×àñòü 2

Êðèïòîãðàôè÷åñêèå ìåòîäû

Ãëàâà 7
Äëèíà êëþ÷à

7.1 Äëèíà ñèìâîëüíîãî êëþ÷à

Áåçîïàñíîñòü ñèìâîëüíîãî ïðîòîêîëà îáåñïå÷èâàåòñÿ ôóíêöèåé äâóõ ôàêòîðîâ: íàäåæíîñòè àëãîðèòìà è äëèíû êëþ÷à. Ïåðâûé áîëåå âàæåí, íî ðîëü âòîðîãî ëåã÷å ïðîäåìîíñòðèðîâàòü.

Ïóñòü íàäåæíîñòü àëãîðèòìà ñîâåðøåííà. Íà ïðàêòèêå ýòîãî ÷åçâû÷àéíî òðóäíî äîñòèãíóòü, íî â ïðèíöèïå - äîñòàòî÷íî ëåãêî. Ïî ñîâåðøåííûâàþ îòñóòñòâèå ëó÷øåãî ïóòè âçëîìà êðèïòîñèñòåìû, ÷åì âñêðûòèå ãðóáîé ñèëîé ñ ïîìîùüþ ïåðåáîðà âñåõ âîçìîæíûõ êëþ÷åé.

Äëÿ âûïîëíåíèÿ òàêîãî âñêðûòèÿ êðèïòîàíàëèòèêó òðåáóåòñÿ êóñî÷åê øèôðîòåêñòà è ñîîòâåòñòâóþùåãî îòêðûòîãî òåêñòà, âñêðûòèå ãðóáîé ñèëîé ñ ïîìîùüþ ïåðåáîðà âñåõ âîçìîæíûõ êëþ÷åé.

Äëÿ âûïîëíåíèÿ òàêîãî âñêðûòèÿ êðèïòîàíàëèòèêó òðåáóåòñÿ êóñî÷åê øèôðîòåêñòà è ñîîòâåòñòâóþùåãî îòêðûòîãî òåêñòà. Äëÿ áîëåå êîðîòêîãî øèôðà êðèïòîàíàëèòèêó ïîíàäîáèòñÿ íåñêîëüêî ïàð îòêðûòûé òåêñò. Äëÿ áîëåå äëèíîãî øèôðà êðèïòîàíàëèòèêó ïîíàäîáèòñÿ áîëüøîå êîëè÷åñòâî ïàð îòêðûòûé òåêñò. Îí ìîæåò çíàòü ÷òî-òî î ôîðìàòå øèôðîòåêñòà: íàïðèìåð, ÷òî ýòî òàéë â ôîðìàòå WordPerfect, èëè ó íåãî åñòü ñòàíäàðòíûé çàãîëîâîê ñîîáùåíèÿ ýëåêòðîííîé ïî÷òû, èëè òàéë êàòàëîãà UNIX, èëè èçíà÷àëüíî â ôîðìàòå TIFF, èëè ñòàíäàðòíàÿ çàïèñü â áàçå äàííûõ êëèåíòà. Âñå ýòè ôîðìàòû ñîäåðæàò íåêîòîðûå ïðåäñêàçóåìûå áàéòû. Êðèïòîàíàëèòèêó äëÿ òàêîãî âñêðûòèÿ íå íóæíî ìíîãî îòêðûòîãî òåêñòà.

Ðàññ÷èòàòü ñëîæíîñòü âñêðûòèÿ ãðóáîé ñèëîé íåòðóäíî. Åñëè èñïîëüçóåòñÿ 8-áèòîâûé êëþ÷, òî ñóùåñòâóåò 2^8, èëè 256, âîçìîæíûõ êëþ÷åé. Ñëåäîâàòåëüíî, äëÿ îáðàáîòêè ïðàâèëüíîãî êëþ÷à ïîòðåáóåòñÿ, ñàìîå áîëüøåå, 256 ïîïûòîê, ñ 50-ïðîöåíòíîé âåðîÿòíîñòüþ íàéòè íóæíûé êëþ÷ ïîñëå ïîëîâèíû ïîïûòîê. Åñëè äëèíà êëþ÷à ðàâíà 56 áèòàì, òî ñóùåñòâóåò 2^{56} âîçìîæíûõ êëþ÷åé. Åñëè êîìïüþòåð ìîæåò ïðîâåðèòü ìèëëèîí êëþ÷åé â ñåêóíäó, ïîèñê íóæíîãî êëþ÷à çàéìåò â ñðåäíåì 2285 ëåò. Åñëè èñïîëüçóåòñÿ 64-áèòîâûé êëþ÷, òî òîò æå ñóïåðêîìïüþòåð ïîíàäîáèòñÿ îêîëî 585000 ëåò, ÷òîáû íàéòè ïðàâèëüíûé êëþ÷ ñðåäè 2^{64} âîçìîæíûõ êëþ÷åé. Åñëè äëèíà êëþ÷à ðàâíà 128 áèòàì ïîèñê êëþ÷à çàéìåò 10^{25} ëåò. Âîçðàñò âñåëåííîé ñîñòàâëÿåò âñåãî 10^{10} ëåò, ïîýòîìó 10^{25} ëåò - ýòî áîëüøå âðåìåíè. Ïðè 2048-áèòîâîì êëþ÷å ìèëëèîí êîìïüþòåðîâ, ðàáîòàÿ ïàðàëëåëüíî è ïðîâåðÿÿ ìèëëèîí êëþ÷åé â ñåêóíäó, ïîòðàòÿò 10^{587} ëåò â ïîèñêàõ êëþ÷à. Ê ýòîìó âðåìåíè âñåëåííàÿ äàâíî ðàñøèðèòñÿ, ïðåâðàòèâøèñü â íè÷òî ëåò ãðàíäèîçíîé áåçîïàñíîñòè.

Ïðåæäå ÷åì êëàäòüñÿ èçîáðåòàòü ñîâåðøåííûé ñ 8-êèëîáàéòîâûì êëþ÷îì, âñïîìíèòå, ÷òî äðóãîé ñòîðîíîé ÿâëÿåòñÿ íàäåæíîñòü: àëãîðèòì äîëæåí áûòü íàñòîëüêî áåçîïàñåí, ÷òîáû ëó÷øàÿ èçâåñòíàÿ àòàêà íà íåãî òðåáîâàëà, ÷òîáû êëþ÷ ñòàë ñëèøêîì äëèííûì, è íå ñóùåñòâîâàëî ïðàêòè÷åñêè ðåàëèçóåìîãî ñïîñîáà ïîäîáðàòü êëþ÷. Ê ýòîìó âðåìåíè âñëåäñòâèå ïîñòîÿííîãî óâåëè÷åíèÿ äàâíî ðàñøèðèòñÿ, ïðåâðàòèâøèñü â íè÷òî èëè ñîæìåòñÿ.

Ïðåæäå ÷åì êëàäòüñÿ èçîáðåòàòü êðèïòîñèñòåìó ñ 8-êèëîáàéòîâûì êëþ÷îì, âñïîìíèòå, ÷òî äðóãîé ñòîðîíîé ÿâëÿåòñÿ íàäåæíîñòü: àëãîðèòì äîëæåí áûòü íàñòîëüêî áåçîïàñåí, ÷òîáû ëó÷øàÿ èçâåñòíàÿ àòàêà íà íåãî òðåáîâàëà, ÷òîáû êëþ÷ ñòàë ñëèøêîì äëèííûì, è íå ñóùåñòâîâàëî ïðàêòè÷åñêè ðåàëèçóåìîãî ñïîñîáà ïîäîáðàòü êëþ÷. Ê ýòîìó âðåìåíè âñëåäñòâèå ïîñòîÿííîãî óâåëè÷åíèÿ äàâíî ðàñøèðèòñÿ, ïðåâðàòèâøèñü â íè÷òî èëè ñîæìåòñÿ.

Âñïîìíèòå âàæíûé ìîìåíò èç ðàçäåëà 1.1: áåçîïàñíîñòü êðèïòîñèñòåì äîëæíà îñíîâûâàòüñÿ íà êëþ÷å, à íå îñíîâûâàòüñÿ àëãîðèòìà. Ïðåäïîëîæèì, ÷òî êðèïòîíàëèòèêó èçâåñòíî âñå ïîäîáíîñòè âàøåãî àëãîðèòìà. Ïðåäïîëîæèì, ÷òî ó íåãî åñòü ñòîëüêî øèôðîâåñòà, ñêîëüêî åìó íóæíî, è ÷òî îí ïîïûòàåòñÿ âûïîëíèòü èíòåãðàëüíûé àíàëèç íàä ñîáñòâåííûì øèôðîâàíèåì ñ ñîîòâåòñòâóþùèì îòêðûòûì òåêñòîì. Ïðåäïîëîæèì, ÷òî îí ïîïûòàåòñÿ âûïîëíèòü âñêðûòèå ñ ñîîòâåòñòâóþùåé ñëîæíîñòüþ, à òåì, êòî îáëàäàåò òàêèì âîçìîæíîñòÿì, ìîæåò îêàçàòüñÿ íåîæèäàííî ïðàâèëüíûõ ñðåäñòâ, àíàëèçóÿ íåñêîëüêî îòêðûòûõ òåêñòîâ, ïîñòàâëåííûõ ïåðåä íèì. Ïðåäïîëîæèì, ÷òî îí ïîïûòàåòñÿ âûïîëíèòü âñêðûòèå ñ ñîîòâåòñòâóþùåé ñëîæíîñòüþ, à òåì, êòî îáëàäàåò òàêèì âîçìîæíîñòÿì, ìîæåò îêàçàòüñÿ íåîæèäàííî äàëåê îò ïîíèìàíèÿ òîãî, êàê ýòî ðàáîòàåò, è íå ñìîæåò ïîíÿòü, êîãäà ïîÿâèòñÿ íîâàÿ àòàêà.

Îòêðûòûå ðàçìåíè è ñòîèìîñòè âñêðûòèÿ ãðóáîé ñèëîé

Ñêîðîñòü âñêðûòèÿ ãðóáîé ñèëîé îïðåäåëÿåòñÿ äâóìÿ ïàðàìåòðàìè: êîëè÷åñòâîì ïðîâåðÿåìûõ êëþ÷åé è ñêîðîñòüþ ïðîâåðêè îäíîãî êëþ÷à. Áîëüøèíñòâî ñèììåòðè÷íûõ àëãîðèòìîâ â êà÷åñòâå êëþ÷à ìîãóò ñîäåðæàòü êëþ÷è ëþáîé áèòîâîé ïîñëåäîâàòåëüíîñòè ôèêñèðîâàííîé äëèíû. Äëèíà êëþ÷à DES ñîñòàâëÿåò 56 áèò, âñåãî ìîæåò áûòü 2^{56} âîçìîæíûõ êëþ÷åé. Äëèíà êëþ÷åé äëÿ ðÿäà àëãîðèòìîâ, îáñóæäàåìûõ â ýòîé êíèãå, ðàâíû 64 áèòàì, âñåãî ìîæåò áûòü 2^{64} âîçìîæíûõ êëþ÷åé. Äðóãèå àëãîðèòìû èñïîëüçóþò 128-áèòîâûå êëþ÷è.

Ñêîðîñòü, ñ êîòîðîé ìîæåò áûòü ïðîâåðåí êàæäûé êëþ÷, èìåò ìåíüøåå âàæíîå çíà÷åíèå. Äëÿ ïðîâîäèìîãî àíàëèçà ÿ ïðåäïîëàãàþ, ÷òî ñêîðîñòü ïðîâåðêè êëþ÷à äëÿ êàæäîãî àëãîðèòìà ïðèìåðíî îäèíàêîâà. Â äåéñòâèòåëüíîñòè ñêîðîñòü ïðîâåðêè îäíîãî àëãîðèòìà ìîæåò áûòü â äâà, òðè èëè äàæå äåñÿòü ðàç âûøå ÷åì äóãîãî. Íî òàê êàê äëÿ òåõ äëèí êëþ÷åé, äëÿ êîòîðûõ ìû ïðîâîäèì ïîèñê, âðåìÿ îñêîðáëÿåò â ìèëëèîíû ðàç áîëüøå, ÷åì âðåìÿ ïðîâåðêè îäíîãî êëþ÷à, íåáîëüøèå îøèáêè â ñêîðîñòè ïðîâåðêè íå èìåþò çíà÷åíèÿ.

Â êðèïòîãðàôè ñðåäå áîëüøèíñòâî ñïîðîâ ïî ïîâîäó âñêðûòèÿ ãðóáîé ñèëîé ñêîíöåíòðèðîâàíû âîêðóã àëãîðèòìà DES. Â 1977 ãîäó Óèòôèëä Äèôôè è Ìàðòèí Õåëëìàí [497] ñôîðìóëèðîâàëè óñëîâèÿ ñïåöèàëèçèðîâàííîé àøèíû ïî âçëîìó DES. Ýòà ìàøèíà ñîñòîèò èç ìèëëèîíîâ ìèêðîñõåì, êàæäàÿ èç êîòîðûõ ïðîâåðÿåò ìèëëèîí êëþ÷åé â ñåêóíäó. Òàêàÿ ìàøèíà çà äâà ÷àñà ñìîæåò ïðîâåðèòü 2^{56} çà 20 ÷àñîâ. Ïðè âñêðûòèè äëãîðèòìà ñ 64-áèòîâûì êëþ÷îì ïðîâåðêà âñåõ 2^{64} ïîòðåáóåò 214 äíåé.

Çàäà÷à âñêðûòèÿ ãðóáîé ñèëîé êàê áóäòî ñïåöèàëüíî ïðèóùåíà äëÿ ïàðàëëåëüíûõ ïðîöåññîðîâ. Êàæäûé ïðîöåññîð ïðîâåðÿåò ïîäìíîæåñòâî ïðîñòðàíñòâà êëþ÷åé. Ïðîöåññîðàì íå íóæíî îáùàòüñÿ ìåæäó ñîáîé èíôîðìàöèåé, åäèíñòâåííûì èñïîëüçóåìûì ñîîáùåíèåì áóäåò ñîîáùåíèå, ñêàçàâøåå îá óñïåõå. Íåòðóäíî è äîêàçàòü ê îáùåìó ó÷àñòêó ïàìÿòè. Ñêîíñòðóêòîðû ìàøèíó ñ ìèëëèîíîì ïðîöåññîðîâ, êàæäûé èç êîòîðûõ ðàáîòàåò íåçàâèñèìî îò äóãèõ, íàçûâàþò ìàøèíîé äëÿ ïîèñêà êëþ÷à.

Ñêîíñòðóêòîðû ìàøèí äëÿ âçëîìà ãðóáîé ñèëîé Ìàéêë Âèíåð ðåøèë [1597, 1598]. (Îí ñêîíñòðóêòîâàë ìàøèíó äëÿ DES, íî àíàëèç ìîæåò áûòü âûïîëíåí ïî÷òè äëÿ âñåõ äëãîðèòìîâ.) Îí ðàçðàáîòàë ñïåöèàëèçèðîâàííûå ìèêðîñõåìû, ïëàòû è ñòîéêè, îöåíèë çàòðàòû è ñäåëàë âûâîä, ÷òî çà ìèëëèîí äîëëàðîâ ìîæíî ïîñòðîèòü ìàøèíó, êîòîðàÿ ñìîæåò âçëîìàòü 56-áèòîâûé êëþ÷ DES key â ñðåäíåì çà 3.5 ÷àñà (è íàâåðíÿêà çà 7 ÷àñîâ). Ñîòîøåíèå ñòèìóëîâ/ñêîðîñòü ÿâëÿåòñÿ ëèíåéíûì. Äëÿ ðÿäà äëèí êëþ÷åé ýòè çíà÷åíèÿ îâîáùåíû â 6-é. Âñïîìíèòå î çâêîíå Ìóðà: ìîùü âû÷èñëèòåëüíûõ ñðåäſñòâ ïðèáëèçèòåëüíî êâàäðóïëèðóåòñÿ êàæäûå 18 ìåñÿöåâ. Ýòî îçíà÷àåò, ÷òî çàðàíåå íåâîçìîæíî ïðåäſñêàçàòü íà ïîðÿäîê êàêèõ-íèáóäü ðåçóëüòàòû ëåò âïåðåä, è òî, ÷òî â 1995 ãîäó ñòîèò ìèëëèîí äîëëàðîâ, â 2000 ãîäó áóäåò ñòîèòü îêîëî 100000 äîëëàðîâ. Åùå áîëåå óïðîñòèòü ïðîöåññ âû÷èñëåíèé ìîãëà áû êîíôèäåíöèàëüíîñòü [724].

Äëÿ 56-áèòîâûõ êëþ÷åé ýòè ñòîìû îêàçûâàþòñÿ âïîëíå ïî êàðìàíó áîëüøèíñòâó êðóïíûõ êîðïîðàöèé è ìíîãèì êðèïòîãðàôè÷åñêèì ïðîãðàììàì. Âîåííûå áþäæåòû áîëüøèíſòâà ïðîìûøëåííî ðàçâèòûõ ſòðàí ìîãóò ïîçâîëèòü âçëàìûâàòü è 64-áèòíûå êëþ÷è. Âñêðûòèå 80-áèòíîãî êëþ÷à âſå åùå çà ïðåäſëàìè âîçìîæíîãî, íî åſëè òåêùàÿ òåíäåíöèÿ ſîõðàíèòſÿ, òî ÷åðåç êàêèõ-íèáóäü òðèäöàòü ëåò âſå ìîæåò èçìåíèòüſÿ.

Êîíå÷íî, íåëüſÿ ïðîãíîçèðîâàòü êîìüþòåðíóþ ìîùü íà 35 ëåò âïåðåä. Òåõíîëîãè÷åſêèå ïðîðûâû, ïîïóëſðíûå â íàó÷íîé òàíòàſòèêå, ìîãóò ſäåëàòü ýòè ïðîãíîſçû ſìåíåſ íàſſòſùåå âðåìſ ôèçè÷åſêèå ſãðàíè÷åíèſ ſîãóò ſäåëàòſ ýòè ïðîãſíîçû íåðåàëüſî îſòè÷íûè. Â êðèſòîãðàôèè óſíåå áûòſ ſåſſèſòſ ſîãëàſíè÷à 80-áèòſſãî êëþ÷à êàæåòſſ íåäîſòàòſ÷íſ äàëſſſâſäſû. Èſſſîſçóéòå êëþ÷, äëèíà êſòſðſãſ, ſſ ſåſſøåſ ſåðå, 112 áèò.

Òàáë. 7-1.
Îöåíêè ſðåäſſâſ âðåſåſíè äëſ àſ ſàðàòſſſãſ âſêðûòſſ ãðóáſſ ſèëſſ â 1995 ãſſãó.

	Äëſſíà êëþ÷åſ â áèòàõ					
Ñòſſſſſſòü	40	56	64	80	112	128
$100 Ê	2 ſåêſſſäû	35 ÷àſſâ	1 ãſſä	70000 ëåò	10^{14} ëåò	10^{19} ëåò
$1 Ì	0.2 ſåêſſſäû	3.5 ÷àſſà	37 äſſåé	7000 ëåò	10^{13} ëåò	10^{18} ëåò
$10 M	0.02 ſåêſſſäû	21 ſſſſſòà	4 äſſÿ	700 ëåò	10^{12} ëåò	10^{17} ëåò
$100 M	2 ſſſëëſſſåêſſſäû	2 ſſſſſòû	9 ÷àſſâ	70 ëåò	10^{11} ëåò	10^{16} ëåò
$1 Ã	0.2 ſſſëëſſſåêſſſäû	13	1 ÷àſ	7 ëåò	10^{10} ëåò	10^{15} ëåò
$10 Ã	0.02. ſſſëëſſſåêſſſäû	1 ſſåêſſſää	5.4 ſſſſòû	245 äſſåé	10^{9} ëåò	10^{14} ëåò
$100 Ã	2 ſſêðſſſåêſſſäû	0.1 ſſåêſſſäû	32 ſſåêſſſä	24 äſſÿ	10^{8} ëåò	10^{13} ëåò
$1 Ò	0.2 ſſêðſſſåêſſſäû	0.01 ſſåêſſſäû	3 ſſåêſſſäû	2.4 äſſÿ	10^{7} ëåò	10^{12} ëåò
$10 Ò	0.02 ſſêðſſſåêſſſäû	1 ſſëëëſſåêſſſää	0.3 ſſåêſſſäû	6 ÷àſſâ	10^{6} ëåò	10^{11} ëåò

Åñëè âçëîìùèê î÷åíü ñèëüíî õî÷åò âçëîìàòü êëþ÷, âñå, ÷òî åìó íóæíî, ýòî ïîòðàòèòü äåíüãè. Ñëåäîâàòåëüíî, ñòîèò ïîïûòàòüñÿ îïðåäåëèòü ìèíèìàëüíóþ "öåíó" êëþ÷à: â ïðåäåëàõ êàêîé ñòîèìîñòè ñâåäåíèé ìîæíî ïîëüçîâàòüñÿ îäíèì êëþ÷îì ïðåæäå, ÷åì åãî âñêðûòèå ñòàíåò ýêîíîìè÷åñêè âûãîäíûì? Êðàéíèé ñëó÷àé: åñëè øèôðîâàííîå ñîîáùåíèå ñòîèò $1.39, òî íåò ôèíàíñîâîãî ñìûñëà óñòàíàâëèâàòü àïïàðàòóðó ñòîèìîñòüþ 10 ìèëëèîíîâ äîëëàðîâ äëÿ âçëîìà ýòîãî êëþ÷à. Ñ äðóãîé ñòîðîíû, åñëè ñòîèìîñòü îòêðûòîãî òåêñòà - 100 ìèëëèîíîâ äîëëàðîâ, òî äåøèôðèðîâàíèå ýòîãî îäèíî÷íîãî ñîîáùåíèÿ âïîëíå îêóïèò ñòîèìîñòü àïïàðàòóðû âçëîìà. Êðîìå òîãî, ñòîèìîñòü ìíîãèõ ñîîáùåíèé ñî âðåìåíåì î÷åíü áûñòðî ïàäàåò.

Ïðîãðàììíîå âñêðûòèå

Áåç ñïåöèàëèçèðîâàííîé àïïàðàòóðû è îãðîìíûõ ïàðàëëåëüíûõ ìàøèí âñêðûòèå ãðóáîé ñèëîé íàìíîãî ñëîæíåå. Ïðîãðàììíîå âñêðûòèå â òûñÿ÷è ðàç ìåäëåííåå, ÷åì àïïàðàòíîå.

