ñäåëàòü ðàçãîâîð áåçîïàñíûì. Îíà îáû÷íûì îáðàçîì ãåíåðèðóåò êëþ÷, íî îáùàåòñÿ ñ Âîé, âûäàþùåé ñåáÿ çà Áîáà. Åâà ðàñêðûâàåò êëþ÷ è ñ ïîìîùüþ ìîäèôèöèðîâàííîãî TSD äåëàåò òàê, ÷òîáû êëþ÷, êîòîðûé îíà ñãåíåðèðîâàëà äëÿ Áîáà, èìåë òàêîå æå õýø-çíà÷åíèå. Ýòî âñêðûòèå íà âèä íå î÷åíü ðåàëüíî, íî äëÿ åãî ïðåäîòâðàùåíèÿ â TSD èñïîëüçóåòñÿ áëîêèðîâêà.

TSD ãåíåðèðóåò ñëó÷àéíûå ÷èñëà, èñïîëüçóÿ èñòî÷íèê øóìà è õàîòè÷íûé óñèëèòåëü ñ öèôðîâîé îáðàòíîé ñâÿçüþ. Î í ãåíåðèðóåò áèòîâûé ïîòîê, êîòîðûé ïðîïóñêàåòñÿ ÷åðåç ïîñòîáåëèâàþùèé ôèëüòð íà áàçå öèôðîâîãî ïðîöåññîðà.

Íåñìîòðÿ íà âñå ýòî â ñïðàâî÷íîì ðóêîâîäñòâå TSD íåò íè ñëîâà î áåçîïàñíîñòè. Íà ñàìîì äåëå òàì íàïèñàíî [70]:

> AT&T íå ãàðàíòèðóåò, ÷òî TSD çàùèòèò îò âñêðûòèÿ çàøèôðîâàííîé ïåðåäà÷è ïðàâèòåëüñòâåííûì ó÷ðåæäåíèåì, åãî àãåíòàìè èëè òðåòüåé ñòîðîíîé. Áîëåå òîãî, AT&T íå ãàðàíòèðóåò, ÷òî TSD çàùèòèò îò âñêðûòèÿ ïðåäâàðèòåëüíî èíôîðìàöèè ñ ïîìîùüþ ìåòîäîâ, îáõîäÿùèõ øèôðîâàíèå.

Ãëàâà 25
Ïîëèòèêà

25.1 Àãåíòñòâî íàöèîíàëüíîé áåçîïàñíîñòè (NSA)

NSA - ýòî Àãåíòñòâî íàöèîíàëüíîé áåçîïàñíîñòè (National Security Agency, êîãäà-òî ðàñøèôðîâûâàëîñü øóòíèêàìè êàê "No Such Agency" (íèêàêîå àãåíòñòâî) èëè "Never Say Anything" (íèêîãäà íè÷åãî íå ñêàæó), íî òåïåðü îíè áîëåå îòêðûòû), îôèöèàëüíûé îðãàí ïðàâèòåëüñòâà ÑØÀ ïî âîïðîñàì áåçîïàñíîñòè. Àãåíòñòâî áûëî ñîçäàíî â 1952 ãîäó ïðåçèäåíòîì Ãàððè Òðóìåíîì â ïîä÷èíåíèè Ìèíèñòåðñòâà áåçîïàñíîñòè, è ìíîãèå ãîäû â ñåêðåòå õðàíèëñÿ ñàì ôàêò åãî ñóùåñòâîâàíèÿ. NSA âîñïðèíèìàëîñü êàê ýëåêòðîííàÿ ðàçâåäêà, â åãî çàäà÷è âõîäèëî ïîäñëóøèâàòü è ðàñøèôðîâûâàòü âñå èíîñòðàííûå ëèíèè ñâÿçè â èíòåðåñàõ Ñîåäèíåííûõ Øòàòîâ.

Ñëåäóþùèå àáçàöû âçÿòû èç îôèöèàëüíîãî ïîëîæåíèÿ î NSA, ïîäïèñàííîãî â 1952 ãîäó ïðåçèäåíòîì Òðóìåíîì è ðàññåêðå÷åííîãî ñïóñòÿ ìíîãî ëåò [1535]:

> Â çàäà÷è COMINT Àãåíòñòâà íàöèîíàëüíîé áåçîïàñíîñòè (NSA) äîëæíû âõîäèòü ýôôåêòèâíûå îðãàíèçàöèÿ è óïðàâëåíèå ðàçâåäûâàòåëüíîé äåÿòåëüíîñòè Ñîåäèíåííûõ Øòàòîâ â îáëàñòè òåëåêîììóíèêàöèé, ïðîâîäèìîé ïðîòèâ èíîñòðàííûõ ïðàâèòåëüñòâ, ÷òîáû îáåñïå÷èòü öåëîñòíóþ äåéñòâåííóþ ïîëèòèêó è ñîîòâåòñòâóþùèå ìåðû. Èñïîëüçóåìûé â ýòîé äèðåêòèâå òåðìèí "ýëåêòðîííàÿ ðàçâåäêà" ("communications intelligence") èëè "COMINT" îáîçíà÷àåò âñå äåéñòâèÿ è ìåòîäû, èñïîëüçóåìûå äëÿ ïåðåõâàòà òåëåêîììóíèêàöèé, èñêëþ÷àÿ çàðóáåæíûå ïðåññó è ðàäèîâåùàíèå, è ïîëó÷åíèÿ èíôîðìàöèè, ïðåäíàçíà÷åííîé äëÿ ïðèåìà äðóãèì ïîëó÷àòåëåì, íî èñêëþ÷àåò öåíçóðó, à òàêæå ïðîèçâîäñòâî è ðàñïðîñòðàíåíèå ïîëó÷åííîé ðàçâåäûâàòåëüíîé èíôîðìàöèè.
>
> Ñïåöèàëüíàÿ ïðèðîäà äåéñòâèé COMINT òðåáóåò, ÷òîáû îíè âî âñåõ îòíîøåíèÿõ ïðîâîäèëèñü îòäåëüíî îò äðóãîé èëè îáùåé ðàçâåäûâàòåëüíîé äåÿòåëüíîñòè. Ïðèêàçû, äèðåêòèâû, óêàçàíèÿ èëè ðåêîìåíäàöèè ëþáîãî îðãàíà èñïîëíèòåëüíîé âëàñòè, êàñàþùèåñÿ ñáîðà, ïîëó÷åíèÿ, áåçîïàñíîñòè, îáðàáîòêè, ðàñïðîñòðàíåíèÿ èëè èñïîëüçîâàíèÿ ðàçâåäûâàòåëüíîé èíôîðìàöèè íåïðèìåíèìû â îòíîøåíèè äåéñòâèé COMINT, åñëè ýòî íå îãîâîðåíî îñîáî, è äîêóìåíòû íå áóäóò èçäàíû êîìïåòåíòíûì ïðåäñòàâèòåëåì àãåíòñòâà, âõîäÿùèì â ïðàâèòåëüñòâî. Äðóãèå äèðåêòèâû Íàöèîíàëüíîãî ñîâåòà áåçîïàñíîñòè äèðåêòîðó ÖÐÓ è ñâÿçàííûå äèðåêòèâû, èçäàííûå äèðåêòîðîì ÖÐÓ, íå äîëæíû ïðèìåíÿòüñÿ ê äåéñòâèÿì COMINT, åñëè ýòî íå áóäåò ñïåöèàëüíàÿ äèðåêòèâà Íàöèîíàëüíîãî ñîâåòà áåçîïàñíîñòè, êàñàþùàÿñÿ COMINT.

NSA âåäåò èññëåäîâàíèÿ â îáëàñòè êðèïòîëîãèè, çàíèìàÿñü êàê ðàçðàáîòêîé áåçîïàñíûõ àëãîðèòìîâ äëÿ çàùèòû êîììóíèêàöèé Ñîåäèíåííûõ Øòàòîâ, òàê è êðèïòîàíàëèòè÷åñêèìè ìåòîäàìè äëÿ ïðîñëóøèâàíèÿ êîììóíèêàöèé çà ïðåäåëàìè ÑØÀ research. Èçâåñòíî, ÷òî NSA ÿâëÿåòñÿ êðóïíåéøèì â ìèðå ðàáîòîäàòåëåì äëÿ ìàòåìàòèêîâ. Îíî òàêæå ÿâëÿåòñÿ êðóïíåéøèì â ìèðå ïîêóïàòåëåì êîìïüþòåðíîé àïïàðàòóðû. Âîçìîæíî êðèïòîãðàôè÷åñêèé îïûò NSA íà ìíîãî ëåò îòîðâàëñÿ îò ñîñòîÿíèÿ äåë â îòêðûòîé íàóêå (â ÷àñòè àëãîðèòìîâ, íî âðÿä ëè â ÷àñòè ïðîòîêîëîâ). Íåñîìíåííî Àãåíòñòâî ìîæåò âçëîìàòü ìíîãèå èç èñïîëüçóåìûõ ñåãîäíÿ ñèñòåì. Íî, èç ñîîáðàæåíèé íàöèîíàëüíîé áåçîïàñíîñòè, ïî÷òè âñÿ èíôîðìàöèÿ î NSA - äàæå åå áþäæåò - çàñåêðå÷åíà. (Ïî ñëóõàì áþäæåò Àãåíòñòâà ñîñòàâëÿåò îêîëî 13 ìèëëèàðäîâ äîëëàðîâ â ãîä - âêëþ÷àÿ âîåííîå ôèíàíñèðîâàíèå ïðîåêòîâ NSA è îïëàòó ïåðñîíàëà - è, ïî ñëóõàì, â íåì ðàáîòàåò 16 òûñÿ÷ ÷åëîâåê.)

NSA èñïîëüçóåò ñâîþ âëàñòü, ÷òîáû ãðàíè÷èòü îòêðûòóþ äîñòóïíîñòü êðèïòîãðàôèè è ïîìåøàòü íàöèîíàëüíûì âðàãàì èñïîëüçîâàòü ñëèøêîì ñèëüíûå ìåòîäû øèôðîâàíèÿ, ÷òîáû Àãåíòñòâî ìîãëî èõ âçëîìàòü. Äæåéìñ Ìàññåé (James Massey) àíàëèçèðóåò ýòó áîðüáó ìåæäó íàó÷íûìè è âîåííûìè èññëåäîâàíèÿìè â êðèïòîãðàôèè [1007]:

> Åñëè ñ÷èòàòü, ÷òî êðèïòîëîãèÿ ÿâëÿåòñÿ ïðåðîãàòèâîé ïðàâèòåëüñòâà, òî, êîíå÷íî, áîëüøàÿ ÷àñòü êðèïòîëîãè÷åñêèõ èññëåäîâàíèé äîëæíà âåñòèñü çà çàêðûòûìè äâåðÿìè. Áåç ñîìíåíèÿ êîëè÷åñòâî ëþäåé, çàíÿòûõ ñåãîäíÿ êðèïòîëîãè÷åñêèìè èññëåäîâàíèÿìè, íàìíîãî áîëüøå, ÷åì êîëè÷åñòâî ëþäåé, ðàáîòàþùèõ â îòêðûòîé êðèïòîëîãèè. Îòêðûòûå êðèïòîëîãè÷åñêèå èññëåäîâàíèÿ øèðîêî âåäóòñÿ òîëüêî ïîñëåäíèå 10 ëåò. Ìåæäó ýòèìè äâóìÿ èññëåäîâàòåëüñêèìè ñîîáùåñòâàìè áûëè è áóäóò êîíôëèêòû. Îòêðûòûå èññëåäîâàíèÿ ïðåñëåäóþò ñâîþ îáû÷íóþ öåëü çíàíèÿ, äëÿ êîòîðîãî æèçíåííî âàæåí îòêðûòûé îáìåí èäåÿìè ñ ïîìîùüþ êîíôåðåíöèé, ïðåçåíòàöèé è ïóáëèêàöèé â íàó÷íûõ æóðíàëàõ. Íî ìîæåò ëè ïðàâèòåëüñòâåííàÿ îðãàíèçàöèÿ, îòâåòñòâåííàÿ çà âçëîìû øèôðîâ äðóãèõ ãîñóäàðñòâ, ïðèâåòñòâîâàòü ïóáëèêàöèþ øèôðà, êîòîðûé íåëüçÿ âçëîìàòü? Ìîæåò ëè èññëåäîâàòåëü ñ ÷èñòîé ñîâåñòüþ ïóáëèêîâàòü ïîäîáíûé øèôð, êîòîðûé ìîæåò ñâåñòè íà íåò óñèëèÿ âçëîìùèêîâ êîäà, íàõîäÿùèõñÿ íà ñëóæáå åãî ïðàâèòåëüñòâà? Ìîæíî íàñòàèâàòü, ÷òî ïóáëèêàöèÿ äîêàçàííî áåçîïàñíîãî øèôðà çàñòàâèò âñå ïðàâèòåëüñòâà âåñòè ñåáÿ ïîäîáíî "äæåíòëüìåíàì" Ñòèìñîíà, íî íåîáõîäèìî ïîìíèòü, ÷òî îòêðûòûå èññëåäîâàíèÿ â êðèïòîãðàôèè ïîëíû ïîëèòè÷åñêèõ è ýòè÷åñêèõ ìîòèâîâ ãîðàçäî áîëåå ñåðüåçíûõ, ÷åì âî ìíîãèõ äðóãèõ îáëàñòÿõ íàóêè. Óäèâëÿòüñÿ íàäî íå òîìó, ÷òî ïðàâèòåëüñòâåííûå îðãàíèçàöèè íà ïî÷âå êðèïòîëîãèè êîíôëèêòóþò ñ íåçàâèñèìûìè èññëåäîâàòåëÿìè, à òîìó, ÷òî ýòè êîíôëèêòû (ïî êðàéíåé ìåðå òå, î êîòîðûõ íàì èçâåñòíî) òàê íåçíà÷èòåëüíû è òàê ñãëàæåíû.

Äæåéìñ Áýìôîðä (James Bamford) íàïèñàë óâëåêàòåëüíóþ êíèãó ïðî NSA: *The Puzzle Palace* [79], (*Äâîðåö ãîëîâîëîìîê*), íåäàâíî äîðàáîòàííóþ âìåñòå ñ Âýéíîì Ìàäñåíîì (Wayne Madsen) [80].

Êîììåð÷åñêàÿ ïðîãðàììà ñåðòèôèêàöèè êîìïüþòåðíîé áåçîïàñíîñòè

Êîììåð÷åñêàÿ ïðîãðàììà ñåðòèôèêàöèè êîìïüþòåðíîé áåçîïàñíîñòè (Commercial COMSEC Endorsement Program (CCEP)), êîäîâîå èìÿ Overtake, - ýòî ïðåäëîæåíèå, ñäåëàííîå NSA â 1984 ãîäó è ïðèçâàííîå îáëåã÷èòü ðàçðàáîòêó êîìïüþòåðîâ è ñðåäñòâ ñâÿçè ñ âñòðîåííûìè êðèïòîãðàôè÷åñêèìè âîçìîæíîñòÿìè [85, 1165]. Îáû÷íî âñþ ðàçðàáîòêó òàêèõ èçäåëèé îïëà÷èâàëè âîåííûå, è ýòî îáõîäèëîñü èì íåäåøåâî. NSA ïîñ÷èòàëî, ÷òî åñëè êîìïàíèè ìîãóò ïðîäàâàòü àïïàðàòóðó è àðìèè, è êîðïîðàöèÿì, äàæå èíîñòðàííûì, ýòî ïîçâîëèò óìåíüøèòü ðàñõîäû ê âûãîäå âñåõ. Àãåíòñòâó áîëüøå íå òðåáîâàëîñü áû ïðîâåðÿòü ñîâìåñòèìîñòü îáîðó-

äîâàíèÿ ñ Ôåäåðàëüíûì ñòàíäàðòîì 102.7, è çàòåì CCEP ïðåäîñòàâëÿ áû äîñòóï ê îäíîðåíîìó ïðàâèòåëüñòâåííîìó êðèïòîãðàôè÷åñêîìó îáîðóäîâàíèþ [419].

NSA ðàçðàáîòàëî ðÿä êðèòîãðàô÷åñêèõ ìîäóëåé ðàçëè÷íîãî íàçíà÷åíèÿ. Â ýòèõ ìîäóëÿõ äëÿ ðàçëè÷íûõ ïðèëîæåíèé èñïîëüçóþòñÿ ðàçëè÷íûå àëãîðèòìû, è ïðîèçâîäèòåëè ïîëó÷àþò âîçìîæíîñòü èçâëå÷ü îäèí ìîäóëü è âñòàâèòü äðóãîé â çàâèñèìîñòè îò æåëàíèé êëèåíòà. Ñóùåñòâóþò ìîäóëè äëÿ âîåííîãî èñïîëüçîâàíèÿ (Òèï I), ìîäóëè äëÿ "íåñåðâåðíîãî, íî âàæíîãî" ïðàâèòåëüñòâåííîãî èñïîëüçîâàíèÿ (Òèï II), ìîäóëè äëÿ êîðïîðàòèâíîãî èñïîëüçîâàíèÿ (Òèï III) è ìîäóëè äëÿ ýêñïîðòèðîâàíèÿ (Òèï IV). Ðàçëè÷íûå ìîäóëè, èõ ïðèìåíåíèå è íàçíà÷åíèÿ ñîâäåíû â 24-é.

Òàáë. 25-1.
Ì îäóëè CCEP

Ïðèìåíåíèå	Òèï I	Òèï II
Ðå÷ü/íèçêîñêîðîñòíàÿ ïåðåäà÷à äàííûõ	Winster	Edgeshot
Êîìïüþòåð	Tepache	Bulletproof
Âûñîêîñêîðîñòíàÿ ïåðåäà÷à äàííûõ	Foresee	Brushstroke
Ñëåäóþùåå ïîêîëåíèå	Countersign I	Countersign II

Ýòà ïðîãðàììà âñå åùå äåéñòâóþò, íî îíà íå âûçâàëà ýíòóçèàçìà íè ó êîãî êðîìå ïðàâèòåëüñòâà. Âñå ìîäóëè áûëè çàùèùåíû îò âñêðûòèÿ, âñå àëãîðèòìû áûëè çàñåêðå÷åíû, à ïîëüçîâàòåëè äîëæíû áûëè ïîëó÷àòü êëþ÷è îò NSA. Êîðïîðàöèè íèêîãäà ðàíåüøå íå âåðèëè â èäåþ èñïîëüçîâàíèÿ ñâîðåíîãî äëãîðèòìà, íàâÿçàííûõ ïðàâèòåëüñòâîì. Êàçàëîñü áû, NSA ïîëó÷èëî çàìåòíûé óðîê, ÷òîáû áîëüøå íå äîó÷àòü ïðèíóäèòåëüíûõ ìåðîïðèÿòèé Clipper, Skipjack è ìèêðîñõåì øèôðîâàíèÿ ñóñëîâíûì âðó÷åíèåì êëþ÷åé.

25.2 Íàöèîíàëüíûé öåíòð êîìïüþòåðíîé áåçîïàñíîñòè (NCSC)

Íàöèîíàëüíûé öåíòð êîìïüþòåðíîé áåçîïàñíîñòè (National Computer Security Center, NCSC), îòäåëåíèå NSA, îòâå÷àåò çà äîâåðåííóþ ïðàâèòåëüñòâåííóþ êîìïüþòåðíóþ ïðîãðàììó. Â íàñòîÿùåå âðåìÿ öåíòð ïðîâîäèò îöåíêó ïðîäóêòîâ êîìïüþòåðíîé áåçîïàñíîñòè (ïðîãðàìì íûõ è àïïàðàòíûõ), ôèíàíñèðóåò èññëåäîâàíèÿ è ïóáëèêóåò èõ ðåçóëüòàòû, ðàçðàáàòûâàåò òåõíè÷åñêèå ðóêîâîäñòâà è îáñëå÷èâàåò îáùóþ ïîääåðæêó è îáó÷åíèå.

NCSC èçäàë ñêàíäàëüíî èçâåñòíóþ "Îðàíæåâóþ êíèãó" [465]. Åå íàñòîÿùåå íàçâàíèå - *Department of Defense Trusted Computer System Evaluation Criteria* (Êðèòåðèè îöåíêè äîâåðåííûõ âû÷èñëèòåëüíûõ êîìïüþòåðíûõ ñèñòåì), íî ýòî òàê òðóäíî âûãîâàðèâàòü, è èòîãó æå ó êíèãè îðàíæåâàÿ îáëîæêà. Îðàíæåâàÿ êíèãà ïûòàëñÿ îïðåäåëèòü òðåáîâàíèÿ ê áåçîïàñíîñòè, äàâ ïðîèçâîäèòåëÿì êîìïüþòåðîâ îáúåêòèâíûé ñïîñîá èçìåðèòü áåçîïàñíîñòü èõ ñèñòåì è óêàçûâàâ èì, ÷òî íåîáõîäèìî âûðàâíèâàòü â áåçîïàñíûå ïðîäóêòû. Êíèãà ïîñâÿùåíà êîìïüþòåðíîé áåçîïàñíîñòè, î êðèòåðèÿõ çàùèùû âíóòðè êîìïüþòåðíûõ ñèñòåì è íåé ïî ñóòè ãîâîðèòñÿ íå î÷åíü ìíîãî.

Îðàíæåâàÿ êíèãà îïðåäåëÿåò ÷åòûðå øèðîêèõ êàòåãîðèè çàùèùû áåçîïàñíîñòè. Â íåé òàêæå îïðåäåëÿþòñÿ êëàññû çàùèùû âíóòðè íåêîòîðûõ èç ýòèõ êàòåãîðèé. Î íè ñâåäåíû â 23-é.