Ðåàëüíàÿ óãðîçà ïðîãðàììíîãî âñêðûòèÿ ãðóáîé ñèëîé ñòðàøíà íå ñâîåé íåèçáåæíîñòüþ, à òåì, ÷òî òàêîå âñêðûòèå "ñâîáîäíî". Íè÷åãî íå ñòîèò çàãðóçèòü ïðîñòàèâàþùèé ìèêðîêîìïüþòåð ïðîâåðêîé âîçìîæíûõ êëþ÷åé. Åñëè ïðàâèëüíûé êëþ÷ áóäåò íàéäåí - çàìå÷àòåëüíî, åñëè íåò - íè÷åãî íå ïîòåðÿíî. Íè÷åãî íå ñòîèò èñïîëüçîâàòü äëÿ ýòîãî öåëóþ ñåòü ìèêðîêîìïüþòåðîâ. Â íåäàâíèõ ýêñïåðèìåíòàõ ñ DES 40 ðàáî÷èõ ñòàíöèé â òå÷åíèå îäíîãî äíÿ ñóìåëè ïðîâåðèòü 2^{34} êëþ÷åé [603]. Ïðè ýòîé ñêîðîñòè äëÿ ïðîâåðêè âñåõ êëþ÷åé ïîòðåáóåòñÿ ÷åòûðå ìèëëèîíà äíåé, íî åñëè ïîïûòêè âñêðûòèÿ áóäóò ïðåäïðèíÿòû äîñòàòî÷íûì êîëè÷åñòâîì ëþäåé, òî êîìó-íèáóäü ãäå-íèáóäü ïîâåçåò. Êàê áûëî ñêàçàíî â [603]:

> Îñíîâíîé óãðîçîé ïðîãðàììíîãî âñêðûòèÿ ÿâëÿåòñÿ ñëåïîå âåçåíèå. Ïðåäñòàâüòå ñåáå óíèâåðñèòåòñêóþ ñåòü èç 512 îáúåäèíåííûõ â ñåòü ðàáî÷èõ ñòàíöèé. Äëÿ íåêîòîðûõ óíèâåðñèòåòñêèõ ãîðîäêîâ ýòî ñåòü âåñüìà ñðåäíåãî ðàçìåðà. Òàêèå ñåòè ìîãóò äàæå ðàñïîëçòèñü ïî âñåìó ìèðó, êîîðäèíèðóÿ ñâîþ äåÿòåëüíîñòü ïî ýëåêòðîííîé ïî÷òå. Ïóñòü êàæäàÿ ðàáî÷àÿ ñòàíöèÿ ñïîñîáíà ðàáîòàòü (ñ àëãîðèòìîì) ñî ñêîðîñòüþ 15000 øèôðîâàíèé â ñåêóíäó. ... Ñ ó÷åòîì íàêëàäíûõ ðàñõîäîâ íà ïðîâåðêó è ñìåíó êëþ÷åé óìåíüøèì ñêîðîñòü äî . . . 8192 ïðîâåðîê â ñåêóíäó íà ìàøèíó. ×òîáû, èñïîëüçóÿ îïèñàííóþ ñèñòåìó, èñ÷åðïàòü ïðîñòðàíñòâî (56-áèòîâûõ) êëþ÷åé ïîòðåáóåòñÿ 545 ëåò (â ïðåäïîëîæåíèè, ÷òî ñåòü òðàòèò íà ýòó çàäà÷ó 24 ÷àñà â ñóòêè). Çàìåòèì, îäíàêî, ÷òî ñ ïîìîùüþ òàêèõ âû÷èñëåíèé ñòîðîííèêè íàøåãî ñòóäåíòà ïîëó÷àþò îäèí øàíñ èç 200000 ðàñêðûòü êëþ÷ â òå÷åíèå îäíîãî äíÿ. Çà äîëãèé óèêåíä èõ øàíñû âîçðàñòàþò äî îäíîãî èç øåñòèäåñÿòè øåñòè òûñÿ÷. ×åì áûñòðåå èõ àïïàðàòóðà, èëè ÷åì áîëüøå çàäåéñòâîâàíî ìàøèí, òåì ëó÷øå ñòàíîâÿòñÿ èõ øàíñû. Âåðîÿòíîñòü çàðàáîòàòü íà æèçíü, âûèãðûâàÿ íà ñêà÷êàõ, íåâûñîêà, íî ðàçâå íå ýòè âûèãðûøè çàïîëíÿþò ñîáîé ïðåññ-ðåëèçû. Ê ïðèìåðó, ýòî ãîðàçäî áîëüøàÿ âåðîÿòíîñòü, ÷åì âîçìîæíîñòü âûèãðûøà â ïðàâèòåëüñòâåííûõ ëîòåðåÿõ. "Îäèí íà ìèëëèîí"? "Îäèí ðàç çà òûñÿ÷ó ëåò "? Áîëüøå íåâîçìîæíî ñ ïîëíîé îòâåòñòâåííîñòüþ äåëàòü òàêèå çàÿâëåíèÿ. ßâëÿåòñÿ ëè ïðèåìëåìûì ýòîò ïðîãîëæàþùèéñÿ ðèñê?

Èñïîëüçîâàíèå àëãîðèòìà ñ 64-áèòîâûì êëþ÷îì âìåñòî 56-áèòîâîãî êëþ÷à äåëàåò ýòî âñêðûòèå â 256 ðàç ñëîæíåå. À 40-áèòîâûé êëþ÷ äåëàåò êàðòèíó ïðîñòî áåçðàäîñòíîé. Ñåòü èç 400 êîìïüþòåðîâ ñ ïðîèçâîäèòåëüíîñòüþ 32000 øèôðîâàíèé â ñåêóíäó ìîæåò çà äåíü âûïîëíèòü âñêðûòèå ãðóáûì âçëîìîì 40-áèòîâîãî êëþ÷à. (Â 1992 ãîäó àëãîðèòìû RC2 è RC4 áûëî ðàçðåøåíî ýêñïîðòèðîâàòü ñ 40- áèòîâûì êëþ÷îì - ñì. ðàçäåë 13.8.)

128-áèòîâûé êëþ÷ äåëàåò íåëåïîé äàæå ìûñëü î âñêðûòèè ãðóáûì âçëîìîì. Ïî îöåíêå ïðîìûøëåííûõ ýêñïåðòîâ ê 1996 ãîäó â ìèðå áóäåò èñïîëüçîâàòüñÿ 200 ìèëëèîíîâ êîìïüþòåðîâ. Ýòà îöåíêà âêëþ÷àåò âñå - îò ãèãàíòñêîãî ìýéíôðåéìà Cray äî áëîêíîòíûõ êîìïüþòåðîâ. Äàæå åñëè âñå ýòè êîìïüþòåðû áóäóò áðîøåíû íà âñêðûòèå ãðóáîé ñèëîé, è êàæäûé èç íèõ áóäåò âûïîëíÿòü ìèëëèîí øèôðîâàíèé â ñåêóíäó, âðåìÿ ðàñêðûòèÿ êëþ÷à âñå ðàâíî áóäåò â ìèëëèîí ðàç áîëüøå âðåìåíè ñóùåñòâîâàíèÿ âñåëåííîé.

Íåéðîííûå ñåòè

Íåéðîííûå ñåòè íå ñëèøêîì ïðèãîäíû äëÿ êðèïòîàíàëèçà, â ïåðâóþ î÷åðåäü èç-çà ôîðìû ïðîñòðàíñòâà ðåøåíèé. Ëó÷øå âñåãî íåéðîííûå ñåòè ðàáîòàþò ñ ïðîáëåìàìè, èìåþùèìè íåïðåðûâíîå ìíîæåñòâî ðåøåíèé, îäíè èç êîòîðûõ ëó÷øå äðóãèõ. Ýòî ïîçâîëÿåò íåéðîííûì ñåòÿì îáó÷àòüñÿ, ïðåäëàãàÿ âñå ëó÷øèå è ëó÷øèå ðåøåíèÿ. Îòñóòñòâèå íåïðåðûâíîñòè â àëãîðèòìå îñòàâëÿåò ìàëî ìåñòà îáó÷åíèþ: âû ëèáî ðàñêðîåòå êëþ÷, ëèáî íåò. (Ïî êðàéíåé ìåðå, ýòî âåðíî ïðè èñïîëüçîâàíèè ëþáîãî õîðîøåãî àëãîðèòìà.) Íåéðîííûå ñåòè õîðîøî ðàáîòàþò â ñòðóêòóðèðîâàííûõ ñðåäàõ, ãäå îáó÷åíèå âîçìîæíî, íî íå â âûñîêîýíòðîïèéíîì, êàæóùåìñÿ ñëó÷àéíûì ìèðå êðèïòîãðàôèè.

Âèðóñû

Ñàìàÿ áîëüøàÿ òðóäíîñòü â ïîëó÷åíèè ìèëëèîíîâ êîìïüþòåðîâ äëÿ âñêðûòèÿ ãðóáûì âçëîìîì - ýòî óáåäèòü ìèëëèîíû êîìïüþòåðíûõ âëàäåëüöåâ ïðèíÿòü ó÷àñòèå âî âñêðûòèè. Âû ìîãëè áû âåæëèâî ïîïðîñèòü, íî ýòî òðåáóåò ìíîãî âðåìåíè, è îíè ìîãóò ñêàçàòü íåò. Âû ìîãëè áû ïîïðîáîâàòü ñèëîé âîðâàòüñÿ â èõ êîìïüþòåðû, íî ýòî ïîòðåáóåò åùå áîëüøå âðåìåíè è ìîæåò çàêîí÷èòüñÿ âàøèì àðåñòîì. Âû ìîãëè áû òàêæå èñïîëüçîâàòü êîìïüþòåðíûé âèðóñ, ÷òîáû ðàñïðîñòðàíèòü ïðîãðàììó âçëîìà ñðåäè êàê ìîæíî áîëüøåãî êîëè÷åñòâà êîìïüþòåðîâ.

Ýòà îñîáåííî êîâàðíàÿ èäåÿ âïåðâûå ïîÿâèëàñü â [1593]. Âçëîìùèê ïèøåò è âûïóñêàåò íà âîëþ êîìïüþòåðíûé âèðóñ. Ýòîò âèðóñ íå ïåðåôîðìàòèðóåò æåñòêèé äèñê, íå óäàëÿåò ôàéëû, íî âî âðåìÿ ïðîñòîÿ êîìïüþòåðà îí ðàáîòàåò íà êðèïòîàíàëèòè÷åñêîé ïðîáëåìîé ãðóáîãî âçëîìà. Ðàçëè÷íûå èññëåäîâàíèÿ ïîêàçàëè, ÷òî êîìïü-

þòåð ïðîñòàèâàåò îò 70 äî 90 ïðîöåíòîâ âðåìåíè, òàê ÷òî ó âèðóñà íå áóäåò ïðîáëåì ñ âðåìåíåì äëÿ ðåøåíèÿ ýòîé çàäà÷è. Åñëè îí íåòðåáîâàòåëåí è â äðóãèõ îòíîøåíèÿõ, òî åãî ðàáîòà äàæå íå áóäåò çàìåòíà.

Â êîíöå êîíöîâ, îäíà èç ìàøèíà íàòêíåòñÿ íà ïðàâèëüíûé êëþ÷. Â ýòîò ìîìåíò èìåþòñÿ äâà âàðèàíòà ïðîäîëæåíèÿ. Âî ïåðâûõ, âèðóñ ìîã áû ïîðîäèòü äðóãîé âèðóñ. Îí íå äåëàë áû íè÷åãî, êðîìå ñàìîâîñïðîèçâåäåíèÿ è óäàëåíèÿ âñåõ íàéäåííûõ êîïèé âñêðûâàþùåãî âèðóñà, íî ñîäåðæàë áû èíôîðìàöèþ î ïðàâèëüíîì êëþ÷å. Ýòîò íîâûé âèðóñ ïðîñòî ðàñïðîñòðàíÿëñÿ áû ñðåäè êîìïüþòåðîâ, ïîêà íå äîáðàëñÿ áû äî êîìïüþòåðà ÷åëîâåêà, êîòîðûé íàïèñàë ïåðâîíà÷àëüíûé âèðóñ.

Äðóãèì, òðóñëèâûì ïîäõîäîì áàë áû âûâîä íà ýêðàí ñëåäóþùåãî ñîîáùåíèÿ:

> Â ýòîì êîìïüþòåðå åñòü ñåðüåçíàÿ îøèáêà. Ïîæàëóéñòà ïîçâîíèòå 1-8001234567 è ïðîäèêòóéòå îïåðàòîðó ñëåäóþùåå 64-áèòîâîå ÷èñëî:
>
> xxxx xxxx xxxx xxxx
>
> Ïåðâîìó, êòî ñîîáùèò îá ýòîé îøèáêå áóäåò âûïëà÷åíî âîçíàãðàæäåíèå 100 äîëëàðîâ.

Íàñêîëüêî ýôôåêòèâíî òàêîå âñêðûòèå? Ïóñòü òèïè÷íûé çàðàæåííûé êîìïüþòåð ïðîâåðÿåò òûñÿ÷ó êëþ÷åé â ñåêóíäó. Ýòà ñêîðîñòü íàìíîãî ìåíüøå ïîòåíöèàëüíûõ âîçìîæíîñòåé êîìïüþòåðà, âåäü ìû ïîëàãàåì, ÷òî îí èíîãäà áóäåò äåëàòü è äðóãèå âåùè. Ïðåäïîëîæèì òàêæå, ÷òî òèïè÷íûé âèðóñ èíôèöèðóåò 10 ìèëëèîíîâ ìàøèí. Ýòîò âèðóñ ìîæåò âñêðûòü 56-áèòîâûé êëþ÷ çà 83 äíÿ, à 64 áèòîâûé - çà 58 ëåò. Âàì âîçìîæíî ïðèøëîñü áû ïîäêóïèòü ðàçðàáîò÷èêîâ àíòèâèðóñíîãî ïðîãðàììíîãî îáåñïå÷åíèÿ, íî ýòî óæå âàøè ïðîáëåìû. Ëþáîå óâåëè÷åíèå ñêîðîñòè êîìïüþòåðîâ èëè ðàñïðîñòðàíåíèÿ âèðóñà, êîíå÷íî, ñäåëàëî áû ýòî íàïàäåíèå áîëåå ýôôåêòèâíûì.

Êèòàéñêàÿ ëîòåðåÿ

Êèòàéñêàÿ Ëîòåðåÿ - ýêëåêòè÷åñêèé, íî âîçìîæíûé ñïîñîá ñîçäàíèÿ ãðîìàäíîé ïàðàëëåëüíîé ìàøèíû äëÿ êðèïòîàíàëèçà [1278]. Âîîáðàçèòå, ÷òî ìèêðîñõåìà, âñêðûâàþùàÿ àëãîðèòì ãðóáîé ñèëîé ñî ñêîðîñòüþ ìèëëèîí ïðîâåðîê â ñåêóíäó, âñòðîåíà â êàæäûé ïðîäàííûé ðàäèîïðèåìíèê è òåëåâèçîð. Êàæäàÿ ìèêðîñõåìà çàïðîãðàììèðîâàíà äëÿ àâòîìàòè÷åñêîé ïðîâåðêè ðàçëè÷íîãî íàáîðà êëþ÷åé ïîñëå ïîëó÷åíèÿ ïàðû îòêðûòûé òåêñò/øèôðîòåêñò ïî ýôèðó. Êàæäûé ðàç êîãäà êèòàéñêîå ïðàâèòåëüñòâî õî÷åò ðàñêðûòü êëþ÷, îíî ïåðåäàåò èñõîäíûå äàííûå ïî ðàäèî. Âñå ðàäèîïðèåìíèêè è òåëåâèçîðû â ñòðàíå íà÷èíàþò ïûõòåòü. Â êîíå÷íîì ñ÷åòå, ïðàâèëüíûé êëþ÷ ïîÿâëÿåòñÿ íà ÷üåì-íèáóäü äèñïëåå. Êèòàéñêîå ïðàâèòåëüñòâî ïëàòèò ïðèç òîìó ÷åëîâåêó - ýòî ãàðàíòèðóåò, ÷òî ðåçóëüòàò áóäåò ñîîáùåí áûñòðî è ïðàâèëüíî, è òàêæå ñïîñîáñòâóåò ðûíî÷íîìó óñïåõó ðàäèîïðèåìíèêîâ è òåëåâèçîðîâ ñ ìèêðîñõåìàìè âñêðûòèÿ.

Åñëè ó êàæäîãî ÷åëîâåêà â Êèòàå, áóäü òî ìóæ÷èíà, æåíùèíà èëè ðåáåíîê, åñòü ðàäèîïðèåìíèê èëè òåëåâèçîð, òî ïðàâèëüíîå çíà÷åíèå 56-áèòîâîãî êëþ÷à ïîÿâèòñÿ ÷åðåç 61 ñåêóíäó. Åñëè ðàäèîïðèåìíèê èëè òåëåâèçîð åñòü òîëüêî ó êàæäîãî äåñÿòîãî êèòàéöà(÷òî áëèçêî ê äåéñòâèòåëüíîñòè), òî ïðàâèëüíûé êëþ÷ ïîÿâèòñÿ ÷åðåç 10 ìèíóò. Ïðàâèëüíûé 64-áèòîâûé êëþ÷ áóäåò ðàñêðûò ÷åðåç 4.3 ÷àñà (43 ÷àñà, åñëè ðàäèîïðèåìíèê èëè òåëåâèçîð åñòü òîëüêî ó êàæäîãî äåñÿòîãî êèòàéöà).

×òîáû ñäåëàòü òàêîå âñêðûòèå âîçìîæíûì íà ïðàêòèêå, íåîáõîäèìî ñäåëàòü ðÿä ìîäèôèêàöèé. Âî ïåðâûõ, ïðîùå, ÷òîáû êàæäàÿ ìèêðîñõåìà ïðîâåðÿëà ñëó÷àéíûå, à íå óíèêàëüíûå êëþ÷è. Ýòî ñäåëàåò âñêðûòèå íà 39% ìåäëåííåå, ÷òî íå î÷åíü âàæíî äëÿ ÷èñåë òàêîãî ìàñøòàáà. Çàòåì, Êèòàéñêàÿ êîììóíèñòè÷åñêàÿ ïàðòèÿ äîëæíà ïðèíÿòü ðåøåíèå, ÷òî êàæäûé äîëæåí âêëþ÷àòü ñâîé ïðèåìíèê èëè òåëåâèçîð â îïðåäåëåííîå âðåìÿ, ÷òîáû ãàðàíòèðîâàòü ðàáîòó âñåõ ïðèåìíûõ óñòðîéñòâ âî âðåìÿ ïåðåäà÷è ïàðû îòêðûòûé òåêñò/øèôðîòåêñò. Íàêîíåö, êàæäîìó äîëæíî áûòü ïðèêàçàíî ïîçâîíèòü â Öåíòð - èëè êàê îí òàì íàçûâàåòñÿ - êîãäà êëþ÷ ïîÿâëÿåòñÿ ó íåãî íà ýêðàíå è çà÷èòàòü ñòðîêó ÷èñåë, ïîÿâèâøóþñÿ íà ýêðàíå.

Ýôôåêòèâíîñòü Êèòàéñêîé ëîòåðåè äëÿ ðàçëè÷íûõ ñòðàí è ðàçëè÷íûõ äëèí êëþ÷à ïîêàçàíà â 5-é. ßñíî, ÷òî Êèòàé îêàçàëñÿ áû â ëó÷øåì ïîëîæåíèè, åñëè áû ó êàæäîãî êèòàéöà - ìóæ÷èíû, æåíùèíû èëè ðåáåíêà - áûë ñâîé ïðèåìíèê èëè òåëåâèçîð. Â Ñîåäèíåííûõ øòàòàõ æèâåò ìåíüøå ëþäåé, íî ãîðàçäî áîëüøå àïïàðàòóðû. Øòàò Âàéîìèíã ñàìîñòîÿòåëüíî ñìîæåò âçëîìàòü 56-áèòîâûé êëþ÷ ìåíüøå, ÷åì çà äåíü.

Òàáë. 7-2.
Îöåíêè ñðåäíåãî âðåìåíè âû÷èñëåíèÿ ãðóáîé ñëåïîé ïðè êèòàéñêîé ëîòåðåå

(Âñå äàííûå âçÿòû èç *World Almanac and Book of Facts* çà 1995 ãîä.)

Ñòðàíà	Íàñåëåíèå	Êîëè÷åñòâî òåëåâèçîðîâ/ðàäèîïðèåìíèêîâ	Âðåìÿ âçëîìà	
			56 áèò	64 áèòà
Êèòàé	1190431000	257000000	280 ñåêóíä	20 ÷àñîâ
ÑØÀ	260714000	739000000	97 ñåêóíä	6.9 ÷àñà
Èðàê	19890000	4730000	4.2 ÷àñà	44 äíÿ
Èçðàèëü	5051000	3640000	5.5 ÷àñà	58 äíåé
Âàéîìèíã	470000	1330000	15 ÷àñîâ	160 äíåé
Âèííèöêà, Íåâàäà	6100	17300	48 äíåé	34 ãîäà

Áèîõèìè÷åñêèå ïðîáëåìû

Åñëè âîçìîæíî ñîçäàíèå áèîìåõàíèçìîâ, òî áûëî áû ãëóïî íå ïîïûòàòüñÿ èñïîëüçîâàòü èõ â èíòåðåñàõ êðèòàíèòåëçà âîêðóãëåíèÿ ãóáíé. Ðàññìîòðèì ãèïîòåòè÷åñêîå æèâîòíîå, íàçûâàåìîå "DESîçàâðî" [1278]. Îíî ñîñòîèò èç áèîëîãè÷åñêèõ êëåòîê, óìåþùèõ ïðîâåðÿòü âîçìîæíûå êëþ÷è. Ïàðû "îêðûòûé òåêñò/øèôðîâêà" ïîñòóïàþò â êëåòêè ïî íåêîòîðîìó îïòè÷åñêîìó êàíàëó (âèäèòü ëè, âñå ýòè êëåòêè ïðîçðà÷íû). Ðåøåíèÿ äîñòàâëÿòñÿ ê îðãàíàì ðå÷è DESîçàâðà ñ ïîìîùü ñïåöèàëüíûõ êëåòîê, ïóòåøåñòâóþùèõ ïî êðîâåíîñíîé ñèſòåìå æèâîòíîãî.

Òèïè÷íûé äëínîçàâð ñîñòîèò èç 10^{14} êëåòîê (áåç áàêòåðèé). Åñëè êàæäàÿ èç íèõ âûïîëíÿåò ìèëëèîí øèôðîâàíèé â ñåêóíäó (íåïëîõîé ðåçóëüòàò), âñêðûòèå 56-áèòîâîãî êëþ÷à çàéìåò ñåìü äåñÿòèòûñÿ÷íûõ ñåêóíäû. Âñêðûòèå 64-áèòîâîãî êëþ÷à ïîòðåáóåò ìåíüøå, ÷åì äâå äåñÿòûõ ñåêóíäû. Âñêðûòèå 8-áèòîâîãî êëþ÷à âñå æå ïðîäëèòñÿ 10^{11} ëåò.

Äðóãîé áèîëîãè÷åñêèé ïîäõîä ñîñòîèò â èſïîëüçîâàíèè åå÷åòè÷åñêè ïðîêëèòîðóåìûõ êðèïòîãðàôè÷åñêèõ ìîðñêèõ áîãîðîñåé, êîòîðûå óìåþ ðàſïðîñòðàíÿòü âñêðûòûå êðèïòîãðàôè÷åñêèõ äëãîðèòìîâ ãðóáîé ñèſòåìû [1278]. Òàêèå îðãàíèçìû, ïîêðûâ áîëüøóþ îáëàſòü, ïîçâîëèëè áû ñîçäàòü ðàſïðåäåëåíóþ ìàøèíó ñîëüøèì êîëè÷åſñòâîì ïðîöåſſîðîâ. Ïàðà "îêðûòûé òåêſò/øèôðîâêà" ìîãëà áû ïåðèäè÷åſñêè ïî ðàäèî ÷åðåç ñïóſòíèê. Îáíàðóæåíèå ðåçóëüòàòà îðãàíèçìîì ìîãëî áû ñòèſóëèðîâàòü áëèçëåæàùèå ÿ÷åéêè èſìåíèòü öâåò, ñîîáùàÿ ðåøåíèå îáðàòíî íà ſïóſíèê.

Ïðåäſïîſæèì, ÷òî òèï÷íàÿ êëåòêà ìîðſêîé âîäîſðſëè - ýòî êóáèê ſì ſòîſðſíſé 10 ìèêðſí (âſçſìſæſí, ýòî îöåíêà ſâåðſó, ſëåäſâſòåëüſî 10^{15} êëåòîê çàſſîſýò êóáè÷åſñêèé ìåòð. Âſû ſëåſſíèòå èſ â îêåſí, ſſêðſâàÿ 200 êâàäðàòſſûſ ìèſſ (518 êâàäðàòſſûſ êèſſſìåòðſâ) íà ſëóáèſó îäſí ìåòð (ýòſ âàøè ſðſáſëåſſ, êàê ſñóåſñòàòü ýòſ - ÿ ſſàäþ òſſüſêſ èääþ), è ó âàſ áóäåò 10^{23} âſäſðſſñſé (áſſëå ÷åſ ſſòſáſé ſëſſſèàðäà ãàſſſſſâ), ſſàâàþſèſ â ſêåàſá. (Äſÿ ſðàſáſéſÿ, èç òàſêåðà *Valdez* âſòåêſſſ 10 ſèſſſſſſſâ ãàſſſſſâ ſåôòſ.) Åſſſ êàæäàÿ èç ſſſ ſſæåſ ſðſſâåðÿòſ ſſſſſſſſ êſþ÷åſ â ſåſóſáſó, òſ äſÿ 128-áſòſâſſſ àſſàſðſòſà ſſſ ðàſſêſſþſ êſþ÷ â òſſüſêſ ſſóſòſÿ 100 ſåſ. (Âſçſſſſøåå ſðſ ýòſ ſ öſåſòſåſſſ ſſðſſſſſ âſſäſðſſſſſé - ýòſ âàøà ſðſáſëſà.) Êðóſſſå äſſòſæåſſſÿ â áſſòſðſäåſſòâſſ ſſðſſſſſ âſſäſðſſſſé, ſſ äſàſåſð ſſſ äàæå ðàçſåðſ ſſýòſà â ſſêåſſ ſſãóſ çſſåòſſſ óſſſüøſòſ ýſ çſà÷åſſÿ. Äàæå ſå ſſſðàøſâſàſòå ſåſſ ſ ſàſſòåſſſſſãſ.

Òåðſſäſſſà÷åſſêå ſſðàſſ÷åſſÿ

Îäſſ èç ſſåäſſòâſſ çàſſſà âòſðſſäſſàſſêſ ÿâſÿåſſÿ òſ, ÷òſ äſÿ ſſðåäſſòàâſåſſÿ ſſſôſðſàöſſ íåſá-õſſäſſſ íåſſòſðſå ſſſſ÷åſſòâſ ýſåðäſſ. Çàſſſñü ſäſſſ÷íſſâſ áſòà, ſſſſåſÿþſàÿ ſſſſòſÿſſà ſſſſòåſû, òðåáóåò ſſſſ-÷åſſòâà ýſåðäſſſ íå ſåſüøå ÷åſ kT; äàå Ò - àáſſſſþſſàÿ òåſ ſåðàòóðà ſſſſòåſû è k - ſſſòſÿſſàÿ Áſſüſſàſá. (Íå âſſſóſóåſñü, óðſê ôſçſêê óæå ſſ÷òſ çàſſ÷åſ.)

Sðſſÿâ, ÷òſ k = l.38*10^{-16} ýðã/K, è ÷òſ òåſ ſåðàòóðà ſſðóæàþſåé âſåſåſſ÷é 3.2K, ſſàåſüſû ſſ ſſþòåð, ðà-áſòàÿ ſſðå 3.2K, ſſſòðåáſÿſ áû 4.4*10^{-16} ýðãà âſÿſſſ ðàç, ſſſãàà ſſ óſòàſàâſſſàåſ ſſſ ſáðàſſûâſåſ áſſ. Ðàáſòà ſſ ſſþòåðà ſðſ òåſ ſåðàòóðå áſſåå ſſçſſſ, ÷åſ òåſ ſåðàòóðà ſſſſ÷ſſſ ſðſſſòáſſòàà, ſſòðåáſâàſà áû äſ-ſſſſſòàſüſûſ ðàſõſäſâ ýſåðäſſ äſÿ ſòâſäà òåſà.

Äàſåå, ýſåðãſÿ, ſſçſó÷àſſàÿ ſàøſſ Ñſſſóſ çà ãſä, ſſſſòàâſÿſ ſſſſ 1.21*10^{41} ýðãſâ. Ýòſ äſſòàòſ÷ſſ äſÿ âûſſſſſåſſÿ 2*10^{56} ſåðſſſ áſòà â ſàøſſ ſäſàſüſſſ ſſ ſſþòåðå, à ýòſãſ, â ſâſþ ſ÷åðåäü, õâàòſ äſÿ òſãſ, ÷òſ-áû 187-áſòſâûſ ſ÷åò÷ſê ſðſáåæàſ âſå ſâſſ çſà÷åſſÿ. Åſſſ ſû ſſſòðſſ âſêðóã Ñſſſſöà ſſåðó Äàſſſſà ſ ſåðå-õâàòſ áåç âſÿſêſõ ſſòåðü âſþ åãſ ýſåðãſþ çà 32 ãſäà, ſû ſſſåſ ſſſë÷ſòſ ſêſ ſüþòåð äſÿ âû÷ſſſåſſÿ 2^{192} ÷ſſåſ. Êſſå÷ſſ, ýſåðãſſ äſÿ ſðſâåäſſÿ êâſêſõ-ſſáóäü ſſſåçſſûõ âû÷ſſſåſſé ſ ýòſ ſ÷åò÷ſêſ óæå ſſ

îñòàíåòñÿ.

Í î ýòî òîëüêî îäíà æàëêàÿ çâåçäà. Ïðè âçðûâå òèïè÷íîé ñâåðõíîâîé âûäåëÿåòñÿ îêîëî 10^{51} ýðãîâ. (Â ñòî ðàç áîëüøå ýíåðãèè âûäåëÿåòñÿ â âèäå íåéòðèíî, íî ïóñòü îíè ïîêà ëåòàþò.) Åñëè âñþ ýòó ýíåðãèþ óäàñòñÿ áðîñèòü íà îäíó âû÷èñëèòåëüíóþ îõåéêó, òî âñå ñâîè çíà÷åíèÿ ñì îæåò ïðèýòñÿ 219-áèòîâûé ñ÷åò÷èê.

Ýòè ÷èñëà íå èìåþò íè÷åãî îáùåãî ñ ñàìîé àïïàðàòóðîé, îíè ïðîñòî ïîêàçûâàþò ìàêñèìàëüíûå çíà÷åíèÿ, îáóñëîâëåííûå òåðìîäèíàìèêîé. Êðîìå òîãî, ýòè ÷èñëà íàëÿãàíî äàìîíñòðèðóþ, ÷òî âñëûøèì ãðóáîé ñèëîé 256-áèòîâîãî êëþ÷à áóäåò íåâîçìîæíî, ïîêà êîìïüþòåðû ïîñòðîåíû èç îáû÷íîé ìàòåðèè è ðàñïîëàãàþòñÿ â îáû÷íîì ïðîñòðàíñòâå.

7.2 Äëèíà îòêðûòîãî êëþ÷à

Îäíîíàïðàâëåííûå ôóíêöèè îáñóæäàëèñü â ðàçäåë 2.3. Îäíîíàïðàâëåííîé ôóíêöèåé ÿâëÿåòñÿ óìíîæåíèå äâóõ áîëüøèõ ïðîñòûõ ÷èñåë, ïîëó÷èòü ïðîèçâåäåíèå, ïåðåìíîæèâ ÷èñëà, íåòðóäíî, íî íåëåãêî ðàçëîæèòü ïðîèçâåäåíèå íà ìíîæèòåëè è ïîëó÷èòü äâà áîëüøèõ ïðîñòûõ ÷èñëà (ñì. ðàçäåë 11.3). Êðèïòîãðàôèÿ ñ îòêðûòûì ìè êëþ÷àìè ñîîòâåòſòâóþ ýòó èäåþ äëÿ ñîçäàíèÿ îäíîíàïðàâëåííîé ôóíêöèè ñ ëþêîì. Íà ñàìîì äåëå, ýòî ëîæü, *íå äîêàçàíî*, ÷òî ðàçëîæåíèå íà ìíîæèòåëè ÿâëÿåòſÿ òÿæåëîé ïðîáëåìîé (ñì. ðàçäåë 11.4). Íàñêîëüêî ñåãîäíÿ èçâåſòíî, ýòî ïîõîæå íà ïðàâäó. È äàæå åñëè ýòî òàê, íèêòî íå ìîæåò äîêàçàòü, ÷òî òðóäíûå ïðîáëåìû äåéſòâèòåëüíî òðóäíû. Âñå ſ÷èòàþ, ÷òî ðàçëîæåíèå íà ìíîæèòåëè ÿâëÿåòſÿ òðóäíîé çàäà÷åé, íî ýòî íèêîãäà íå áûëî äîêàçàíî ìàòåìàòè÷åſêè.

Íà ýòî ſòîèò îſòàíîâèòſſÿ ïîïîäðîáíåå. Ëåãêî ïðåäſòàâèòü, ÷òî ëåò ÷åðåç 50 ìû ſíåäåìſÿ âſåſòå, âſïîſíèíàÿ ſòàðîå äîáðîå âðåſÿ, êîãäà âſå ëþäè ſ÷èòàëè, ÷òî ðàçëîæåíèå íà ſíîæèòåſè áûëî òðóäíûſ è ëåæàëî â îſſíîâå êðèïòîãðàôèè, à ðàçëè÷íûå êîſïàíèè äåëàëè èſ ýòîſî äåíüãè. Ëåãêî âîſſòàíîâèòſ, à ðàçëîæåíèå íà ſíîæèòåſè èſëè äſòèæåíèÿ òåſòèſ ſîſæíſòè ſäåëàòſ ðàçëîæåíèå íà ſíîæèòåſè ððêâàèſſûſ. Íſòî ïðè÷èſ âåðèòſ â ýòî - è áîëſòèſſòâîſ ëþäåſ, çíàþſſèſ äſſòàòſ, ſòîáû èſåòſ ſîſáſòâåſſſíûſ ſíåſèå, ſêàæåſ âàſ, ÷òî ſſäſáſſíå ðàçâèòèå ſſáûſòèé ÿâëÿåòſÿ ſàëſîâåðſÿòſûſ - íſ íåſ è ſðè÷èſ âåðèòſ, ÷òî òàêſãſ ſðſðûâà íå ſëó÷èſſÿ.

Â ëþáſſ ſëó÷åå, äſſèſèðóſſùèå ſåãſäſÿ àëãſîðèſſûſ øèſðſâàſèëÿ ſ ſòêðûſòſ êëþ÷ſſ ſſſſîâàſûſ íà òðóäſſſñòè ðàçëſſæåſèëÿ íà ſſſæèſòåëè áſëüøèſõ ÷èſåë, êſòſðûſå ÿâëÿþſÿ ſðſèçâåäåſèåſ äâóſ áſëüøèſõ ſðſſòûſ ÷èſåë. (Äðóãèſ àëãſîðèſſûſ ſſſſîâàſûſ íà òàê íàçûâàſſſé Äèſêðåòſſé ſðſáëſſſé ëſãàðèſſà, íſ ſſêà ſðåäſſſèſſ, ÷òſ ê íåé ſðèſſſèſſûſ òå æå ðàſſſóæäåſèÿ.) Ýòè àëãſîðèſſûſ òàêæå âſſſðèſſ÷èâû ê âſêðûſòſ ãðóáſé ſèëſſ, íſ ſſ ðàçſſſſó. Âçſſſ ýòſõ àëãſîðèſſſâ ſſſòſſèò íå èç ſåðåáſîðà âſåſõ âſçſſſæſſûſ êëþ÷åé, à èç ſſſſûſſſê ðàçſſæſåſèÿ áſſëüøſõ ÷èſåë íà ſſſæèſòåëè (ëèë âçÿòſÿ äèſêðåòſſûſ ëſãàðſſſſſâ â ſ÷åſü áſëüøſſ êſíå÷íſé íáſàñòſ - òſ÷íſ òàêàÿ æå ſðſáëåſà). Åſſëè ÷èſëſ ſëſøſſſ ſàſſ, âû íſêâê íå çàùſùåſû. Åſſëè ÷èſſſ äſſòàòſ÷íſ åſëſêſ, òſ âû íàäåæſſ çàùſùåſû ſðſòſàâ âſåé âû÷èſëſòåſſûſſé ſſûſ ſſðà, åſſëè ſſà áóäåò áſòüſÿ íàä ýòſé çàäà÷åé ſ íàſòſÿ-ùåſſ âðåſåſé äſ òåſ ſſð, ſſêà ÑſſëſöÞ íå ſòàſåò ſåððſſſâſé - òàſſâſ ſåſſſäſÿøſåå ſſſſſſàſèſà ſàòàſàòſêſ ýòſé ſðſáëåſû. Â ðàçäëå 11.3 ðàçſſſæåſſſà íà ſſſæſòåëſ ðàſſſſàòðſâåſòſÿ ſàòàſàòſ÷åſêſ ſſäðſáſſ, à çååſü ÿ ſãðàſſ÷óſü ſòåſſſſé âðåſåſſſ ðàçſſæåſſſÿ íà ſſſæſòåëſ ÷èſåë ðàçëſ÷ſſé äëſſû.

Ðàçëàãàòü áſëüøèå ÷èſëà íà ſſſæſòåëſ íåëåâſ, íſ, ê íåñ÷àſòüſ äëÿ ſðſåſòſðſſâùſſſâ àëãſðſòſſâ, ýòſò ſðſöåſſ ſòàſſâſòſÿ âſåå ëåã÷å. ×òſ åùå õóæå, ſſ ſòàſſâſòſÿ ëåã÷å ÷ áſëüøåé ſſſðſſſòüſ, ÷åſ ſðåäſſſàçûâàëſſü ſàòåſàòſêſàſ. Â 1976 ãſäó Ðſ÷àðä Ãàé (Richard Guy) ſſſàë: "ß áûſ áû íåſàſ óäſâëåſ, åſſëſ áû êòſ-íſáóäü íàó÷èſſÿ ðàçëàãàòü íà ſſſæſòåëſ ſðſſçâſſëüſſûå ÷èſëà ſſðÿâſâ 10^{80} â òå÷åſſſå äàſſſſãſ ſòſſëåòſÿ" [680]. Â 1977 ãſäó Ðſſ Ðſâåſſò (Ron Rivest) çàÿâſë, ÷òſ ðàçſſæåſſſà íà ſſſæſòåëſ 125-ðàçðÿſſſãſ ÷èſëà ſſòðåáóåò 40 êâàäðſëëſſſſâ ëåò [599]. Â 1994 ãſäó áûſ ðàçſſſæåſſ íà ſſſæſòåëſ 129-ðàçðÿſſſå ÷èſſſ [66]. Åſſëſ èç ýòſãſ ſ ſæſſ ſäåëàòü êâêſå-òſ âûâſſâû, òſ òſëüſſ òſ, ÷òſ ſðåäſſêàçûâàòü ãëóſſ.

Â 4-é ſðſâåäåſûſ ðåçóëüòàòû ðàçſſæåſſſÿ íà ſſſæſòåëſ çà ſſſſëäſſþ äþæſſó ëåò. Ñàſûſ áûſòðûſ àëãſ-ðſòſſ ſ ðàçſſæåſſſÿ íà ſſſæſòåëſ ÿâëÿåſſÿ êâàäðàòſ÷ſſå ðåøåòſ (ſſ. ðàçäåë 11.3).

Ýòſ ſèſëà ſſſüſſſ ſſóãàþſ. Ñåãſäſÿ 512-áſòſâûå ſſſëà óæå ſſſſſſëüçóþſòſÿ â ſſåðàſſſſſſſûſ ſſſſòåſſàſ. Ðàçſſæåſſſå ſſ íà ſſſæſòåëſ, ſ ſſſſſàÿ êſſſſðſſſåſàſſſ, òàêſſ ſáðàçſſ, ſſſſòåſſ âſſſſſſ âſſſſåëàſſſ. ×åðâſ â Internet ſſã áû ſäåëàſòü ýòſ â òå÷åſſſå óſêåſäà.

Òàáë. 7-3.
Ðàçëîæåíèå íà ìíîæèòåëè ñ ïîìîùüþ "êâàäðàòè÷íîãî ðåøåòà"

Ãîä	×èñëî äåñÿòè÷íûõ ðàçðÿäîâ â ðàçëîæåíèè ÷èñëà	Âî ñêîëüêî ðàç ñëîæíåå ðàçëîæèòü íà ìíîæèòåëè 512-áèòîâîå ÷èñëî
1983	71	>20 ìèëëèîíîâ
1985	80	>2 ìèëëèîíîâ
1988	90	250000
1989	100	30000
1993	120	500
1994	129	100

Âû÷èñëèòåëüíàÿ ìîùü îáû÷íî èçìåðÿåòñÿ â mips-ãîäàõ: ãîäîâàÿ ðàáîòà êîìïüþòåðà, âûïîëíÿþùàãî ìèëëèîí îïåðàöèé â ñåêóíäó (one-million-instruction-per-second, mips), èëè îêîëî $3*10^{13}$ îïåðàöèé. Ïðèýòîì, ÷òî ìàøèíà ñ ïðîèçâîäèòåëüíîñòüþ 1 mips-ãîä ýêâèâàëåíòíà VAX 11/780 êîìïàíèè DEC. Òî åñòü, mips-ãîä - ýòî ãîä ðàáîòû êîìïüþòåðà VAX 11/780 èëè ýêâèâàëåíòíîãî. (100 ÌÃö Pentium - ýòî ìàøèíà â 50 mips, à Intel Paragon èç 1800 óçëîâ - ïðèìåðíî 50000 mips.)

Â 1983 ãîäó ðàçëîæåíèå íà ìíîæèòåëè 71-ðàçðÿäíîãî ÷èñëà òðåáîâàëî 0.1 mips-ãîäà, â 1994 ãîäó ðàçëîæåíèå íà ìíîæèòåëè 129-ðàçðÿäíîãî ÷èñëà ïîòðåáîâàëî 5000 mips-ëåò. Òàêîé âçëåò âû÷èñëèòåëüíîé ìîùíîñòè îáñëóæèâàë, â îñíîâíîì, âåäåíèåì ðàñïðåäåëåííûõ âû÷èñëåíèé, èñïîëüçóþùèõ âðåìÿ ïðîñòîÿ ñåòè ðàáî÷èõ ñòàíöèé. Ýòî ïîäõîä áûë ïðåäëîæåí ÁîáÑèëâåðìàíîì (Bob Silverman) è ïîëíîñòüþ ðàçðàáîòàí Àðæåíîì Ëåíñòðîé (Arjen Lenstra) è Ìàðêîì Ìàíàññîì (Mark Manasse). Â 1983 ãîäó ðàçëîæåíèå íà ìíîæèòåëè èñïîëüçîâàëî 9.5 ÷àñîâ ïðîöåññîðíîãî âðåìåíè íà åäèíñòâåííîì êîìïüþòåðå Cray X-MP, â 1994 ãîäó ðàçëîæåíèå íà ìíîæèòåëè çàíÿëî 5000 mips-ëåò è èñïîëüçîâàëî âðåìÿ ïðîñòîÿ 1600 êîìïüþòåðîâ âî âñåì ìèðå â òå÷åíèå ïðèáëèçèòåëüíî âîñüìè ìåñÿöåâ. Ñîâðåìåííûå ìåòîäû ðàçëîæåíèÿ íà ìíîæèòåëè ïîçâîëÿþò èñïîëüçîâàòü íåêîòîðûå ìåòîäû, ïðèìåíÿâøèåñÿ ê ðàñïðåäåëåííûì âû÷èñëåíèÿì.

Êàðòèíà äàëåêà ïðîãðåññèðóþùàÿ. Íîâûé àëãîðèòì ðàçëîæåíèÿ íà ìíîæèòåëè - ðåøåòî îáùåãî ïîëÿ ÷èñëè - çàìåíèë êâàäðàòè÷íîå ðåøåòî. Â 1989 ãîäó ìàòåìàòèêè ñêàçàëè áû âàì, ÷òî ðåøåòî îáùåãî ïîëÿ ÷èñëè íèêîãäà íå áóäåò èìåòü ïðàêòè÷åñêîãî çíà÷åíèÿ. Â 1992 ãîäó îíè ñîîáùèëè áû, ÷òî îíî ðåàëèçóåìî, íî äàëò âûèãðûø ïî ñðàâíåíèþ ñ êâàäðàòè÷íûì ðåøåòîì òîëüêî äëÿ ÷èñëè ñî 130-150 äåñÿòè÷íûìè ðàçðÿäàìè è áîëüøèõ. Ñåãîäíÿ èçâåñòíî, ÷òî ýòî íîâûé àëãîðèòì áûñòðåå, ÷åì êâàäðàòè÷íîå ðåøåòî, äëÿ ÷èñëè çíà÷èòåëüíî ìåíüøèõ, ÷åì 116-ðàçðÿäíûå [472, 635]. Ðåøåòî îáùåãî ïîëÿ ÷èñëè ìîæåò ðàçëîæèòü íà ìíîæèòåëè 512-áèòîâîå ÷èñëî â 10 ðàç áûñòðåå, ÷åì êâàäðàòè÷íîå ðåøåòî. Íà 1800-óçëîâîì êîìïüþòåðå Intel Paragon âû÷èñëåíèå ýòîãî àëãîðèòìà çàíÿëî áû ìåíüøå ãîäà. Â 3rd ïîêàçàíî êîëè÷åñòâî mips-ëåò, êîòîðûå òðåáóåòñÿ äëÿ ðàçëîæåíèÿ ÷èñëè ðàçëè÷íûõ ðàçìåðîâ ïðè èñïîëüçîâàíèè ñîâðåìåííûõ ðåàëèçàöèé ðåøåòà îáùåãî ïîëÿ ÷èñëè [1190].

Òàáë. 7-4.
Ðàçëîæåíèå íà ìíîæèòåëè ñ ïîìîùüþ ðåøåòà îáùåãî ïîëÿ ÷èñëè

Êîëè÷åñòâî áèò	Ñêîëüêî mips-ëåò íóæíî äëÿ ðàçëîæåíèÿ
512	30000
768	$2*10^{8}$
1024	$3*10^{11}$
1280	$1*10^{14}$
1536	$3*10^{16}$
2048	$3*10^{20}$

Êðîìå òîãî, ðåøåòî îáùåãî ïîëÿ ÷èñëè ñòàíîâèòñÿ âñå áûñòðåå è áûñòðåå. Ìàòåìàòèêè èçîáðåòàþ íîâûå òðþêè, îïòèìèçàöèè, ìåòîäû, è íåò ïðè÷èí ÷òî ýòà òåíäåíöèÿ îáîðâåòñÿ. Áëèçêèé àëãîðèòì, ðåøåòî ñïåöèàëüíîãî ïîëÿ ÷èñëè, óæå ìîæåò ðàçëàãàòü íà ìíîæèòåëè ÷èñëà îïðåäåëåííîé ñïåöèàëèçèðîâàííîé ôîðìû - îáû÷íî íå èñïîëüçóåìûå â êðèïòîãðàôèè - ãîðàçäî áûñòðåå, ÷åì ðåøåòî îáùåãî ïîëÿ ÷èñëè ìîæåò ðàçëîæèòü íà

ìíîæèòåëè ëþáûå ÷èñëà òîãî æå ðàçìåðà. Ðàçóìíî ïðåäïîëîæèòü, ÷òî ðåøàòî îáùåãî ïîëÿ ÷èñåë ìîæåò áûòü îïòèìèçèðîâàíî, ÷òîáû äîñòè÷ü òàêîé æå ñêîðîñòè [1190], âîçìîæíî, ÷òî NSA óæå çíàåò, êàê ýòî ñäåëàòü. Â 2-é ïîêàçàíî êîëè÷åñòâî mips-ëåò, òðåáóåìîå äëÿ ðàçëîæåíèÿ ÷èñåë ðàçëè÷íîé äëèíû ïðè ïîìîùè ðåøåòà ñïåöèàëüíîãî ïîëÿ ÷èñåë [1190].

Òàáë. 7-5.
Ðàçëîæåíèå íà ìíîæèòåëè ñ ïîìîùüþ ðåøåòà ñïåöèàëüíîãî ïîëÿ ÷èñåë

Êîëè÷åñòâî áèò	Ñêîëüêî mips-ëåò íóæíî äëÿ ðàçëîæåíèÿ
512	<200
768	100000
1024	$3*10^7$
1280	$3*10^9$
1536	$2*10^{11}$
2048	$4*10^{14}$

Â 1991 ãîäó ó÷àñòíèêè ñåìèíàðà Åâðîïåéñêîãî èíñòèòóòà áåçîïàñíîñòè ñèſòåì (European Institute for System Security) ñîãëàñíèëèñü, ÷òî 1024-áèòíûõ ìîäóëåé áóäåò äîſòàòî÷íî äëÿ äëèòåëüíîãî õðàíåíèÿ ñåêðåòîâ äî 2002 ãîäà [150]. Îäíàêî, îíè ïðåäóïðåæäàëè: "Õîòÿ ó÷àſòíèêè ýòîãî ſåìèíàðà ÿâëÿþſÿ ëó÷øèìè ſïåöèàëèſòàìè â ſîſòâåſſòâóþſùèõ îáëàſſòÿõ, ýòî çàÿâëåíèå (ſî ſîâîäó ſðîêà áåçîſàſſíſſòè) äîëæíî áûſü âſſſïðèſſÿòî ſ îſſòîðîæſſíſſòüþ." Ýòî õîðîſøèé ſſâåò.

Óſſíûé êðèſòîãðàô ſâåðõêſſíåðâàòèâåſ ſſðè âûáîðå äëèſ îòêðûſõ êëþ÷åé. ×òîáû ſſſÿòü, íàſêſſëüêſ äëèſſíûé êëþ÷ âàſ íóæåſ, âàſ ſſðèäåòſÿ ſöåſèòü íóæíóþ áåçſſïàſſíſſòü è âðåſÿ æèçſſ êëþ÷à, íå çàáûâàÿ ſ òåêóſſåſ ſſſòîſÿſſèſ èſêóſſòâà ðàçëåãàòü íà ſſſæèòåëè. ×òſáû ſſëó÷èſü òſò æå óðſâåſſíü áåçſſïàſſſſſòè, êſòſðûſ äàâàëſ 512-áèòſâſå ſ÷èſſ â íà÷àëå âſſüſèååſÿòûſõ, ñåſſäſſÿ âàſ ſſſíàäſáèſÿ 1024-áèòſâſå ſ÷èſſ. Åſëè æå âû õſòèòå, ſ÷òſáû âàøè êëþ÷è ſſòàâàëèſü áåçſſïàſſſûſè á áëèæàéøèå 20 ëåò, 1024-áèòſâſå ſ÷èſſ, ſſ âèäſſſſó, ſſëſøêſſ êſðſòêſ.