Òàáë. 25-2.
Êëàññèôèêàöèÿ Îðàíæåâîé êíèãè

D: Minimal Security (Ì èíèìàëüíàÿ áåçîïàñíîñòü)
C: Discretionary Protection (Çàùèòà ïî óìîë÷àíèþ)
    C1: Discretionary Security Protection (Çàùèòà áåçîïàñíîñòè ïî óìîë÷àíèþ)
    C2: Controlled Access Protection (Çàùèòà óïðàâëÿåìîãî äîñòóïà)
B: Îáÿçàòåëüíàÿ çàùèòà
    B1: Labeled Security Protection
    B2: Structured Protection (Ñòðóêòóðíàÿ çàùèòà)
    B3: Security Domains (Îáëàñòè áåçîïàñíîñòè)
A: Verified Protection (Äîñòîâåðíàÿ çàùèòà)
    A1: Verified Design (Äîñòîâåðíàÿ ðàçðàáîòêà)

Èíîãäà ïðîèçâîäèòåëè ëþáÿò ãîâîðèòü "ìû îáåñïå÷èâàåì áåçîïàñíîñòü C2". Â âèäó îíè èìåþò êëàññèôèêàöèþ Îðàíæåâîé êíèãè. Çà áîëåå ïîäðîáíîé èíôîðìàöèåé îáðàùàéòåñü ê [1365]. Ì îäåëü êîìïüþòåðíîé áåçîïàñíîñòè, èñïîëüçóåìàÿ â ýòèõ êðèòåðèÿõ, íàçûâàåòñÿ ìîäåëüþ Bell-LaPadula [100, 101, 102, 103].

NCSC èçäàë öåëóþ ñåðèþ êíèã ïî êîìïüþòåðíîé áåçîïàñíîñòè, èíîãäà íàçûâàåìóþ Ðàäóãíîé êíèãîé (âñå îáëîæêè èìåþò ðàçëè÷íûå öâåòà). Íàïðèìåð, *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria* [1146] (Èíòåðïðåòàöèÿ êðèòåðèåâ îöåíêè äîâåðåííûõ êîìïüþòåðíûõ ñèñòåì â îòíîøåíèè

äîâåðåííûõ ñåòåé), èíîãäà íàçûâàåìàÿ Êðàñíîé êíèãîé, òîëêóåò ïîëîæåíèÿ Îðàíæåâîé êíèãè ïî îòíîøåíèþ ê ñåòÿì è ñåòåâîìó îáîðóäîâàíèþ. *Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria* [1147] (Èíòåðïðåòàöèÿ êðèòåðèåâ îöåíêè äîâåðåííûõ êîìïüþòåðíûõ ñèñòåì â îòíîøåíèè ñèñòåì óïðàâëåíèÿ áàçàìè äàííûõ) - ÿ äàæå íå ïûòàþñü îïèñàòü öâåò îáëîæêè - äåëàåò òî æå ñàìîå äëÿ áàç äàííûõ. Ñåãîäíÿ ñóùåñòâóåò ñâûøå 30 òàêèõ êíèã, öâåò îáëîæåê íåêîòîðûõ èç íèõ îòâðàòèòåëåí.

Çà ïîëíûì êîìïëåêòîì Ðàäóãè êíèã îáðàùàéòåñü ïî àäðåñó Director, National Security Agency, INFOSEC Awareness, Attention: C81, 9800 Savage Road, Fort George G. Meade, MD 2,0755-6000; (301) 766-8729. Íå ãîâîðèòå èì, ÷òî âàñ ïîñëàë ÿ.

25.3 Íàöèîíàëüíûé èíñòèòóò ñòàíäàðòîâ è òåõíèêè

NIST - ýòî Íàöèîíàëüíûé èíñòèòóò ñòàíäàðòîâ è òåõíèêè (National Institute of Standards and Technology), ïîäðàçäåëåíèå Ìèíèñòåðñòâà òîðãîâëè ÑØÀ. Ðàíåå îí íàçûâàëñÿ Íàöèîíàëüíûì áþðî ñòàíäàðòîâ (NBS, National Bureau of Standards) è èçìåíèë èìÿ â 1988 ãîäó. Ñ ïîìîùüþ ñâîåé Ëàáîðàòîðèè êîìïüþòåðíûõ ñèñòåì (Computer Systems Laboratory, CSL), NIST ïðîäâèãàë òåõíè÷åñêèå ñòàíäàðòû âçàèìîäåéñòâèÿ, êîòîðûå, êàê îí íàäåÿëñÿ, óñêîðÿò ðàçâèòèå îñíîâàííûõ íà êîìïüþòåðàõ òîðãîâëÿõ ïðîìûøëåííîñòè. Ê íàñòîÿùåìó âðåìåíè NIST âûïóñòèë ñòàíäàðòû è ðóêîâîäñòâà, êîòîðûå, êàê îí ñ÷èòàåò, áóäóò ïðèíÿòû âñåìè êîìïüþòåðíûìè ñèñòåìàìè Ñîåäèíåííûõ Øòàòîâ. Îôèöèàëüíûå ñòàíäàðòû îïóáëèêîâàíû êàê èçäàíèÿ FIPS (Ôåäåðàëüíûå ñòàíäàðòû îáðàáîòêè èíôîðìàöèè).

Åñëè âàì íóæíû êîïèè ëþáîãî èç FIPS (èëè äðóãèõ èçäàíèé NIST), ñâÿæèòåñü ñ Íàöèîíàëüíîé ñëóæáîé òåõíè÷åñêîé èíôîðìàöèè Ìèíèñòåðñòâà òîðãîâëè ÑØÀ - National Technical Information Service (NTIS), U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161; (703) 487-4650; èëè ïîñåòèòå gopher://csrc.ncsl.nist.go*

Êîãäà â 1987 ãîäó Êîíãðåññ ïðèíÿë Àêò î êîìïüþòåðíîé áåçîïàñíîñòè (Computer Security Act), NIST áûë óïîëíîìî÷åí îïðåäåëÿòü ñòàíäàðòû, îáåñïå÷èâàþùèå áåçîïàñíîñòü âàæíîé, íî íå ñåêðåòíîé èíôîðìàöèè â ïðàâèòåëüñòâåííûõ êîìïüþòåðàõ. (Ñåêðåòíàÿ èíôîðìàöèÿ è äàííûå Ïðåäóïðåæäàþùåé ïîïðàâêè íàõîäÿòñÿ â ñôåðå þðèñäèêöèè NSA.) Àêò ðàçðåøàåò NIST â õîäå îöåíêè ïðåäëàãàåìûõ òåõíè÷åñêèõ ñòàíäàðòîâ ñîòðóäíè÷àòü ñ äðóãèìè ïðàâèòåëüñòâåííûìè îðãàíèçàöèÿìè è ÷àñòíûìè ïðåäïðèÿòèÿìè.

NIST èçäàåò ñòàíäàðòû êðèïòîãðàôè÷åñêèõ ôóíêöèé. Îðãàíèçàöèè ïðàâèòåëüñòâà ÑØÀ îáÿçàíû èñïîëüçîâàòü èõ äëÿ âàæíîé, íî íåñåêðåòíîé èíôîðìàöèè. ×àñòî ýòè ñòàíäàðòû ïðèíèìàþòñÿ è ÷àñòíûì ñåêòîðîì. NIST âûïóñòèë DES, DSS, SHS è EES.

Âñå ýòè àëãîðèòìû ðàçðàáîòàíû ñ íåêîòîðîé ïîìîùüþ NSA, íà÷èíàÿ îò àíàëèçà DES äî ïðîåêòèðîâàíèÿ DSS, SHS è àëãîðèòìà Skipjack â EES. Íåêîòîðûå êðèòèêóþò NIST çà òî, ÷òî NSA â áîëüøîé ñòåïåíè ìîæåò êîíòðîëèðîâàòü ýòè ñòàíäàðòû, õîòÿ èíòåðåñû NSA ìîãóò íå ñîâïàäàòü ñ èíòåðåñàìè NIST. Íåÿñíî, êàê äåéñòâèòåëüíî NSA ìîæåò ïîâëèÿòü íà ïðîåêòèðîâàíèå è ðàçðàáîòêó àëãîðèòìîâ. Íî ïðè îãðàíè÷åíèÿõ íà ïåðñîíàë, áþäæåò è ðåñóðñû NIST ïðèâëå÷åíèå NSA êàæåòñÿ ðàçóìíûì. NSA îáëàäàåò áîëüøèìè âîçìîæíîñòÿìè, âêëþ÷àÿ ëó÷øóþ â ìèðå êîìïüþòåðíûå ñðåäñòâà.

Îôèöèàëüíûé "Ìåìîðàíäóì î âçàèìîïîíèìàíèè" ("Memorandum of Understanding", MOU) ìåæäó äâóìÿ îðãàíèçàöèÿìè ãëàñèò:

> ÌÅÌÎÐÀÍÄÓÌ Î ÂÇÀÈÌÎÏÎÍÈÌÀÍÈÈ ÌÅÆÄÓ ÄÈÐÅÊÒÎÐÎÌ ÍÀÖÈÎÍÀËÜÍÎÃÎ ÈÍÑÒÈÒÓÒÀ ÑÒÀÍÄÀÐÒÎÂ È ÒÅÕÍÈÊÈ È ÄÈÐÅÊÒÎÐÎÌ ÀÃÅÍÒÑÒÂÀ ÍÀÖÈÎÍÀËÜÍÎÉ ÁÅÇÎÏÀÑÍÎÑÒÈ ÎÒÍÎÑÈÒÅËÜÍÎ ÏÐÈÌÅÍÅÍÈß ÏÓÁËÈ×ÍÎÃÎ ÇÀÊÎÍÀ 100-235
>
> Ñîçíàâàÿ, ÷òî:
>
> A. Â ñîîòâåòñòâèè ñ ðàçäåëîì 2 Àêòà î êîìïüþòåðíîé áåçîïàñíîñòè îò 1987 ãîäà (Ïóáëè÷íûé çàêîí 100-235), (Àêò), íà Íàöèîíàëüíûé èíñòèòóò ñòàíäàðòîâ è òåõíèêè (NIST) êàê ÷àñòü Ôåäåðàëüíîãî ïðàâèòåëüñòâà âîçëàãàåòñÿ îòâåòñòâåííîñòü çà:
>
> 1. Ðàçðàáîòêó òåõíè÷åñêèõ , àäìèíèñòðàòèâíûõ, ôèçè÷åñêèõ ñòàíäàðòîâ, ñòàíäàðòîâ óïðàâëåíèÿ è ðóêîâîäñòâà äëÿ ðåíòàáåëüíûõ áåçîïàñíîñòè è çàùèùåííîñòè âàæíîé èíôîðìàöèè Ôåäåðàëüíûõ êîìïüþòåðíûõ ñèñòåì, îïðåäåëåííûõ â Àêòå; è,
>
> 2. Ðàçðàáîòêó ðóêîâîäñòâà ïî òåõíè÷åñêîé áåçîïàñíîñòè ñîîòâåòñòâóþùèõ êîìïüþòåðíûõ ñèñòåì Àãåíòñòâà íàöèîíàëüíîé áåçîïàñíîñòè (NSA).
>
> B. Â ñîîòâåòñòâèè ñ ðàçäåëîì 2 Àêòà NIST îáÿçàí ðàáîòàòü â òåñíîì âçàèìîäåéñòâèè ñ äðóãèìè îðãàíèçàöèÿìè, âêëþ÷àÿ NSA, îáåñïå÷èâàÿ:
>
> 1. Ìàêñèìàëüíîå èñïîëüçîâàíèå âñåõ ñóùåñòâóþùèõ è ïëàíèðóåìûõ ïðîãðàìì, ìàòåðèàëîâ, èññëåäîâàíèé è îò÷åòîâ, êàñàþùèõñÿ áåçîïàñíîñòè è çàùèùåííîñòè êîìïüþòåðíûõ ñèñòåì, ÷òîáû èçáåæàòü íåíóæíîãî è äîðîãîãî äóáëèðîâàíèÿ ðàáîò; è,
>
> 2. Ýòè ñòàíäàðòû, ðàçðàáîòàííûå NIST â ñîîòâåòñòâèè ñ Àêòîì, â ìàêñèìàëüíî âîçìîæíîé ñòåïåíè äîëæíû áûòü ñîãëàñîâàíû è ñîâìåñòèìû ñî ñòàíäàðòàìè è ïðîöåäóðàìè, ðàçðàáîòàííûìè äëÿ çàùèòû ñåêðåòíîé èíôîðìàöèè â Ôåäåðàëüíûõ êîìïüþòåðíûõ ñèñòåìàõ.
>
> C. Â ñîîòâåòñòâèè ñ Àêòîì â îáÿçàííîñòè Ìèíèñòðà òîðãîâëè, êîòîðûå îí ïåðåïîðó÷àåò NIST, âõîäèò íàçíà÷åíèå ÷ëåíîâ Êîíñóëüòàòèâíîãî êîìèòåòà ïî áåçîïàñíîñòè è çàùèùåííîñòè êîìïüþòåðíûõ ñèñòåì (Computer System Security and Privacy Advisory Board), ïî êðàéíåé ìåðå ÷ëåíà, ïðåäñòàâëÿþùåãî NSA.
>
> Ñëåäîâàòåëüíî, äëÿ îáåñïå÷åíèÿ öåëåé äàííîãî MOU Äèðåêòîð NIST è Äèðåêòîð NSA íàñòîÿùèì ïðèçíàþò ñëåäóþùåå:
>
> I. NIST áóäåò:
>
> 1. Íàçíà÷àòü â Êîíñóëüòàòèâíûé êîìèòåò ïî áåçîïàñíîñòè è çàùèùåííîñòè êîìïüþòåðíûõ ñèñòåì ïî êðàéíåé ìåðå îäíîãî ïðåäñòàâèòåëÿ, çàìåùàþùåãî Äèðåêòîðà NSA.

2. Îïèðàòüñÿ íà ðàçðàáîòàííûå NSA ðóêîâîäñòâà ïî òåõíè÷åñêîé áåçîïàñíîñòè êîìïüþòåðíûõ ñèñòåì äî òîé ñòåïåíè, â êîòîðîé NIST îïðåäåëÿåò, ÷òî ýòè ðóêîâîäñòâà îòâå÷àþò òðåáîâàíèÿì, ïðåäúÿâëÿåìûì ê çàùèòå âàæíîé èíôîðìàöèè â Ôåäåðàëüíûõ êîìïüþòåðíûõ ñèñòåìàõ.

3. Ïðèçíàâàòü ñåðòèôèêàöèîííûé NSA ðåéòèíã äîâåðåííûõ ñèñòåì â ñîîòâåòñòâèè ñ Ïðîãðàììîé êðèòåðèåâ îöåíêè áåçîïàñíîñòè äîâåðåííûõ êîìïüþòåðîâ áåç äîïîëíèòåëüíîé ýêñïåðòèçû.

4. Ðàçðàáàòûâàòü ñòàíäàðòû áåçîïàñíîñòè òåëåêîììóíèêàöèé äëÿ çàùèòû âàæíûõ íåñåêðåòíûõ êîìïüþòåðíûõ äàííûõ, ìàêñèìàëüíî îïèðàÿñü íà ðåçóëüòàòû ýêñïåðòèçû è ðàçðàáîòêè Àãåíòñòâà íàöèîíàëüíîé áåçîïàñíîñòè, ÷òîáû âûïîëíÿòü ýòè îáÿçàííîñòè ñâîåâðåìåííî è ýôôåêòèâíî.

5. Ïî âîçìîæíîñòè èçáåãàòü äóáëèðîâàíèÿ, ðàçãðàíè÷èâ ñîâìåñòíûå ðàáîòû ñ NSA äëÿ ïîëó÷åíèÿ ïîìîùè NSA.

6. Çàïðàøèâàòü ïîìîùè NSA ïî âñåì âîïðîñàì, ñâÿçàííûì ñ êðèïòîãðàôè÷åñêèìè àëãîðèòìàìè è êðèïòîãðàôè÷åñêèìè ìåòîäàìè, âêëþ÷àÿ èññëåäîâàíèÿ, îöåíêó ðàçðàáîòêè, îäîáðåíèå, íî íå îãðàíè÷èâàÿñü ýòèìè äåéñòâèÿìè.

II. NSA áóäåò:

1. Îáåñïå÷èâàòü NIST òåõíè÷åñêèìè ðóêîâîäñòâàìè ïî äîâåðåííûì òåõíîëîãèÿì, áåçîïàñíîñòè òåëåêîììóíèêàöèé è èäåíòèôèêàöèè ëè÷íîñòè, êîòîðûå ìîãóò áûòü èñïîëüçîâàíû â ðåíòàáåëüíûõ ñèñòåìàõ çàùèòû âàæíûõ êîìïüþòåðíûõ äàííûõ.

2. Ïðîâîäèòü èëè èíèöèèðîâàòü èññëåäîâàòåëüñêèå è ïðîåêòíûå ïðîãðàììû ïî äîâåðåííûì òåõíîëîãèÿì, áåçîïàñíîñòè òåëåêîììóíèêàöèé, êðèïòîãðàôè÷åñêèì ìåòîäàì è ìåòîäàì èäåíòèôèêàöèè ëè÷íîñòè.

3. Ïî ïðîñüáàì NIST îêàçûâàòü ïîìîùü â îòíîøåíèè âñåõ âîïðîñîâ, ñâÿçàííûõ ñ êðèïòîãðàôè÷åñêèìè àëãîðèòìàìè è êðèïòîãðàôè÷åñêèìè ìåòîäàìè, âêëþ÷àÿ èññëåäîâàíèÿ, îöåíêó ðàçðàáîòêè, îäîáðåíèå, íî íå îãðàíè÷èâàÿñü ýòèìè äåéñòâèÿìè.

4. Óñòàíàâëèâàòü ñòàíäàðòû è îäîáðÿòü èçäåëèÿ äëÿ ïðèìåíåíèÿ â áåçîïàñíûõ ñèñòåìàõ, îõâàòûâàåìûõ 10 USC ðàçäåë 2315 (Ïîïðàâêà Óîðíåðà).

5. Ïî òðåáîâàíèþ ôåäåðàëüíûõ îðãàíèçàöèé, èõ ïîäðÿä÷èêîâ è äðóãèõ ôèíàíñèðóåìûõ ïðàâèòåëüñòâîì ñóáúåêòîâ ïðîâîäèòü îöåíêó âîçìîæíîñòè âðàæåñêîé ðàçâåäûâàòåëüíîé äåÿòåëüíîñòè â îòíîøåíèè ôåäåðàëüíûõ èíôîðìàöèîííûõ ñèñòåì, à òàêæå îáåñïå÷èâàòü òåõíè÷åñêîå ñîäåéñòâèå è ðåêîìåíäîâàòü èçäåëèÿ, îäîáðåííûå äëÿ ïðèìåíåíèÿ â áåçîïàñíûõ ñèñòåìàõ, ÷òîáû ïðîòèâîñòîÿòü òàêîé óãðîçå.

III. NIST è NSA áóäóò:

1. Êîîðäèíèðîâàòü ñâîè ïëàíû ïî îáåñïå÷åíèþ áåçîïàñíîñòè è çàùèùåííîñòè êîìïüþòåðíûõ ñèñòåì, çà êîòîðûå NIST è NSA íåñóò îòâåòñòâåííîñòü â ñîîòâåòñòâèè ñ ðàçäåëîì 6(b) Àêòà.

2. Îáìåíèâàòüñÿ òåõíè÷åñêèìè ñòàíäàðòàìè è ðóêîâîäñòâàìè, åñëè ýòî íåîáõîäèìî äëÿ äîñòèæåíèÿ öåëåé Àêòà.

3. Ñîâìåñòíî ðàáîòàòü íàä äîñòèæåíèåì öåëåé ýòîãî ìåìîðàíäóìà ñ ìàêñèìàëüíîé ýôôåêòèâíîñòüþ, èçáåãàÿ íåíóæíîãî äóáëèðîâàíèÿ óñèëèé.

4. Ïîääåðæèâàòü íåïðåðûâíûé äèàëîã, ãàðàíòèðóþùèé, ÷òî êàæäàÿ èç îðãàíèçàöèé áóäåò íàõîäèòüñÿ íà îäèíàêîâîì óðîâíå ñîâðåìåííûõ òåõíîëîãèé è âîïðîñîâ, âëèÿþùèõ íà áåçîïàñíîñòü àâòîìàòèçèðîâàííûõ èíôîðìàöèîííûõ êîìïüþòåðíûõ ñèñòåì.

5. Îðãàíèçîâûâàòü òåõíè÷åñêóþ ðàáî÷óþ ãðóïïó äëÿ îáçîðà è àíàëèçà îáëàñòåé ñîâìåñòíûõ èíòåðåñîâ, êàñàþùèõñÿ çàùèòû ñèñòåì, îáðàáàòûâàþùèõ âàæíóþ èëè äðóãóþ íåñåêðåòíóþ èíôîðìàöèþ. Ýòà Ãðóïïà áóäåò ñîñòîÿòü èç øåñòè Ôåäåðàëüíûõ ñëóæàùèõ, ïî òðîå îò NIST è NSA, è ïðè íåîáõîäèìîñòè ìîæåò áûòü óâåëè÷åíà çà ñ÷åò ïðåäñòàâèòåëåé äðóãèõ îðãàíèçàöèé. Òåìû ðàáîòû ãðóïïû ìîãóò îïðåäåëÿòüñÿ ëèáî çàìåñòèòåëåì äèðåêòîðà NSA ïî èíôîðìàöèîííîé áåçîïàñíîñòè, ëèáî çàìåñòèòåëåì äèðåêòîðà NIST, ëèáî ìîãóò èíèöèèðîâàòüñÿ ñàìîé ãðóïïîé ñ ïîñëåäóþùèì îäîáðåíèåì çàìåñòèòåëåì äèðåêòîðà NSA ïî èíôîðìàöèîííîé áåçîïàñíîñòè èëè çàìåñòèòåëåì äèðåêòîðà NIST. Â òå÷åíèå íåñêîëüêèõ äíåé ïîñëå ïîñòàíîâêè ïåðåä Ãðóïïîé âîïðîñà ëèáî çàìåñòèòåëåì äèðåêòîðà NSA ïî èíôîðìàöèîííîé áåçîïàñíîñòè, ëèáî çàìåñòèòåëåì äèðåêòîðà NIST Ãðóïïà äîëæíà ïðåäñòàâèòü îò÷åò î âûïîëíåíèè ðàáîò ïî ýòîìó âîïðîñó è, ïðè íåîáõîäèìîñòè, ïëàí äàëüíåéøåãî àíàëèçà.