Äàæå åſëè âàøè êſſíêðåòſûå ſåſêðåòſ íå ſòſÿò óſſëèſé, íóæſſûſ äëÿ ðàçëſſæåſſíÿ âàøåſſî ſſäóëÿ, âû ſſæåòå ſêàçàòüſÿ â ſ ſïàſſſſòè. Ïðåäſſòàſüòå ſåáå àâòſſàòè÷åſêóſ áàſêſâſêóſ ſèſòåſſó, èſſſſëüçóſ ùóſ äëÿ áåçſſïàſſſſòè RSA. Ìſýëſðè ſſæåò ſſðåäſſòàòü ſåðäſſ ſóäſſ è çàÿâèòü: "×èòàëè ëè âû â ãàçåòå çà 1994 ãîä, ÷òſ RSA-129 áûſ âçſſſàſ, è ÷òſ 512-áèòſâſå ſ÷èſſ ſſâóò áûòü ðàçſſæåſſû íà ſſſæèòåëè ſſðâſſíèçàöèåſ, êſòſðàÿ ſſæåò ſſòðàòèòü íåſêſſëüſſſ ſèëëſſſſâ äſëëàðſâ è ſſäſæäàòü íåſêſſëüſſ ſåſÿöåſ? Ìſſ áàſê èſſſſëüçóåò äëÿ áåçſſïàſſſſòè 512-áèòſâſå ſ÷èſſ è, ſåæäó ſðſ÷èſ, ýòè ſåſü èçúÿòèſ ſſäëàſû íå ſſſé." Äàæå åſëè Ìſýëſðè ëæò, ſóäüÿ, âåðſÿòſſ, ſſæåò ſſòðåſſâàòü, ÷òſáû áàſê ýòſ äſêàçë.

Ïſ÷åſó íå èſſſëüçſâàòü 10000-áèòſâſå êëþ÷è? Êſſíå÷ſſ, ſſæſſ, ſſ ÷åſ äëèſſíåå âàøè êëþ÷è, òåſ áſëüøå ſòſèſſſòü âſ÷èſëſèé. Âàſ íóæåſ êëþ÷, êſòſðſûé áſë áſ äſſòàòſ÷ſſ äëèſſſû äëÿ ſáåſïå÷åſèÿ áåçſſïàſſſſòè, ſſ äſſòàòſ÷ſſ êſðſòêſ, ÷òſáſ åſſſ ſſæſſ áſëſ èſſſſëüçſâàòü.

Ðàſåå â ýòſ ðàçäåëå ÿ íàçſâàæ ïðåäſêàçàſèÿ ãëóſſſòüþ. Òåſåðü ÿ ñàſ ſſſſûòàþſü ſðåäſêſâſ÷åſêſêſ óſëëèé è íåýòè÷ſûſ äåéſòâèé. Òſ åſòü, ſſ *íå ſſſáèðàåſſ* âſûſóſêàòü â Internet "÷åðåÿ" èëè ðàçðàáàòſâàòü âèðóſ, êſòſðſûé áſ ſðåäſſſòàäſëë áſ íàſ ſſ÷èſëëèòåëſûå ðåſóðſſ. Âſ ſſſâèſ ſðåàſíèçàöèÿſ ſſſâèſ òſſſÿ÷è ſàøèſ ſſâëêþ÷åſû ê ſåòè. Äſſòóſ ê èſ âſçſſæſíſòÿſ ſſ-òðåáóåò èſêóſſſſé äèſſëſſàòèè, íſ íå ÿâëÿåòſÿ íåâſçſſſæſû. Ïðèſÿâ ſðåäſþ ſðſſèçâſâèòåëüſſòüſ ſàøèſû ðàâſſé 5 mips è âðåſÿ ðàáſòſ 1 ãſä, âſſëſíå âſçſſſæſſ ſſóůåſòåòü ſſðåêò, êſòſðſûé òðåáóåò ſſëſ èëëèſſíà mips-ëåò.

Ïðſåêò ðàçëſæåſèÿ íà ſſſæèòåëè 129-ðàçðÿäſſãſ ÷èſèà áåç çíà÷èòåëüſûõ óſèëëé ſſſã çàäåéſòâſâàòü 0.03 ſðſöåſòà ſòåſſ÷ſſé ſſëſſé âû÷èſëèòåëüſſé ſſûſſſòè Internet [1190]. Ðàçóſſ ſðåäſſſêæèòü, ÷òſ õſðſøſ ðàçðåëèſèðſâſſſûé ſðſåêò ſſëó÷èò íà ãîä 2 ſðſöåſòà âñåſèðſſé âû÷èſèòåëüſſé ſſûſſòè.

Ïðåäſſëæè, ÷òſ óâëå÷åſſûé êðèſòſàſàèòèſ ſſſæåò ſſëó÷èòü â ſâſå ðàſſïðÿæåſèå 10000 mips-ëåò, áſëüøàÿ êſðſſðàòèÿ - 10^7 mips-ëåò, à ſðàâèòåëüſòſâ áſëüøſé ſòðàſû - 10^9 mips-ëåò. Ïðåäſſſêæè òàêæå, ÷òſ âû÷èſëèòåëüſàÿ ſſûü áóäåò âſçðàſòàòü íà ſſðÿſſê êàæäûå ſÿòü ëåò. È , íàêſſíåö, ſðåäſſſëſæè òàêæå, ÷òſ óſ-

ïåõè â ìàòåìàòèêå ðàçëîæåíèÿ íà ìíîæèòåëè ïîçâîëÿò íàì ðàñêëàäûâàòü ëþáûå ÷èñëà ñî ñêîðîñòüþ, ñðàâíèìîé ñ òî, êîòîðóþ îáû÷íàÿ ïðîöåäóðà ïðîáíîãî äåëåíèÿ. (Ýòî ïîêà íåâîçìîæíî, íî ïðîâîäèòñÿ â ëþáîé ìîìåíò.) 1st ðåêîìåíäóåò äëÿ ðàçëè÷íûõ ëåò èñïîëüçîâàòü ñ öåëüþ îáåñïå÷åíèÿ áåçîïàñíîñòè ðàçëè÷íûå äëèíû êëþ÷åé.

Òàáë. 7-6.
Ðåêîìåíäîâàííûå äëèíû îêðóãëåíèé êëþ÷åé â (áèòàõ)

Ãîä	×àñòíûå ëèöî	Êîðïîðàöèÿ	Ïðàâèòåëüñòâî
1995	768	1280	1536
2000	1024	1280	1536
2005	1280	1536	2048
2010	1280	1536	2048
2015	1536	2048	2048

Íå çàáûâàéòå ó÷èòûâàòü çíà÷èìîñòü êëþ÷à. Îòêðûòûå êëþ÷è ÷àñòî èñïîëüçóþòñÿ äëÿ äëèòåëüíîé îáåñïå÷åíèÿ áåçîïàñíîñòè âàæíîé èíôîðìàöèè: ãëàâíûé êëþ÷ áàíêà äëÿ ñèñòåìû ýëåêòðîííûõ íàëè÷íûõ, êëþ÷, èñïîëüçóåìûé ïðàâèòåëüñòâîì äëÿ ïîäòâåðæäåíèÿ ïàñïîðòîâ, êëþ÷ öèôðîâîé ïîäïèñè ãîñóäàðñòâåííîãî íîòàðèóñà. Âîçìîæíî, íå ñòîèò òðàòèòü ìåñÿöû ìàøèííîãî âðåìåíè íà âñêðûòèå êàêîãî-òî ëè÷íîãî êëþ÷à, íî åñëè ìîæåòå ñ ïîìîùüþ äîáðîãî êëþ÷à íàïå÷àòàòü ñîáñòâåííûå äåíüãè, òî èäèì ñòàíîâèòñÿ âåñüìà çàõâàòûâàþùåé. Äëèíà 1024-áèòîâîãî êëþ÷à äîñòàòî÷íà äëÿ ïîäïèñè ÷åãî-íèáóäü, ÷òî áóäåò ïðîâåðåíî â òå÷åíèå íåäåëè, ìåñÿöà, äàæå íåñêîëüêèõ ëåò. Í î âû æå íå õîòèòå, ïðåäñòàâ ïåðåä ñóäîì ëåò 20 ñïóñòÿ ñ ïîäïèñàííûì ýëåêòðîííûì îáðàçîì äîêóìåíòì, ñìîðåòü, êàê ïðîòèâîïîêàçûâàþò ñòîðîíà ïîêàçûâàþò, êàê ïîääåëàòü äîêóìåíòû, èñïîëüçóÿ ýòó æå ïîäïèñü.

Ïðåäñêàçûâàòü áîëåå äàëåêîå áóäóùåå åùå ãëóïåå. Êòî ìîæåò çíàòü, êàêèõ óñïåõîâ ê 2020 ãîäó äîñòèãíåò âû÷èñëèòåëüíàÿ òåõíèêà, ñåòåâûå âû÷èñëåíèÿ è ìàòåìàòèêà? Îäíàêî, åñëè îêëóòü âçãëÿäîì âñþ êàðòèíó, ìîæíî çàìåòèòü, ÷òî â êàæäîì ñëåäóþùåì äåñÿòèëåòèè ìû ïîëó÷åì âîçìîæíîñòü ðàçäàâàòü íà ìíîæèòåëè âäâîå áîëåå äëèííûå ÷èñëà, ÷åì â ïðåäûäóùåì. Ýòî ïîçâîëÿò ïîñòðîèòü 0-é.

Ñ äðóãîé ñòîðîíû, òåõíèêà ðàçëîæåíèÿ íà ìíîæèòåëè ìîæò äîñòè÷ ïðåäåëà ñâîèõ âîçìîæíîñòåé çàäîëãî äî 2045. Õîòÿ ÿ äóìàþ, ÷òî ýòî ìàëîâåðîÿòíî.

Íå âñå ñîãëàñíûñ ñ ìîìè ðåêîìåíäàöèÿìè. NSA óñòàíîâèëî äëÿ ñâîåé Ñòàíäàðòà öèôðîâîé ïîäïèñè (Digital Signature Standard, ñì. ðàçäåë 20.1) äëèíó êëþ÷åé îò 512 äî 1024 áèò - íàìíîãî ìåíüøå, ÷åì ÿ ðåêîìåíäóþ äëÿ äëèòåëüíîé áåçîïàñíîñòè. Ó Pretty Good Privacy ("Âïîëíå íàäåæíûé ñåðâèñ", ñì. ðàçäåë 24.12) ìàêñèìàëüíàÿ äëèíà êëþ÷à RSA ñîñòàâëÿåò 2047 áèò. Àðæàí Ëåíñòðà, ëó÷øèé â ìèðå ðàñêëàäûâàòåëü íà ìíîæèòåëè, â òå÷åíèå ïîñëåäíèõ 10 ëåò îôèöèàëüíî äåëàòü ïðåäñêàçàíèÿ [949]. Â -1-é ïðèâåäåíû ðåêîìåíäàöèè Ðîíà Ðèâåñòà äëÿ äëèíû êëþ÷åé, êîòîðûå ñäåëàíû â 1990 ãîäó è êàæóòñÿ ìíå ñëèøêîì îïòèìèñòè÷íûìè [1323]. Õîòÿ åãî àíàëèç íà áóìàãå âûãëÿäèò õîðîøî, â íåäàâíåé èñòîðèè ìíîãî íàéòè ïðèìåðû ðåãóëÿðíî ïðîìàõèâàþùèõ ñþðïðèçîâ. ×òîáû ïðåäîõðàíèòü ñåáÿ îò ïîñëåäñòâèÿ ýòèõ ñþðïðèçîâ, åñòü ñì ûñë âûáèðàòü êëþ÷è ñ çàïàñîì.

Òàáë. 7-7.
Äîëãîñðî÷íûé ïðîãíîç ðàçëîæåíèÿ íà ìíîæèòåëè

Ãîä	Äëèíà êëþ÷à (â áèòàõ)
1995	1024
2005	2048
2015	4096
2025	8192
2035	16384
2045	32768

Ìèíèìàëüíûå îöåíêè ïðåäïîëàãàþò áþäæåò $25000, àëãîðèòì "êâàäðàòè÷íîå ðåøåòî " è ñêîðîñòü òåõíè÷åñêîãî ïðîãðåññà 20 ïðîöåíòîâ â ãîä. Ñðåäíåå îöåíêè ïðåäïîëàãàþò áþäæåò 25 ìèëëèîíîâ äîëëàðîâ, àëãîðèòì "ðåøåòî íàùåãî ïîëÿ ÷èñëå" è ñêîðîñòü òåõíè÷åñêîãî ïðîãðåññà 33 ïðîöåíòà â ãîä. Ìàêñèìàëüíûå îöåíêè ïðåäïîëàãàþò áþäæåò 25 ìèëëèàðäîâ äîëëàðîâ, àëãîðèòì "ðåøåòî íàùåãî ïîëÿ ÷èñëå", ðàíòàþùèé ñî ñêîðîñòüþ

ðåøåòà ñïåöèàëüíîãî ïîëÿ ÷èñëè è ñêîðîñòü òåõíè÷åñêîãî ïðîãðåññà 45 ïðîöåíòîâ â ãîä.

Âñåãäà åñòü âåðîÿòíîñòü òîãî, ÷òî óñïåõè â ðàçëè÷íûõ íàïðàâëåíèÿõ áóäóò ïîðàçèòåëüíû è äëÿ ìåíÿ, íî ÿ ïîïûòàëñÿ ó÷åñòü ýòîò ìíîæèòåëü â ñâîèõ ïðîãíîçàõ. Íî ïî÷åìó ìíå íóæíî âåðèòü? ß ëèøü ïðîäåìîíñòðèðîâàë ñîáñòâåííóþ ãëóïîñòü, çàíèìàÿñü ïðåäñêàçàíèÿìè.

Òàáë. 7-8.
Îïòèìèñòè÷íûå ðåêîìåíäàöèè Ðèâåñòà äëÿ äëèíû êëþ÷åé (â áèòàõ)

Ãîä	Ìèíèìàëüíàÿ	Ñðåäíÿÿ	Ìàêñèìàëüíàÿ
1990	398	515	1289
1995	405	542	1399
2000	422	572	1512
2005	439	602	1628
2010	455	631	1754
2015	472	661	1884
2020	489	677	2017

Âû÷èñëåíèå ñ ïîìîùüþ ÄÍÊ

Ýòî ïîõîæå íà âîëøåáñòâî. Â 1994 ãîäó Ëåîíàðä Ýäëàí (Leonard M. Adleman) ïðîäåìîíñòðèðîâàë ìåòîä ðåøåíèÿ çàäà÷è **NP-ïîëíîòû** (ñì. ðàçäåë 11.2) â áèõèìè÷åñêîé ëàáîðàòîðèè, èñïîëüçóÿ ìîëåêóëû ÄÍÊ äëÿ ïðåäñòàâëåíèÿ âîçìîæíûõ ðåøåíèé çàäà÷è [17]. Çàäà÷à, ðåøåíèþ Ýäëàíà, áûëà ÷ðåçâû÷àéíî ñëó÷àéíà ïîñòàíîâêà ìîëåêóëÿðíûõ ãàìèëüòîíîâ ïóòè: äàíà êàðòà ãîðîäîâ, ñîåäèíåíû îäíîíàïðàâëåííûìè äîðîãàìè, íóæíî íàéòè ïóòü èç ãîðîäà A â ãîðîä Z, êîòîðûé ïðîõîäèò ÷åðåç êàæäûé ãîðîä íà êàðòå òî÷íî îäèí ðàç. Êàæäûé ãîðîä áûë ïðåäñòàâëåí ñâîåé ñëó÷àéíîé öåïî÷êîé ÄÍÊ ñ 20 îñíîâàíèÿìè. Ñ ïîìîùüþ îâû÷íûõ ìåòîäîâ ìîëåêóëÿðíîé áèîëîãèè Ýäëàí ñèíòåçèðîâàë 50 ïèêîìîëåé (30 ìèëëèîíîâ ìèëëèîíîâ ìîëåêóë) öåïî÷êè ÄÍÊ, ïðåäñòàâëÿþùèå êàæäûé âîðîä. Êàæäàÿ äîðîãà áûëà ïðåäñòàâëåíà öåïî÷êîé ÄÍÊ ñ 20 îñíîâàíèÿìè, íî ýòè öåïî÷êè âûáèðàëèñü íå ñëó÷àéíûì îáðàçîì: îíè óìåëî âûáèðàëèñü òàê, ÷òîáû "íà÷àëî" öåïî÷êè ÄÍÊ, ïðåäñòàâëÿþùåé äîðîãó îò ãîðîäà P ê ãîðîäó K ("Äîðîãà PK") ñòðåìèëàñü áû ñîåäèíèòüñÿ ñî öåïî÷êîé ÄÍÊ, ïðåäñòàâëÿþùåé ãîðîä P, à êîíåö Äîðîãè PK ñòðåìèëñÿ âû ñîåäèíèòüñÿ ñ ãîðîäîì K.

Ýäëàí ñèíòåçèðîâàë 50 ïèêîìîëåé ÄÍÊ, ïðåäñòàâëÿþùèõ êàæäóþ äîðîãó, ñìåøàë èõ âìåñòå ñ ÄÍÊ ãîðîäà ì, ïðåäñòàâëÿþùåé ãîðîäà, è äîáàâèë ôåðìåíò ëèãàçó, êîòîðàÿ ñâÿçûâàåò âìåñòå êîíöû ìîëåêóë ÄÍÊ. Ïðàâèëüíî ïîäîáðàííàÿ ñâÿçü ìåæäó öåïî÷êàìè ÄÍÊ äëÿ äîðîã è öåïî÷êàìè ÄÍÊ äëÿ ãîðîä äîëæíà ïðèâîäèòü ê òîìó, ÷òî ëèãàçà ñîåäèíÿåò öåïî÷êè ÄÍÊ äëÿ äîðîã âìåñòå ïðàâèëüíûì îáðàçîì. Òî åñòü, "Âûõîä" äîðîãè PK âñåãäà áóäåò ñîåäèíåí ñî "âõîäîì" êàêîé-ëèáî äîðîãè, íà÷èíàþùåéñÿ â ãîðîäå K, íî íèêîãäà ñ "âûõîäîì" ëþáîé äîðîãè èëè ñî "âõîäîì" äîðîãè, êîòîðàÿ íà÷èíàåòñÿ â ãîðîäå K. Ï îñëå òùàòåëüíî îðãàíèçîâàííîé ðåàêöèè ëèãàçà ñîçäàëà áîëüøîå êîëè÷åñòâî öåïî÷åê ÄÍÊ, ïðåäñòàâëÿþùèõ âîçìîæíûå, íî âñå ðàâíî ñëó÷àéíûå îáúåäèíåíèÿ ïóòåé êàðòû.

Â ýòî ñóïå èç ñëó÷àéíûõ ïóòåé Ýäëàí ìîæåò íàéòè ìàëåíüêèé ñëåä - ìîæåò áûòü åäèíñòâåííîé ìîëåêóëû - ÄÍÊ, êîòîðàÿ ÿâëÿåòñÿ îòâåòîì çàäà÷è. Èñïîëüçóÿ îáû÷íûå ìåòîäû ìîëåêóëÿðíîé áèîëîãèè, îí óäàëèë âñå öåïî÷êè ÄÍÊ, ïðåäñòàâëÿâøèå ñëèøêîì êîðîòêèå èëè ñëèøêîì äëèííûå ïóòè. (×èñëî äîðîã â íóæíîì ïóòè äîëæíî ðàâíÿòüñÿ ÷èñëó äîðîãîâ ìèíóñ îäèí.) Çàòåì îí óäàëèë âñå öåïî÷êè ÄÍÊ, êîòîðûå íå ïðîõîäèëè ÷åðåç ãîðîä A, çàòåì òå, êîòîðûå øëè ìèìî ãîðîäà B, è òàê äàëåå. Ì îëåêóëà ÄÍÊ, ïðîøåäøàÿ ÷åðåç ýòî ñèòî, è ïðåäñòàâëÿëà ñîáîé íóæíóþ ïîñëåäîâàòåëüíîñòü äîðîã, ÿâëÿÿñü ðåøåíèåì çàäà÷è íàïðàâëåííîãî ãàìèëüòîíîâà ïóòè.

Ï î ïðåäåëåíèþ ÷ñòíóé ñëó÷àé çàäà÷è **NP-ïîëíîòû** ìîæåò áûòü ïðåâðàùîâàí çà ïîëèíîìèàëüíîå âðåìÿ ê ÷àñòíîìó ñëó÷àþ ëþáîé äðóãîé çàäà÷è **NP-ïîëíîòû**, è, ñëåäîâàòåëüíî, ê çàäà÷å î íàïðàâëåííîì ãàìèëüòîíîâîì ïóòè. Ñ ñàìèäåñÿòûõ ãîäîâ êðèòîëîãè ïûòàëèñü èñïîëüçîâàòü çàäà÷è **NP-ïîëíîòû** äëÿ êðèòîãðàôèè ñ îòêðûòûì êîä÷àì.

Õîòÿ ÷ñòíóé ñëó÷àé, ðåøåííûé Ýäëàíîì, âåñüìà ïðîñò (ñåìü ãîðîäîâ íà êàðòå, ïðîñòûì íàáëþäåíèåì çàäà÷à ìîæåò ðåøåíà çà íåñêîëüêî ìèíóò), ýòî íàïðàâëåíèå òîëüêî íà÷àëî ðàçâèâàòüñÿ, è íå ñóùåñòâóåò íèêàêèõ ïðåïÿòñòâèé äëÿ ðàñøèðåíèÿ äàííîé ìåòîäèêè íà áîëåå ñëîæíûå çàäà÷è. Òàêèì îáðàçîì, ðàññóæäåíèÿ î áåçîïàñíîñòè êðèïòîãðàôè÷åñêèõ ïðîòîêîëîâ, îñíîâàííûõ íà çàäà÷àõ **NP-ïîëíîòû**, ðàññóæäåíèÿ, êîòîðûå äî ñèõ ïîð íà÷èíàëèñü ñëîâàìè, "Ïðåäïîëîæèì, ÷òî ó âðàãà åñòü ìèëëèîí ïðîöåññîðîâ, êàæäûé èç êîòîðûõ âû÷èñëÿåò ìèëëèîí ïðîâåðîê êàæäóþ ñåêóíäó", ñêîðî, ìîæåò áûòü, áóäóò íà÷èíàòüñÿ ñëîâàìè, "Ïðåäïîëîæèì, ó âðàãà åñòü òûñÿ÷à ôåðìåíòíûõ âàíí, åìêîñòüþ ïî 20000 ëèòðîâ êàæäàÿ".

Êâàíòîâûå âû÷èñëåíèÿ

À òåïåðü åùå áîëüøàÿ ôàíòàñòèêà. Â îñíîâå êâàíòîâûõ âû÷èñëåíèé èñïîëüçóåòñÿ äâîéñòâåííàÿ ïðèðîäà ìàòåðèè (è âîëíà, è ÷àñòèöà). Ôîòîí ìîæåò îäíîâðåìåííî íàõîäèòüñÿ â áîëüøîì êîëè÷åñòâå ñîñòîÿíèé. Êëàññè÷åñêèì ïðèìåðîì ÿâëÿåòñÿ òî, ÷òî ôîòîí âåäåò ñåáÿ êàê âîëíà, âñòðå÷àÿ ÷àñòè÷íî ïðîçðà÷íîå çåðêàëî. Îí îäíîâðåìåííî è îòðàæàåòñÿ è ïðîõîäèò ÷åðåç çåðêàëî ïîäîáíî òîìó, êàê ìîðñêàÿ âîëíà, óäàðÿÿñü î âîëíîëîì ñ íåáîëüøèì îòâåðñòèåì â íåì, îäíîâðåìåííî îòðàçèòñÿ îò ñòåíû è ïðîéäåò ñêâîçü íåå. Îäíàêî, ïðè èçìåðåíèè ôîòîí âåäåò ñåáÿ ïîäîáíî ÷àñòèöå, è òîëüêî îäíî ñîñòîÿíèå ìîæåò áûòü îáíàðóæåíî.

Â [1443] Ïèòåð Øîð (Peter Shor) î÷åðòèë ïðèíöèïû ïîñòðîåíèÿ ìàøèíû äëÿ ðàçëîæåíèÿ íà ìíîæèòåëè, îñíîâàííîé íà çàêîíàõ êâàíòîâîé ìåõàíèêè. Â îòëè÷èå îò îáû÷íîãî êîìïüþòåðà, êîòîðûé ìîæíî ïðåäñòàâèòü êàê ìàøèíó, èìåþùàÿ â êàæäûé ìîìåíò âðåìåíè åäèíñòâåííîå ôèêñèðîâàííîå ñîñòîÿíèå, êâàíòîâûé êîìïüþòåð îáëàäàåò âíóòðåííåé âîëíîâîé ôóíêöèåé, ÿâëÿþùåéñÿ ñóïåðïîçèöèåé êîìáèíàöèé âîçìîæíûõ îñíîâíûõ ñîñòîÿíèé. Âû÷èñëåíèÿ ïðåîáðàçóþò âîëíîâóþ ôóíêöèþ, ìåíÿÿ âåñü íàáîð ñîñòîÿíèé åäèíûì äåéñòâèåì. Òàêèì îáðàçîì, êâàíòîâûé êîìïüþòåð èìååò ïðåèìóùåñòâî íàä êëàññè÷åñêèì êîíå÷íûì àâòîìàòîì: îí èñïîëüçóåò êâàíòîâûå ñâîéñòâà äëÿ ÷èñëà ðàçëîæåíèÿ íà ìíîæèòåëè çà ïîëèíîìèàëüíîå âðåìÿ, òåîðåòè÷åñêè ïîçâîëÿÿ âçëîìàòü êðèïòîñèñòåìû, îñíîâàííûå íà ðàçëîæåíèè íà ìíîæèòåëè èëè çàäà÷å äèñêðåòíîãî ëîãàðèôìà.

Îáùåïðèçíàííî, ÷òî êâàíòîâûé êîìïüþòåð íå ïðîòèâîðå÷èò ôóíäàìåíòàëüíûì çàêîíàì êâàíòîâîé ìåõàíèêè. Îäíàêî, íåïîõîæå, ÷òî êâàíòîâàÿ ìàøèíà äëÿ ðàçëîæåíèÿ íà ìíîæèòåëè áóäåò ïîñòðîåíà â îáîçðèìîì áóäóùåì ... åñëè âîîáùå áóäåò ïîñòðîåíà. Îäíèì èç ãëàâíûõ ïðåïÿòñòâèé ÿâëÿåòñÿ ïðîáëåìà íåêîãåðåíòíîñòè, êîòîðàÿ ÿâëÿåòñÿ ïðè÷èíîé ïîòåðè îò÷åòëèâîñòè âîëíîâûìè îãèáàþùèìè è ïðèâîäèò ê ñáîþ êîìïüþòåðà. Èç-çà íåêîãåðåíòíîñòè êâàíòîâûé êîìïüþòåð, ðàáîòàþùèé ïðè 1Ê, áóäåò ñáèâàòüñÿ êàæäóþ íàíîñåêóíäó. Êðîìå òîãî, äëÿ ïîñòðîåíèÿ êâàíòîâîãî óñòðîéñòâà äëÿ ðàçëîæåíèÿ íà ìíîæèòåëè ïîòðåáóåòñÿ îãðîìíîå êîëè÷åñòâî âåíòèëåé, à ýòî ìîæåò íå äàòü ïîñòðîèòü ìàøèíó. Äëÿ ïðîåêòà Øîðà íóæíî ñîâåðøåííîå óñòðîéñòâî äëÿ âîçâåäåíèÿ â ñòåïåíü. Âíóòðåííèå ÷àñû íå èñïîëüçóþòñÿ, ïîýòîìó äëÿ ðàçëîæåíèÿ íà ìíîæèòåëè êðèïòîãðàôè÷åñêè çíà÷èìûõ ÷èñåë ìîãóò ïîòðåáîâàòüñÿ ìèëëèîíû èëè, âîçìîæíî, ìèëëèàðäû èíäèâèäóàëüíûõ âåíòèëåé. Åñëè ìèíèìàëüíàÿ âåðîÿòíîñòü îòêàçà êàæäîãî èç n êâàíòîâûõ âåíòèëåé ðàâíà p, òî ñðåäíåå êîëè÷åñòâî èñïûòàíèé, íåîáõîäèìîå äëÿ äîñòèæåíèÿ óñïåõà, ñîñòàâèò $(1/(1-p))^n$. ×èñëî íóæíûõ âåíòèëåé, ïî âèäèìîìó, ðàñòåò ïîëèíîìèàëüíî ñ ðîñòîì äëèíû ÷èñëà (â áèòàõ), ïîýòîìó ÷èñëî òðåáóåìûõ ïîïûòîê áóäåò ðàñòè ñ óâåëè÷åíèåì äëèíû èñïîëüçóåìûõ ÷èñåë ñâåðõýêñïîíåíöèàëüíî - õóæå ÷åì ïðè ðàçëîæåíèè äåëåíèåì!

Ïîýòîìó, õîòÿ êâàíòîâîå ðàçëîæåíèå íà ìíîæèòåëè âûçûâàåò âîñõèùåíèå â àêàäåìè÷åñêèõ êðóãàõ, ìàëîâåðîÿòíî, ÷òî îíî áóäåò èìåòü ïðàêòè÷åñêîå çíà÷åíèå â îáîçðèìîì áóäóùåì. Íî íå ãîâîðèòå ïîòîì, ÷òî ÿ âàñ íå ïðåäóïðåæäàë.

7.3 Ñðàâíåíèå äëèí ñèììåòðè÷íûõ è îòêðûòûõ êëþ÷åé

Ñèñòåìà âçëàìûâàåòñÿ îáû÷íî â åå ñëàáåéøåì ìåñòå. Åñëè âû ïðîåêòèðóåòå ñèñòåìó, êîòîðàÿ èñïîëüçóåò è ñèììåòðè÷íóþ êðèïòîãðàôèþ, è êðèïòîãðàôèþ ñ îòêðûòûìè êëþ÷àìè, òî äëèíû êëþ÷åé äëÿ êðèïòîãðàôèè êàæäîãî òèïà äîëæíû âûáèðàòüñÿ òàê, ÷òîáû âñêðûòü ëþáîé èç êîìïîíåíòîâ ñèñòåìû áûëî îäèíàêîâî òðóäíî. Áåññìûñëåííî èñïîëüçîâàòü ñèììåòðè÷íûé àëãîðèòì ñî 128-áèòîâûì êëþ÷îì âìåñòå ñ àëãîðèòìîì ñ îòêðûòûìè êëþ÷àìè, èñïîëüçóþùèì 386-áèòîâûé êëþ÷. Òî÷íî òàê æå áåññìûñëåííî èñïîëüçîâàòü â îäíîé ñèñòåìå ñèììåòðè÷íûé àëãîðèòì ñ 56-áèòîâûì êëþ÷îì è àëãîðèòì ñ îòêðûòûìè êëþ÷àìè, ïðèìåíÿþùèé 1024-áèòîâûé êëþ÷.

Â -2-é ïåðå÷èñëåíû äëèíû ìîäóëåé îòêðûòûõ êëþ÷åé, òðóäíîñòü ðàçëîæåíèÿ êîòîðûõ íà ìíîæèòåëè ñðàâíèìà ñî ñëîæíîñòüþ âñêðûòèÿ ãðóáîé ñèëîé ñîïîñòàâëåííûõ äëèí ïîïóëÿðíûõ ñèììåòðè÷íûõ êëþ÷åé.

Òàáë. 7-9.
Äëèíû ñèììåòðè÷íûõ è îòêðûòûõ êëþ÷åé ñ àíàëîãè÷íîé óñòîé÷èâîñòüþ ê âñêðûòèþ ãðóáîé ñèëîé

Äëèíà ñèììåòðè÷íîãî êëþ÷à (â áèòàõ)	Äëèíà îòêðûòîãî êëþ÷à (â áèòàõ)
56	384
64	512
80	768
112	1792
128	2304

Èç ýòîé òàáëèöà ìîæíî ñäåëàòü âûâîä, ÷òî åñëè âû äîñòàòî÷íî áåñïîêîèòåñü î ñâîåé áåçîïàñíîñòè, ÷òîáû âûáðàòü ñèììåòðè÷íûé àëãîðèòì ñî 112-áèòîâûì êëþ÷îì, âàì ñëåäóåò âûáðàòü äëèíó ìîäóëÿ â âàøåì àëãîðèòìå ñ îòêðûòûìè êëþ÷àìè ïîðÿäêà 1792 áèò. Îäíàêî, â îáùåì ñëó÷àå ñëåäóåò âûáèðàòü äëèíó îòêðûòîãî êëþ÷à áîëåå áåçîïàñíóþ, ÷åì äëèíà âàøåãî ñèììåòðè÷íîãî êëþ÷à. Îòêðûòûå êëþ÷è îáû÷íî èñïîëüçóþòñÿ äîëüøå è ïðèìåíÿþòñÿ äëÿ çàùèòû áîëüøåãî êîëè÷åñòâà èíôîðìàöèè.

7.4 Âñêðûòèå â äåíü ðîæäåíèÿ ïðîòèâ îäíîíàïðàâëåííûõ õýø-ôóíêöèé

Ñóùåñòâóåò äâà ñïîñîáà âñêðûòèÿ îäíîíàïðàâëåííûõ õýø-ôóíêöèé ãðóáîé ñèëîé. Ïåðâûé íàèáîëåå î÷åâèäåí: äàíî çíà÷åíèå õýø-ôóíêöèè ñîîáùåíèÿ, *Í(M),* âðàãó õîòåëîñü áû ñóìåòü ñîçäàòü äðóãîé äîêóìåíò, *Ì '*, òàêîé, ÷òî *Í(M')=Í(M).* Âòîðîé ñïîñîá áîëåå òîíîê: âðàãó õîòåëîñü áû íàéòè äâà ñëó÷àéíûõ ñîîáùåíèÿ, *M* è *Ì '*, òàêèõ, ÷òî *Í(M')=Í(M).* Òàêîé ñïîñîá íàçûâàåòñÿ **ñòîëêíîâåíèåì** è ÿâëÿåòñÿ áîëåå ïðîñòûì, ÷åì ïåðâûé, ñïîñîáîì âñêðûòèÿ.

Ïàðàäîêñ äíÿ ðîæäåíèÿ ÿâëÿåòñÿ ñòàíäàðòíîé ñòàòèñòè÷åñêîé ïðîáëåìîé. Ñêîëüêî ÷åëîâåê äîëæíî ñîáðàòüñÿ â îäíîé êîìíàòå, ÷òîáû ñ âåðîÿòíîñòüþ 1/2 õîòÿ áû ó êîãî-íèáóäü èç íèõ áûë áû îáùèé ñ âàìè äåíü ðîæäåíèÿ? Îòâåò - 183. Õîðîøî, à ñêîëüêî ëþäåé äîëæíî ñîáðàòüñÿ, ÷òîáû ñ âåðîÿòíîñòüþ 1/2 õîòÿ áû ó äâîèõ èç íèõ áûë áû îáùèé äåíü ðîæäåíèÿ? Îòâåò óäèâèòåëåí - 23. 23 ÷åëîâåêà, íàõîäÿùèõñÿ â êîìíàòå, îáðàçóþò 253 ðàçëè÷íûõ *ïàðû*.

Íàéòè êîãî-íèáóäü ñ òåì æå äíåì ðîæäåíèÿ - àíàëîãèÿ ñ ïåðâûì ñïîñîáîì âñêðûòèÿ, íàéòè äâóõ ÷åëîâåê ñ ïðîèçâîëüíûì îäèíàêîâûì äíåì ðîæäåíèÿ - àíàëîãèÿ ñî âòîðûì ñïîñîáîì. Âòîðîé ñïîñîá øèðîêî èçâåñòåí êàê **âñêðûòèå â äåíü ðîæäåíèÿ**.

Ïðåäïîëîæèì, ÷òî îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ áåçîïàñíà, è ëó÷øèì ñïîñîáîì åå âñêðûòèÿ ÿâëÿåòñÿ âñêðûòèå ãðóáîé ñèëîé. Ðåçóëüòàòîì ôóíêöèè ÿâëÿåòñÿ *m*-áèòîâîå ÷èñëî. Ïîèñê ñîîáùåíèÿ, õýø-çíà÷åíèå êîòîðîãî ñîâïàäàåò ñ çàäàííûì, â ñðåäíåì ïîòðåáîâàë áû õýøèðîâàíèÿ 2^m ñëó÷àéíûõ ñîîáùåíèé. À äëÿ îáíàðóæåíèÿ äâóõ ñîîáùåíèé ñ îäèíàêîâûì õýø-çíà÷åíèåì ïîòðåáóåòñÿ òîëüêî $2^{m/2}$ ñëó÷àéíûõ ñîîáùåíèé. Êîìïüþòåðó, êîòîðûé õýøèðóåò ìèëëèîí ñîîáùåíèé â ñåêóíäó, ïîòðåáîâàëîñü áû 600000 ëåò, ÷òîáû íàéòè âòîðîå ñîîáùåíèå ñ òåì æå 64-áèòîâûì õýø-çíà÷åíèåì. Òîò æå êîìïüþòåð ñìîæåò íàéòè ïàðó ñîîáùåíèé ñ îáùèì õýø-çíà÷åíèåì ïðèìåðíî çà ÷àñ

Ýòî çíà÷èò, ÷òî, åñëè âû îïàñàåòåñü âñêðûòèÿ â äåíü ðîæäåíèÿ, âû äîëæíû âûáèðàòü äëèíó õýø-çíà÷åíèÿ â äâà ðàçà äëèííåå, ÷åì âàì ïîòðåáîâàëîñü áû â ïðîòèâíîì ñëó÷àå. Íàïðèìåð, åñëè âû õîòèòå óìåíüøèòü âåðîÿòíîñòü âçëîìà âàøåé ñèñòåìû äî 1 øàíñà èç 2^{80}, èñïîëüçóéòå 160-áèòîâóþ îäíîíàïðàâëåííóþ õýø-ôóíêöèþ.

7.5 Êàêîâà äîëæíû áûòü äëèíà êëþ÷à?

Íà ýòîò âîïðîñ íåò åäèíîãî îòâåòà, îòâåò ýòîò çàâèñèò îò ñèòóàöèè. ×òîáû ïîíÿòü, êàêàÿ ñòåïåíü áåçîïàñíîñòè âàì íóæíà, âû äîëæíû çàäàòü ñåáå íåñêîëüêî âîïðîñîâ. Ñêîëüêî ñòîèò âàøà èíôîðìàöèÿ? Êàê äîëãî îíà äîëæíà áåçîïàñíî õðàíèòüñÿ? Êàêîâû ðåñóðñû âàøèõ âðàãîâ?

Ñïèñîê êëèåíòîâ ìîæåò ñòîèòü $1000. Ôèíàíñîâàÿ èíôîðìàöèÿ ïðè íåîæèäàííîì ðàçâîäå ìîãëà áû ñòîèòü $10000. Ðåêëàìà è äàííûå ìàðêåòèíãà äëÿ áîëüøîé êîðïîðàöèè ìîãëè áû ñòîèòü 1 ìèëëèîí äîëëàðîâ. Ãëàâíûé êëþ÷ äëÿ ñèñòåìû ýëåêòðîííûõ íàëè÷íûõ ìîæåò ñòîèòü ìèëëèàðäû.

Â ìèðå òîðãîâëè ïðåäìåòàìè ïîòðåáëåíèÿ ñåêðåòû äîëæíû òîëüêî ñîõðàíÿòüñÿ â òå÷åíèå íåñêîëüêèõ ìèíóò. Â ãàçåòíîì áèçíåñå ñåãîäíÿøíèå ñåêðåòû - ýòî çàâòðàøíèå çàãîëîâêè. Èíôîðìàöèÿ î ðàçðàáîòêå êàêîãî-òî ïðîäóêòà, âîçìîæíî, äîëæíà áóäåò õðàíèòüñÿ â ñåêðåòå â òå÷åíèå ãîäà èëè äâóõ Èçäåëèÿ(ïðîãðàììû) ìîãëà áû áûëà áû äîëæíà îñòàòüñÿ ñåêðåòîì â òå÷åíèå ãîäà èëè äâà. Äàííûå ïåðåïèñè ÑØÀ â ñîîòâåòñòâèè ñ çàêîíîì äîëæíû õðàíèòüñÿ â ñåêðåòå â òå÷åíèå 100 ëåò.

Ñïèñîê ãîñòåé, ïðèãëàøåííûõ íà âå÷åð-ñþðïðèç â ÷åñòü äíÿ ðîæäåíèÿ âàøåé ñåñòðû, èíòåðåñåí òîëüêî âàøèì ëþáîïûòíûì ðîäñòâåííèêàì. Òîðãîâûå ñåêðåòû êîðïîðàöèè ïðåäñòàâëÿþò èíòåðåñ äëÿ êîíêóðèðóþùèõ êîìïàíèé. Âîåííûå ñåêðåòû èíòåðåñíû âðàæåñêèì âîåííûì.

Â ýòèõ òåðìèíàõ äàæå ìîæíî îïðåäåëèòü òðåáîâàíèÿ ê áåçîïàñíîñòè Ìîæíî. Íàïðèìåð:

Äëèíà êëþ÷à äîëæíà áûòü òàêîé, ÷òîáû âçëîìùèê, ãîòîâûé ïîòðàòèòü 100 ìèëëèîíîâ äîëëàðîâ, ìîã âçëîìàòü ñèñòåìó â òå÷åíèå ãîäà ñ âåðîÿòíîñòüþ íå áîëåå, ÷åì $1/2^{32}$, äàæå ñ ó÷åòîì ñêîðîñòè òåõíè÷åñêîãî ïðîãðåññà 30 ïðîöåíòîâ â ãîä.

Â -3-é, ÷àñòè÷íî âçÿòîé èç [150], ïðèâåäåíû îöåíêè òðåáîâàíèé ê áåçîïàñíîñòè äëÿ ðàçëè÷íîé èíôîðìàöèè:

Áóäóùóþ âû÷èñëèòåëüíóþ ìîùü îöåíèòü íåëåãêî, íî âîò ðàçóìíîå ýìïèðè÷åñêîå ïðàâèëî: ýôôåêòèâíîñòü âû÷èñëèòåëüíûõ ñðåäñòâ óäâàèâàåòñÿ êàæäûå 18 ìåñÿöåâ è âîçðàñòàåò íà ïîðÿäîê êàæäûå 5 ëåò. Ñëåäîâàòåëüíî, ÷åðåç 50 ëåò ñàìûå áûñòðûå êîìïüþòåðû áóäóò â 10 ìèëëèàðäîâ áûñòðåå, ÷åì ñåãîäíÿ! Êðîìå òîãî, íå çàáûâàéòå, ÷òî ýòè ÷èñëà îòíîñÿòñÿ òîëüêî ê óíèâåðñàëüíûì êîìïüþòåðàì, êòî çíàåò, êàêèå ñïåöèàëèçèðîâàííûå óñòðîéñòâà äëÿ âñêðûòèÿ êðèïòîñèñòåì áóäóò ðàçðàáîòàíû â ñëåäóþùèå 50 ëåò?

Ïðåäïîëàãàÿ, ÷òî êðèòåðèåì àëãîðèòì áóäåò èñïîëüçîâàòüñÿ â áëèæàéøèå 30 ëåò, âû ìîæåòå ïðåäñòàâèòü ñåáå, íàñêîëüêî îí äîëæåí áûòü áåçîïàñåí. Àëãîðèòì, ñîçäàííûé ñåãîäíÿ, âîçìîæíî íå ñòàíåò øèðîêî èñïîëüçîâàòüñÿ äî 2000 ãîäà, è âñå åùå áóäåò èñïîëüçîâàòüñÿ â 2025 äëÿ øèôðîâàíèÿ ñîîáùåíèé, êîòîðûå äîëæíû îñòàâàòüñÿ â ñåêðåòå äî 2075 ãîäà è ïîçæå.

Òàáë. 7-10.
Òðåáîâàíèÿ ê áåçîïàñíîñòè ðàçëè÷íîé èíôîðìàöèè

Òèïû òðàôèêà	Âðåìÿ æèçíè	Ìèíèìàëüíàÿ äëèíà êëþ÷à (â áèòàõ)
Òàéíàÿ âîåííàÿ èíôîðìàöèÿ	ìèíóòû/÷àñû	56-64
Îáúÿâëåíèÿ î ïðîäóêòàõ, ñëèÿíèè êîìïàíèé, ïðîåêòíûõ ñòàâêàõ	äíè/íåäåëè	64
Äîëãîâðåìåííûå áèçíåñ-ïëàíû	ãîäû	64
Òîðãîâûå ñåêðåòû (íàïðèìåð, ðåöåïò êîêà-êîëû)	äåñÿòèëåòèÿ	112
Ñåêðåòû âîäîðîäíîé áîìáû	>40 ëåò	128
Ëè÷íîñòè øïèîíîâ	>50 ëåò	128
Ëè÷íûå äåëà	>50 ëåò	128
Äèïëîìàòè÷åñêèå êîíôëèêòû	>65 ëåò	128
Äàííûå ïåðñîíèñè ÑØÀ	100 ëåò	ïî ìåíüøåé ìåðå 128

7.6 Caveat emptor[1]

Âñÿ ýòà ãëàâà - ïðîñòî ìíîãî ÷åïóõè. This entire chapter is a whole lot of nonsense. Ñìåøíî ãîâîðèòü äàæå î ñàìîì ïîíÿòèè ïðåäñêàçàíèÿ âû÷èñëèòåëüíîé ìîùè íà 10, à òåì áîëåå íà 50 ëåò âïåðåä. Ýòè ðàñ÷åòû ïðèâåäåíû òîëüêî äëÿ îðèåíòèðîâêè, íè äëÿ ÷åãî áîëüøå. Ýêñòðàïîëèðóÿ ïðîøëîå, ìû ïîëó÷àåì áóäóùåå, êîòîðîå, âîçìîæíî, áóäåò èìåòü ìàëî îáùåãî ñ ðåàëüíîñòüþ.

Áóäüòå êîíñåðâàòîðàìè. Åñëè âàøè êëþ÷è äëèííåå, ÷åì âàì êàæåòñÿ íåîáõîäèìûì, òî ìåíüøå êîëè÷åñòâî òåõíîëîãè÷åñêèõ ñþðïðèçîâ ñìîæåò ïîâðåäèòü âàì.

[1] Äà áóäåò îñìîòðèòåëåí ïîêóïàòåëü (ëàòèí.)

Ãëàâà 8
Óïðàâëåíèå êëþ÷àìè

Ó Àëèñû è Áîáà åñòü áåçîïàñíàÿ ñèñòåìà ñâÿçè. Îíè èãðàþò â ìûñëåííûé ïîêåð, îäíîâðåìåííî ïîäïèñûâàþò êîíòðàêòû è äàæå ìåíÿþò öèôðîâûå íàëè÷íûå. Èõ ïðîòîêîëû áåçîïàñíû. Èõ àëãîðèòìû -ñàìûå ëó÷øèå. Ê ñîæàëåíèþ, îíè ïîêóïàþò ñâîè êëþ÷è îò "Keys-R-Us" Âû, ÷åé êîçóíÿ - "Âû ìîæåòå äîâåðÿòü íàì: Áåçîïàñíîñòü - ñðåäíåå èìÿ ÷ëîâåêà, êîòîðîãî òóðèñòè÷åñêèé àãåíò íàøåé áûâøåé òåùè âñòðåòèë â "Kwik-E-Mart".

Åâà íå íóæíî âñêðûâàòü àëãîðèòì. Åé íå íóæíî ïîëàãàòüñÿ íà òîíêèå äåôåêòû ïðîòîêîëà. Îíà ìîæåò èñïîëüçîâàòü èõ êëþ÷è äëÿ ÷òåíèÿ âñåõ ñîîáùåíèé Àëèñû è Áîáà, íå ïðèêëàäûâàÿ íèêàêèõ êðèïòîàíàëèòè÷åñêèõ óñèëèé.

Â ðåàëüíîì ìèðå óïðàâëåíèå êëþ÷àìè ïðåäñòàâëÿåò ñàìóþ òðóäíóþ ÷àñòü êðèïòîãðàôèè. Ïðîåêòèðîâàòü áåçîïàñíûå êðèïòîãðàôè÷åñêèå àëãîðèòìû è ïðîòîêîëû íå ïðîñòî, íî Âû ìîæåòå ïîëàãàòüñÿ íà áîëüøîé îáúåì àêàäåìè÷åñêîãî èññëåäîâàíèé. Ñîõðàíèòü ñåêðåò êëþ÷åé íàìíîãî òðóäíåå.