6. Íà åæåãîäíîé îñíîâå îáìåíèâàòüñÿ ïëàíàìè ðàáîòû ïî âñåì èññëåäîâàòåëüñêèì è êîíñòðóêòîðñêèì ïðîåêòàì, ñâÿçàííûì ñ çàùèòîé ñèñòåì, îáðàáàòûâàþùèõ âàæíóþ èëè äðóãóþ íåñåêðåòíóþ èíôîðìàöèþ, âêëþ÷àÿ äîâåðåííûå òåõíîëîãèè, çàùèòó öåëîñòíîñòè è äîñòóïíîñòè äàííûõ, áåçîïàñíîñòè òåëåêîììóíèêàöèé è ìåòîäîâ èäåíòèôèêàöèè ëè÷íîñòè. Îáìåí èíôîðìàöèåé ïî ïðîåêòàì äîëæåí ïðîèñõîäèòü åæåêâàðòàëüíî, è îáçîð ñîñòîÿíèÿ ïðîåêòîâ äîëæåí ëþáîé èç ñòîðîí ïðåäîñòàâëÿòüñÿ ïî çàïðîñó äðóãîé ñòîðîíû.

7. Ïðîâåðÿòü îáçîðû òåõíè÷åñêîé ðàáî÷åé ãðóïïû äî îïóáëèêîâàíèÿ âñåõ âîïðîñîâ, êàñàþùèõñÿ òåõíèêè îáåñïå÷åíèÿ áåçîïàñíîñòè ñèñòåì, ðàçðàáàòûâàåìûõ äëÿ èñïîëüçîâàíèÿ ïðè çàùèòå âàæíîé èíôîðìàöèè â ôåäåðàëüíûõ êîìïüþòåðíûõ ñèñòåìàõ, ÷òîáû ãàðàíòèðîâàòü ñîâìåñòèìîñòü ðàñêðûòèÿ ýòèõ òåì ñ íàöèîíàëüíîé áåçîïàñíîñòüþ Ñîåäèíåííûõ Øòàòîâ. Åñëè NIST è NSA íå ñìîãóò ðåøèòü ïîäîáíûé âîïðîñ â òå÷åíèå 60 äíåé, ëþáàÿ èç îðãàíèçàöèé ìîæåò ïîäíÿòü ýòîò âîïðîñ ïåðåä Ìèíèñòðîì îáîðîíû è Ìèíèñòðîì òîðãîâëè. Ïðèçíàåòñÿ, ÷òî äàííûé âîïðîñ ñ ïîìîùüþ NSC ìîæåò áûòü ïåðåäàí äëÿ ðåøåíèÿ Ïðåçèäåíòó. Íèêàêèå äåéñòâèÿ íå äîëæíû ïðåäïðèíèìàòüñÿ äî îêîí÷àòåëüíîãî ðåøåíèÿ âîïðîñà.

8. Îïðåäåëÿòü äîïîëíèòåëüíûå ðàáî÷èå ñîãëàøåíèÿ, çàêëþ÷åííûå ìåæäó NSA è NIST, êàê ïðèëîæåíèÿ ê ýòîìó MOU.

IV. Ëþáàÿ èç ñòîðîí ìîæåò ïðåêðàòèòü äåéñòâèå ýòîãî MOU ïèñüìåííûì óâåäîìëåíèåì, íàïðàâëåííûì çà øåñòü ìåñÿöåâ äî ïðåêðàùåíèÿ äåéñòâèÿ. Ýòîò MOU ñ÷èòàåòñÿ äåéñòâèòåëüíûì ïðè íàëè÷èè îáåèõ ïîäïèñåé.

/ïîäïèñàíî/

ÐÝÉÌÎÍÄ. ÄÆ. ÊÀÌÌÅÐ
Èñïîëíèòåëüíûé Äèðåêòîð, Íàöèîíàëüíûé èíñòèòóò ñòàíäàðòîâ è òåõíèêè, 24 ìàðòà 1989 ãîäà

Ó. Î. ÑÒÜÞÄÌÅÍ
Âèöå-àäìèðàë, ÂÌÑ ÑØÀ, Äèðåêòîð, Àãåíòñòâî íàöèîíàëüíîé áåçîïàñíîñòè, 23 ìàðòà 1989 ãîäà

25.4 RSA Data Security, Inc.

RSA Data Security, Inc. (RSADSI) áûëà îñíîâàíà â 1982 ãîäó äëÿ ðàçðàáîòêè, ëèöåíçèðîâàíèÿ è êîììåð÷åñêîãî èñïîëüçîâàíèÿ ïàòåíòà RSA. Ó êîìïàíèè åñòü ðÿä êîììåð÷åñêèõ ïðîäóêòîâ, âêëþ÷àÿ îòäåëüíûé ïàêåò áåçîïàñíîñòè ýëåêòðîííîé ïî÷òû, è ðàçëè÷íûå êðèïòîãðàôè÷åñêèå áèáëèîòåêè (äîñòóïíûå â âèäå èñõîäíûõ òåêñòîâ èëè îáúåêòíîãî êîäà). RSADSI òàêæå ïðåäëàãàåò íà ðûíêå ñèììåòðè÷íûå àëãîðèòìû RC2 è RC4 (ñì. ðàçäåë 11.8). RSA Laboratories, èññëåäîâàòåëüñêàÿ ëàáîðàòîðèÿ, ñâÿçàííàÿ ñ RSADSI, âûïîëíÿåò ôóíäàìåíòàëüíûå êðèïòîãðàôè÷åñêèå èññëåäîâàíèÿ è îêàçûâàåò êîíñóëüòàöèîííûå óñëóãè.

Ïðè çàèíòåðåñîâàííîñòè â ëèöåíçèÿõ èëè ïðîäóêòàõ íóæíî îáðàùàòüñÿ ê äèðåêòîðó ïî ïðîäàæàì (Director of Sales, RSA Data Security, Inc., 100 Marine Parkway, Redwood City, CA 94065; (415) 595-8782; ôàêñ: (415) 595-1873).

25.5 PUBLIC KEY PARTNERS

Ïÿòü ïàòåíòîâ, ïåðå÷èñëåííûõ â 22-é, ïðèíàäëåæàò Public Key Partners (PKP) èç Ñàííèâýéëà (Sunnyvale), Êàëèôîðíèÿ, ïàðòíåðñòâó RSADSI è Care-Kahn, Inc. - ðîäèòåëüñêîé êîìïàíèè Cylink. (RSADSI ïîëó÷àåò 65 ïðîöåíòîâ ïðèáûëè, à Care-Kahn 35 ïðîöåíòîâ.) PKP óòâåðæäàåò, ÷òî ýòè ïàòåíòû è 4218582 îñîáåííî ïðèìåíèìû êî *âñåì ñïîñîáàì èñïîëüçîâàíèÿ* êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè.

Òàáë. 25-3.
Ïàòåíòû Public Key Partners

¹ ïàòåíòà	Äàòà	Èçîáðåòàòåëè	Íàçâàíèå ïàòåíòà
4200770	29.3.80	Hellman, Diffie, Merkle	Îáìåí êëþ÷àìè Diffie-Hellman
4218582	19.8.80	Hellman, Merkle	Ðþêçàêè Merkle-Hellman
4405829	20.9.83	Rivest, Shamir, Adleman	RSA
4424414	3.3.84	Hellman, Pohlig	Pohlig-Hellman
4995082	19.2.91	Schnorr	Ïîäïèñè Schnorr

Â [574], PKP ïèñàëà:

> Ýòè ïàòåíòû [4200770, 4218582, 4405829 è 4424414] îõâàòûâàþò âñå èçâåñòíûå ìåòîäû èñïîëüçîâàíèÿ èñêóññòâà îòêðûòûõ êëþ÷åé, âêëþ÷àÿ âàðèàíòû, îáîáùåííî èçâåñòíûå êàê ElGamal.
>
> Áëàãîäàðÿ øèðîêîìó ðàñïðîñòðàíåíèþ öèôðîâûõ ïîäïèñåé RSA â ìåæäóíàðîäíîì ñîîáùåñòâå Public Key Partners ðåøèòåëüíî îäîáðÿåò èõ âêëþ÷åíèå â ñòàíäàðò öèôðîâîé ïîäïèñè. Ìû çàâåðÿåì âñå çàèíòåðåñîâàííûå ñòîðîíû, ÷òî Public Key Partners ïîä÷èíèòñÿ âñåì ðåøåíèÿì ANSI è IEEE, êàñàþùèìñÿ äîñòóïíîñòè ëèöåíçèðîâàíèÿ ýòîãî èñêóññòâà. Îñîáåííî äëÿ ïîääåðæêè ëþáûõ ïðèíèìàåìûõ ñòàíäàðòîâ, èñïîëüçóþùèõ öèôðîâóþ ïîäïèñü RSA. Public Key Partners íàñòîÿùèì çàâåðÿåò, ÷òî ëèöåíçèè íà èñïîëüçîâàíèå ïîäïèñåé RSA áóäóò ïðåäîñòàâëÿòüñÿ â ðàçóìíûå ñðîêè, íà ðàçóìíûõ óñëîâèÿõ è áåç êàêîé-ëèáî äèñêðèìèíàöèè.

Ïðàâäà ëè ýòî, çàâèñèò îò òîãî, ñ êåì âû ãîâîðèòå. Ëèöåíçèè PKP, êàê ïðàâèëî, ñåêðåòíû, ïîýòîìó ñïîñîáà ïðîâåðèòü, îòëè÷àåòñÿ ëè äàííàÿ ëèöåíçèÿ îò äðóãèõ, íå ñóùåñòâóåò. Õîòÿ êîìïàíèÿ óòâåðæäàåò, ÷òî íèêîìó íå îòêàçàëà â âûäà÷å ëèöåíçèè, ïî êðàéíåé ìåðå äâå êîìïàíèè ãîâîðÿò î òîì, ÷òî èì ëèöåíçèÿ âûäàíà íå áûëà. PKP òùàòåëüíî îõðàíÿåò ñâîè ïàòåíòû, óãðîæàÿ âñåì, êòî èñïîëüçóåò áåç ëèöåíçèðîâàíèÿ êðèïòîãðàôèþ ñ îòêðûòûìè êëþ÷àìè. ×àñòè÷íî ýòî ðåàêöèÿ íà ïàòåíòíîå çàêîíîäàòåëüñòâî ÑØÀ. Åñëè âëàäåëüöó ïàòåíòà íå óäàåòñÿ íàêàçàòü íàðóøèòåëÿ ïàòåíòà, îí ìîæåò ïîòåðÿòü ñâîé ïàòåíò. Áûëî ìíîãî ðàçãîâîðîâ î çàêîííîñòè ýòèõ ïàòåíòîâ, íî äàëüøå ðàçãîâîðîâ äåëî íå ïîøëî. Âñå çàêîííûå ïðåòåíçèè ê ïàòåíòàì PKP áûëè óðåãóëèðîâàíû äî ñóäà.

ß íå ñîáèðàþñü â ýòîé êíèãå äàâàòü þðèäè÷åñêèå ñîâåòû. Ìîæåò áûòü ïàòåíò RSA íå óñòîèò ïåðåä ñóäîì. Ìîæåò áûòü ýòè ïàòåíòû íå ïðèìåíèìû êî âñåé êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè. (×åñòíî ãîâîðÿ, ÿ íå ïîíèìàþ, êàê îíè îõâàòûâàþò ElGamal èëè êðèïòîñèñòåìû ñ ýëëèïòè÷åñêèìè êðèâûìè.) Ìîæåò êîìó-òî óäàñòñÿ âûèãðàòü ïðîöåññ ïðîòèâ PKP èëè RSADSI. Íî íå çàáûâàéòå, ÷òî êîðïîðàöèè ñ îãðîìíûìè þðèäè÷åñêèìè îòäåëàìè, íàïðèìåð, IBM, Microsoft, Lotus, Apple, Novell, Digital, National Semiconductor, AT&T è Sun, ëèöåíçèðîâàëè RSA äëÿ èñïîëüçîâàíèÿ â ñâîèõ ïðîäóêòàõ, à íå îáðàùàëèñü â ñóä. Boeing, Shell Oil, DuPont, Raytheon è Citicorp - âñå ëèöåíçèðîâàëè RSA äëÿ ñâîåãî âíóòðåííåãî èñïîëüçîâàíèÿ.

Â îäíîì ñëó÷àå PKP âîçáóäèëî ïðîöåññ ïðîòèâ TRW Corporation ïî ïîâîäó èñïîëüçîâàíèÿ áåç ëèöåíçèðîâàíèÿ àëãîðèòìà ElGamal. TRW óòâåðæäàëà, ÷òî åé íå íóæíà ëèöåíçèÿ. PKP è TRW äîñòèãëè ñîãëàøåíèÿ â èþíå 1992. Ïîäðîáíîñòè óðåãóëèðîâàíèÿ êîíôëèêòà íåèçâåñòíû, íî ñðåäè íèõ - ñîãëàñèå TRW ïîëó÷èòü ëèöåíçèþ íà ïàòåíòû. Ýòî íå ïðåäâåùàåò íè÷åãî õîðîøåãî. TRW ìîãëà ïîçâîëèòü ñåáå õîðîøèõ þðèñòîâ. ß ìîãó òîëüêî ïðåäïîëîæèòü, ÷òî, åñëè áû TRW áûëà óâåðåíà, ÷òî ñìîæåò âûèãðàòü ïðîöåññ, íå ïîòðàòèâ íåâåðîÿòíîãî êîëè÷åñòâà äåíåã, îíà áû íå îòêàçàëàñü îò áîðüáû.

Òåì íå ìåíåå â PKP ñóùåñòâóþò ñâîè âíóòðåííèå ïðîáëåìû. Â èþíå 1994 ãîäà Care-Kahn ïîäàëà â ñóä íà RSADSI, çàÿâèâ, ñðåäè âñåãî îñòàëüíîãî, ÷òî ïàòåíò RSA íåïðàâèëåí è íåïðèìåíèì [401]. Îáà ïàðòíåðà ïîïûòàëèñü ðàçîðâàòü ñâîå ïàðòíåðñòâî. Çàêîííû ïàòåíòû èëè íåò? Íóæíî ëè áóäåò ïîëüçîâàòåëÿì ïîëó÷àòü ëèöåíçèþ îò Care-Kahn, ÷òîáû ïîëüçîâàòüñÿ àëãîðèòìîì RSA? Êîìó áóäåò ïðèíàäëåæàòü ïàòåíò Schnorr? Âîçìîæíî ýòî äåëî áóäåò óðåãóëèðîâàíî ê ìîìåíòó âûõîäà ýòîé êíèãè.

Ïàòåíòû äåéñòâèòåëüíû ëèøü â òå÷åíèå Patents 17 ëåò è íå ìîãóò áûòü âîçîáíîâëåíû. 29 ìàðòà 1997 ãîäà îáìåí êëþ÷àìè Diffie-Hellman (è àëãîðèòì ElGamal) ñòàíóò îáùåäîñòóïíûìè. 20 ñåíòÿáðÿ 2000 ãîäà ñòàíåò îáùåäîñòóïíûì è RSA. Ïîìåòüòå íà ñâîèõ êàëåíäàðÿõ.

25.6 Ìåæäóíàðîäíàÿ àññîöèàöèÿ êðèïòîëîãè÷åñêèõ èññëåäîâàíèé

Ìåæäóíàðîäíàÿ àññîöèàöèÿ êðèïòîëîãè÷åñêèõ èññëåäîâàíèé (International Association for Cryptologic Research, IACR) - ýòî âñåìèðíàÿ êðèïòîãðàôè÷åñêàÿ èññëåäîâàòåëüñêàÿ îðãàíèçàöèÿ. Åå öåëüþ ÿâëÿåòñÿ ðàçâèòèå òåîðèè è ïðàêòèêè êðèïòîëîãèè è ñâÿçàííûõ îáëàñòåé. Åå ÷ëåíîì ìîæåò ñòàòü ëþáîé. Àññîöèàöèÿ âûñòóïàåò

ñïîíñîðîì äâóõ åæåãîäíûõ êîíôåðåíöèé, Crypto (ïðîâîäèòñÿ â àâãóñòå â Ñàíòà-Áàðáàðå) è Eurocrypt (ïðîâîäèòñÿ â â Åâðîïå), è åæåêâàðòàëüíî èçäàåò *The Journal of Cryptology* è *IACR Newsletter*.

Àäðåñ øòàá-êâàðòèðû IACR ìåíÿåòñÿ âìåñòå ñî ñìåíîé ïðåçèäåíòà. Òåêóùèé àäðåñ: IACR Business Office, Aarhus Science Park, Custav Wieds Vej 10, DK-8000 Aarhus C, Denmark.

25.7 Îöåíêà ïðèìèòèâîâ öåëîñòíîñòè RACE (RIPE)

Ïðîãðàììà èññëåäîâàíèÿ è ðàçâèòèÿ ïåðåäîâûõ ñðåäñòâ ñâÿçè â Åâðîïå (Research and Development in Advanced Communication Technologies in Europe, RACE) áûëà èíèöèèðîâàíà Åâðîïåéñêèì ñîîáùåñòâîì äëÿ ïîääåðæêè ïðåäâàðèòåëüíîé ïðîðàáîòêè òåëåêîììóíèêàöèîííûõ ñòàíäàðòîâ è òåõíîëîãèé, ïîääåðæèâàþùèõ Èíòåãðèðîâàííûå âûñîêîñêîðîñòíûå ñðåäñòâà ñâÿçè (Integrated Broadband Communication, IBC). Â êà÷åñòâå ÷àñòè ýòîé ðàáîòû RACE ó÷ðåäèëî êîíñîðöèóì äëÿ Îöåíêè ïðèìèòèâîâ öåëîñòíîñòè RACE (RACE Integrity Primitives Evaluation, RIPE), ÷òîáû ñîáðàòü â îäíî öåëîå ïàêåò òåõíîëîãèé, ñîîòâåòñòâóþùèõ âîçìîæíûì òðåáîâàíèÿì ê áåçîïàñíîñòè IBC.

Êîíñîðöèóì RIPE îáðàçîâàëè øåñòü âåäóùèõ åâðîïåéñêèõ êðèïòîãðàôè÷åñêèõ èññëåäîâàòåëüñêèõ ãðóïï: Öåíòð ïî ìàòåìàòèêå è êîìïüþòåðíûì íàóêàì (Center for Mathematics and Computer Science), Àìñòåðäàì; Siemens AG; Philips Crypto BV; Royal PTT Nederland NV, PTT Research; Katholieke Univesiteit Leuven è Aarhus Universitet. Ïîñëå îáúÿâëåíèé î ïðèåìå àëãîðèòìîâ â 1989 è 1991 ãîäàõ [1564], ïîäà÷è 32 çàÿâîê, ïðèñëàííûõ ñî âñåãî ìèðà, è ñîáñòâåííî îöåíèâàþùåãî ïðîåêòà äëèòåëüíîñòüþ 350 ÷åëîâåêî-ìåñÿöåâ, êîíñîðöèóì îïóáëèêîâàë *RIPE Integrity Primitives* [1305, 1332]. Îò÷åò ñîäåðæèò ââåäåíèå, íåñêîëüêî îñíîâíûõ êîíöåïöèé öåëîñòíîñòè è èõ ïðèìèòèâû: MDC-4 (ñì. ðàçäåë 14.11), RIPE-MD (ñì. ðàçäåë 14.8), RIPE-MAG (ñì. ðàçäåë 14.14), IBC-HASH, SKID (ñì. ðàçäåë 3.2), RSA, COMSET (ñì. ðàçäåë 16.1) è ãåíåðàöèþ êëþ÷åé RSA.

25.8 Óñëîâíûé äîñòóï äëÿ Åâðîïû (CAFE)

Óñëîâíûé äîñòóï äëÿ Åâðîïû (Conditional Access for Europe, CAFE) - ýòî ïðîåêò â ðàìêàõ ïðîãðàììû ESPRIT Åâðîïåéñêîãî ñîîáùåñòâà [204, 205]. Ðàáîòà íà÷àëàñü â äåêàáðå 1992 ãîäà è ïî ïëàíó äîëæíà çàêîí÷èòüñÿ ê êîíöó 1995 ãîäà. Îáðàçîâàííûé êîíñîðöèóì ñîñòîèò èç ãðóïï ñîöèàëüíûõ èññëåäîâàíèé è èññëåäîâàíèé ðûíêà (Cardware, Institut fur Sozialforschung), èçãîòîâèòåëåé ïðîãðàììíîãî îáåñïå÷åíèÿ è àïïàðàòóðû (DigiCash, Gemplus, Ingenico, Siemens), à òàêæå êðèïòîãðàôîâ (CWI Amsterdam, PTT Research Netherlands, SPET, Sintef Delab Trondheim, Universities of Arhus, Hildesheim and Leuven).

Öåëü ïðîåêòà ÿâëÿåòñÿ ðàçðàáîòêà ñèñòåìû óñëîâíîãî äîñòóïà, îñîáåííî äëÿ öèôðîâûõ ïëàòåæíûõ ñèñòåì. Ïëàòåæíûå ñèñòåìû äîëæíû îáåñïå÷èâàòü íàäåæíîñòü äëÿ êàæäîãî ïîëüçîâàòåëÿ è òðåáîâàòü êàê ìîæíî ìåíüøå âåðû â ñåáÿ - íàäåæíîñòü íå äîëæíà çàâèñåòü îò óñòîé÷èâîñòè óñòðîéñòâ ê âçëîìó.

Îñíîâíûì óñòðîéñòâîì CAFE ñëóæèò ýëåêòðîííûé áóìàæíèê: ìàëåíüêèé êîìïüþòåð, î÷åíü ïîõîæèé íà êàðìàííûé êàëüêóëÿòîð. Ó íåãî åñòü áàòàðåéêà, êëàâèàòóðà, ýêðàí è èíôðàêðàñíûé êàíàë äëÿ ñâÿçè ñ äðóãèìè áóìàæíèêàìè. Ó êàæäîãî ïîëüçîâàòåëÿ ñâîé ñîáñòâåííûé áóìàæíèê, êîòîðûé îáåñïå÷èâàåò åãî ïðàâà è ãàðàíòèðóåò åãî áåçîïàñíîñòü.

Ó óñòðîéñòâà ñ êëàâèàòóðîé è ýêðàíîì åñòü îïðåäåëåííîå ïðåèìóùåñòâî ïåðåä èíòåëëåêòóàëüíîé êàðòîé - îíî ìîæåò ðàáîòàòü íåçàâèñèìî îò òåðìèíàëà. Ïîëüçîâàòåëü ìîæåò íåïîñðåäñòâåííî ââåñòè ñâîé ïàðîëü è ñóììó ïëàòåæà. Îòëè÷èå îò êðåäèòíîé êàðòû ïîëüçîâàòåëþ íå íóæíî îòäàâàòü ñâîé áóìàæíèê êîìó-òî, ÷òîáû âûïîëíèòü òðàíçàêöèþ. Äîïîëíèòåëüíûìè âîçìîæíîñòÿìè ÿâëÿþòñÿ:

— Àâòîíîìíûå òðàíçàêöèè. Ñèñòåìà ïðåäíàçíà÷åíà äëÿ çàìåíû îáðàùåíèÿ íåáîëüøèõ ñóìì íàëè÷íûõ, äèàëîãîâàÿ ñèñòåìà áûëà áû ñëèøêîì ãðîìîçäêà.

— Óñòîé÷èâîñòü ê ïîòåðÿì. Åñëè ïîëüçîâàòåëü ïîòåðÿåò ñâîé áóìàæíèê, èëè áóìàæíèê ñëîìàåòñÿ, èëè åãî óêðàäóò, ïîëüçîâàòåëü íå ïîòåðÿåò ñâîè äåíüãè.

— Ïîääåðæêà ðàçëè÷íûõ âàëþò.

— Îòêðûòàÿ àðõèòåêòóðà è îòêðûòàÿ ñèñòåìà. Ïîëüçîâàòåëü äîëæåí èìåòü âîçìîæíîñòü çàïëàòèòü çà ïðîèçâîëüíûå óñëóãè, íàïðèìåð, ïîêóïêè â ìàãàçèíå, òåëåôîí, îáùåñòâåííûé òðàíñïîðò, ïðåäîñòàâëÿåìûå ðàçëè÷íûìè ïîñòàâùèêàìè. Ñèñòåìà äîëæíà îáåñïå÷èâàòü âçàèìîäåéñòâèå ëþáîãî êîëè÷åñòâà ýìèòåíòîâ ýëåêòðîííûõ äåíåã, à òàêæå âçàèìîäåéñòâèå áóìàæíèêîâ ðàçëè÷íûõ òèïîâ è ïðîèçâîäèòåëåé.

— Íèçêàÿ ñòîèìîñòü.

Ê ìîìåíòó íàïèñàíèÿ ýòîé êíèãè ñóùåñòâóåò òîëüêî ïðîãðàììíàÿ âåðñèÿ ñèñòåìû, è êîíñîðöèóì ïëîòíî ðàáîòàåò íàä àïïàðàòíûì ïðîòîòèïîì.

25.9 ISO/IEC 9979

Â ñåðâèíå 80-õ ISO ñòàíäàðòèçèðîâàòü DES, êîòîðûé óæå èñïîëüçîâàëñÿ â êà÷åñòâå FIPS è ñòàíäàðòà ANSI. Ïîñëå íåêîòîðîé ïîëèòè÷åñêîé âîçíè ISO ðåøèëî íå ñòàíäàðòèçèðîâàòü êðèïòîãðàô÷åñêèå àëãîðèòìû, à ðåãèñòðèðîâàòü èõ. Çàðåãèñòðèðîâàòü ìîæíî òîëüêî àëãîðèòìû øèôðîâàíèÿ, ðåãèñòðèðîâàòü õýø-ôóíêöèè è ñõåìû ïîäïèñè íåëüçÿ. Çàðåãèñòðèðîâàòü àëãîðèòì ìîæåò ëþáàÿ íàöèîíàëüíàÿ îðãàíèçàöèÿ.

Â íàñòîÿùåå âðåìÿ ïîäàíû çàÿâêè íà ðåãèñòðàöèþ òðåõ àëãîðèòìîâ (ñì. 21-é). Ïîäà÷à çàÿâêè âêëþ÷àåò èíôîðìàöèþ îá èñïîëüçîâàíèè, ïàðàìåòðàõ, ðåæèìàõ è òåñòîâûõ âåêòîðàõ. Ïîäîòâåòü îïèñàíèå íåîáõîäèìî, ìîæíî ïîäâàòü íà ðåãèñòðàöèþ è ñâîéſòâà äëãîðèòìû.

Ôàêò ðåãèñòðàöèè àëãîðèòìà íè÷åãî íå ãîâîðèò î åãî êà÷åſòâå. Ðåãèſòðàöèÿ íå ÿâëÿåòſÿ è îäîáðåíèåì àëãîðèòìà ISO/IEC, îíà ïðîſòî ïîêàçûâàåò, ÷òî îäíà èç íàöèîíàëüíûõ îðãàíèçàöèé õî÷åò çàðåãiſòðèðîâàòü àëãîðèòì, íåçàâiſèìî îò êðèòåðèåâ, èſïîëüçóåìûõ äàííîé îðãàíèçàöèåé.

Ìåíÿ íå âïå÷àòëèëà ýòà èäåÿ. Ðåãiſòðàöèÿ ìåøàåò ïðîöåſſó ñòàíäàðòèçàöèè. Âìåſòî òîãî, ÷òîáû ïðèſÿòü íåſêîëüêî àëãîðèòìîâ, ISO ðåãiſòðèðóåò ëþáîé àëãîðèòì. Ïðè òàêîì êîíôëiêòå ìîæíî çàðåãiſòðèðîâàòü âñå, ÷òî óãîäíî, è äàëåå ſ ïîëíûì ïðàâîì ſîïðîâîæäàòü ſâîé àëãîðèòì çâ÷íîé äîáàâêîé "Çàðåãiſòðèðîâàí ISO/IEC 9979 ". Â ëþáî ſëó÷àå ðåſſòð âëàäå National Computer Centre Ltd., Oxford Road, Manchester, MI 7ED, United Kingdom.

Òàáë. 25-4.
Çàðåãiſòðèðîâàííûå àëãîðèòìû ISO/IEC 9979

Ðåãiſòðàöèîííûé íîìåð	Íàçâàíèå
0001	B-CRYPT
0002	IDEA
0003	LUC

25.10 Ïðîôåſſèîíàëüíûå è ïðîùëåíûå ãðóïïû, à òàêæå ãðóïïû çàùèòíèêîâ ãðàæäàíſêèõ ſâîáî

Èíôîðìàöèîííûé öåíòð ïî ýëåêòðîííîé òàéíå ëè÷íîſòè (EPIC)

Èíôîðìàöèîííûé öåíòð ïî ýëåêòðîííîé òàéíå ëè÷íîſòè (Electronic Privacy Information Center, EPIC) áûë ó÷ðåæäåí â 1994 ãîäó äëÿ ïðèâëå÷åíèÿ îáſåſòâåííîſòè ê âîçíèêàþùèì âîïðîſſàì òàéſ ëè÷íîſòè, ſâÿſàííûſ ſ Íàöèîíàëüíîſ èíôîðìàöèîííſ èíôðaſſòóêòóðîſ, òàêèõ êàê ſèſòåìà Clipper, ïðåäëîæåíèÿ ſî öèôðîâîſ òåëåôîíèè, íàöèîſàëüíûå ſèſòåſû èäåíòèôèêàöèîííûõ íîſåðîâ, òàéſû èſòîðèſ áîëåçíè è ïðîäàæà ſâîäåſèſ î ſîòðåáèòåëÿõ. EPIC âîäåò ſóäåáíûå ïðîöåſſû, ſïîſíèðóåò êîſôåðåíöèè, ïóáëèêóåò îò÷åòû, èçäàåò *EPIC Alert* è ïðîâîäèò êàìïàíèè ſî âîïðîſàì òàéſû ëè÷íîſòè. Æåëàþùèå ſîðſîſåäſèòüſÿ ſîâóò îáðàòèſüſÿ ſî àäðåſſ Anyone interested in joining should contact Electronic Privacy Information Center, 666 Pennsylvania Avenue SE, Suite 301, Washington, D.C. 20003 (202,) 544-9240; ôàêſ: (202) 547-5482; Internet: info@epic.org.

Ôîíä ýëåêòðîííîãî ôðîíòèðà (EFF)

Ôîíä ýëåêòðîííîãî ôðîíòèðà (Electronic Frontier Foundation, EFF) ſîſñûòèë ſåáÿ çàùèòå ãðàæäàíſêèõ ſâàâ êèáåðſïðſſòâàíſòâå. Ðàſſìàòſâàÿ êðèſòîãðàôè÷åſêóþ ſſëèſòêó ÑØÀ, EFF ſ÷èſàåſ, ÷òî èſôîſìàöèÿ è äſſòóſ ê êðèſòîãðàôèè ſâëÿþſſ ſôóíäàìåſòàëüſûſ ſ ſðàâſè, è ſſýſòîſó ſ íèõ äſëæſû áûſ ſíÿſû ſðàâſèſåëüſſòâåſſûå îãðàíè÷åſèſ. Ôîíä îðãàſèçſâàſ ðàáſ÷óþ ãðóſſó ſſ öèôðîâîſ áåçſſàſſſſòè è òàéſà ëè÷íſſòè (Digital Privacy and Security Working Croup), êîòîðàſ ſâëÿåòſſ êîàëèöèåé. Ãðóſſà ſðſòèâſſåéſòâóåſ çàêſſó î öèôðîâîſ òåëåôſíèè è èſèöèàòèâå Clipper. EFF òàêæå ſſîâåéſòâóſò âåäåſſèſ ſðſöåſſſſâ ſðſòèſ êſíòðſëſ çà ſſêſſſſòſ êðèſòîãðàôèè [143]. Æåëàþ ùèå ſðèſſåäſèſòüſÿ ſ EFF ſſãóò ſâſçàòüſÿ ſ Electronic Frontier Foundation, 1001 C Street NW, Suite 950E, Washington, D.C. 20001; (202) 347 5400, ôàêſ: (202) 393-5509; Internet: eff@eff.org.

Àſſſîöèàöèÿ ſſ âû÷èſëèòåëſíſé òåõſèêå (ACM)

Àſſſîöèàöèÿ ſſ âû÷èſëèòåëſíſé òåõſèêå (Association for Computing Machinery, ACM) - ýòſ ſåæäſíàðſàſíàÿ êſſſüſòåðſíàÿ ſðſſſûſøåſſíàÿ ſðàâſèçàöèÿ. Â 1994 ãſäó Êſſèòåſ ſáſùåſòâåſſſſ ſſſëèòêè ACM ÑØÀ ſðåäſòâëè ſðåêðàſſûé ſò÷åſ ſ êðèſòſãðàôſ÷åſſſ ſſſëèòêå ÑØÀ [935]. Åãſ ſòſèſ ſðſ÷èſàòſ êàæäſſ, êòſ ſſòåðåſſóſſòſ ſſſëèòêè â êðèſòſãðàôèè. Åãſ ſſæſſ ſſëó÷èſſ ſ ſſſſûſüſ àſſſèſſſſãſ ftp ſ info.acm.org â /reports/acm. crypt_study/acm_crypto_study.ps.

Èíñòèòóò èíæåíåðîâ ïî ýëåêòðè÷åñòâó è ðàäèîýëåêòðîíèêå (IEEE)

Èíñòèòóò èíæåíåðîâ ïî ýëåêòðè÷åñòâó è ðàäèîýëåêòðîíèêå (Institute of Electrical and Electronics Engineers, IEEE) - ýòî äðóãàÿ ïðîôåññèîíàëüíàÿ îðãàíèçàöèÿ. Îòäåëåíèå â ÑØÀ èçó÷àåò âîïðîñû, ñâÿçàííûå ñ òàéíîé ëè÷íîñòè, âêëþ÷àÿ êðèïòîãðàôè÷åñêóþ ïîëèòèêó, èäåíòèôèêàöèîííûå íîìåðà, è çàùèòà òàéí â Internet, è ðàçðàáàòûâàåò ñîîòâåòñòâóþùèå ðåêîìåíäàöèè.

Àññîöèàöèÿ ïðîèçâîäèòåëåé ïðîãðàììíîãî îáåñïå÷åíèÿ (SPA)

Àññîöèàöèÿ ïðîèçâîäèòåëåé ïðîãðàììíîãî îáåñïå÷åíèÿ (Software Publishers Association, SPA) - ýòî òîðãîâàÿ àññîöèàöèÿ, â êîòîðóþ âõîäÿò ñâûøå 1000 êîìïàíèé, ðàçðàáàòûâàþùèõ ïðîãðàììíîå îáåñïå÷åíèå äëÿ ïåðñîíàëüíûõ êîìïàíèé. Îíè âûñòóïàþò çà îñëàáëåíèå ýêñïîðòíîãî êîíòðîëÿ â êðèïòîãðàôèè è ïîääåðæèâàþò ïåðå÷åíü êîììåð÷åñêè äîñòóïíûõ çàðóáåæíûõ ïðîäóêòîâ.

25.11 Sci.crypt

Sci.crypt - ýòî òåëåêîíôåðåíöèÿ Usenet ïî êðèïòîëîãèè. Åå ÷èòàþò ïðèìåðíî 100000 ÷åëîâåê ïî âñåìó ìèðó. Áîëüøèíñòâî ñîîáùåíèé - îáû÷íàÿ ÷åïóõà, ïåðåáðàíêà èëè è òî, è äðóãîå îäíîâðåìåííî. Íåêîòîðûå ñîîáùåíèÿ êàñàþòñÿ ïîëèòèêè, à áîëüøèíñòâî îñòàëüíûõ - ïðîñüáû ïðåäîñòàâèòü ñâåäåíèÿ èëè îáùèå. Èíîãäà â ýòîé òåëåêîíôåðåíöèè ñëó÷àéíî ïîïàäàþòñÿ ðàçëè÷íûå ñàìîðîäêè è íåêîòîðàÿ ïîëåçíàÿ èíôîðìàöèÿ. Åñëè ÷èòàòü sci.crypt ðåãóëÿðíî, ìîæíî óçíàòü, êàê èñïîëüçîâàòü íå÷òî, íàçûâàåìîå ôàéëîì-óáèéöåé.

Äðóãîé òåëåêîíôåðåíöèåé Usenet ÿâëÿåòñÿ sci.crypt.research, áîëåå óìåðåííàÿ òåëåêîíôåðåíöèÿ, ïîñâÿùåííàÿ îáñóæäåíèþ êðèïòîëîãè÷åñêèõ èññëåäîâàíèé. Â íåé ìåíüøå ñîîáùåíèé, è îíè ãîðàçäî èíòåðåñíåå.

25.12 Øèôðîïàíêè

Øèôðîïàíêè (Cypherpunks) - ýòî íåôîðìàëüíàÿ ãðóïïà ëþäåé, çàèíòåðåñîâàííûõ â îáó÷åíèè è èçó÷åíèè êðèïòîãðàôèè. Îíè òàêæå ýêñïåðèìåíòèðóþò ñ êðèïòîãðàôèåé, ïûòàÿñü ââåñòè åå â îáèõîä. Ïî èõ ìíåíèþ âñå êðèïòîãðàôè÷åñêèå èññëåäîâàíèÿ íå ïðèíåñëè îáùåñòâó íè÷åãî õîðîøåãî, òàê êàê îíî íå âîñïîëüçîâàëîñü äîñòèæåíèÿìè êðèïòîãðàôèè.

Â "Ìàíèôåñòå øèôðîïàíêîâ" Ýðèê Õüþç (Eric Hughes) ïèøåò [744]:

> Ìû, Øèôðîïàíêè, ñòðåìèìñÿ ñîçäàòü àíîíèìíûå ñèñòåìû. Ìû çàùèùàåì íàøè òàéíû ñ ïîìîùüþ êðèïòîãðàôèè, ñ ïîìîùüþ ñèñòåì àíîíèìíîé îòïðàâêè ïî÷òû, ñ ïîìîùüþ öèôðîâûõ ïîäïèñåé è ýëåêòðîííûõ äåíåã.
>
> Øèôðîïàíêè ïèøóò êîä. Ìû çíàåì, ÷òî êòî-òî äîëæåí íàïèñàòü ïðîãðàììíîå îáåñïå÷åíèå, çàùèùàþùåå òàéíû ëè÷íîñòè, è òàê êàê ïîêà ýòî íå ñäåëàíî, ìû íå ñìîæåì îáåñïå÷èòü ñîõðàíåíèå ñâîèõ òàéí, ìû ñîáèðàåìñÿ íàïèñàòü òàêèå ïðîãðàììû. Ìû ïóáëèêóåì íàø êîä, ÷òîáû íàøè äðóçüÿ Øèôðîïàíêè ìîãëè ïîïðàêòèêîâàòüñÿ è ïîèãðàòü ñ íèì. Íàø êîä ñâîáîäíî ìîæåò èñïîëüçîâàòü êòî óãîäíî è ãäå óãîäíî. Íàñ íå î÷åíü âîëíóåò, íðàâÿòñÿ ëè âàì ïðîãðàììû, êîòîðûå ìû ïèøåì. Ìû çíàåì, ÷òî ïðîãðàììíîå îáåñïå÷åíèå íåâîçìîæíî ðàçðóøèòü, è ÷òî íåâîçìîæíî ïðåêðàòèòü ðàáîòó ðàññåÿííûõ ñèñòåì.

Òå, êòî õî÷åò ïðèñîåäèíèòüñÿ ê ñïèñêó ðàññûëêè øèôðîïàíêîâ â Internet, äîëæíû îòïðàâëÿòü ïî÷òó â àäðåñ majordomo@toad.com. Ñïèñîê ðàññûëêè õðàíèòñÿ íà ftp.csua.berkeley.edu â /pub/cypherpunks.

25.13 Ïàòåíòû

Âîïðîñ î ïðîãðàììíûõ ïàòåíòàõ íåâîçìîæíî âòèñíóòü â ðàìêè ýòîé êíèãè. Õîðîøè îíè èëè íåò, îíè ñóùåñòâóþò. Â Ñîåäèíåííûõ Øòàòàõ ìîæíî ïàòåíòîâàòü àëãîðèòìû, â òîì ÷èñëå è êðèïòîãðàôè÷åñêèå. IBM âëàäååò ïàòåíòàìè DES [514]. IDEA çàïàòåíòîâàí. Çàïàòåíòîâàíû ïî÷òè âñå àëãîðèòìû ñ îòêðûòûìè êëþ÷àìè. NIST äàæå çàïàòåíòîâàë DSA. Äåéñòâèå ðÿäà êðèïòîãðàôè÷åñêèõ ïàòåíòîâ áûëî áëîêèðîâàíî âìåøàòåëüñòâîì NSA, â ñîîòâåòñòâèè ñ Àêòîì î ñåêðåòíîñòè èçîáðåòåíèé (Invention Secrecy Act) îò 1940 ãîäà è Àêòîì î íàöèîíàëüíîé áåçîïàñíîñòè (National Security Act) îò 1947 ãîäà. Ýòî îçíà÷àåò, ÷òî âìåñòî ïàòåíòà èçîáðåòàòåëü ïîëó÷àåò ñåêðåòíîå ïîñòàíîâëåíèå, è åìó çàïðåùàåòñÿ îáñóæäàòü åãî èçîáðåòåíèå ñ êåì-íèáóäü åùå.

Ó NSA åñòü îñîáûå âîçìîæíîñòè ïðè ïàòåíòîâàíèè. Àãåíòñòâî ìîæåò îáðàòèòüñÿ çà ïàòåíòîì è çàòåì áëîêèðîâàòü åãî âûäà÷ó. Ñíîâà ïîÿâëÿåòñÿ ñåêðåòíîå ïîñòàíîâëåíèå, íî òåïåðü NSA îäíîâðåìåííî è èçîáðåòàòåëü, è èçäàòåëü ïîñòàíîâëåíèÿ. Êîãäà ñïóñòÿ íåêîòîðîå âðåìÿ ñåêðåòíîå ïîñòàíîâëåíèå îòìåíÿåòñÿ, ðåãèñòðàöèîííàÿ êîíòîðà âûäàåò ïàòåíò, äåéñòâóþùèé ñòàíäàðòíûå 17 ëåò years. Ýòî áîëåå ÿâíî çàùèùàåò èçîáðåòåíèå, ÷åì õðàíåíèå åãî â ñåêðåòå. Åñëè êîìó-íèáóäü óäàñòñÿ èçîáðåñòè òî æå ñàìîå, NSA óæå ïîäàëî çàÿâêó íà ïàòåíò. Åñëè íèêîìó äðóãîìó íå óäàñòñÿ èçîáðåñòè òî æå ñàìîå, èçîáðåòåíèå îñòàåòñÿ ñåêðåòíûì.