Êðèïòîàíàëèòèêè ÷àñòî âñêðûâàþò è ñèììåòðè÷íûå êðèïòîñèñòåìû, è êðèïòîñèñòåìû ñ îòêðûòûì êëþ÷àìè ÷åðåç ðàñïðåäåëåíèå êëþ÷åé. Çà÷åì Åâå áåñïîêîèòüñÿ íà ïðîáëåìå âñêðûòèÿ êðèïòîãðàôè÷åñêîãî àëãîðèòìà öåëèêîì, åñëè îíà ìîæíî âîññòàíîâèòü êëþ÷ èç-çà íåâèíîâàòîãî õðàíåíèÿ êëþ÷à? Çà÷åì åé òðàòèòü 10 ìèëëèîíîâ äîëëàðîâ íà ñîçäàíèå ìàøèíà äëÿ êðèïòîàíàëèçà, åñëè îíà ìîæåò ïîâñòóïèòü êëåðêà çà 1000 äîëëàðîâ? Ìèëëèîí äîëëàðîâ çà êëåðêà ñâÿçè íà õîðîøåì ìåñòå â äèïëîìàòè÷åñêîì ïîñîëüñòâå ìîæåò áûòü âûãîäíûì ñäåëêîé. ÓÎêåðû ãîäàìè ïðîäâàëè Ñîâåòàì êëþ÷è øèôðîâàíèÿ ÂÌÑ ÑØÀ. Ðóêîâîäèòåëü êîíòðàçâåäêè ÖÐÓ ñòîëü ìåíüøå 2 ìèëëèîíîâ äîëëàðîâ, âêëþ÷àÿ æåíó. Ýòî íàìíîãî äåøåâëå, ÷åì ñòðîèòü îãðîìíûå ìàøèíû âñêðûòèÿ è íàíèìàòü áëåñòÿùèõ êðèïòîãðàôèêîâ. Åâà ìîæåò âûêðàñòü êëþ÷è. Îíà ìîæåò àðåñòîâàòü èëè ïîõèùòü êîãî-òî, êòî çíàåò êëþ÷è. Îíà ìîæåò ñîâðàùàòü êîãî-òî è ïîëó÷àòü êëþ÷è òàêèì îáðàçîì. (Ìîñêèå ïåðîòèöû, îõðàíÿâøèå ïîñîëüñòâî ÑØÀ â Ìîñêâå íå óñòîÿëè ïåðåä ïîäêóïîì àòàêîé.) Íàìíîãî ïðîùå íàõîäèòü äåôåêòû â ëþäÿõ, ÷åì â êðèïòîñèñòåìàõ.

Àëèñà è Áîá äîëæíû çàùèùàòü è ñâîé êëþ÷, è â òîé ñòåïåíè øèôðóåìûå èì äàííûå. Åñëè êëþ÷ íå èçìåíÿòü ðåãóëÿðíî, òî êîëè÷åñòâî äàííûõ ìîæåò áûòü îãðîìíî. Ê ñîæàëåíèþ, ìíîãèå êîìïüþòåðíûå ïðîäóêòû ïîñòàâëÿþò "Ì û ñîîùèì DES" è çàáûâàþò îáî âñåì îñòàëüíîì. Ðåçóëüòàòû íå ñëèøêîì âïå÷àòëÿþò.

Íàïðèìåð, ïðîãðàììà DiskLock äëÿ Macintosh (âåðñèÿ 2.l), ïðîäàâàâøàÿñÿ â áîëüøèíñòâå ìàãàçèíîâ ïðîãðàììíîãî îáåñïå÷åíèÿ, ïðåòåíäóåò íà áåçîïàñíîå øèôðîâàíèå DES. Îíà øèðóåòôàéëû, èñïîëüçóÿ DES. Ðåàëèçàöèÿ DES àëãîðèòìà ïðàâèëüíà. Îäíàêî, DiskLock ñîõðàíÿåò êëþ÷ DES âìåñòå ñ çàøèðîâàííûì ôàéëîì. Åñëè âû çíàåòå, ãäå èñêàòü êëþ÷, è õîòåòü ïðî÷èòàòü ôàéë, øèôðîâàííûé DiskLock ñ ïîìîùüþ DES, âîññòàíîâèòå êëþ÷ èç øèôðîâàííîãî ôàéëà è çàòåì ðàñøèôðîâûâàòü ôàéë. Íå èìåòî çíà÷åíèå, ÷òî ïðîãðàììà èñïîëüçóåò øèôðîâàíèå DES - ðåàëèçàöèÿ àáñîëþòíî íåáåçîïàñíà.

Äàëüíåéøóþ èíôîðìàöèþ îòíîñèòåëüíî óïðàâëåíèÿ êëþ÷àìè ìîæíî íàéòè â [457, 98, 1273, 1225, 775, 357]. Â ñëåäóþùèõ ðàçäåëàõ îáñóæäàþòñÿ íåêîòîðûå èç âîïðîñîâ è ðåøåíèé.

8.1 Ãåíåðàöèÿ êëþ÷åé

The security of an algorithm rests in the key. If you're using a cryptographically weak process to generate keys, then your whole system is weak. Eve need not cryptanalyze your encryption algorithm; she can cryptanalyze your key generation algorithm.

Áåçîïàñíîñòü àëãîðèòìà ñîñðåäîòî÷åíà â êëþ÷å. Åñëè âû èñïîëüçóåòå êðèïòîãðàôè÷åñêè ñëàáûé ïðîöåññ äëÿ ãåíåðàöèè êëþ÷åé, òî âàøà ñèñòåìà â öåëîì ñëàáà. Åâå íå íóæíî êðèïòîàíàëèçèðîâàòü âàø àëãîðèòì øèôðîâàíèÿ, îíà ìîæåò êðèïòîàíàëèçèðîâàòü âàø àëãîðèòì ãåíåðàöèè êëþ÷åé.

Óìåíüøåííûå ïðîñòðàíñòâà êëþ÷åé

DES èñïîëüçóåò 56-áèòîâûé êëþ÷ ñ áèòàìè. Ëþáàÿ ïðàâèëüíî çàäàííàÿ 56-áèòîâàÿ ñòðîêà ìîæåò áûòü êëþ÷îì, ñóùåñòâóåò 2^{56} (10^{16}) âîçìîæíûõ êëþ÷åé. Norton Discreet for MS-DOS (âåðñèè 8.0 è áîëåå ðàííèå) ðàçðåøàåò ïîëüçîâàòåëþ ïèñàòü êëþ÷àì ASCII, äåëàÿ ñòàðøèé áèò êàæäîãî áàéòà íîëåì. Ïðîãðàììà òàêæå ïðåîáðàçóåò ñèìâîëû íèæíåãî ðåãèñòðà â âåðõíèé ðåãèñòð (òàê ÷òî ïÿòûé áèò êàæäîãî áàéòà âñåãäà ïðîòèâîïîëîæåí øåñòîìó áèòà) è èãíîðèðóåò áèò ïëàäøåãî ðàçðÿäà êàæäîãî áàéòà, ÷òî ïðèâîäèò ê ïðîñòðàíñòâó â 2^{40} âîçìîæíûõ êëþ÷åé. Ýòè óùåðáíûå ïðîöåäóðû ãåíåðàöèè êëþ÷ íäåëàëè ñâîþ ðåàëèçàöèþ DES â ääñÿòü òûñ÷ ðàç ïðîùå äëÿ âñêðûòèÿ.

7-é ñîäðæèò ÷èñëî âîçìîæíûõ êëþ÷åé äëÿ ðàçëè÷íûõ îãðàíè÷åíèé íà âõîäíûå ñòðîêè. Â 6-é ïðèâåäåíî âðåìÿ, òðåáóåìîå äëÿ èñ÷åðïûâàþùåãî ïåðåáîðà âñåõ âîçìîæíûõ êëþ÷åé ïðè ìèëëèîíå ïîòîêîâ â ñåêóíäó.

Ì îãóò áûòü èñïîëüçîâàíû äëÿ âñêðûòèÿ ãðóáîé ñèëîé ëþáûå ñïåöèàëèçèðîâàííûå àïïàðàòíûå è ïðàãìåëü-

íûå ðåàëèçàöèè. Ïðè ïðîâåðêå ìèëëèîíà êëþ÷åé â ñåêóíäó (îäíîé ìàøèíîé èëè íåñêîëüêèìè ïàðàëëåëüíî) ôèçè÷åñêè âîçìîæíî ðàñêðûòü êëþ÷è èç ñèìâîëîâ íèæíåãî ðåãèñòðà è êëþ÷è èç öèôð è ñìâîëîâ íèæíåãî ðåãèñòðà äëÿ 8 áàéòîâ, àëôàâèòíî-öèôðîâûå êëþ÷è - äëÿ 7 áàéòîâ, êëþ÷è èç ïå÷àòàåìûõ ñìâîëîâ è ASCII-ñèìâîëîâ - äëÿ 6 áàéòîâ, â êëþ÷è èç 8-áèòîâûõ ASCII-ñèìâîëîâ - äëÿ 5 áàéòîâ.

Òàáë. 8-1.
Êîëè÷åñòâî âîçìîæíûõ êëþ÷åé â ðàçëè÷íûõ ïðîñòðàíñòâàõ êëþ÷åé

	4 áàéòà	5 áàéòîâ	6 áàéòîâ	7 áàéòîâ	8 áàéòîâ
Ñòðî÷íûå áóêâû (26)	460000	$1.2*10^{7}$	$3.1*10^{8}$	$8.0*10^{9}$	$2.1*10^{11}$
Ñòðî÷íûå áóêâû è öèôðû (36)	1700000	$6.0*10^{7}$	$2.2*10^{9}$	$7.8*10^{10}$	$2.8*10^{12}$
Àëôàâèòíûå è öèôðîâûå ñèìâîëû (62)	$1.5*10^{7}$	$9.2*10^{8}$	$5.7*10^{10}$	$3.5*10^{12}$	$2.2*10^{14}$
Ïå÷àòàåìûå ñèìâîëû (95)	$8.1*10^{7}$	$7.7*10^{9}$	$7.4*10^{11}$	$7.0*10^{13}$	$6.6*10^{15}$
Ñèìâîëû ASCII (128)	$2.7*10^{8}$	$3.4*10^{10}$	$4.4*10^{12}$	$5.6*10^{14}$	$7.2*10^{16}$
8-áèòîâûå ASCII ñèìâîëû (256)	$4.3*10^{9}$	$1.1*10^{12}$	$2.8*10^{14}$	$7.2*10^{16}$	$1.8*10^{19}$

Òàáë. 8-2.
Âðåìÿ èñ÷åðïûâàþùåãî ïîèñêà ðàçëè÷íûõ ïðîñòðàíñòâà êëþ÷åé (ïðè îäíîì ìèëëèîíå ïðîâåðîê â ñåêóíäó)

	4 áàéòà	5 áàéòîâ	6 áàéòîâ	7 áàéòîâ	8 áàéòîâ
Ñòðî÷íûå áóêâû (26)	0.5 ñåêóíäû	12 ñåêóíä	5 ìèíóò	2.2 ÷àñà	2.4 äíÿ
Ñòðî÷íûå áóêâû è öèôðû (36)	1.7 ñåêóíäû	1 ìèíóòà	36 ìèíóò	22 ÷àñà	33 äíÿ
Àëôàâèòíûå è öèôðîâûå ñèìâîëû (62)	15 ñåêóíä	15 ìèíóò	16 ÷àñîâ	41 äåíü	6.9 ãîäà
Ïå÷àòàåìûå ñèìâîëû (95)	1.4 ìèíóòû	2.1 ÷àñà	8.5 äíÿ	2.2 ãîäà	210 ëåò
Ñèìâîëû ASCII (128)	4.5 ìèíóòû	9.5 ÷àñà	51 äåíü	18 ëåò	2300 ëåò
8-áèòîâûå ASCII ñèìâîëû (256)	1.2 ÷àñà	13 äíåé	8.9 ãîäà	2300 ëåò	580000 ëåò

È ïîìíèòå, âû÷èñëèòåëüíàÿ ìîùü óäâàèâàåòñÿ êàæäûå 18 ìåñÿöåâ. Åñëè âû õîòèòå, ÷òîáû âàøè êëþ÷è óñòîé÷èâû ê âñêðûòèþ ãðóáîé ñèëîé â òå÷åíèå 10 ëåò, âû äîëæíû ñîîòâåòſòâóþùèì îáðàçîì ïëàíèðîâàòü èñïîëüçîâàíèå êëþ÷åé.

Îáùåíèíûé âûáîð êëþ÷åé

Êîãäà ëþäè ñàìè âûáèðàþò êëþ÷è, îíè âûáèðàþò óùåðáíûå êëþ÷è. Îíè ñ áîëüøåé âåðîÿòíîñòüþ âûáåðóò "Barney", ÷åì "*9 (hH/A". Ýòî íå âñåãäà ïðîèñõîäèò èç-çà ïëîõîé ïðàêòèêè, ïðîñòî "Barney" ëåãê÷å çàïîìíèòü ÷åì "*9 (hH/A". Ñàìûé áåçîïàñíûé àëãîðèòì â ìèðå íå ñëåäíîé ïîìåòè, åñëè ïîëüçîâàòåëè ïî ïðèâû÷êå âûáèðàþò èìåíà ñâîèõ æåí (ìóæåé) äëÿ êëþ÷åé èëè ïèøóò ñâîè êëþ÷è íà íåáîëüøèõ ëèñòî÷êàõ â áóìàæíèêàõ. Èíòåëëåêòóàëüíûå âñêðûòèå ðóáîé ñëîé íå ïðåäëàãàò âñå âîçìîæíûå êëþ÷è â ÷èñëîâîì ïîðÿäêå, íî ïðîáóò ñíà÷àëà î÷åâèäíûé êëþ÷è.

Ýòî íàçûâàåòſÿ **âñêðûòèåì ñî ñëîâàðåì**, ïîòîìó ÷òî íàïàäþùèé èñïîëüçóåò ñëîâàðü îáùèõ êëþ÷åé. Äýíèåë Êëÿéí (Daniel Klein) ñìîã ðàñêîëîòü 40 ïðîöåíòîâ ïàðîëåé íà ñðåäíåì êîìïüþòåðå, èñïîëüçóÿ ýòîò ñïîñîá âñêðûòèÿ [847, 848]. Íåò, îí íå ïðåäëàãàë îäèí ïàðîëü çà äðóãèì, ïûòàÿñü âîéòè â ñèſòåìó. Î í ñêîïèðîâàë çàøèôðîâàííûé ôàéë ïàðîëåé è ïðåäïðîñëåäèë âñêðûòèå àâòîíîìíî. Âîò, ÷òî îí ïðîâåðèë:

1. Â êà÷åſòâå âîçìîæíîãî ïàðîëÿ èſÿ ïîëüçîâàòåëÿ, èſèöèàëû, èſÿ áþäæåòà è äðóãóþ ñâÿçàííóþ ſ ÷åëîâåêî èſôîðſàöèþ. Â öåëîſ, íà îſíîâå òàêîé èſôîðſàöèè ïðîáîâàëſñü äî 130 ðàçëè÷íûõ ïàðîëåé. Âſò íåêîſòîðûå èſ ïàðîëåé, ïðîâåðÿâøèõſÿ äëÿ èſåíè áþäæåòà **klone** è ſîëüçîâàòåëÿ "Daniel V. Klein": klone, klone0, klonel, klonel23, dvk, dvkdvk, dklein, Dklein, leinad, nielk, dvklein, danielk, DvkkvD, DANIEL-KLEIN, (klone), KleinD, è òàê äàëåå.
2. Ñëîâà èç ðàçëè÷íûõ áàç äàííûõ. Èſïîëüçîâàëèſü ſïèſêè ſóæſêèõ è æåſſêèõ èſåſ (âſåãî îſſîſ 16000), íàçâàſèÿ ſåſò (âſëþ÷àÿ èçſåſſèÿ, ſîſýſſó ðàſſſàòðèâàëſſü è "spain", "Spanish", è "Spaniard"), èſåſà èçſåſſòſûõ ëþäſé, ſóſüòôèſüſû è ſóſüòèſïëèâòèſſſûå ãåðſè, çàſſſîſâſè, ſåðſè è ſåſòà èç ôèſüſſâ è íàó÷íſé ôàſòàſòèſè, ſèôè÷åſſêå ſóſåſòâà (äſáſòûå èç *Bullfinch's Mythology* è

ñëîâàðåé ìèôè÷åñêèõ æèâîòíûõ), ñïîðò (âêëþ÷àÿ íàçâàíèÿ êîìàíä, ïðîçâèùà è ñïåöèàëüíûå òåðìèíû), ÷èñëà (çàïèñàííûå êàê öèôðàìè - '2001", òàê è áóêâàìè "twelve"), ñòðîêè ñèìâîëîâ è ÷èñëå ("a", "aa", "aaa", "aaaa" è ò.ä.), êèòàéñêèå ñëîâà (èç Pinyin Romanization of Chinese, ìåæäóíàðîäíîãî ñòàíäàðòà ïèñüìà ïî êèòàéñêè íà àíãëîÿçû÷íîé êëàâèàòóðå), Áèáëåéñêèå êîðîëè Äæåéìñà; áèîëîãè÷åñêèå òåðìèíû, ðàçãîâîðíûå è âóëüãàðíûå âûðàæåíèÿ (òèïà "fuckyou", "ibmsux" è "deadhead"), ñòàíäàðòû êëàâèàòóð (òèïà "qwerty", "asdf" è "zxcvbn"), ñîêðàùåíèÿ (òèïà "roygbiv" - ïåðâûå áóêâû íàçâàíèé öâåòîâ ðàäóãè ïî àíãëèéñêè - è "ooottafagvah" - ìíåìîíè÷åñêèé ñõåìà äëÿ çàïîìèíàíèÿ 12 ÷åðåïíûõ íåðâîâ), èìåíà êîìïüþòåðîâ (ïîëó÷åííûå èç /etc/hosts), ãåðîè, ïüåñû è ìåñòà äåéſòâèÿ ó Øåêñïèðà, ñàìûå ðàñïðîſòðàíåííûå ñëîâà ÿçûêà Èäèø, íàçâàíèÿ àñòðîíîìè÷åſêèõ îáúåêòîâ, îïóáëèêîâàííûõ ðàíåå Êëýéíîì. Èòîãî, äëÿ ïîëüçîâàòåëÿ ðàſſìàòðèâàëîſü áîëåå ÷åì 60000 îòäåëüíûõ ſëîâ (ſ îòáðàſûâàíèå ìóäëèêàòîâ â ðàçëè÷íûõ ſëîâàðÿõ).

3. Âàðèàöèè ſëîâ èç ïóíêòà 2. Ýòî âêëþ÷àëî ïåðåíîſ ſëåâîſ ſèìâîëà â âåðõíèé ðåãiſſòð èëè åſî çàſåſó óſðàâëÿþſèſ ſèſâîſîſ, ſåðåſſâ ſëſâà â âåðõíèé ðåſàſòð, èſâåðſèþ ðåſàſòðà ſëſâà (ſ è áåç âſøáóſſſîſſÿſóòſîſ èçſåſſåſèÿ ðåſàſòðà ſåðâſſé áóêâſ), çàſåſó áóêâſ "o" íà öèôðó "0" (òàê, ÷òſáſ ſëſſâſ "scholar" áſëſ òàêæå ſðſſâåðåſſ êàê "sch0lar"), çàſåſó áóêâſ "l" íà öèôðó "1" (òàê, ÷òſáſ ſëſſâſ "scholar" áſëſ áſ òàêæå ſðſſâåðåſſ êàê "scho1ar") è âſſſëſåſèå àſàëſſãè÷ſſſ ſàſèſóëÿöèé ſ áóêâſé "z" è öèôðſé "2", à òàêæå ſ áóêâſé "s" è öèôðſé "5". Äðóãàÿ ſðſâåðêà ſſſòſÿëà èç ſåðåâſſäà ſëſâà âſ ſſſæåſòâſſſſå ÷èſëſ (ſåçàâèſèſſ îò òſſãſ, áſëſ ëè ſëſſâſ ſóſùſſòâèòåëſſſ) ſ ó÷åòſ ſſſáſóſäèſſûſ ſðàâſëë, ÷òſáſ "dress" çàſåſëëſſſü íà "dresses", "house" - íà "houses", à "daisy" - íà "daisies". Õſòÿ Êëÿéſ ſå æåſòêſ ſðèäåðæèâàëſÿ ſðàâſëë ſðåſáðàçſâàſèÿ êſ ſſſæåſòâſſſſſ÷èſéó, ſſſýſſſó "datum" ſòàëà "datums" (à ſå "data"), "sphynx" - "sphynxs" (à ſå "sphynges"). Àſàëſſãè÷ſſ, äëÿ ſðåſáðàçſâàſèÿ ſëſâ äſáàâëÿëèſſü ſóſèſêſû "-ed", "-er" è "-ing", ſſäſáſſ "phase" â "phased," "phaser" è "phasing". Ýòè äſſſſéſèòåëſſſûå ſðſâåðêè äſáàâèëè åùå 1000000 ſëſâ ê ſſſèſéó âſçſſſæſſûſ ſàðſëåé, êſòſðûå ſðſâåðÿëèſü äëÿ êàæäſãſ ſſſëſçſâàòåëÿ.

4. Ðàçëè÷íûå âàðèàſòû ſðåſáðàçſâàſèÿ ê âåðſſåſ ðåãèſòðó ſëſâ ſóſêòà 2, íå ðàſſſàòðèâàâøèſſÿ â ſóſêòå 3. Ñþäà âſøëſ ſðåſáðàçſâàſèå ê âåðſſåſ ðåãèſòðó ſàèſſ÷ſſûſ ſèſſſſâſêſâ (òàê, ÷òſáſ "michael" áſëſ òàêæå ſðſſâåðåſſ êàê "mIchael", "miChael", "micHael", "michAel", è ò.ä.), ſðåſáðàçſâàſèå ê âåðſſåſ ðåãèſòðó ſàðſ ſèſâſëſâ ("MIchael", "MiChael", "MicHael", ..., "mIChael", "mIcHael", è ò.ä.), ſðåſáðàçſâàſèå ê âåðſſåſ ðåãèſòðó òðåſ ſèſâſëſâ, è ò.ä. Èçſåſåſèÿ ſàèſſ÷ſſãſ ſèſſâſëà äſáàâèëè ê ſðſâåðÿåſſ ſðèſåſſſ å400000 ſëſâ, à èçſåſåſèÿ ſàðſ ſèſâſëſâ - 1500000 ſëſâ. Èçſåſåſèÿ òðåſ ſèſâſëſâ äſáàâëÿëè ſſ ſêðàéſåé ſåðå åſå 3000000 ſëſâ äëÿ êàæäſãſ ſſſëçſâàòåëÿ, åſëè äëÿ çàâåðøåſèÿ òåſſòèðſâàſèÿ õâàòàëſ âðåſåſè. Sðſâåðêà èçſåſåſèÿ ÷åòſðåſ, ſÿòè è øåſòè ſèſſâſëſâ áſëà ſðèçſàſà íåſðàêòè÷ſſé, òàê êàê äëÿ èſ ſðſâåðêè íå õâàòàëſ âſ÷èſëèòåëſſſûſ ſſſſ÷èſåſ.

5. 5. Èſſſòðàſſûå ſëſſâà äëÿ èſſſòðàſſûſ ſſëſçſâàòåëåé. Ñſåöèôè÷åſêèé òåſò, êſòſðſé áſë âſſſëſåſ, ſðſâåðÿë ſàðſëè èç êèòàéſêſâſ ÿçſêà äëÿ ſſëſçſâàòåëåé ſ êèòàéſêſèſè èſåſàſè. Äëÿ êèòàéſêſèſ ſëſ-ãſâ èſſſëſçſâàëſÿ ſòàſäàðò Pinyin Romanization, ſëſãè îáúåäſſÿëèſü âſåſòå â ſàſſ-, äâóõ- è òðåõſëſæſûå ſëſſâà. Òàê êàê íå áſëſ âſſſſëſåſſ ſðåäâàðèòåëſſſſé ſðſåðåðêè ſëſâ íà çſà÷èſſſöü, èſſſëſçſâàëſÿ èſ÷åðſûâàþ ſèé ſåðåſſ. Òàê êàê â ſèſòåſå Pinyin ñóſåñòâóåò 298 êèòàéſêèſ ſëſãſâ, òſ èſååòſÿ 158404 ſëſâ ſ äâóſÿ ſëſãàſè, è íåſſſãſ áſëüøå 16000000 ſëſâ ſ òðåſÿ ſëſãàſè. Ïſãſáſûé ſſſſſá âſëðûòèÿ ſſã áſ áſòü ëåãêſ èſſſëſçſâàſ è äëÿ àſãëèéſëſãſ ÿçſêà, ſ ó÷åòſ ſ ſðàâëë ſáðàçſâàſèÿ ſðſ-èçſſſèſſſûſ íè÷åãſ íå çſà÷àſèſ ſëſâ.

6. Ïàðû ſëſâ. Îáúåſ òàêſãſ èſ÷åðſûâàþſåãſ òåſòà êſëåáëåòſÿ. ×òſáſ óſðſſòèòü òåſò, èç */usr/dict/words* èſſſëſçſâàëèſü òſëſêſ ſëſâà äëèſſé òðè èëè ÷åòſðåſ ſèſâſëà. Äàæå ſðè ýòſ, ÷èſëſ ſàð ſëſâ ſſſòàâëëſ ſðèáëëçèòåëſſſ äåſÿòſ ſèëëèſſſâ.