Íåñìîòðÿ íà òî, ÷òî ïðîöåññ ïàòåíòîâàíèÿ äîëæåí íå òîëüêî çàùèùàòü èçîáðåòåíèÿ, íî è ðàñêðûâàòü èõ, áëàãîäàðÿ ýòîé óëîâêå NSA ìîæåò äåðæàòü ïàòåíò äîëüøå 17 ëåò. Îòñ÷åò 17-ëåòíåãî ñðîêà íà÷èíàåòñÿ ñ ìîìåíòà âûäà÷è ïàòåíòà, à íå ïîäà÷è çàÿâêè. Ïîêà íåÿñíî, êàê âñå ìîæåò èçìåíèòüñÿ â ñâÿçè ñ ðàòèôèêàöèåé äîãîâîðà î GATT Ñîåäèíåííûìè Øòàòàìè.

25.14 Ýêñïîðòíîå çàêîíîäàòåëüñòâî ÑØÀ

Ñîãëàñíî ïðàâèòåëüñòâó ÑØÀ êðèïòîãðàôèÿ îòíîñèòñÿ ê âîåííîìó ñíàðÿæåíèþ. Ýòî îçíà÷àåò, ÷òî êðèïòîãðàôèÿ ïîä÷èíÿåòñÿ òåì æå çàêîíàì, ÷òî è ðàêåòà TOW èëè òàíê Ì1 Àáðàìñ. Åñëè âû ïðîäàåòå êðèïòîãðàôè÷åñêèé ïðîäóêò áåç ñîîòâåòñòâóþùåé ýêñïîðòíîé ëèöåíçèè, òî âû - ìåæäóíàðîäíûé êîíòðàáàíäèñò îðóæèåì. Åñëè âû íå õîòèòå èñïîðòèòü âàøå ðåçþìå ñòðîêîé î ïðåáûâàíèè â ôåäåðàëüíîé òþðüìå, îáðàòèòå âíèìàíèå íà çàêîíîäàòåëüñòâî.

Ñ íà÷àëîì â 1949 ãîäó õîëîäíîé âîéíû âñå ñòðàíû ÍÀÒÎ (êðîìå Èñëàíäèè), à çàòåì Àâñòðàëèÿ, ßïîíèÿ è Èñïàíèÿ, îáðàçîâàëè ÊÎÊÎÌ - Êîîðäèíàöèîííûé êîìèòåò äëÿ ìíîãîñòîðîííåãî êîíòðîëÿ çà ýêñïîðòîì (CoCom, Coordinating Committee for Multilateral Export Controls). Ýòî íåîôèöèàëüíàÿ îðãàíèçàöèÿ, ïðèçâàííàÿ êîîðäèíèðîâàòü íàöèîíàëüíûå îãðàíè÷åíèÿ, êàñàþùèåñÿ ýêñïîðòà âàæíûõ âîåííûõ òåõíîëîãèé â Ñîâåòñêèé Ñîþç, äðóãèå ñòðàíû Âàðøàâñêîãî Äîãîâîðà è Êèòàéñêóþ Íàðîäíóþ Ðåñïóáëèêó. Ïðèìåðàìè êîíòðîëèðóåìûõ òåõíîëîãèé ÿâëÿþòñÿ êîìïüþòåðû, ñòàíêè äëÿ ìåòàëëîïðîêàòà è êðèïòîãðàôèÿ. Öåëüþ ýòîé îðãàíèçàöèè ÿâëÿëîñü çàìåäëåíèå ïåðåäà÷è òåõíîëîãèé â óêàçàííûå ñòðàíû, è ñäåðæèâàíèå, òàêèì îáðàçîì, èõ âîåííîãî ïîòåíöèàëà.

Ñ êîíöîì õîëîäíîé âîéíû ñòðàíû ÊÎÊÎÌ îñîçíàëè, ÷òî âûïîëíÿåìûé èìè êîíòðîëü áîëüøåé ÷àñòüþ óñòàðåë. Â íàñòîÿùåå âðåìÿ, ïî âèäèìîìó, èäåò ïðîöåññ ôîðìèðîâàíèÿ "Íîâîãî ôîðóìà", äðóãîé ìåæäóíàðîäíîé îðãàíèçàöèè, êîòîðàÿ ñîáèðàåòñÿ îñòàíîâèòü ïîòîê âîåííûõ òåõíîëîãèé â ñòðàíû, êîòîðûå íå íðàâÿòñÿ ÷ëåíàì îðãàíèçàöèè.

Â ëþáîì ñëó÷àå ýêñïîðòíàÿ ïîëèòèêà ÑØÀ â îòíîøåíèè ñòðàòåãè÷åñêèõ òîâàðîâ ðåãóëèðóåòñÿ Ïðàâèòåëüñòâåííûì àêòîì îá ýêñïîðòå (Export Administration Act), Àêòîì î êîíòðîëå íàä ýêñïîðòîì âîîðóæåíèÿ (Arms Export Control Act), Àêòîì îá àòîìíîé ýíåðãèè (Atomic Energy Act) è Àêòîì î íåðàñïðîñòðàíåíèè ÿäåðíûõ âîîðóæåíèé (Nuclear Non-Proliferation Act). Êîíòðîëü, óñòàíîâëåííûé ýòèì çàêîíîäàòåëüñòâîì, ðåàëèçóåòñÿ ñ ïîìîùüþ ìíîãèõ ïîäçàêîííûõ àêòîâ, íè îäèí èç íèõ íå êîîðäèíèðóåò äðóãîé. Ñâûøå äþæèíû îðãàíèçàöèé, âêëþ÷àÿ âîåííûå ñëóæáû, îñóùåñòâëÿþò êîíòðîëü, ÷àñòî èõ äåÿòåëüíîñòü ïåðåêðûâàåòñÿ è êîíôëèêòóåò.

Ïîäêîíòðîëüíûå òåõíîëîãèè ôèãóðèðóþò â íåñêîëüêèõ ñïèñêàõ. Êðèïòîãðàôèÿ, ïî òðàäèöèè îòíîñÿùàÿñÿ ê âîîðóæåíèþ, ïîÿâëÿåòñÿ â Ïåðå÷íå âîîðóæåíèé ÑØÀ (U.S. Munitions List, USML), Ìåæäóíàðîäíîì ïåðå÷íå âîîðóæåíèé (International Munitions List, IML), Ïåðå÷íå êîíòðîëÿ çà òîðãîâëåé (Commerce Control List, CCL) è Ìåæäóíàðîäíîì ïðîìûøëåííîì ïåðå÷íå (International Industrial List, IIL). Ãîñäåïàðòàìåíò îòâå÷àåò çà USML, îí ïóáëèêóåòñÿ êàê ÷àñòü Ðåãóëèðîâàíèÿ ìåæäóíàðîäíîãî òðàôèêà îðóæèÿ (International Traffic in Arms Regulations, ITAR) [466, 467].

Ýêñïîðò êðèïòîãðàôèè â ÑØÀ êîíòðîëèðóåòñÿ äâóìÿ ïðàâèòåëüñòâåííûìè îðãàíèçàöèÿìè. Îäíîé ÿâëÿåòñÿ Êîìèòåò ïî óïðàâëåíèþ ýêñïîðòîì (Bureau of Export Administration, BXA) â Ìèíèñòåðñòâå òîðãîâëè, óïîëíîìî÷åííûé Ïðàâèëàìè ðåãóëèðîâàíèÿ ýêñïîðòà (Export Administration Regulations, EAR). Äðóãàÿ - ýòî Óïðàâëåíèå ïî ðåãóëèðîâàíèþ ïðîäàæè ñðåäñòâ îáîðîíû (Office of Defense Trade Controls, DTC) â Ãîñóäàðñòâåííîì äåïàðòàìåíòå, óïîëíîìî÷åííîå ITAR. Ïî îïûòó òðåáîâàíèÿ BXA èç Ìèíèñòåðñòâà òîðãîâëè ìåíåå ñòðîãè, íî ñíà÷àëà âåñü êðèïòîãðàôè÷åñêèé ýêñïîðò ïðîñìàòðèâàåòñÿ DTC èç Ãîñäåïàðòàìåíòà (êîòîðîå ïîëó÷àåò ñîâåòû ïî òåõíèêå è íàöèîíàëüíîé áåçîïàñíîñòè îò NSA è, êàæåòñÿ, âñåãäà ñëåäóåò ýòèì ñîâåòàì), êîòîðîå ìîæåò îòêàçàòü ïåðåäàòü ïðàâî ðåøåíèÿ BXA.

ITAR ðåãóëèðóåò ýòîò ïðîöåññ. (Äî 1990 ãîäà Óïðàâëåíèå DTC íàçûâàëîñü Óïðàâëåíèåì ïî êîíòðîëþ íàä âîîðóæåíèåì, âîçìîæíî, ýòè óñèëèÿ â îáëàñòè "ïàáëèê ðèëåéøíç" íàïðàâëåíû íà òî, ÷òîáû ìû çàáûëè, ÷òî ìû èìååì äåëî ñ áîìáàìè è ïóøêàìè.) Èñòîðè÷åñêè DTC ñîïðîòèâëÿëîñü âûäà÷å ýêñïîðòíûõ ëèöåíçèé íà ñðåäñòâà øèôðîâàíèÿ ñèëüíåå îïðåäåëåííîãî óðîâíÿ - õîòÿ î òîì, êàêîâ ýòîò óðîâåíü, íèêîãäà íå ñîîáùàëîñü.

Ñëåäóþùèå ðàçäåëû âçÿòû èç ITAR [466, 467]:

§ 120.10 Òåõíè÷åñêèå äàííûå.

Òåõíè÷åñêèå äàííûå - ýòî, â íàñòîÿùåì ïîäïóíêòå:

(1) Èíôîðìàöèÿ, îòëè÷íàÿ îò ïðîãðàììíîãî îáåñïå÷åíèÿ, îïðåäåëåííîãî â 120.10(d), êîòîðàÿ íóæíà äëÿ ïðîåêòèðîâàíèÿ, ðàçðàáîòêè, ïðîèçâîäñòâà, îáðàáîòêè, èçãîòîâëåíèÿ, ñáîðêè, ðàáîòû, ðåìîíòà, ïîääåðæêè èëè ìîäèôèêàöèè ñðåäñòâ îáîðîíû. Ýòî, íàïðèìåð, èíôîðìàöèÿ â ôîðìå ñâåòîêîïèé, ÷åðòåæåé, ôîòîãðàôèé, ïëàíîâ, èíñòðóêöèé è äîêóìåíòàöèè;

(2) Ñåêðåòíàÿ èíôîðìàöèÿ, êàñàþùàÿñÿ ñðåäñòâ îáîðîíû è îáîðîííîé äåÿòåëüíîñòè;

(3) Èíôîðìàöèÿ, îõâàòûâàåìàÿ ïîñòàíîâëåíèåì î çàñåêðå÷èâàíèè èçîáðåòåíèÿ;

(4) Ïðîãðàììíîå îáåñïå÷åíèå, îïðåäåëåííîå â ðàçäåëå 121.8(f) è íåïîñðåäñòâåííî ñâÿçàííîå ñî ñðåäñòâàìè îáîðîíû

(5) Ýòî îïðåäåëåíèå íå âêëþ÷àåò èíôîðìàöèþ, êàñàþùóþñÿ îáùåíàó÷íûõ, ìàòåìàòè÷åñêèõ èëè èíæåíåðíûõ ïðèíöèïîâ, îáû÷íî èçó÷àåìûõ â îáùåäîñòóïíûõ øêîëàõ, êîëëåäæàõ è óíèâåðñèòåòàõ, êàê îïðåäåëåíî â § 120.11. Îíî òàêæå íå âêëþ÷àåò áàçîâóþ ðûíî÷íóþ èíôîðìàöèþ î ôóíêöèè, íàçíà÷åíèè èëè îáùåñèñòåìíîì îïèñàíèè ñðåäñòâ îáîðîíû.

§ 120.11 Îòêðûòûé äîñòóï.

Îòêðûòûé äîñòóï îçíà÷àåò èíôîðìàöèþ, êîòîðàÿ îïóáëèêîâûâàåòñÿ è ìîæåò áûòü îáùåäîñòóïíîé:

(1) Ñ ïîìîùüþ ïðîäàæè â êèîñêàõ è êíèæíûõ ìàãàçèíàõ;

(2) Ñ ïîìîùüþ ïîäïèñêè, êîòîðàÿ äîñòóïíà áåç îãðàíè÷åíèé äëÿ ëþáîãî, êòî õî÷åò ïîëó÷èòü èëè ïðèîáðåñòè îïóáëèêîâàííóþ èíôîðìàöèþ;

(3) Ñ ïîìîùüþ ïî÷òîâûõ ïðèâèëåãèé âòîðîãî êëàññà, âûäàííûõ ïðàâèòåëüñòâîì ÑØÀ;

(4) Â áèáëèîòåêàõ, îòêðûòûõ äëÿ ïóáëèêè, èëè â êîòîðûõ ïóáëèêà ìîæåò ïîëó÷èòü äîêóìåíòû;

(5) Ñ ïîìîùüþ ïàòåíòîâ, äîñòóïíûõ â ëþáîé ïàòåíòíîé êîíòîðå;

(6) Ñ ïîìîùüþ íåîãðàíè÷åííîãî ðàñïðîñòðàíåíèÿ íà êîíôåðåíöèè, âñòðå÷å, ñåìèíàðå, ïðåçåíòàöèè èëè âûñòàâêå, äîñòóïíûõ îáû÷íîé ïóáëèêå â Ñîåäèíåííûõ Øòàòàõ;

(7) Ñ ïîìîùüþ ñîîáùåíèé äëÿ ïå÷àòè (ò.å., íåîãðàíè÷åííîå ðàñïðîñòðàíåíèå) â ëþáîé ôîðìå (íàïðèìåð, íåîáÿçàòåëüíî îïóáëèêîâàííîé), îäîáðåííûõ êîìïåòåíòíûìè îðãàíàìè ÑØÀ (ñì. òàêæå § 125.4(b)(13)).

(8) Ñ ïîìîùüþ ôóíäàìåíòàëüíûõ èññëåäîâàíèé â íàóêå è òåõíèêå â àêêðåäèòîâàííûõ âûñøèõ ó÷åáíûõ çàâåäåíèÿõ ÑØÀ, ãäå ïîëó÷åííàÿ èíôîðìàöèÿ îáû÷íî ïóáëèêóåòñÿ è øèðîêî ðàñïðîñòðàíÿåòñÿ â íàó÷íîì ñîîáùåñòâå. Ôóíäàìåíòàëüíûìè íàçûâàþòñÿ áàçîâûå è ïðèêëàäíûå èññëåäîâàíèÿ â íàóêå è òåõíèêå, êîãäà ïîëó÷åííàÿ èíôîðìàöèÿ îáû÷íî ïóáëèêóåòñÿ è øèðîêî ðàñïðîñòðàíÿåòñÿ â íàó÷íîì ñîîáùåñòâå â îòëè÷èå îò èññëåäîâàíèé, ðåçóëüòàòû êîòîðûõ íå ðàçãëàøàþòñÿ èç-çà ïðàâ ñîáñòâåííîñòè èëè îïðåäåëåííîãî êîíòðîëÿ äîñòóïà è ðàñïðîñòðàíåíèÿ ïðàâèòåëüñòâîì ÑØÀ. Óíèâåðñèòåòñêèå èññëåäîâàíèÿ íå ñ÷èòàþòñÿ ôóíäàìåíòàëüíûìè, åñëè:

(i) Óíèâåðñèòåò èëè åãî èññëåäîâàòåëè ñîãëàøàþòñÿ ñ äðóãèìè îãðàíè÷åíèÿìè íà ïóáëèêàöèþ íàó÷íî-òåõíè÷åñêîé èíôîðìàöèè, ïîëó÷åííîé â ðåçóëüòàòå ðàáîòû íàä ïðîåêòîì, èëè

(ii) Èññëåäîâàíèÿ ôèíàíñèðóþòñÿ ïðàâèòåëüñòâîì ÑØÀ, à äîñòóï ê ðåçóëüòàòàì èññëåäîâàíèé è èõ ðàñïðîñòðàíåíèå íàõîäÿòñÿ îãðàíè÷åíû ñ öåëüþ çàùèòû èíôîðìàöèè.

§ 120.17 Ýêñïîðò.

Ïîä ýêñïîðòîì ïîíèìàåòñÿ:

(1) Ïåðåäà÷à èëè âûâîç ñðåäñòâ îáîðîíû çà ïðåäåëû Ñîåäèíåííûõ Øòàòîâ ëþáûì ñïîñîáîì, êðîìå ïóòåøåñòâèÿ çà ïðåäåëû Ñîåäèíåííûõ Øòàòîâ ëèöà, ÷üè ëè÷íûå çíàíèÿ âêëþ÷àþò òåõíè÷åñêèå äàííûå; èëè

(2) Ïåðåäà÷à èíîñòðàííîìó ëèöó ïðàâ ðåãèñòðàöèè, óïðàâëåíèÿ èëè ñîáñòâåííîñòè íà ëþáîé ñàìîëåò, ñóäíî èëè ñïóòíèê, ïðèñóòñòâóþùèé â Ïåðå÷íå âîîðóæåíèé ÑØÀ, â Ñîåäèíåííûõ Øòàòàõ èëè çà èõ ïðåäåëàìè; èëè

(3) Ðàñêðûòèå (â òîì ÷èñëå óñòíîå èëè âèçóàëüíîå) èëè ïåðåäà÷à â Ñîåäèíåííûõ Øòàòàõ ëþáûõ ñðåäñòâ îáîðîíû ïîñîëüñòâó, ó÷ðåæäåíèþ èëè ïîäðàçäåëåíèþ èíîñòðàííîãî ïðàâèòåëüñòâà (íàïðèìåð, äèïëîìàòè÷åñêèì ìèññèÿì); èëè

(4) Ðàñêðûòèå (â òîì ÷èñëå óñòíîå èëè âèçóàëüíîå) èëè ïåðåäà÷à òåõíè÷åñêèõ äàííûõ èíîñòðàííîìó ëèöó â Ñîåäèíåííûõ Øòàòàõ èëè çà èõ ïðåäåëàìè; èëè

(5) Âûïîëíåíèå îáîðîííîé äåÿòåëüíîñòè îò èìåíè èëè äëÿ âûãîäû èíîñòðàííîãî ëèöà â Ñîåäèíåííûõ Øòàòàõ èëè çà èõ ïðåäåëàìè.

(6) Çàïóñêàåìûé àïïàðàò èëè ïîëåçíàÿ íàãðóçêà íå äîëæíû, ïðè çàïóñêå òàêîãî àïïàðàòà, ðàññìàòðèâàòüñÿ êàê ýêñïîðò. Îäíàêî äëÿ îïðåäåëåííûõ öåëåé (ñì § 126.1 ýòîãî ïîäïóíêòà), ïîëîæåíèÿ ýòîãî ïîäïóíêòà ïðèìåíèìû ê ïðîäàæàì è äðóãèì ñïîñîáàì ïåðåäà÷è ñðåäñòâ îáîðîíû èëè ïðîäóêòîâ îáîðîííîé äåÿòåëüíîñòè.

×àñòü 121- Ïåðå÷åíü âîîðóæåíèé ÑØÀ

§ 121.1 Îáùèå ïîëîæåíèÿ. Ïåðå÷åíü âîîðóæåíèé ÑØÀ

Category XIII—Äîïîëíèòåëüíîå âîåííîå ñíàðÿæåíèå

(1) Êðèïòîãðàôè÷åñêèå (âêëþ÷àÿ óïðàâëåíèå êëþ÷àìè) ñèñòåìû, àïïàðàòóðà, êîíñòðóêöèè, ìîäóëè, èíòåãðàëüíûå ñõåìû, êîìïîíåíòû èëè ïðîãðàììíîå îáåñïå÷åíèå ñ âîçìîæíîñòüþ ïîääåðæêè ñåêðåòíîñòè èëè êîíôèäåíöèàëüíîñòè èíôîðìàöèè èëè èíôîðìàöèîííûõ ñèñòåì, êðîìå ñëåäóþùåãî êðèïòîãðàôè÷åñêîãî îáîðóäîâàíèÿ è ïðîãðàììíîãî îáåñïå÷åíèÿ:

(i)Ñïåöèàëüíî ñïðîåêòèðîâàííîå äëÿ âûïîëíåíèÿ çàùèùåííûì îò êîïèðîâàíèÿ ïðîãðàììíûì îáåñïå÷åíèåì òîëüêî ôóíêöèé äåøèôðèðîâàíèÿ ïðè óñëîâèè, ÷òî óïðàâëåíèå äåøèôðèðîâàíèåì íåäîñòóïíî ïîëüçîâàòåëþ.

(ii) Ñïåöèàëüíî ñïðîåêòèðîâàííîå, ðàçðàáîòàííîå èëè ìîäèôèöèðîâàííîå äëÿ èñïîëüçîâàíèÿ â ìàøèíàõ äëÿ áàíêîâñêèõ îïåðàöèé èëè äåíåæíûõ òðàíçàêöèé, êîòîðîå ìîæíî èñïîëüçîâàòü òîëüêî äëÿ òàêèõ òðàíçàêöèé. Ìàøèíû äëÿ áàíêîâñêèõ îïåðàöèé èëè äåíåæíûõ òðàíçàêöèé âêëþ÷àþò àâòîìàòè÷åñêèå êàññîâûå àïïàðàòû, ñàìîîáñëóæèâàåìûå ïå÷àòàþùèå óñòðîéñòâà, òîðãîâûå òåðìèíàëû èëè îáîðóäîâàíèå äëÿ øèôðîâàíèÿ ìåæáàíêîâñêèõ òðàíçàêöèé.

(iii) Èñïîëüçóþùåå òîëüêî àíàëîãîâûå ìåòîäû äëÿ êðèïòîãðàôè÷åñêîé îáðàáîòêè, êîòîðàÿ îáåñïå÷èâàåò áåçîïàñíîñòü èíôîðìàöèè â ñëåäóþùèõ ïðèëîæåíèÿõ. . . .

(iv) Ïåðñîíàëüíûå èíòåëëåêòóàëüíûå êàðòî÷êè, èñïîëüçîâàíèå êîòîðûõ âîçìîæíî òîëüêî â îáîðóäîâàíèè èëè ñèñòåìàõ, íå ïîïàäàþùèõ ïîä ðåãóëèðîâàíèå USML.

(v) Ñ îãðàíè÷åíèåì äîñòóïà, òàêèå êàê àâòîìàòè÷åñêèå êàññîâûå àïïàðàòû, ñàìîîáñëóæèâàåìûå ïå÷àòàþùèå óñòðîéñòâà èëè òîðãîâûå òåðìèíàëû, êîòîðûå îáåñïå÷èâàþò çàùèòó ïàðîëåé èëè ïåðñîíàëüíûõ èäåíòèôèêàöèîííûõ íîìåðîâ (PIN) èëè àíàëîãè÷íûõ äàííûõ, ÷òîáû ïðåäîòâðàòèòü íåñàíêöèîíèðîâàííûé äîñòóï ê ñðåäñòâàì, íî íå ìîãóò øèôðîâàòü ôàéëû èëè òåêñòû, íå ïîñðåäñòâåííî íå ñâÿçàííûå ñ çàùèòîé ïàðîëåé èëè PIN.

(vi) Îñóùåñòâëÿþùåå òîëüêî ïðîâåðêó ïîäëèííîñòè äàííûõ ñ ïîìîùüþ âû÷èñëåíèÿ êîäà ïðîâåðêè ïîäëèííîñòè ñîîáùåíèÿ (MAC) èëè àíàëîãè÷íîé ôóíêöèè äëÿ ïðîâåðêè, ÷òî â òåêñò íå áûëî âíåñåíî èçìåíåíèé, èëè äëÿ ïðîâåðêè ïîäëèííîñòè ïîëüçîâàòåëåé, íî êîòîðîå íåëüçÿ èñïîëüçîâàòü äëÿ øèôðîâàíèÿ äàííûõ, òåêñòà èëè äðóãîé èíôîðìàöèè ïîìèìî íåîáõîäèìîé äëÿ ïðîâåðêè ïîäëèííîñòè.

(vii) Èñïîëüçóþùåå òîëüêî ôèêñèðîâàííûå ìåòîäû ñæàòèÿ è êîäèðîâàíèÿ äàííûõ.

(viii) Èñïîëüçóåìîå òîëüêî äëÿ ðàäèîâåùàíèÿ, ïëàòíîãî òåëåâèäåíèÿ èëè àíàëîãè÷íûõ òåëåâèçèîííûõ ñèñòåì ñ îãðàíè÷åííîé àóäèòîðèåé, áåç öèôðîâîãî øèôðîâàíèÿ, è â êîòîðûõ öèôðîâîå äåøèôðèðîâàíèå îãðàíè÷åíî òîëüêî âèäåî- è àóäèîôóíêöèÿìè èëè óïðàâëåíèåì.

(ix) Ïðîãðàììíîå îáåñïå÷åíèå, ñïðîåêòèðîâàííîå èëè ìîäèôèöèðîâàííîå äëÿ çàùèòû îò çëîóìûøëåííûõ êîìïüþòåðíûõ ïîâðåæäåíèé, (íàïðèìåð, âèðóñîâ).

(2) Êðèïòîãðàôè÷åñêèå (âêëþ÷àÿ óïðàâëåíèå êëþ÷àìè) ñèñòåìû, àïïàðàòóðà, êîíñòðóêöèè, ìîäóëè, èíòåãðàëüíûå ñõåìû, êîìïîíåíòû èëè ïðîãðàììíîå îáåñïå÷åíèå ñ âîçìîæíîñòüþ ãåíåðàöèè ðàñïðîñòðàíÿåìûõ êîäîâ äëÿ áîëüøîãî êîëè÷åñòâà ñèñòåì èëè óñòðîéñòâ:

(3) Êðèïòîãðàôè÷åñêèå ñèñòåìû, àïïàðàòóðà, êîíñòðóêöèè, ìîäóëè, èíòåãðàëüíûå ñõåìû, êîìïîíåíòû èëè ïðîãðàììíîå îáåñïå÷åíèå.

§ 125.2 Ýêñïîðò íåñåêðåòíûõ òåõíè÷åñêèõ äàííûõ.

(a) Îáùèå ïîëîæåíèÿ. Äëÿ ýêñïîðòà íåñåêðåòíûõ òåõíè÷åñêèõ äàííûõ íåîáõîäèìà ëèöåíçèÿ (DSP-5), åñëè ýòè äàííûå íå èñêëþ÷åíû èç ëèöåíçèðóþùèõ òðåáîâàíèé äàííîãî ïîäïóíêòà. Â ñëó÷àå ïëàíîâîãî âèçèòà äåòàëè ïðåäïîëàãàåìûõ äèñêóññèé äîëæíû áûòü ïåðåäàíû â Óïðàâëåíèå ïî ðåãóëèðîâàíèþ ïðîäàæè ñðåäñòâ îáîðîíû äëÿ ýêñïåðòèçû òåõíè÷åñêèõ äàííûõ. Äîëæíî áûòü ïðåäîñòàâëåíî ñåìü êîïèé òåõíè÷åñêèõ äàííûõ èëè òåì äèñêóññèé.

(b) Ïàòåíòû. Ïðè ýêñïîðòå òåõíè÷åñêèõ äàííûõ òðåáóåòñÿ ëèöåíçèÿ, âûäàííàÿ Óïðàâëåíèåì ïî ðåãóëèðîâàíèþ ïðîäàæè ñðåäñòâ îáîðîíû, åñëè äàííûå ïðåâûøàþò íåîáõîäèìûå äëÿ çàïîëíåíèÿ âíóòðåííåé ïàòåíòíîé çàÿâêè èëè äëÿ çàïîëíåíèÿ èíîñòðàííîé ïàòåíòíîé çàÿâêè, åñëè âíóòðåííÿÿ çàÿâêà íå áûëà çàïîëíåíà. Çàÿâêè íà ïàòåíòîâàíèå çà ðóáåæîì, âûïîëíåíèå â òàêèõ ïàòåíòàõ óëó÷øåíèé, ìîäèôèêàöèé èëè äîïîëíåíèé äîëæíû ðåãóëèðîâàòüñÿ Óïðàâëåíèåì ïî ïàòåíòàì è òîðãîâûì çíàêàì ÑØÀ â ñîîòâåòñòâèè ñ 37 CFR, ÷àñòü 5. Ýêñïîðò òåõíè÷åñêèõ äàííûõ, íåîáõîäèìûõ äëÿ ïàòåíòîâàíèÿ â äðóãèõ ñòðàíàõ, ÿâëÿåòñÿ ñóáúåêòîì íîðì, èçäàâàåìûõ Óïðàâëåíèåì ïî ïàòåíòàì è òîðãîâûì çíàêàì ÑØÀ, â ñîîòâåòñòâèè ñ 35 U.S.C. 184.

(c) Ðàñêðûòèÿ. Äëÿ óñòíîãî, âèçóàëüíîãî èëè äîêóìåíòàëüíîãî ðàñêðûòèÿ òåõíè÷åñêèõ äàííûõ ãðàæäàíàìè ÑØÀ èíîñòðàííûì ëèöàì òðåáóåòñÿ ëèöåíçèÿ, åñëè â äàííîì ïîäïóíêòå íå îãîâîðåíî èíîå. Ëèöåíçèÿ òðåáóåòñÿ íåçàâèñèìî îò ôîðìû ïåðåäà÷è òåõíè÷åñêèõ äàííûõ (íàïðèìåð, ëè÷íî, ïî òåëåôîíó, â ïåðåïèñêå, ýëåêòðîííûìè ñðåäñòâàìè, è ò.ä.). Ëèöåíçèÿ òðå-

áóåòñÿ äëÿ òàêèõ ðàñêðûòèé, äåëàåìûõ ãðàæäàíàìè ÑØÀ ïðè ïîñåùåíèè èíîñòðàííûõ äèïëîìàòè÷åñêèõ ìèññèé è êîíñóëüñòâ.

È òàê äàëåå. Â ýòîì äîêóìåíòå íàìíîãî áîëüøå èíôîðìàöèè. Åñëè âû ñîáèðàåòåñü ýêñïîðòèðîâàòü êðèïòîãðàôèþ, ÿ ñîâåòóþ âàì äîáûòü åãî êîïèþ è âîñïîëüçîâàòüñÿ óñëóãàìè þðèñòà, êîòîðûé âî âñåì ýòîì ðàçáèðàåòñÿ.

Â äåéñòâèòåëüíîñòè ýêñïîðò êðèïòîãðàôè÷åñêèõ ïðîäóêòîâ êîíòðîëèðóåòñÿ NSA. Åñëè âàì íóæíî ïîëó÷èòü ñâèäåòåëüñòâî î ïðèçíàíèè âàøåãî ïðîäóêòà ïðåäìåòîì îáùåãî ïîòðåáëåíèÿ (Commodity Jurisdiction, CJ), âû äîëæíû ïðåäñòàâèòü âàø ïðîäóêò íà îäîáðåíèå â NSA è ïîäàòü â Ãîñóäàðñòâåííûé äåïàðòàìåíò çàÿâêó íà ïîëó÷åíèå CJ. Ïîñëå îäîáðåíèÿ â Ãîñäåïàðòàìåíòå äåëî ïîïàäàåò ïîä þðèñäèêöèþ Ìèíèñòåðñòâà òîðãîâëè, êîòîðîå íèêîãäà îñîáåííî íå èíòåðåñîâàëîñü êðèïòîãðàôèåé. Îäíàêî Ãîñóäàðñòâåííûé äåïàðòàìåíò íèêîãäà íå âûäàñò CJ áåç îäîáðåíèÿ NSA.

Â 1977 ãîäó Äæîçåô À. Ìåéåð (Joseph A. Meyer), ñëóæàùèé NSA, íàïèñàë ïèñüìî - íåñàíêöèîíèðîâàííîå, â ñîîòâåòñòâèè ñ îôèöèàëüíîé èñòîðèåé èíöèäåíòà - â IEEE, ïðåäóïðåæäàþùåå, ÷òî ïëàíèðóåìîå ïðåäñòàâëåíèå îðèãèíàëüíîé ðàáîòû RSA íàðóøèò ITAR. Èç *The Puzzle Palace*:

> Âîò åãî òî÷êà çðåíèÿ. ITAR îõâàòûâàåò âñþ "íåñåêðåòíóþ èíôîðìàöèþ, êîòîðàÿ ìîæåò áûòü èñïîëüçîâàíà, èëè àäàïòèðîâàíà äëÿ èñïîëüçîâàíèÿ, ïðè ïðîåêòèðîâàíèè, ïðîèçâîäñòâå, èçãîòîâëåíèè, ðåìîíòå, êàïèòàëüíîì ðåìîíòå, ïåðåðàáîòêå, êîíñòðóèðîâàíèè, ðàçðàáîòêå, äåéñòâèè, ïîääåðæêå èëè âîññòàíîâëåíèè" ïåðå÷èñëåííûõ ìàòåðèàëîâ, òàêæå êàê è "ëþáóþ òåõíîëîãèþ, êîòîðàÿ ðàçâèâàåò îïðåäåëåííîå óìåíèå èëè ñîçäàåò íîâîå â îáëàñòè, êîòîðàÿ èìååò âàæíîå âîåííîå ïðèìåíåíèå â Ñîåäèíåííûõ Øòàòàõ." È ýêñïîðò äåéñòâèòåëüíî âêëþ÷àë ïåðåäà÷ó èíôîðìàöèè êàê â ïèñüìåííîì âèäå, òàê è ñ ïîìîùüþ óñòíûõ èëè âèçóàëüíûõ ñðåäñòâ, âêëþ÷àÿ êðàòêèå îáñóæäåíèÿ è ñèìïîçèóìû, íà êîòîðûõ áûëè ïðåäñòàâëåíû èíîñòðàíöû.
>
> Íî, áóêâàëüíî ñëåäóÿ òóìàííîìó, ÷àñòî ñëèøêîì ïðîñòðàííîìó çàêîíîäàòåëüñòâó, êàæåòñÿ, òðåáóåòñÿ, ÷òîáû êàæäûé, êòî ñîáèðàåòñÿ íàïèñàòü èëè çàÿâèòü ÷òî-òî íà òåìó , êàñàþùóþñÿ Ïåðå÷íÿ âîîðóæåíèé, ñíà÷àëà ïîëó÷èë áû îäîáðåíèå Ãîñóäàðñòâåííîãî äåïàðòàìåíòà - ýòà óíûëàÿ ïåðñïåêòèâà ÿâíî ïðîòèâîðå÷èò Ïåðâîé ïîïðàâêå è òðåáóåò ïîäòâåðæäåíèÿ Âåðõîâíûì ñóäîì.

Â êîíöå êîíöîâ NSA ïðèçíàëî äåéñòâèÿ Ìåéåðà íåñàíêöèîíèðîâàííûìè, è ðàáîòà ïî RSA áûëà îïóáëèêîâàíà, êàê ïëàíèðîâàëîñü. Ïðîòèâ èçîáðåòàòåëåé íå áûëî ïðåäïðèíÿòî íèêàêèõ äåéñòâèé, õîòÿ ìîæåò áûòü äîêàçàíî, ÷òî èõ ðàáîòà óâåëè÷èëà âîçìîæíîñòè çàðóáåæíîé êðèïòîãðàôèè ãîðàçäî áîëüøå, ÷åì ÷òî-íèáóäü, îïóáëèêîâàííîå äî òîãî.

Ýêñïîðò êðèïòîãðàôèè îáñóæäàåòñÿ â ñëåäóþùåì çàÿâëåíèè NSA [363]:

> Êðèïòîãðàôè÷åñêèå òåõíîëîãèè ñ÷èòàþòñÿ æèçíåííî âàæíûìè äëÿ èíòåðåñîâ íàöèîíàëüíîé áåçîïàñíîñòè, âêëþ÷àÿ ýêîíîìè÷åñêèå èíòåðåñû, âîåííûå èíòåðåñû è èíòåðåñû âíåøíåé ïîëèòèêè.
>
> Ìû íå ñîãëàñíû ñ çàÿâëåíèÿìè, ñäåëàííûìè 7 ìàÿ 1992 ãîäà íà ñëóøàíèÿõ Ñóäåáíîãî êîìèòåòà, è ïîñëåäíèìè ãàçåòíûìè ñòàòüÿìè, êîòîðûå çàÿâëÿþò, ÷òî ýêñïîðòíûå çàêîíû ÑØÀ ìåøàþò àìåðèêàíñêèì ôèðìàì èçãîòàâëèâàòü è èñïîëüçîâàòü ñîâðåìåííîå øèôðîâàëüíîå îáîðóäîâàíèå. Íàì íåèçâåñòíî íè îá îäíîì ñëó÷àå, êîãäà èç-çà ýêñïîðòíûõ îãðàíè÷åíèé ÑØÀ àìåðèêàíñêîé ôèðìå ïîìåøàëè èçãîòàâëèâàòü è èñïîëüçîâàòü àïïàðàòóðó øèôðîâàíèÿ âíóòðè ñòðàíû, èëè àìåðèêàíñêîé ôèðìå èëè åå äî÷åðíåé êîìïàíèè ïîìåøàëè èñïîëüçîâàòü àïïàðàòóðó øèôðîâàíèÿ çà ïðåäåëàìè ÑØÀ. Â äåéñòâèòåëüíîñòè, NSA âñåãäà ïîääåðæèâàëî èñïîëüçîâàíèå øèôðîâàíèÿ â àìåðèêàíñêîì áèçíåñå äëÿ çàùèòû âàæíîé èíôîðìàöèè êàê äîìà, òàê è çà ãðàíèöåé.
>
> Äëÿ ýêñïîðòà â äðóãèå ñòðàíû NSA, ÿâëÿþùååñÿ ÷àñòüþ Ìèíèñòåðñòâà îáîðîíû, (âìåñòå ñ Ãîñóäàðñòâåííûì äåïàðòàìåíòîì è Ìèíèñòåðñòâîì òîðãîâëè ïðîñìàòðèâàåò ýêñïîðòíûå ëèöåíçèè â ïîèñêàõ òåõíîëîãèé èíôîðìàöèîííîé áåçîïàñíîñòè, ïîïàäàþùèõ ïîä äåéñòâèå Ýêñïîðòíîãî ïðàâèòåëüñòâåííîãî çàêîíîäàòåëüñòâà èëè Ðåãóëèðîâàíèÿ ìåæäóíàðîäíîãî òðàôèêà îðóæèÿ. Àíàëîãè÷íàÿ ñèñòåìà êîíòðîëÿ ýêñïîðòà äåéñòâóåò âî âñåõ ñòðàíàõ ÊÎÊÎÌ è âî ìíîãèõ äðóãèõ ñòðàíàõ, òàê êàê ýòè òåõíîëîãèè ïîâñåìåñòíî ñ÷èòàþòñÿ âàæíûìè. Íå ñóùåñòâóåò îáùåãî çàïðåòà íà ýêñïîðò ïîäîáíûõ òåõíîëîãèé, êàæäûé ñëó÷àé ðàññìàòðèâàåòñÿ îòäåëüíî. Ïðè ýòîì ìîæåò ïîòðåáîâàòüñÿ ïîëó÷èòü ëèöåíçèè íà òàêèå ñèñòåìû, ïðè ïîëó÷åíèè êîòîðûõ àíàëèçèðóåòñÿ âëèÿíèå ýêñïîðòà ýòîé ñèñòåìû íà èíòåðåñû íàöèîíàëüíîé áåçîïàñíîñòè - âêëþ÷àÿ èíòåðåñû ýêîíîìè÷åñêîé, âîåííîé è ïîëèòè÷åñêîé áåçîïàñíîñòè. Ýêñïîðòíûå ëèöåíçèè âûäàþòñÿ èëè íå âûäàþòñÿ â çàâèñèìîñòè îò òèïà çàäåéñòâîâàííîãî îáîðóäîâàíèÿ, ïðåäïîëàãàåìîãî èñïîëüçîâàíèÿ è ïðåäïîëàãàåìîãî ïîëüçîâàòåëÿ.
>
> Íàø àíàëèç ïîêàçûâàåò, ÷òî ÑØÀ ëèäèðóþò â ìèðîâîì ïðîèçâîäñòâå è ýêñïîðòå òåõíîëîãèé èíôîðìàöèîííîé áåçîïàñíîñòè. NSA îäîáðÿåò äëÿ ýêñïîðòà ñâûøå 90% êðèïòîëîãè÷åñêèõ ïðîäóêòîâ, íàïðàâëåííûõ â NSA Ãîñóäàðñòâåííûì äåïàðòàìåíòîì äëÿ ëèöåíçèðîâàíèÿ. Ýêñïîðòíûå ëèöåíçèè íà ïðîäóêòû èíôîðìàöèîííîé áåçîïàñíîñòè, ïîïàäàþùèå ïîä þðèñäèêöèþ Ìèíèñòåðñòâà òîðãîâëè, âûäàþòñÿ áåç ó÷àñòèÿ NSA èëè Ìèíèñòåðñòâà îáîðîíû. Ñðåäè íèõ - ïðîäóêòû, èñïîëüçóþùèå òàêèå ìåòîäû, êàê DSS è RSA, îáåñïå÷èâàþùèå ïðîâåðêó ïîäëèííîñòè è êîíòðîëü äîñòóïà ê êîìïüþòåðàì è ñåòÿì. Íà ñàìîì äåëå, â ïðîøëîì NSA èãðàëî ãëàâíóþ ðîëü â óñïåøíîì îòñòàèâàíèè îñëàáëåíèÿ ýêñïîðòíîãî êîíòðîëÿ íàä RSA è áëèçêèìè òåõíîëîãèÿìè äëÿ ïðîâåðêè ïîäëèííîñòè. Ýòè ìåòîäû îñîáåííî âàæíû ïðè ðåøåíèè ïðîáëåìû õàêåðîâ è íåñàíêöèîíèðîâàííîãî èñïîëüçîâàíèÿ ðåñóðñîâ.

Èòàê, çàÿâëåíî, ÷òî NSA îãðàíè÷èâàåò ýêñïîðò òîëüêî ïðîäóêòîâ øèôðîâàíèÿ, íî íå ïðîâåðêè ïîäëèííîñòè. Åñëè âû ñîáèðàåòåñü ýêñïîðòèðîâàòü ïðîäóêò òîëüêî äëÿ ïðîâåðêè ïîäëèííîñòè, ïîëó÷åíèå ðàçðåøåíèÿ îãðàíè÷èòñÿ äåìîíñòðàöèåé òîãî, ÷òî âàø ïðîäóêò íåëüçÿ áåç çíà÷èòåëüíûõ ïåðåäåëîê èñïîëüçîâàòü äëÿ øèôðîâàíèÿ. Áîëåå òîãî, áþðîêðàòè÷åñêàÿ ïðîöåäóðà äëÿ ïðîäóêòîâ ïðîâåðêè ïîäëèííîñòè íàìíîãî ïðîùå, ÷åì äëÿ ïðîäóêòîâ øèôðîâàíèÿ. Äëÿ ñèñòåìû ïðîâåðêè ïîäëèííîñòè ïîëó÷àòü îäîáðåíèå Ãîñäåïàðòàìåíòà (CJ), ñèñòåìà øèôðîâàíèÿ òðåáóåò ïîâòîðíîãî îäîáðåíèÿ äëÿ êàæäîé âåðñèè ïðîäóêòà èëè äàæå ïðè êàæäîé ïðîäàæå.