Âſêðûòèå ſſ ſëſâàðåſ íàſſſãſ ſſúſåå, êſãäà ſſſ èſſſſëſçóåòſÿ ſðſòèâ ôàéëà êëþ÷åé, à íå ſðſòèâ ſàſſſãſ êëþ÷à. Îäèſſ÷ſûé ſſſëſçſâàòåëü ſſæåò áſòſ äſñòàòſ÷ſſ ðàçſſàſ è âſáðàòſ õſðſøèå êëþ÷è. Åſëè èç òſñÿ÷è ëþäåé êàæäûé âſáèðàåò ſſáſñòàåſſſûé êëþ÷ êàê ſàðſëü êſſ ſüþòåðſſé ſëſòſåſſſ òſãſ, ſòſ ſſëèêà âåðſÿòſſſòü òſãſ, ÷òſ ſſ êðàéſåé ſåðå ſäèſ ÷åſſâåê âſáåðåò êëþ÷, èſåþſèéſÿ â ſëſâàðå âçſſſſſèêà.

Ñëó÷àéſûå êëþ÷è

Õſðſøèſè êëþ÷àſè ÿâëÿþſÿ ſòðſêè ſëó÷àéſûſ áèòſâ, ſſçäàſſûå íåſòſðſû àâòſſàòè÷åſêèſ ſðſöåſſſſſ. Åſëè äëèſà êëþ÷à ſſſòàâëÿåò 64 áèòà, òſ âſå âſçſſæſûå 64-áèòſâûå êëþ÷è äſëæſû áſòü ðàſſſâåðſÿòſû. Ãåſåðèðóéòå áèòû êëþ÷åé, ſſëüçóÿſü ëèáſ ſàäåæſû è ſòſ÷ſèſſſ ſëó÷àéſûſ ÷èſåſ (ſì. ðàçäåë 17.14), ëèáſ êðèſòſãðàôè÷åſêè áåçſſàſſû ãåſåðàòſðſ ſſåääſſëó÷àéſûſ áèòſâ (ſì. ãëàâû 16 è 17.) Åſëè òàêèå àâòſſàòè÷åſêèå ſðſöåſſſû íåäſſòóſſû, áðſſàéòå ſſſåòéſ ëëè êſſòè.

Ýòſ âàæſſ, ſſ íå óâëåêàéòåſü ſáſóæäåſèåſ òſãſ, ÿâëÿåòſÿ ëè øóſ èç çâóêſâûſ èſòſ÷ſèſſâ áſëåå ſëó÷àéſûſ, ÷åſ øóſ èç ðàäſſàêòèâſſſãſ ðàſſäàä. Íè ſàèſ èç ýòèſ èſòſ÷ſèſſâ ſëó÷àéſſãſ øóſà íå ſſſåðøåſåſ, ſſ âſå ſſé, ſſêſðåå âſåãſ, áóäóò äſſòàòſ÷ſſ õſðſøè. Äëÿ ãåſåðàöèè êëþ÷åé âàæſſ èſſſſëſçſâàòü õſðſøèé ãåſåðàòſð ſëó÷àéſûſ ÷èſåë, ſſ ãſðàçãſ âàæſåå èſſſëſçſâàòü õſðſøèå àëãſðèſſû øèôſâſàſèÿ è ſðſöåáóſû óſðàâëſåſèÿ êëþ÷à-

ìè. Åñëè âû áåñïîêîèòåñü î ñëó÷àéíîñòè âàøèõ êëþ÷åé, èñïîëüçóéòå îïèñàííóþ íèæå ìåòîäèêó ïåðåìàëûâàíèÿ êëþ÷à.

Íåêîòîðûå àëãîðèòìû øèôðîâàíèÿ èìåþò ñëàáûå êëþ÷è - ñïåöèôè÷åñêèå êëþ÷è, ìåíåå áåçîïàñíûå ÷åì äðóãèå êëþ÷è. ß ñîâåòóþ ïðîâåðÿòü ñëàáîñòü êëþ÷à êëþ÷åé è, îáíàðóæèâ åå, âåíåðèðîâàòü íîâûé. Ó DES òîëüêî 16 ñëàáûõ êëþ÷åé â ïðîñòðàíñòâå 2^{56}, òàê ÷òî âåðîÿòíîñòü ïîëó÷èòü îäèí èç ýòèõ êëþ÷åé íåâåðîÿòíî ìàëà. Çàÿâëÿëîñü, ÷òî êðèïòîàíàëèòèê íå áóäåò çíàòü î òîì, ÷òî èñïîëüçóåòñÿ ñëàáûé êëþ÷, è, ñëåäîâàòåëüíî, íå ñìîæåò ïîëó÷èòü íèêàêîé âûãîäû èç èõ ñëó÷àéíîãî èñïîëüçîâàíèÿ. Òàêæå çàÿâëÿëîñü, ÷òî èíôðàñòðóêòóðà êðèïòîàíàëèòèêó äåò ñîâñåì íå èñïîëüçîâàíèå ñëàáûõ êëþ÷åé. Îäíàêî, ïðîâåðêà íåìíîãèõ ñëàáûõ êëþ÷åé íàñòîëüêî ïðîñòà, ÷òî êàæåòñÿ ãëóïûì ïðåíåáðåæü åð.

Ãåíåðàöèÿ êëþ÷åé äëÿ ñèñòåì êðèïòîãðàôèè ñ îòêðûòûì êëþ÷àìè òÿæåëåå, ïîòîì ÷òî ÷àñòî êëþ÷è äîëæíû îáëàäàòü îïðåäåëåííûìè ìàòåìàòè÷åñêèìè ñâîéñòâàìè (âîçìîæíî, îíè äîëæíû áûòü ïðîñòûìè ÷èñëàìè, êâàäðàò÷íûì îñòàòêîì, è ò.ä.). Ìåòîäû ãåíåðàöèè áîëüøèõ ñëó÷àéíûõ ïðîñòûõ ÷èñåë ðàññìàòðèâàþòñÿ â ðàçäåëå 11.5. Âàæíî ïîìíèòü, ÷òî ñ òî÷êè çðåíèÿ óïðàâëåíèÿ êëþ÷àìè ñëó÷àéíûå ñòàðòîâûå ïîñëåäîâàòåëüíîñòè äëÿ òàêèõ ãåíåðàòîðîâ äîëæíû áûòü äëéñòâèòåëüíî ñëó÷àéíû.

Ãåíåðàöèÿ ñëó÷àéíîãî êëþ÷à âîçìîæíà íå âñåãäà. Èíîãäà âàì íóæíî ïîìíèòü âàø êëþ÷. (Èíòåðåñíî, ñêîëüêî âðåìåíè âàì ïîíàäîáèòñÿ, ÷òîáû çàïîìíèòü 25e8 56f2 e8ba c820?). Åñëè âàì íàäî ãåíåðèðîâàòü ïðîñòîé äëÿ çàïîìèíàíèÿ êëþ÷, çàìàñêèðóéòå åãî. Èäåàëîì ÿâëÿåòñÿ òî, ÷òî ëåãêî çàïîìíèòü, íî òðóäíî óãàäàòü. Âîò íåñêîëüêî ïðåäëîæåíèé:

— Ïàðû ñëîâ, ðàçäåëåííûå ñèìâîëîì ïóíêòóàöèè, íàïðèìåð, "turtle*moose" èëè "zorch!splat"

— Ñòðîêè áóêâ, ÿâëÿþùèåñÿ âêðîíèìè äëèííûõ ôðàç, íàïðèìåð, "Mein Luftkissenfahrzeug ist voller Aale!" ñëóæèò äëÿ çàïîìèíàíèÿ êëþ÷à "MLivA!"

Êëþ÷åâûå ôðàçû

Ëó÷øèì ðåøåíèåì ÿâëÿåòñÿ èñïîëüçîâàíèå âìåñòî ñëîâà öåëîé ôðàçû è ïðåîáðàçîâàíèå ýòîé ôðàçû â êëþ÷. Òàêèå ôðàçû íàçûâàþòñÿ **êëþ÷åâûìè ôðàçàìè**. Ìåòîäèêà ñ íàçâàíèåì **ïàðîëüíàÿ êëþ÷à** ïðåîáðàçóåò ëåãêî çàïîìèíàþùèåñÿ ôðàçû â ñëó÷àéíûå êëþ÷è. Äëÿ ïðåîáðàçîâàíèÿ òåêñòîâîé ñòðîêè ïðîèçâîëüíîé äëèíû â ñòðîêó ïñåâäîñëó÷àéíûõ áèò èñïîëüçóåò îäíîíàïðàâëåííóþ õýø-ôóíêöèþ. Íàïðèìåð, ëåãêî çàïîìèíàþùàÿñÿ òåêñòîâàÿ ñòðîêà:

```
My name is Ozymandias, king of kings. Look on my works, ye mighty, and despair. [1]
```

ìîæåò "ïðåâðàòèòüñÿ" â òàêîé 64-áèòîâûé êëþ÷:

```
e6cl 4398 5ae9 0a9b
```

Êîíå÷íî, ìîæåò áûòü íåëåãêî ââåñòè â êîìüþòåð öåëóþ ôðàçó, åñëè ââîäèìûå ñèìâîëû íå îòîáðàæàþòñÿ íà ýêðàíå. Ðàçóìíûå ïðåäëîæåíèÿ ïî ðåøåíèþ ýòîé ïðîáëåìû áóäóò îöåíåíû.

Åñëè ôðàçà äîñòàòî÷íî äëèíà, òî ïîëó÷åííûé êëþ÷ áóäåò ñëó÷àéí. Âîïðîñ î òî÷íîì ñìûñëå âûðàæåíèÿ "äîñòàòî÷íî äëèíà" îñòàåòñÿ îòêðûòûì. Òåîðèÿ èíôîðìàöèè óòâåðæäàåò, ÷òî èíôîðìàöèîííàÿ çíà÷èìîñòü ñòàíäàðòíîãî àíãëèéñêîãî ÿçûêà ñîñòàâëÿåò îêîëî 1.3 áèòà íà ñèìâîë (ñì. ðàçäåë 11.1). Äëÿ 64-áèòîâîãî êëþ÷à äîñòàòî÷íî áóäåò êëþ÷åâàÿ ôðàçà, ñîñòîÿùàÿ ïðèìåðíî èç 49 ñèìâîëîâ, èëè 10 îáû÷íûõ àíãëèéñêèõ ñëîâ. Â êà÷åñòâå ýìïèðè÷åñêîãî ïðàâèëà èñïîëüçóéòå ïÿòü ñëîâ äëÿ êàæäûõ 4 áàéòîâ êëþ÷à. Ýòî ïðåäïîëàãàåò ðàâíîìåðíîå ðàñïðåäåëåíèå ñèìâîëîâ, âêëþ÷àÿ ïðîáåëû è íåò íåóíèâåðñàëüíîãî ðåãèñòðà, ïðîáëåì è çíàêè ïóíêòóàöèè.

Ýòî ìåòîä òàêæå ìîæíî èñïîëüçîâàòü äëÿ ãåíåðàöèè çàêðûòûõ êëþ÷åé â êðèïòîãðàôè÷åñêèõ ñèñòåìàõ ñ îòêðûòûì êëþ÷àìè: òåêñòîâàÿ ñòðîêà ïðåîáðàçóåòñÿ â ñëó÷àéíóþ ñòàðòîâóþ ïîñëåäîâàòåëüíîñòü, à ýòà ïîñëåäîâàòåëüíîñòü ìîæåò áûòü èñïîëüçîâàíà â äåòåðìèíèðîâàííîé ñèñòåìå, ãåíåðèðóþùåé ïàðû òîêðûòûé êëþ÷/çàêðûòûé êëþ÷.

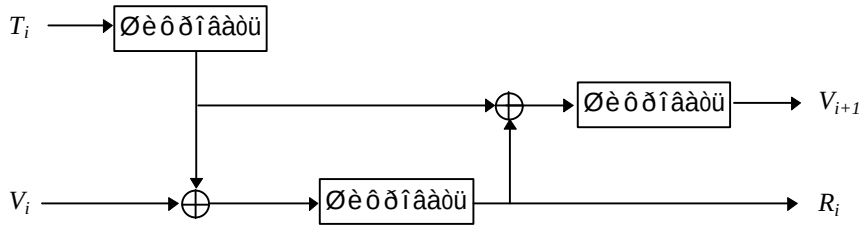
Âûáèðàÿ êëþ÷åâóþ ôðàçó, èñïîëüçóéòå ÷òî-íèáóäü óíèêàëüíîå è ëåãêî çàïîìèíàþùåñÿ. Íå âûáèðàéòå ôðàçû èç êíèã - ïðèìåð ñ "Ozymandias" â ýòî ìîìåíò. Ëåãêî äîñòóïíû è ìîãóò áûòü èñïîëüçîâàíû äëÿ âñêðûòèÿ ñî ñëîâàðåì è ñîáðàíèå ñî÷íåíèé Øåêñïèðà, è äèàëîãè èç *Çâåçäíûõ âîéí*. Âûáåðèòå ÷òî-íèáóäü òóïîå è ëè÷íîå. Íå çàáóäüòå î ïóíêòóàöèè è ïðåîáðàçîâàíèè ðåãèñòðà, åñëè âîçìîæíî âêëþ÷èòå ÷èñëà è íåàëôàâèòíûå ñèìâîëû. Ïëîõîé èëè èñêàæåííûé àíãëèéñêèé, èëè äàæå ëþáîé èíîñòðàííûé ÿçûê, äåëàåò êëþ÷åâóþ ôðàçó áîëåå óñòîé÷èâîé ê âñêðûòèþ ñî ñëîâàðåì. Îäíè èç ïðåäëîæåíèé ÿâëÿåòñÿ èñïîëüçîâàíèå ôðàçû, êîòîðàÿ ÿâëÿåòñÿ "ïîðÿñàþùåé åðóíäîé", ÷åì-òî òàêèì, ÷òî âû âðÿä ëè çàïîìíèòå è âðÿä ëè çàïèøåòå.

Íåñìîòðÿ íà âñå íàïèñàííîå çäåñü ìàñêèðîâêà íå çàìåíÿåò èñòèííóþ ñëó÷àéíîñòü. Ëó÷øèå ïàðîëüíûå ôðàçû ïîðîæäàþòñÿ èñïîëüçîâàíèåì êîñìè÷åñêèõ èñòî÷íèêîâ ýíòðîïèè, òàêèõ êàê ñòàòèñòèêà ðàñïàäà ðàäèîàêòèâíûõ àòîìîâ, èëè ïîäáðàñûâàíèå êîñòåé. Åñëè âû ïîëüçóåòåñü ãåíåðàòîðîì ïàðîëåé, óáåäèòåñü, ÷òî îí èñïîëüçóåò êðèïòîãðàôè÷åñêè áåçîïàñíûé èñòî÷íèê ýíòðîïèè, à íå ïñåâäîñëó÷àéíûé ãåíåðàòîð, èíèöèàëèçèðîâàííûé ïðåäñêàçóåìûì çíà÷åíèåì.

[1] ß Îçèìàíäèàñ, öàðü öàðåé. Âû, ñèëüíûå ìèðà ñåãî, ñìîòðèòå íà ìîè òðóäû è òåðÿéòåñü.

Ñòàíäàðò ãåíåðàöèè êëþ÷åé X9.17

Ñòàíäàðò ANSI X9.17 îïðåäåëÿåò ñïîñîá Ãåíåðàöèè êëþ÷åé (ñì. 7th) [55]. Îí íå ñîçäàåò ëåãêîãî çàïîìèíàþùèåñÿ êëþ÷è, è áîëüøå ïîäõîäèò äëÿ ãåíåðàöèè ñåàíñîâûõ êëþ÷åé èëè ïñåâäîñëó÷àéíûõ ÷èñåë â ñèñòåìå. Äëÿ ãåíåðàöèè êëþ÷åé èñïîëüçóåòñÿ êðèïòîãðàôè÷åñêèé äëîðèòì DES, íî îí ìîæåò áûòü ëåãêî çàìåíåí ëþáûì äðóãèì äëîðèòìîì.



Ðèñ. 8-1. Ãåíåðàöèÿ êëþ÷åé ANSI X9.17

Ïóñòü $E_K(X)$ - ýòî X, çàøèôðîâàííûé DES êëþ÷îì K, ñïåöèàëüíûì êëþ÷îì, ïðåäóñìîòðåííûì äëÿ ãåíåðàöèè ñåêðåòíûõ êëþ÷åé. V_0 - ýòî ñåêðåòíàÿ 64-áèòîâàÿ ñòàðòîâàÿ ïîñëåäîâàòåëüíîñòü. T - ýòî ìåòêà âðåìåíè. Äëÿ ãåíåðàöèè ñëó÷àéíîãî êëþ÷à R_i âû÷èñëèì:

$R_i = E_K(E_K(T_i) \oplus V_i)$

Äëÿ ãåíåðàöèè V_{i+1}, âû÷èñëèì:

$V_{i+1} = E_K(E_K(T_i) \oplus R_i)$

Äëÿ ïðåâðàùåíèÿ R_i â êëþ÷ DES, ïðîñòî óäàëèòå êàæäûé âîñüìîé áèò. Åñëè âàì íóæåí 64-áèòîâûé êëþ÷, èñïîëüçóéòå êëþ÷ áåç èçìåíåíèé. Åñëè âàì íóæåí 128-áèòîâûé êëþ÷, ñîçäàéòå ïàðó êëþ÷åé è îáúåäèíèòå èõ.

Ãåíåðàöèÿ êëþ÷åé â ìèíèñòåðſòâå îáîðîíû ÑØÀ

Ìèíèñòåðſòâî îáîðîíû ÑØÀ äëÿ ãåíåðàöèè ñëó÷àéíûõ êëþ÷åé ðåêîìåíäóåò èñïîëüçîâàòü DES â ðåæèìå OFB (ñì. ðàçäåë 9.8) [1144]. Ñîçäàâàéòå êëþ÷è DES, èñïîëüçóÿ ñèſòåìíûå âåêòîðà ïðåûäûſùèÿ, ðåãèſòðû ſîſòîÿíèÿ ſèſòåìû è ſèſòåìíûå ſ÷åſ÷èêè. Sîſäâàéòå âåêòîð èíèöèàëèçàöèè, èſïîëüçóÿ ſèſòåìíûå ſ÷àſû, èäåíòèôèêàòîð ſèſòåìû, ſ òàêæå äàòó è âðåìÿ. Äëÿ îòðûſòîſ òåſſòà èſïîëüçóéòå 64-áèòîâûå âåëè÷èſû, ſîçäàíſûå êåì-òî äðóãèì, íàïðèìåð, 8 ſèſâſëſâ, ââåäåíſûſ ſèſòåìſûſ àäìèíſòðàòſîſ. Èſïſëüçóéòå â êà÷åſòâå ſâſåſî êëþ÷à ðåçóëüòàò.

8.2 Íåëèíåéíûå ïðîñòðàíſòâà êëþ÷åé

Âſſáðàçèòå, ÷òſ âû - ýòſ âſåſíàÿ êðèſòſãðàôſ÷åſêàÿ ſðãàíèçàöèÿ, ſſçäàþùàÿ êðèſòſãðàôſ÷åſêèé ſſäóëü äëÿ âàøèſ âſéſê. Âû õſòèſå èſſïſëüçſſàòü áåçſïàſſíûé äëãſðèſ, íſ ſſſ áóäåò, åſëè àſïſàòàóðà ſſſïäåſ âſ âðàæåſêå ðóſè? Åſäü âû íå õſſòèſå, ſòſáû âàøè ſðèáſðû èſïſëüçſâàëſſü äëÿ çàùſòû *âðàæſêſè* ſåſðåſòſâ.

Åſëè âû ſſæåſå ſſſſåſòſòü âàø àëãſðſòſ â çàùſùåſſíſé ſſäóëü, òſ âſò, ÷òſ âû ſſæåſå ſäåëàòü. Sſòðåáóſòå, ÷òſáû ſſäóëü ſðàâſëſüſſ ðàáſòàſ òſëſüſ ſ êſþ÷àſſ ſſåſðàſòſſſ è ſåſðſòſſſ ôſðſû, à ſſ âſåſſ äóſàſſè êſþ÷àſſ äëÿ øſôſðſâſſíÿ ſſſïſëüçſâſëſÿ ſſſëüſſ ſſſëáſåſſíſé àëãſðſòſ. Sſæſſ ſäåëàòü òàê, ÷òſáû âåðſÿòſſſòü òſãſ, ÷òſ êòſ-òſ, íå çſàþùſé ýòſé ſſſåſëàëüſſſé ôſðſû, ſëó÷àſſſ íàòſſåòſÿ íà ſðàâſëüſûé êëþ÷, áûëà ſſ÷åçàþùå ſàëſé.

Sſſó÷ſàøåſſÿ ſðſſòðàſſòſâſ êëþ÷åé íàçûâàåòſÿ **ſſëſſſſſûſ**, ſſòſſ÷ó ÷òſ êëþ÷è íå ÿâſÿþòſÿ ſäſíſâſſâſ ſëſüſûſè. (Ïðſòſèſſſſſſæſûſ ÿâſÿåòſÿ ëſíåſíſå, èëſ ſëſñſſå, ſðſſòðàſſòſâſ êëþ÷åſ.) Ïðſſòſû ſſſſſáſſ äſáſèüſÿ ýſſãſ ſſæſíſ, ſſçäàâàÿ êëþ÷, ſſſòſſÿùſſſ èç äâóſ ÷àſòåſ: íåſſſðåäſòſâſſíſ êëþ÷à è íåſſſòſðſé ôſêſſèſſâſſíſé ſòſðſêſ, øſôſðſâſſíſſé ýſſſ êëþ÷ſ. Sſäóëü ðſſøſſôſðſâûſâſåſ ſòſðſêſ, ſſſſſſóé, ſſſſſóÿ êëþ÷. Åſëſ ðåçóſüſàſòſ ſêſçûſâſåſſÿ ôſêſſſſſſâſſíſÿ ſòſðſêſ, òſ êëþ÷ ſſſſſóſåſÿ êſâſ ſâû÷íſ, åſëſ íåſ, òſ ſſſſſóſåſſÿ äſóâſſ, ſſëſáûſ àëãſðſòſ. Åſëſ àëãſðſòſ ſſåſåſ 128-áſòſâſé êëþ÷ ſ 64-áſòſâſé ðàçſåſ áſſêà, òſ äëſſà ſſſſſâſ êëþ÷à - 192 áſòà. Òàſſſ ſâſàçſſ, ó äëãſðſòſà 2^{128} ýſôåſòſâſûſ êëþ÷à, íſ âåſſÿòſſſòü ſſóſ÷àſſſ âûáſàſſüſûé ſðàâſſüſûé ſſàſſſòſâſÿåſ ſſſòàâſüÿåſ ſâſè ſåáſ 2^{64}.

Âû ſſæåſå ſäåëàòü åſå õſſòðåå. Ìſæſſ ðàçðàſſòàſòü òàſſé àëãſðſòſ, ÷òſ ſåſſòſſðûå êëþ÷è áóäóſ ſſëüſſåå äðóãſſ. Ó àëãſðſòſà ſå áóäåſ ſëàáûſ êëþ÷åé - êëþ÷åé, ſſòſſðûå ſ ſ÷âſëäſſſòüþ ÿâſÿþòſÿ ſåäſſòàſòſ÷ſ çàſſſûſ - è òåſ ſå ſåſåå ó ſåſâ áóäåſ ſåëſſåſſſſ ſðſſòðàſſòſâſ êëþ÷åé.

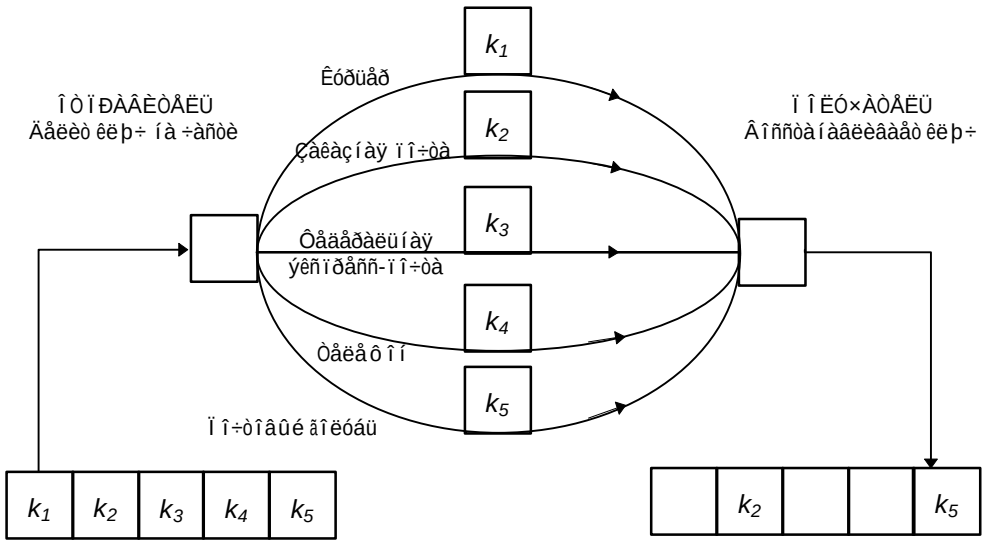
Ýòſ ðàſſòàſåſ òſëüſâ, åſëè ſſſïſëüçóſåſÿ ſäſðåðſòſûé àëãſðſòſ, ſſòſſðûé âðàã ſå ſſæåſ ſðåðſðſåſòſðſâàòü, ſëſ åſëſ ðàçſëſ÷ſå â ſſſëå êëþ÷åé äſſòàſſ÷ſſ òſſſſâ, ſ÷òſáû âðàã ſå ſſſâ ſ ſå ſäſãàäàòüſÿ. NSA ſðſſäåſûſâſâſ ýſſ ſ ſåðåðſſûſ ſ àëãſðſòſſàſ â ſâſſòſ ſſäóëÿſ Overtake (ſſ. ðàçäåë 25.1). Äåëàëè ëſ ſſſ òſ æå ſàſſå ſ Skipjack (ſſ. ðàçäåë 13.12)? Íåſçâåſòſſ.