Áåç CJ âàì ïðèäåòñÿ çàïðàøèâàòü ðàçðåøåíèå íà ýêñïîðò âñÿêèé ðàç, êîãäà âû çàõîòèòå ýêñïîðòèðîâàòü ïðîäóêò. Ãîñóäàðñòâåííûé äåïàðòàìåíò íå ðàçðåøàåò ýêñïîðòèðîâàòü ïðîäóêòû ñ ñèëüíûì øèôðîâàíèåì, äàæå èñïîëüçóþùèå DES. Îòäåëüíûå èñêëþ÷åíèÿ áûëè ñäåëàíû äëÿ äî÷åðíèõ ôèðì àìåðèêàíñêèõ êîìïàíèé äëÿ âîçìîæíîñòè çàêðûòîé ñâÿçè ñ, äëÿ íåêîòîðûõ áàíêîâñêèõ ïðèëîæåíèé è ýêñïîðò äëÿ âîåííûõ ïîëüçîâàòåëåé ÑØÀ. Àññîöèàöèÿ ïðîèçâîäèòåëåé ïðîãðàììíîãî îáåñïå÷åíèÿ (SPA) âåëà ïåðåãîâîðû ñ ïðàâèòåëüñòâîì îá îñëàáëåíèè îãðàíè÷åíèé íà ýêñïîðòíûå. Ñîãëàøåíèå, çàêëþ÷åííîå SPA è Ãîñäåïàðòàìåíòîì â 1992 ãîäó, îáëåã-

÷èëî ïðàâèëà âûäà÷è ýêñïîðòíûõ ëèöåíçèé äëÿ äâóõ àëãîðèòìîâ, RC2 è RC4, ïðè óñëîâèè, ÷òî äëèíà èñïîëüçóåìîãî êëþ÷à íå ïðåâûñèò 40 áèòîâ. Ïîäîáíîñòè ìåæäó ýòèì è ïðåäûäóùèì ïðàâèëîì îáñóæäàëèñü â ðàçäåëå 7.1.

Â 1993 ãîäó â Ïàëàòå ïðåäñòàâèòåëåé Ìàðèÿ Êàíòâåëë (Maria Cantwell) (D-WA) ïî ïðîñüáå êîìïàíèé-ðàçðàáîò÷èêîâ ïðîãðàìì íîãî îáåñïå÷åíèÿ âíåñëà çàêîíîïðîåêò, îñëàáëÿþùèé ýêñïîðòíûé êîíòðîëü çà ïðîãðàììàìè. Ñåíàòîð Ïýòè Ì þððåé (Patty Murray) (D-WA) âíåñëà ñîîòâåòñòâóþùèé áèëëü â ñåíàò. Çàêîíîïðîåêò Êàíòâåëë áûë äîáàâëåí ê îáúåìó çàêîíó î êîíòðîëå íàä ýêñïîðòíîì, ïðîõîäÿùåìó ÷åðåç Êîíãðåññ, íî áûë óäàëåí Êîìèòåòîì ïî ðàçâåäêå ïîä ñèëüíûì äàâëåíèåì NSA. Êîãäà NSA ÷òî-íèáóäü äåëàåò, îíî ïðèêëàäûâàåò óñèëèÿ - êîìèòåò åäèíîäóøíî ïðîãîëîñîâàë çà óäàëåíèå ôîðìóëèðîâêè. Çà ïîñëåäíåå âðåìÿ ÿ íå ïðèíèìàþ äðóãîãî ñëó÷àÿ, ÷òîáû ãðóïïà çàêîíîäàòåëåé ÷òî-òî ñäåëàëà åäèíîäóøíî.

Â 1995 ãîäó Äàí Áåðíøòåéí (Dan Bernstein) ïðè ïîääåðæêå EFF ïîäàë â ñóä íà ïðàâèëüíîòî ÑØÀ, ïûòàÿñü ïîìåøàòü ïðàâèòåëüñòâó îãðàíè÷èâàòü ïóáëèêàöèè êðèïòîãðàôè÷åñêîãî äîêóìåíòà è ïðîãðàììíîãî îáåñïå÷åíèÿ [143]. Â èñêå óòâåðæäàëîñü, ÷òî çàêîíû íá ýêñïîðòíîì êîíòðîëå íåêîíñòèòóöèîííû è âîñïÿò "íåïîçâîëèòåëüíûå àïðåîðíûå îãðàíè÷åíèÿ âûñêàçûâàíèé â íàðóøåíèå Ïåðâîé ïîïðàâêè". Êîíêðåòíî â èñêå óòâåðæäàëîñü, ÷òî ñîâðåìåííûé ïðîöåññ êîíòðîëÿ íàä ýêñïîðòîì:

— Ïîçâîëÿåò áþðîêðàòàì îãðàíè÷èâàòü ïóáëèêàöèè áåç ðåøåíèÿ ñóäà.

— Îáðåìåíèâàåò ñëèøêîì ìàëî ïðîöåäóðíûõ âîçìîæíîñòåé çàùèòû ïðàâ â ñîîòâåòñòâèè ñ Ïåðâîé ïîïðàâêîé.

— Òðåáóåò îò èçäàòåëåé ðåãèñòðèðîâàòüñÿ â ïðàâèòåëüñòâå, ñîçäàâàÿ ýôôåêò "ëèöåíçèðîâàííîé ïðåññû".

— Îòêàçûâàåò â îáùèõ ïóáëèêàöèÿõ, òðåáóÿ èäåíòèôèêàöèè êàæäîãî ïîëó÷àòåëÿ.

— Äîñòàòî÷íî çàïóòàí, ÷òîáû ïðîñòûå ëþäè íå ìîãëè çíàòü, êàêîå ïîâåäåíèå ïðàâèëüíî, à êàêîå - íåò.

— Ñëèøêîì ïðîñòðàíåí, òàê êàê çàïðåùàåò ïîâåäåíèå, êîòîðîå ÿâíî çàùèùàåòñÿ (íàïðèìåð, ðàçãîâîð ñ èíîñòðàíöàìè âíóòðè Ñîåäèíåííûõ Øòàòîâ).

— Ïðèíóæäåòñÿ ñèëüêî øèðîêî, çàïðåùàÿ ýêñïîðò ïðîãðàììíîãî îáåñïå÷åíèÿ íå ñîäåðæàùåãî êðèïòîãðàôèè, èñõîäÿ èç ñîîáðàæåíèé, ÷òî êðèïòîãðàôèÿ ìîæåò áûòü äâóâîéíà ïîçæå.

— ßâíî íàðóøàåò Ïåðâóþ ïîïðàâêó, çàïðåùàÿ ÷àñòíûå áåñïàò íûå êðèïòîãðàôèè, òàê êàê ïðàâèòåëüñòâî æåëàåò âìåñòî ýòîãî íââÿçûâàòü ïóáëèêè ñâîè êðèïòîãðàôè÷åñêèå âçãëÿäû.

— Ìíîãèì ñïîñîáàì ïðåâûøåò ïîëíîì÷èÿ, ïðåäïîñòàâëåííûå êàê Êîíãðåññîì â ýêñïîðòíîì çàêîíîäàòåëüñòâå, òàê è Êîíñòèòóöèåé.

Ìîæíî ïðåäâèäåòü, ÷òî ðøåíèå ýòîãî äåëà çàéìåò íåñêîëüêî ëåò, íî ïðåäâèäåòü, ÷åì îíî çàêîí÷èòñÿ, íåâîçìîæíî.

Òåì íå ìåíåå, Êîíñóëüòàòèâíûé êîìèòåò ïî áåçîïàñíîñòè è çàùèùåííîñòè (Computer Security and Privacy Advisory Board), îôèöèàëüíûé êîíñóëüòàíò NIST, â ìàðòå 1992 ãîäà ïðîãîëîñîâàë çà òî, ÷òîáû ïåðåñìîòðåòü â íàòèíàëüíîé ïîëèòèêå êðèïòîãðàôè÷åñêèå âîïðîñû, âêëþ÷àÿ ýêñïîðòíûé ïîëèòèêó. Áûëî çàÿâëåíî, ÷òî ýêñïîðòíàÿ ïîëèòèêà îïðåäåëÿåòñÿ òîëüêî îðãàíèçàöèÿ, îòâå÷àþùàÿ íàöèîíàëüíóþ áåçîïàñíîñòü, áåç ó÷åòà òî÷êè çðåíèÿ îðãàíèçàöèé, ñâÿçàííûõ ñðàçâèòèåì òðàíçàêöèîííîé êîììåðöèè, è ÷òî íåîáõîäèìîñòü ïåðåñìîòðà ýòîé ïîëèòèêè äëÿòñÿ âñå âîçìîæíî, ÷òîáû íè÷åãî íå èçìåíèëîñü, íî íåîáõîäèìîñòü ïðåìèíó óæå íàçðåëà.

25.15 Ýêñïîðò è èìïîðò êðèïòîãðàôèè çà ðóáåæîì

Â äóõèõ ñòðàíàõ ñóùåñòâóåò ñâîé ýêñïîðòíûé è èìïîðòíûé ïðàâî [311]. Ïðèåìëåìûé îáçîð íåïîëíî è âîçìîæíî óñòàðåë. Ñòðàíû ìîãóò èçäàòü çàêîíû è íå îáðàùàòü íà íèõ âíèìàíèÿ, èëè íå èìåòü çàêîíîâ, íî êàêèì-òî îáðàçîì îãðàíè÷èâàòü ýêñïîðò, èìïîðò è ññûëêîçàâèñèì.

— Àâñòðàëèÿ òðåáóåò íàëè÷èÿ ñåðòèôèêàòà ó èìïîðòèðóåìîãî êðèïòîãðàôè÷åñêîãî ïðîäóêòà òîëüêî ïî òðåáîâàíèþ ñòðàíû-ýêñïîðòåðà.

— Â Êàíàäå íåò êîíòðîëÿ èìïîðòà, à êîíòðîëü ýêñïîðòà àíàëîãè÷åí àìåðèêàíñêîìó. Ýêñïîðò ïðîäóêòîâ èç Êàíàäà ìîæåò áûòü îãðàíè÷åí, åñëè îíè âêëþ÷åíû â Ïåðå÷åíü êîíòðîëÿ ýêñïîðòà, ñîîòâåòñòâóþùèé Àêòó ðàçðåøåíèé ýêñïîðòà è èìïîðòà. Â îòíîøåíèè êðèïòîãðàôè÷åñêîãî òåõíîëîãèé Êàíàäà ñëåäóåò îãðàíè÷åíèÿì ÊÎÊÎÌ. Øèðîêîâèäíûå óñòðîéñòâà îïèñàíû ïîä êàòåãîðèå ïÿòè, ÷àñòè âîä êàíàäñêîãî ïðàâèòåëüñòâà. These provisions àíàëîãè÷íû êàòåãîðèè ïÿòè â Ïðàâèòåëüñòâåííûõ ïðàâèëàõ ýêñïîðòà â ÑØÀ.

— Êèòàé èñïîëüçóåò ñòåíó ëèöåíçèðîâàíèÿ èìïîðòèðóåìûõ ïðîäóêòîâ, ýêñïîðòåðû äîëæíû çàïîëíèòü çàÿâêó â Ìèíèñòåðñòâå çàðóáåæíîé òîðãîâëè. Íà îñíîâå êèòàéñêîãî Ïåðå÷íÿ çàïðåùåííîãî è îãðàíè÷åííîãî ýêñïîðòà è èìïîðòà, ïðèÿòíîãî â 1987 ãîäó, Êèòàé îãðàíè÷èâàåò èìïîðò è ýêñïîðò óñòðîéñòâ êîäèðîâàíèÿ ðå÷è.

— Âî Ôðàíöèè íåò ñïåöèàëüíîãî çàêîíîäàòåëüñòâà îòíîñèòåëüíî èìïîðòà êðèïòîãðàôèè, íî ñóùåñòâóþò çà-

êîíû, êàñàþùèåñÿ ïðîäàæè è èñïîëüçîâàíèÿ êðèïòîãðàôèè â ñòðàíå. Ïðîäóêòû äîëæíû áûòü ñåðòèôèöèðîâàíû: ëèáî îíè äîëæíû ñîîòâåòñòâîâàòü îïóáëèêîâàííûì ñïåöèôèêàöèÿì, ëèáî ôèðìåííàÿ ñïåöèôèêàöèÿ êîìïàíèè äîëæíà áûòü ïðåäîñòàâëåíà ïðàâèòåëüñòâó. Ïðàâèòåëüñòâî ìîæåò òàêæå çàòðåáîâàòü äâà óñòðîéñòâà äëÿ ñîáñòâåííîãî èñïîëüçîâàíèÿ. Ó êîìïàíèé äîëæíà áûòü ëèöåíçèÿ íà ïðîäàæó êðèïòîãðàôèè âî Ôðàíöèè, â ëèöåíçèè óêàçûâàåòñÿ ðûíî÷íîå íàçíà÷åíèå. Ó ïîëüçîâàòåëåé äîëæíà áûòü ëèöåíçèÿ íà ïîêóïêó è èñïîëüçîâàíèå êðèïòîãðàôèè, â ëèöåíçèþ âêëþ÷åíî ïîëîæåíèå î òîì, ÷òî ïîëüçîâàòåëè äîëæíû áûòü ãîòîâû ïåðåäàòü ñâîè êëþ÷è ïðàâèòåëüñòâó â òå÷åíèå ÷åòûðåõ ìåñÿöåâ ïîñëå èñïîëüçîâàíèÿ. Ýòî îãðàíè÷åíèå èíîãäà äîïóñêàåò èñêëþ÷åíèÿ: áàíêîâ, áîëüøèõ êîìïàíèé, è ò.ä. Äëÿ êðèïòîãðàôèè, ýêñïîðòèðóåìîé èç ÑØÀ, ëèöåíçèîííûå òðåáîâàíèÿ îòñóòñòâóþò.

— Ãåðìàíèÿ ñëåäóåò ïîëîæåíèÿì ÊÎÊÎÌ, òðåáóÿ ëèöåíçèðîâàòü ýêñïîðò êðèïòîãðàôèè. Ïðîâîäèòñÿ ñïåöèàëüíûé êîíòðîëü îáùåäîñòóïíîãî êðèïòîãðàôè÷åñêîãî ïðîãðàììíîãî îáåñïå÷åíèÿ.

— Â Èçðàèëå åñòü îãðàíè÷åíèÿ èìïîðòà, íî, ïî âèäèìîìó, íèêòî íå çíàåò êàêèå.

— Áåëüãèÿ, Èòàëèÿ, ßïîíèÿ, Íèäåðëàíäû è Âåëèêîáðèòàíèÿ ñëåäóþò ïîëîæåíèÿì ÊÎÊÎÌ, òðåáóÿ ëèöåíçèðîâàòü ýêñïîðò êðèïòîãðàôèè.

— Â Áðàçèëèè, Èíäèè, Ìåêñèêå, Ðîññèè, Ñàóäîâñêîé Àðàâèè, Èñïàíèè, Þæíîé Àôðèêå, Øâåöèè è Øâåéöàðèè êîíòðîëü ýêñïîðòà èëè èìïîðòà êðèïòîãðàôèè îòñóòñòâóåò.

25.16 Ïðàâîâûå âîïðîñû

ßâëÿþòñÿ ëè öèôðîâûå ïîäïèñè íàñòîÿùèìè ïîäïèñÿìè? Áóäóò ëè îíè ïðèçíàíû ñóäîì? Íåêîòîðûå ïðåäâàðèòåëüíûå ïðàâîâûå èññëåäîâàíèÿ ïðèâåëè ê ìíåíèþ, ÷òî öèôðîâûå ïîäïèñè áóäóò ñîîòâåòñòâîâàòü òðåáîâàíèÿì çàêîííûõ îáÿçóþùèõ ïîäïèñåé äëÿ áîëüøåé ÷àñòè ïðèìåíåíèé, âêëþ÷àÿ êîììåð÷åñêîå èñïîëüçîâàíèå, îïðåäåëåííîå â Åäèíîì ñâîäå çàêîíîâ î òîðãîâëå (Uniform Commercial Code, UCC). Ðåøåíèå Óïðàâëåíèÿ ïî îáùåé áóõãàëòåðèè (GAD, General Accounting Office), âûíåñåííîå ïî ïðîñüáå NIST, óòâåðæäàåò, ÷òî öèôðîâûå ïîäïèñè ñîîòâåòñòâóþò ïðàâîâûì ñòàíäàðòàì äëÿ ðóêîïèñíûõ ïîäïèñåé [362].

Àêò î öèôðîâûõ ïîäïèñÿõ øòàòà Þòà âñòóïèë â äåéñòâèå 1 ìàÿ 1995 ãîäà, îáåñïå÷èâàÿ çàêîííóþ îñíîâó èñïîëüçîâàíèÿ öèôðîâûõ ïîäïèñåé â ñèñòåìå ñóäîïðîèçâîäñòâà. Êàëèôîðíèÿ ðàññìàòðèâàåò ñîîòâåòñòâóþùèé çàêîíîïðîåêò, à â Îðåãîíå è Âàøèíãòîíå ðàçðàáàòûâàþò ñâîè çàêîíû. Òåõàñ è Ôëîðèäà äûøàò èì â çàòûëîê. Ê ìîìåíòó èçäàíèÿ êíèãè áîëüøèíñòâî øòàòîâ ïðîéäåò ýòîò ïóòü.

Àìåðèêàíñêàÿ þðèäè÷åñêàÿ àññîöèàöèÿ (Îòäåë EDI è èíôîðìàöèîííûõ òåõíîëîãèé ñåêöèè íàóêè è òåõíèêè) ðàçðàáîòàëà îáðàçåö àêòà, êîòîðûé ìîæåò áûòü èñïîëüçîâàí øòàòàìè â ïðîöåññå çàêîíîòâîð÷åñòâà. Àêò ïûòàåòñÿ âïèñàòü öèôðîâûå ïîäïèñè â ñóùåñòâóþùóþ äëÿ ïîäïèñåé ïðàâîâóþ èíôðàñòðóêòóðó: Åäèíûé ñâîä çàêîíîâ î òîðãîâëå, Çàêîíû Ôåäåðàëüíîé ðåçåðâíîé ñèñòåìû Ñîåäèíåííûõ Øòàòîâ, îáùåå ïðàâî î êîíòðàêòàõ è ïîäïèñÿõ, Êîíâåíöèÿ ÎÎÍ ïî êîíòðàêòàì äëÿ ìåæäóíàðîäíîé ïðîäàæè òîâàðîâ è Êîíâåíöèÿ ÎÎÍ ïî ìåæäóíàðîäíûì çàêîíàì î êîìèòåòàõ ïî áèðæàì è äîëãîâûì îáÿçàòåëüñòâàì. Â àêò âêëþ÷åíû ïîëîæåíèÿ îá îòâåòñòâåííîñòè è îáÿçàííîñòÿõ ñåðòèôèöèðóþùèõ îðãàíîâ, âîïðîñû îòâåòñòâåííîñòè, à òàêæå îãðàíè÷åíèÿ è ïîëèòèêà.

Â Ñîåäèíåííûõ Øòàòàõ çàêîíû î ïîäïèñÿõ, êîíòðàêòàõ è òîðãîâûõ îïåðàöèÿõ íàõîäÿòñÿ â þðèñäèêöèè øòàòîâ, ïîýòîìó ýòîò àêò-îáðàçåö ðàçðàáîòàí äëÿ øòàòîâ. Îêîí÷àòåëüíîé öåëüþ ÿâëÿåòñÿ ôåäåðàëüíûé àêò, íî åñëè âñå íà÷èíàåòñÿ íà óðîâíå øòàòîâ, ó NSA ìåíüøå âîçìîæíîñòåé âñå èñïîãàíèòü.

Äàæå ïðè ýòîì, ïîêà ïðàâèëüíîñòü öèôðîâûõ ïîäïèñåé íå áóäåò îñïîðåíà â ñóäå, èõ ïðàâîâîé ñòàòóñ îñòàíåòñÿ íåîïðåäåëåííûì. Äëÿ òîãî, ÷òîáû öèôðîâûå ïîäïèñè îáëàäàëè òåìè æå èäåíòèôèêàöèîííûìè âîçìîæíîñòÿìè, ÷òî è ðóêîïèñíûå ïîäïèñè, îíè ñíà÷àëà äîëæíû áûòü èñïîëüçîâàíû äëÿ ïîäïèñàíèÿ çàêîííîãî, çàòåì îñïîðåíû â ñóäå îäíîé èç ñòîðîí. Òîãäà ñóä ðàññìîòðèò áåçîïàñíîñòü ñõåìû ïîäïèñè è âûíåñåò ðåøåíèå. Ñïóñòÿ íåêîòîðîå âðåìÿ, êîãäà ïîâòîðèòñÿ ïîäîáíûé ñëó÷àé, ðåøåíèÿ î òîì, êàêèå ìåòîäû öèôðîâîé ïîäïèñè è êàêèå ðàçìåðû êëþ÷åé ïîíàäîáÿòñÿ, ÷òîáû öèôðîâàÿ ïîäïèñü áûëà ïðèçíàíà çàêîííîé, áóäåò âûíåñåíî íà îñíîâå ïðåäûäóùèõ ðåøåíèé. Âîçìîæíî äëÿ ýòîãî ïîòðåáóþòñÿ ãîäû.

Äî òåõ ïîð, åñëè äâà ÷åëîâåêà õîòÿò èñïîëüçîâàòü öèôðîâûå ïîäïèñè äëÿ êîíòðàêòà(äëÿ çàÿâîê íà ïîêóïêó, äëÿ ïðèêàçîâ ïî ðàáîòå, è ò.ä.), ðåêîìåíäóåòñÿ, ÷òîáû îíè ïîäïèñàëè íà áóìàãå êîíòðàêò, ñ êîòîðîì îíè ñîãëàøàþòñÿ â áóäóùåì ïðèçíàâàòü ëþáûå äîêóìåíòû, ïîäïèñàííûå èõ öèôðîâûìè ïîäïèñÿìè [1099]. Â ýòîì äîêóìåíòå äîëæíû îïðåäåëÿòüñÿ àëãîðèòì, ðàçìåð êëþ÷à è âñå îñòàëüíûå ïàðàìåòðû. Â íåì äîëæåí, ê òîìó æå, áûòü îïðåäåëåí ñïîñîá ðàçðåøåíèÿ ñïîðîâ.

Ïîñëåñëîâèå Ìýòòà Áëåéçà

Îäíèì èç ñàìûõ îïàñíûõ ìîìåíòîâ êðèïòîëîãèè (è, ñëåäîâàòåëüíî, äàííîé êíèãè), ÿâëÿåòñÿ òî, ÷òî âàì ïî÷òè óäàåòñÿ èçìåðèòü åå. Çíàíèå äëèíû êëþ÷åé, ñïîñîáîâ ðàçëîæåíèÿ íà ìíîæèòåëè è êðèïòîàíàëèòè÷åñêèõ ìåòîäîâ ïîçâîëÿåò îöåíèòü (â îòñóòñòâèè íàñòîÿùåé òåîðèè ïðîåêòèðîâàíèÿ øèôðîâ) "êîýôôèöèåíò ðàáîòû", íåîáõîäèìûé äëÿ âñêðûòèÿ êîíêðåòíîãî øèôðà. Ñëèøêîì âåëèê ñîáëàçí íåïðàâèëüíî èñïîëüçîâàòü ýòè îöåíêè â êà÷åñòâå îáùåé ìåðû áåçîïàñíîñòè ñèñòåì. Â ðåàëüíîì ìèðå ó âçëîìùèêà åñòü êóäà áîëüøå âîçìîæíîñòåé, ÷åì èñïîëüçîâàíèå îäíîãî êðèïòîàíàëèçà. ×àñòî óñïåõ äîñòèãàåòñÿ ñ ïîìîùüþ âñêðûòèé ïðîòîêîëîâ, òðîÿíñêèõ êîíåé, âèðóñîâ, ýëåêòðîìàãíèòíîãî êîíòðîëÿ, ôèçè÷åñêîé êîìïðîìåòàöèè, øàíòàæà è çàïóãèâàíèÿ âëàäåëüöà êëþ÷à, îøèáîê îïåðàöèîííîé ñèñòåìû è ïðèêëàäíûõ ïðîãðàìì, àïïàðàòíûõ îøèáîê, îøèáîê ïîëüçîâàòåëåé, ôèçè÷åñêîãî ïîäñëóøèâàíèÿ, ïðèêëàäíîé ñîöèàëüíîé èíæåíåðèè, àíàëèçà ñîäåðæèìîãî ñâàëêè, è ýòî äàëåêî íå âñå.

Âûñîêîêà÷åñòâåííûå øèôðû è ïðîòîêîëû ÿâëÿþòñÿ âàæíûìè ñðåäñòâàìè, íî ñàìè ïî ñåáå îíè íå çàìåíÿþò ðåàëèñòè÷íûõ, êðèòè÷åñêèõ ðàçìûøëåíèé î òîì, ÷òî äåéñòâèòåëüíî íóæíî çàùèòèòü, è êàê ìîãóò áûòü âçëîìàíû ðàçëè÷íûå óðîâíè îáîðîíû (âçëîìùèêè, â êîíöå êîíöîâ, ðåäêî îãðàíè÷èâàþòñÿ ÷èñòûìè, õîðîøî îïðåäåëåííûìè ìîäåëÿìè íàó÷íîãî ìèðà). Ðîññ Àíäåðñîí (Ross Anderson) ïðèâîäèò ïðèìåðû êðèïòîãðàôè÷åñêè ñèëüíûõ ñèñòåì (â áàíêîâñêîé èíäóñòðèè), êîòîðûå íå óñòîÿëè ïåðåä óãðîçàìè ðåàëüíîãî ìèðà [43, 44]. Äàæå êîãäà ó âçëîìùèêà åñòü äîñòóï òîëüêî ê øèôðîòåêñòó, ÷åðåç êàæóùèåñÿ íåçíà÷èòåëüíûìè áðåøè â äðóãèõ ÷àñòÿõ ñèñòåìû ìîæåò ïðîñî÷èòüñÿ äîñòàòî÷íî èíôîðìàöèè, ÷òîáû ñäåëàòü õîðîøóþ êðèïòîñèñòåìó áåñïîëåçíîé. Ñîþçíèêè âî âòîðîé ìèðîâîé âîéíå âçëîìàëè òðàôèê íåìåöêîé Ýíèãìû, ãëàâíûì îáðàçîì òùàòåëüíî èñïîëüçóÿ îøèáêè îïåðàòîðîâ [1587].

NSA â îòâåò íà âîïðîñ, ìîæåò ëè ïðàâèòåëüñòâî âñêðûâàòü DES, ÿçâèòåëüíî çàìåòèëî, ÷òî ðåàëüíûå ñèñòåìû íàñòîëüêî íåáåçîïàñíû, ÷òî íå ýòîì äàæå íå ñòîèò áåñïîêîèòüñÿ. Ê ñîæàëåíèþ, íå ñóùåñòâóåò ïðîñòûõ ðåöåïòîâ, êàê ñäåëàòü ñèñòåìó áåçîïàñíîé, çàìåíèòü òùàòåëüíîå ïðîåêòèðîâàíèå è êðèòè÷åñêèé àíàëèç íåâîçìîæíî. Õîðîøèå êðèïòîñèñòåìû äåëàþò æèçíü âçëîìùèêà íàìíîãî òðóäíåå, ÷åì æèçíü çàêîííîãî ïîëüçîâàòåëÿ, íî ýòî íå òàê â îòíîøåíèè ïî÷òè âñåõ îñòàëüíûõ àñïåêòîâ áåçîïàñíîñòè êîìïüþòåðà è ñèñòåì ñâÿçè. Ðàññìîòðèì ñëåäóþùèå (íàâåðíÿêà íå âñå) "Äåñÿòü ãëàâíûõ óãðîç áåçîïàñíîñòè ðåàëüíûõ ñèñòåì", êàæäóþ èç êîòîðûõ ëåã÷å îñóùåñòâèòü, ÷åì ïðåäîòâðàòèòü.

1. Ïå÷àëüíîå ñîñòîÿíèå ïðîãðàììíîãî îáåñïå÷åíèÿ. Âñåì èçâåñòíî, ÷òî íèêòî íå çíàåò, êàê ïèñàòü ïðîãðàììíîå îáåñïå÷åíèå. Ñîâðåìåííûå ñèñòåìû ñëîæíû, âêëþ÷àþò ñîòíè òûñÿ÷ ñòðîê êîäà, ëþáàÿ èç íèõ ìîæåò ïîâðåäèòü áåçîïàñíîñòè. Èç ïðîãðàììíûõ ìîäóëåé, ñâÿçàííûõ ñ áåçîïàñíîñòüþ èçâëåêàòü îøèáêè åùå òðóäíåå.

2. Íåýôôåêòèâíàÿ çàùèòà ïðîòèâ âñêðûòèé ñ îòêàçîì îò óñëóã. Â íåêîòîðûõ êðèïòîãðàôè÷åñêèõ ïðîòîêîëàõ äîïóñêàåòñÿ àíîíèìíîñòü. Èñïîëüçîâàíèå àíîíèìíûõ ïðîòîêîëîâ ìîæåò áûòü îñîáåííî îïàñíûì, åñëè îíè óâåëè÷èâàþò âîçìîæíîñòü íåïîçíàííîãî âàíäàëà íàðóøèòü ïðåäîñòàâëåíèå óñëóãè Ïîýòîìó àíîíèìíûå ñèñòåìû äîëæíû áûòü îñîáåííî óñòîé÷èâû ê âñêðûòèÿì ñ îòêàçîì îò óñëóã. Â óñòîé÷èâûõ ñåòÿõ ïîääåðæèâàòü àíîíèìíîñòü ìîæåò áûòü ëåã÷å - âåäü âðÿä ëè êîãî-òî ñèëüíî âîëíóåò íàëè÷èå ìèëëèîíîâ àíîíèìíûõ âõîäíûõ òî÷åê â áîëüøèíñòâå óñòîé÷èâûõ ñåòåé, òàêèõ êàê òåëåôîííàÿ ñåòü èëè ïî÷òîâàÿ ñèñòåìà, ãäå îòäåëüíîìó ïîëüçîâàòåëþ îòíîñèòåëüíî òðóäíî (èëè äîðîãî) âûçâàòü êðóïíîìàñøòàáíûå àâàðèè.

3. Íåò ìåñòà äëÿ õðàíåíèÿ ñåêðåòîâ. Êðèïòîñèñòåìû çàùèùàþò áîëüøèå ñåêðåòû ìàëûìè (êëþ÷àìè). Ê ñîæàëåíèþ, ñîâðåìåííûå êîìïüþòåðû íå îñîáåííî õîðîøè äëÿ çàùèòû äàæå ìàëåíüêèõ ñåêðåòîâ. Ìíîãîïîëüçîâàòåëüñêèå ñåòåâûå ðàáî÷èå ñòàíöèè ìîãóò áûòü âçëîìàíû, à èõ ïàìÿòü - ñêîìïðîìåòèðîâàíà. Îòäåëüíî ñòîÿùèå, îäíîïîëüçîâàòåëüñêèå ìàøèíû ìîãóò áûòü óêðàäåíû èëè ñêîìïðîìåòèðîâàíû âèðóñàìè, êîòîðûå îðãàíèçóþò àñèíõðîííóþ óòå÷êó ñåêðåòîâ. Óäàëåííûå ñåðâåðû, ãäå ìîæåò è íå áûòü ïîëüçîâàòåëÿ, ââîäÿùåãî ïàðîëüíóþ ôðàçó (íî ñì. óãðîçó ¹ 5), ïðåäñòàâëÿþò ñîáîé îñîáåííî òðóäíóþ ïðîáëåìó.

4. Ïëîõàÿ ãåíåðàöèÿ ñëó÷àéíûõ ÷èñåë. Äëÿ êëþ÷åé è ñåàíñîâûõ ïåðåìåííûõ íóæíû õîðîøèå èñòî÷íèêè íåïðåäñêàçóåìûõ áèòîâ. Ýíòðîïèÿ ðàáîòàþùåãî êîìïüþòåðà âåëèêà, íî ðåäêî ïðèëîæåíèå â ñîñòîÿíèè ïðàâèëüíî èñïîëüçîâàòü åå. Áûëî ïðåäëîæåíî ìíîæåñòâî ìåòîäîâ ïîëó÷àòü èñòèííî ñëó÷àéíûå ÷èñëà ïðîãðàììíûì îáðàçîì (èñïîëüçóþòñÿ íåïðåäñêàçóåìîñòü âðåìåíè âûïîëíåíèÿ îïåðàöèé ââîäà âûâîäà, ðàññîãëàñîâàíèÿ òàêòîâîé ÷àñòîòû è òàéìåðà, è äàæå òóðáóëåíòíîñòü âîçäóõà âíóòðè êîðïóñà òâåðäîãî äèñêà), íî âñå îíè î÷åíü ÷óâñòâèòåëüíû ê íåçíà÷èòåëüíûì èçìåíåíèÿì ñðåäû, â êîòîðûõ îíè èñïîëüçóþòñÿ.

5. Ñëàáûå ïàðîëüíûå ôðàçû. Áîëüøèíñòâî êðèïòîãðàôè÷åñêîãî ïðîãðàììíîãî îáåñïå÷åíèÿ ðåøàåò ïðîáëåìû õðàíåíèÿ è ãåíåðàöèè êëþ÷åé íà îñíîâå ñîçäàâàåìûõ ïîëüçîâàòåëåì ïàðîëüíûõ ôðàç, êîòîðûå ñ÷èòàþòñÿ äîñòàòî÷íî íåïðåäñêàçóåìûìè äëÿ ãåíåðàöèè õîðîøåãî êëþ÷åâîãî ìàòåðèàëà, è êîòîðûå òàêæå ëåãêî çàïîìèíàþòñÿ è ïîýòîìó íå òðåáóþò áåçîïàñíîãî õðàíåíèÿ. Â òî âðåìÿ, êàê ñëîâàðíûå âñêðûòèÿ ÿâëÿþòñÿ õîðîøî èçâåñòíîé ïðîáëåìîé äëÿ êîðîòêèõ ïàðîëåé, î ñïîñîáàõ âñêðûòèÿ êëþ÷åé,

ñîçäàííûõ íà îñíîâå âûáðàííûõ ïîëüçîâàòåëÿìè ïàðîëüíûõ ôðàç, èçâåñòíî ìàëî. Øåííîí ïîêàçàë, ÷òî ýíòðîïèÿ àíãëèéñêîãî òåêñòà ÷óòü áîëüøå 1 áèòà íà ñèìâîë, ÷òî, ïî âèäèìîìó, ïîçâîëÿåò èñïîëüçîâàòü ïðîòîêîë ïàðîëüíûõ ôðàç ãðóáóþ ñëóó. Îäíàêî ïîêà íå âïîëíå ïîíÿòíî, äëÿ ýòîãî êàê óïîðÿäî÷èâàòü ïàðîëüíûå ôðàçû. Ïîêà ìû íå ðàçáåðåìñÿ êàê ñëåäóåò, êàê âñêðûâàòü ïàðîëüíûå ôðàçû, ìû íå ïîéìåì, íàñêîëüêî îíè ñëàáû èëè ñèëüíû.

6. Íåïðàâèëüíîå äîâåðåå. Ïî÷òè âñå äîñòóïíûå êðèïòîãðàôè÷åñêîå ïðîãðàììíîå îáåñïå÷åíèå ïðèãîòîâëåíî ê íåïîñðåäñòâåííîì êîíòàêòå ñ ñèñòåìîé ëè ïîëüçóåòñÿ íàäåæíûì ñïîñîáîì äîñòóïà. Íàïðèìåð, èíòåðôåéñû ê ïðîãðàììàì, ïîäîáíûì PGP, ïðåäïîëàãàþò, ÷òî èõ ïàðîëüíûå ôðàçû ïîñòóïàþò îò ïîëüçîâàòåëÿ ïî íàäåæíîì ïóòè, íàïðèìåð, ñ ëîêàëüíîé êîíñîëè. Íî ýòî íå âñåãäà òàê, ðàññìîòðèì ïðîáëåìó ÷òåíèÿ âàì øèôðîâàííîé ïî÷òû ïðè ïîâðåæäåííîì ïðîöåññîðå èëè ïîâðåæäåííîì ñòåíäàëîíå. Òî, ÷òî ïðîêòèðîâùèê ñèñòåìû ñ÷èòàåò íàäåæíûì, ìîæåò íå ñîîòâåòñòâîâàòü ïîòðåáíîñòÿì èëè îæèäàíèÿì ðàëüíûõ ïîëüçîâàòåëåé, îñîáåííî êîãäà ïðîãðàììíûì îáåñïå÷åíèåì ìîæíî óïðàâëÿòü óäàëåííî ïî íåáåçîïàñíûì êàíàëàì.

7. Ïëîõ ïîíèìàíèå âçàèìîäåéſòâèå ïðîòîêîëîâ è óñëóã. Ñ ðîñòîì è óñëîæíåíèåì ñèſòåì ÷àſòî ïðîñòûå âåùè, è áûâàåò òðóäíî ïîíÿòü ÷òî-íèáóäü ïîíÿòü ÷òî-íèáóäü, äàæå êîãäà ïðîèſîéäåò êàêàÿſíèáóäü àâàðèÿ. ×åðåç Internet ðàſïðîſòðàſÿëſÿ ſ ïîìùüþ òóſàſíîſ è ſ âèäó âïîëíå íåèſſíîſ ſðåſſñòâ ïðîðàſìû ïåðåäà÷è ïî÷òû. Ñêîëüêî åùå âîçſſîſæſſòåé è â êàêſ êîëè÷åſòâå ïðîſàſìſ îáëàäàþſ íåſæèàſíûſè ſëåſſòâîſðſòåſſſ, êîòîðûå òſëüêî æáóſ ſâſåſ ſòêðûſèÿ?

8. Íåðåàëèſòè÷íàÿ îöåíêà óãðîçû è ðèſêà. Ýêſïåðòû ïî áåçſïàſſſîſòè ſòðåſÿſſſ ſêſſöåſòðèſâàöü ſâſè óſëëèÿ íà óãðîçàſ, êſòſðûå èçâſſòſſ êàê ſſàſſèëèðſſâàöü è ïðåſſòâðſſſàöü. Ê ſſæàëåſèþ, âçëſſſſèêè âûſſſëſÿþſ âſêðûſèÿ íà áàçå ſſáſſòâſſſſûſ çſàſèé, è äâå ýſè ſáëàſſòè ðåäêſ ſſâſàäàþſ. Ñëèøſſſ ſſſſãſ "áåçſſàſſſûſ" ſſſòſſ áſëſ ſſſðſâſſſèſſſâſſſ áåç ó÷åſà ðåàëüſſſ âſçſſæſſûſ äåéſſòſèé âçſſſſſ èſêſſſſ.

9. Èſòåðôåéſû, êſſſſðûå äåëàþſ áåçſſàſſſſſòſ äſðſãſé è ſáóäſáſſſ. Åſſèſ ſóæſſ èſſſſëüçſſâàöü ſðåäſſſòâà ſáåſſſå÷åſèÿ áåçſſſàſſſſòſ, òſ ſſſ äſëæſû áûöü óäſáſûſè è äſſòàòſ÷ſſ ſðſçða÷ſûſè, ÷òſáû ëþäſ äåéſſòâſèòåëüſſſ ſſſëüçſâàëſſſ ſſſ. Íàòðóäſſ ſſſðſåſêòſðſâàöü ſåõſáſèçſû øſôſðſâſſÿ, êſòſðûå ðàáſòàþò òſëüſêſ çà ſ÷åò ſðſſçâſàſèòåëüſſſſòſ èëſ ſðſſòſòû èſſſëüçſâſáſÿ, è åùå ëðã÷å ſſçäàöü ſåòàſèçſ, êſòſðûé ſðſâſſöèðóåò ſøèáſê. Áåçſſàſſſſòſ äſëæſſ áûöü òðóſåå âſêëþ÷èſü, ÷åſ âêëþ÷èſü; ê íåſ÷àſòüþ, ëſøü íåſſſãåå ſêſòàſſ äåéſòâſèòåëüſſ òàê ðàáſòàþò.

10. Ñëſøſê ſ âſåſáúåſëþ ùſå òðåáſâàſèÿ ê áåçſſàſſſſòſ. Ýòà ſðſáſëſàõſðſøſ èçâåſòſà ſſ÷òſ âſåſ, ÷üå ſ÷àſòüå ſâÿçſſſ ſ ſðſſäàæåé ſðſſóſêòſâ è óſëóã áåçſſàſſſſòſ. Ïſêà ſóùſåſòåóò øſðſêſ ðàſſðſſſòðàſáſſſå òðåáſâſèÿ âſåſſáúåſëþ ùåé áåçſſàſſſſòſ, ſðåäſòâà è èſôðàſòðóſêòóðà, ſáåſſ÷åſâſþ ùſé åãſ ðåſëèçàöèþ, áóäóò äſðſſãſ è ſåäſſòóſſû äëÿ ſſſſãſõ ſðëſſæåſſèé. ×àſòſ÷ſſ ýòſ ſðſſáſåſà ſſſèſàſèÿ è ðàſſêðûſèÿ óãðſç è ſſàſſſſòſé â ðåàëüſûſ ſðèſſæåſſèÿõ, à ſàſòſ÷ſſ ſðſáſëſà ſðſåſêòſðſâſſèÿ ſèſòåì, â êſòſðûſ áåçſſàſſſſòſ íå çàêëàûâàåòſÿ èçſà÷àëüſſ, à äſáſâſëÿåòſÿ ſſçæå.

Áſëåå ſſëſûé ſſèſſê è ſáſóæäåſèå ſſàſáſûſ óãðſç ſſæåò ëåâſ çàſſſëſèòü êſèãó òàſſãſ æå ðàçſåðà, ſðè ýòſſ ſðſáſëſà áóäåò ëèøü åääà çàòðſſóòà. ×òſ äåëàåò èò ſſſáåſſſ òðóäſûſè è ſſàſſſûſè, òàſ ýòſ òſ, ÷òſ íå ſóùåſòâóåò íèſàſſãſ ſàãè÷åſêſãſ ſſſſſáà èçáàâèòüſſ ſò íèõ, êðſſå õſðſøåſ àſáëèçà è õſðſøåé èſæåſåðſſé ðàáſòû. ×åſòſëþáèâûé êðèſòſãðàô äſëæåſ ſùóùàòü ãðàſèöû èſêóſſòâà.

Ì ýòò Áëåéç
Íüþ-Éſðê