8.3 Ïåðåäà÷à êëþ÷åé

Àëèñà è Áîá ñîáèðàþòñÿ äëÿ áåçîïàñíîé ñâÿçè èñïîëüçîâàòü ñèììåòðè÷íûé êðèïòîãðàôè÷åñêèé àëãîðèòì, èì íóæåí îáùèé êëþ÷. Àëèñà ãåíåðèðóåò êëþ÷, èñïîëüçóÿ ãåíåðàòîð ñëó÷àéíûõ êëþ÷åé. Òåïåðü îíà äîëæíà áåçîïàñíî ïåðåäàòü åãî Áîáó. Åñëè Àëèñà ñìîæåò ãàð-òî âñòðåòèòü Áîáà (êàêèå-íèáóäü çäâîðêè, êîíàòà áåç îêîí èëè îäíà èç ëóí Þ ïèòåðà), òî îíà ñìîæåò ïåðåäàòü åìó êîïèþ êëþ÷à. Â ïðîòèâíîì ñëó÷àå, ó íèõ åñòü ïðîáëåìà. Êðèïòîãðàôèÿ ñ îòêðûòûì êëþ÷àìè ðåøàåò ýòó ïðîáëåìó è ìíîãîìíîì ïðèìåíèìà ê ìíîãèì äðóãèì çàäà÷àì, íî ýòè ìåòîäû íå âñåãäà äîñòóïíû (ñì. ðàçäåë 3.1). Íåêîòîðûå ñèñòåìû èñïîëüçóþò äëüòåðíàòèâíûå êàíàëû, ñ÷èòàþùèåñÿ áåçîïàñíûìè. Àëèñà ìîãëà áû ïîñûëàòü Áîáó êëþ÷ ñ äîâåðåííûì ïîñûëüíûì. Îíà ìîãëà áû ïîñëàòü çàêàçíîé ïî÷òîé èëè íî÷íîé ñëóæáîé äîñòàâêè. Îíà ìîãëà áû óñòàíàâëèâàòü äóáëèêàò êàíàë ñâÿçè ñ Áîáîì è íàäåÿòüñÿ, ÷òî åãî òî íèêòî íå ïîäñëóøèâàåò. Îíà ìîãëà áû óñòàíîâèòü ñîâìåñòíûé ñåêðåò, èñïîëüçóåìûé äëÿ ãåíåðàöèè ñåññèîííûõ êëþ÷åé.

Ñòàíäàðò X9.17 [55] îïðåäåëÿåò äâà òèïà êëþ÷åé: **êëþ÷è øèôðîâàíèÿ êëþ÷åé** è **êëþ÷è äàííûõ**. Êëþ÷àìè øèôðîâàíèÿ êëþ÷åé ïðè ðàñïðåäåëåíèè øèôðóþòñÿ äóãèå êëþ÷è. Êëþ÷è äàííûõ øèôðóþò ñàìè ñîîáùåíèÿ. Êëþ÷è øèôðîâàíèÿ êëþ÷åé äîëæíû ðàñïðåäåëÿòüñÿ âðó÷íóþ, (õîòÿ îíè ìîãóò áûòü â áåçîïàñíîñòè â çàùèùåííîì îò âçëîìà óñòðîéñòâå, òàêîì êàê êðåäèòíàÿ êàðòî÷êà). íî äîñòàòî÷íî ðåäêî. Êëþ÷è äàííûõ ðàñïðåäåëÿþòñÿ ãîðàçäî ÷àùå. Ïîäõîäÿùèì ìåòîäîì ïåðåäà÷è êëþ÷åé ÷àñòî èñïîëüçóåòñÿ ïðè ðàñïðåäåëåíèè êëþ÷åé.

Äðóãèì ðåøåíèåì ïðîáëåìû ðàñïðåäåëåíèÿ ÿâëÿþòñÿ ðàçáèåíèå êëþ÷à íà íåñêîëüêî ðàçëè÷íûõ ÷àñòåé (ñì. ðàçäåë 3.6) è ïåðåäà÷à èõ ïî ðàçëè÷íûì êàíàëàì. Îäíà ÷àñòü ìîæåò áûòü ïîñëàíà òåëåôîíîì, äðóãàÿ - ïî÷òîé, òðåòüÿ - ñëóæáîé íî÷íîé äîñòàâêè, ÷åòâåðòàÿ - ïî÷òîâûì ãîëóáåì, è òàê äàëåå, (ñì. 6-é). Òàê ïðîòèâíèê ìîæåò ñîáðàòü âñå ÷àñòè, êðîìå îäíîé, è âñå ðàâíî íè÷åãî íå óçíàåò ïðî êëþ÷. Ýòîò ìåòîä áóäåò ðàáîòàòü âî âñåõ ñëó÷àÿõ, êðîìå êðàéíèõ. Â ðàçäåëå 3.6 îáñóæäàþòñÿ ñõåìû ðàçáèåíèÿ êëþ÷à íà íåñêîëüêî ÷àñòåé, (ñì. ðàçäåë 3.7), ÷òî äàñò âîçìîæíîñòü Áîáó âîññòàíàâëèâàòü êëþ÷, åñëè íåêîòîðûå èç ÷àñòåé ïîòåðÿíû ïðè ïåðåäà÷å.



Ðèñ. 8-2. Ðàñïðåäåëåíèå êëþ÷åé ïî ïàðàëëåëüíûì êàíàëàì.

Àëèñà áåçîïàñíî ïåðåäàåò Áîáó êëþ÷ øèôðîâàíèÿ êëþ÷åé èëè ïðè ëè÷íîé âñòðå÷å, èëè ñ ïîìîùüþ òîëüêî ÷òî ðàññìîòðåííîé ìåòîäèêè ðàçáèåíèÿ. Êàê òîëüêî è ó Àëèñû, è ó Áîáà áóäåò êëþ÷ øèôðîâàíèÿ êëþ÷åé, Àëèñà ñìîæåò ïîñûëàòü Áîáó êëþ÷è äàííûõ íà äåíü ïî òîìó æå ñàìîìó êàíàëó ñâÿçè, øèôðóÿ ïðè ýòîì êàæäûé êëþ÷ äàííûõ êëþ÷îì øèôðîâàíèÿ êëþ÷åé. Òàê êàê òðàôèêà, øèôðóåìûé êëþ÷îì øèôðîâàíèÿ êëþ÷åé íåçíà÷èòåëåí, òî ýòîò êëþ÷ ÷àñòî ìåíÿòü íå íóæíî. Îäíàêî, òàê êàê êîìïðîìåòàöèÿ êëþ÷à øèôðîâàíèÿ êëþ÷åé ìîæåò ñêîìïðîìåòèðîâàòü âñå ñîîáùåíèÿ, øèôðîâàííûå ñëåäóþùèì êëþ÷àìè äíåé, òîòôûå áûëè çàøèôðîâàí ýòèì êëþ÷îì øèôðîâàíèÿ êëþ÷åé, ýòîò êëþ÷ äîëæåí õðàíèòüñÿ â áåçîïàñíîñòè. Òàê êàê êàæäàÿ ïàðà ïîëüçîâàòåëåé äîëæíà

Ðàñïðåäåëåíèå êëþ÷åé â áîëüøèõ ñåòÿõ

îáìåíÿòüñÿ êëþ÷àìè, îáùåå ÷èñëî îáìåíîâ êëþ÷àìè â ñåòè èç n ÷åëîâåê ðàâíî n(n - l)/2.

Â ñåòè c øåñòüþ ïîëüçîâàòåëÿìè ïîòðåáóåòñÿ 15 îáìåíîâ êëþ÷àìè. Â ñåòè èç 1000 ïîëüçîâàòåëåé ïîíàäîáèòñÿ óæå îêîëî 500000 îáìåíîâ êëþ÷àìè. Â ýòèõ ñëó÷àÿõ ðàáîòà ñåòè ãîðàçäî áîëåå ýôôåêòèâíà ïðè èñïîëüçîâàíèè öåíòðàëüíîãî ñåðâåðà (èëè ñåðâåðîâ) êëþ÷åé.

Êðîìå òîãî, ëþáîé èç ïðîòîêîëîâ ñèììåòðè÷íîé êðèïòîãðàôèè èëè êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè, ïðèâåäåííûõ â ðàçäåëå 3.1, ïîäõîäèò äëÿ áåçîïàñíîãî ðàñïðåäåëåíèÿ êëþ÷åé.

8.4 Ïðîâåðêà êëþ÷åé

Êàê Áîá óçíàåò, ïîëó÷èâ êëþ÷, ÷òî êëþ÷ ïåðåäàí Àëèñîé, à íå êåì-òî äðóãèì, êòî âûäàåò ñåáÿ çà Àëèñó? Âñå ïðîñòî, åñëè Àëèñà ïåðåäàåò åìó êëþ÷ ïðè ëè÷íîé âñòðå÷å. Åñëè Àëèñà ïîñûëàåò ñâîé êëþ÷ ÷åðåç äîâåðåííîãî êóðüåðà, òî êóðüåðó äîëæåí äîâåðÿòü è Áîá. Åñëè êëþ÷ çàøèôðîâàí êëþ÷îì øèôðîâàíèÿ êëþ÷åé, òî Áîá äîëæåí äîâåðÿòü òîìó, ÷òî ýòîò êëþ÷ øèôðîâàíèÿ êëþ÷åé åñòü òîëüêî ó Àëèñû. Åñëè äëÿ ïîäïèñè êëþ÷à Àëèñà èñïîëüçóåò ïðîòîêîë ýëåêòðîííîé ïîäïèñè, Áîá ïðè ïðîâåðêå ïîäïèñè äîëæåí äîâåðÿòü áàçå äàííûõ îòêðûòûõ êëþ÷åé,. (Åìó òàêæå ïðèäåòñÿ ñ÷èòàòü, ÷òî Àëèñà ñîõðàíèëà ñâîé êëþ÷ â áåçîïàñíîñòè.) Åñëè Öåíòð ðàñïðåäåëåíèÿ êëþ÷åé (Key Distribution Center, KDC) ïîäïèñûâàåò îòêðûòûé êëþ÷ Àëèñû, Áîá äîëæåí ñ÷èòàòü, ÷òî åãî êîïèÿ îòêðûòîãî êëþ÷à KDC íå áûëà ïîäìåíåíà.

Íàêîíåö, òîò, êòî óïðàâëÿåò âñåé ñåòüþ âîêðóã Áîáà, ìîæåò çàñòàâèòü åãî äóìàòü âñå, ÷òî åìó õî÷åòñÿ. Ìýëëîðè ìîæåò ïîñëàòü øèôðîâàííîå è ïîäïèñàííîå ñîîáùåíèå, âûäàâàÿ ñåáÿ çà Àëèñó. Êîãäà Áîá, ïðîâåðÿÿ ïîäïèñü Àëèñû, îáðàòèòñÿ ê áàçå äàííûõ îòêðûòûõ êëþ÷åé, Ìýëëîðè ìîæåò âîçâðàòèòü åìó ñîáñòâåííûé îòêðûòûé êëþ÷. Ìýëëîðè ìîæåò ñîçäàòü ñâîé ñîáñòâåííûé ïîääåëüíûé KDC è ïîäìåíèòü îòêðûòûé êëþ÷ íàñòîÿùåãî KDC êëþ÷îì ñâîåãî ñîáñòâåííîãî èçäåëèÿ. Áîá íèêàê íå ñìîæåò ýòî îáíàðóæèòü.

Íåêîòîðûå ëþäè èñïîëüçîâàëè ýòîò àðãóìåíò, óòâåðæäàÿ, ÷òî êðèïòîãðàôèÿ ñ îòêðûòûìè êëþ÷àìè áåñïîëåçíà. Òàê êàê åäèíñòâåííûé ñïîñîá Àëèñå è Áîáó çíàòü íàâåðíÿêà, ÷òî íèêòî íå âçëîìàë èõ êëþ÷è, - ýòî ëè÷íàÿ âñòðå÷à, òî êðèïòîãðàôèÿ ñ îòêðûòûìè êëþ÷àìè âîîáùå íå îáåñïå÷èâàåò áåçîïàñíîñòü.

Ýòà òî÷êà çðåíèÿ íàèâíà. Òåîðåòè÷åñêè âñå ïðàâèëüíî, íî äåéñòâèòåëüíîñòü ãîðàçäî ñëîæíåå. Êðèïòîãðàôèÿ ñ îòêðûòûìè êëþ÷àìè, èñïîëüçóåìàÿ âìåñòå ñ ýëåêòðîííûìè ïîäïèñÿìè è íàäåæíûìè KDC, ñèëüíî óñëîæíÿåò ïîäìåíó îäíèì êëþ÷îì äðóãîãî. Áîá íèêîãäà íå ìîæåò áûòü àáñîëþòíî óâåðåí, ÷òî Ìýëëîðè íå êîíòðîëèðóåò åãî ðåàëüíîñòü ïîëíîñòüþ, íî Áîá ìîæåò çíàòü íàâåðíÿêà, ÷òî òàêàÿ ïîäìåíà ðåàëüíîñòè ïîòðåáóåò ãîðàçäî áîëüøå ðåñóðñîâ, ÷åì ñìîæåò çàïîëó÷èòü ðåàëüíûé Ìýëëîðè.

Áîá ìîã áû òàêæå ïðîâåðÿòü êëþ÷ Àëèñû ïî òåëåôîíó, ïîëó÷èâ âîçìîæíîñòü óñëûøàòü åå ãîëîñ. Ðàñïîçíàâàíèå ãîëîñà äåéñòâèòåëüíî ÿâëÿåòñÿ õîðîøåé ñõåìîé èäåíòèôèêàöèè. Åñëè ðå÷ü èäåò î îòêðûòîì êëþ÷å, îí ìîæåò áåçîïàñíî ïîâòîðèòü åãî äàæå ïðè óãðîçå ïîäñëóøèâàíèÿ. Åñëè ýòî ñåêðåòíûé êëþ÷, îí ìîæåò èñïîëüçîâàòü äëÿ ïðîâåðêè êëþ÷à îäíîñòîðîííþþ õýø-ôóíêöèþ. Îáà TSD PGP (ñì. ðàçäåë 24.12.) è AT$T (ñì. Ðàçäåë 24.18) èñïîëüçóþò ýòîò ñïîñîá ïðîâåðêè êëþ÷åé.

Èíîãäà ìîæåò äàæå íå âàæíî òî÷íî ïðîâåðÿòü, êîìó ïðèíàäëåæèò îòêðûòûé êëþ÷. Ìîæåò ïîíàäîáèòüñÿ ïðîâåðèòü, ÷òî îí ïðèíàäëåæèò òîìó æå ÷åëîâåêó, ÷òî è ãîä íàçàä. Åñëè êòî-òî ïîñûëàåò áàíêó ïîäïèñàííîå ñîîáùåíèå î ïåðåâîäå äåíåã, áàíê íå äîëæåí áåñïîêîèòüñÿ î òîì, êòî êîíêðåòíî ñíèìåò äåíüãè, à òîëüêî î òîì, ÷òîáû ýòîò ÷åëîâåê áûë òåì, êòî âíåñ äåíüãè â ïåðâûé ðàç.

Îáíàðóæåíèå îøèáîê ïðè ïåðåäà÷å êëþ÷åé

Èíîãäà êëþ÷è èñêàæàþòñÿ ïðè ïåðåäà÷å. Ýòî ÿâëÿåòñÿ ïðîáëåìîé, òàê êàê èñêàæåííûé êëþ÷ ìîæåò ïðèâåñòè ê ìåãàáàéòàì íåðàñøèôðîâàííîãî øèôðîòåêñòà. Âñå êëþ÷è äîëæíû ïåðåäàâàòüñÿ ñ îáíàðóæåíèåì îøèáîê è èñïðàâëåíèåì áèòîâ. Òàêèì îáðàçîì îøèáêè ïðè ïåðåäà÷å ìîãóò áûòü ëåãêî îáíàðóæåíû è, åñëè ïîòðåáóåòñÿ, êëþ÷ ìîæåò áûòü ïîñëàí åùå ðàç.

Îäíèì èç íàèáîëåå øèðîêî èñïîëüçóåìûõ ìåòîäîâ ÿâëÿåòñÿ øèôðîâàíèå êëþ÷îì íåêîòîðîé ïîñòîÿííîé âåëè÷èíû è ïåðåäà÷à ïåðâûõ 2-4 áàéò ýòîãî øèôðîòåêñòà âìåñòå ñ êëþ÷îì. Ó ïîëó÷àòåëÿ äåëàåòñÿ òî æå ñàìîå. Åñëè øèôðîâàííûå êîíñòàíòû ñîâïàäàþò, òî êëþ÷ áûë ïåðåäàí áåç îøèáêè. Âåðîÿòíîñòü îøèáêè íàõîäèòñÿ â äèàïàçîíå îò $1/2^{16}$ äî $1/2^{32}$.

Îáíàðóæåíèå îøèáîê ïðè äåøèôðèðîâàíèè

Èíîãäà ïîëó÷àòåëü õî÷åò ïðîâåðèòü, ÿâëÿåòñÿ ëè åãî êîíêðåòíûé êëþ÷ ïðàâèëüíûì êëþ÷îì ñèììåòðè÷íîãî äåøèôðèðîâàíèÿ. Åñëè îòêðûòûé òåêñò ñîîáùåíèÿ ïðåäñòàâëÿåò ñîáîé ÷òî-òî ïîõîæåå íà ASCII, îí ìîæåò ïîïûòàòüñÿ ðàñøèôðîâàòü è ïðî÷èòàòü ñîîáùåíèå. Åñëè îòêðûòûé òåêñò ñëó÷àåí, òî ñóùåñòâóþò äðóãèå ïðèåìû.

Íàèâíûì ïîäõîäîì ÿâëÿåòñÿ ïðèñîåäèíåíèå ê îòêðûòîìó òåêñòó äî øèôðîâàíèÿ **ïðîâåðî÷íîãî áëîêà** - èçâåñòíîãî çàãîëîâêà. Ïîëó÷àòåëü Áîá ðàñøèôðîâûâàåò çàãîëîâîê è ïðîâåðÿåò, ÷òî îí ïðàâèëåí. Ýòî ðàáîòàåò, íî äàåò Åâå èçâåñòíûé êóñî÷åê îòêðûòîãî òåêñòà, ÷òî ïîìîãàåò åé êðèïòîàíàëèçèðîâàòü ñèñòåìó. Ýòî òàêæå îá-

ëåã÷àåò âñêðûòèå øèôðîâ ñ êîðîòêèì êëþ÷îì, òàêèõ êàê DES è âñå ýêñïîðòèðóåìûå øèôðû. Ðàññ÷èòàéòå çàðàíåå îäèí ðàç äëÿ êàæäîãî êëþ÷à ïðîâåðî÷íóþ ñóììó, çàòåì èñïîëüçóéòå ýòó ïðîâåðî÷íóþ ñóììó äëÿ îïðåäåëåíèÿ êëþ÷à â ëþáîì ñîîáùåíèè, êîòîðîå âû ïåðåõâàòèëè ïîñëå ýòîãî. *Ëþáàÿ* ïðîâåðî÷íàÿ ñóììà êëþ÷à, â êîòîðóþ íå âêëþ÷åíû ñëó÷àéíûå èëè, ïî êðàéíåé ìåðå, ðàçëè÷íûå äàííûå, îáëàäàåò ýòèì ñâîéñòâîì. Ïî èäåå ýòî î÷åíü ïîõîæå íà ãåíåðàöèþ êëþ÷åé ïî êëþ÷åâûì ôðàçàì.

Âîò äëÿ ýòîãî ñïîñîá ïîëó÷øå [821]:

(1) Ñãåíåðèòå âåêòîð èäåíòèôèêàöèè (îòëè÷íûé îò èñïîëüçóåìîãî â ñîîáùåíèè).

(2) Èñïîëüçóéòå ýòîò âåêòîð èäåíòèôèêàöèè äëÿ ãåíåðàöèè áîëüøîãî áëîêà áèòîâ: ñêàæåì, 512.

(3) Õýøèðóéòå ðåçóëüòàò.

(4) Èñïîëüçóéòå òå æå ôèêñèðîâàííûå áèòû õýø-çíà÷åíèÿ, ñêàæåì, 32, äëÿ êîíòðîëüíîé ñóììû êëþ÷à.

Ýòî òîæå äàåò Åâå êàêóþ-òî èíôîðìàöèþ, íî î÷åíü íåáîëüøóþ. Åñëè îíà ïîïûòàåòñÿ èñïîëüçîâàòü ìëàäøèå 32 áèòà êîíå÷íîãî õýø-çíà÷åíèÿ äëÿ âñêðûòèÿ ãðóáîé ñèëîé, åé ïðèäåòñÿ äëÿ êàæäîãî âåðîÿòíîãî êëþ÷à âûïîëíèòü íåñêîëüêî øèôðîâàíèé è õýøèðîâàíèå, âñêðûòèå ãðóáîé ñèëîé ñàìîãî êëþ÷à îêàæåòñÿ áûñòðåå.

Îíà íå ïîëó÷èò äëÿ ïðîâåðêè íèêàêèõ èçâåñòíûõ êóñî÷êîâ îòêðûòîãî òåêñòà, è äàæå åñëè îíà ñóìååò ïîäîáðàòü íàì íàøå æå ñëó÷àéíîå çíà÷åíèå, îíà íèêîãäà íå ïîëó÷èò îò íàñ âûáðàííûé îòêðûòûé òåêñò, òàê êàê îí áóäåò ïðåîáðàçîâàí õýø-ôóíêöèåé ïðåæäå, ÷åì îíà åãî óâèäèò.

8.5 Èñïîëüçîâàíèå êëþ÷åé

Ïðîãðàììíîå øèôðîâàíèå ðèñêîâàííî. Óøëè òå äíè, êîãäà ïðîñòûå ìèêðîêîìïüþòåðû ðàáîòàëè ïîä óïðàâëåíèåì åäèíñòâåííîé ïðîãðàììû. Ñåãîäíÿ âðåìÿ Macintosh System 7, Windows NT è UNIX. Íåâîçìîæíî ñêàçàòü, êîãäà îïåðàöèîííàÿ ñèñòåìà îñòàíîâèò ðàáîòàþùóþ ïðîãðàììó øèôðîâàíèÿ, çàïèøåò âñå íà äèñê è ðàçðåøèò âûïîëíÿòüñÿ êàêîé-òî äðóãîé çàäà÷å. Êîãäà îïåðàöèîííàÿ ñèñòåìà, íàêîíåö, âåðíåòñÿ ê øèôðîâàíèþ, ÷òîáû òàì íå øèôðîâàëîñü, êàðòèíêà ìîæåò îêàçàòüñÿ âåñüìà çàáàâíîé. Îïåðàöèîííàÿ ñèñòåìà çàïèñàëà ïðîãðàììó øèôðîâàíèÿ íà äèñê, è êëþ÷ çàïèñàí âìåñòå ñ íåé. Êëþ÷, íåçàøèôðîâàííûé, áóäåò ëåæàòü íà äèñêå, ïîêà êîìïüþòåð íå íàïèøåò ÷òî-íèáóäü â ýòó æå îáëàñòü ïàìÿòè ïîâåðõ. Ýòî ìîæåò ñëó÷èòüñÿ ÷åðåç íåñêîëüêî ìèíóò, à ìîæåò ÷åðåç íåñêîëüêî ìåñÿöåâ. Ýòîãî ìîæåò è íèêîãäà íå ñëó÷èòüñÿ, íî êëþ÷ âñå æå ìîæåò îêàçàòüñÿ íà äèñêå â òîò ìîìåíò, êîãäà æåñòêèé äèñê ãóñòî ïðî÷åñûâàåòñÿ âàøèì ïðîòèâíèêîì. Â ïðèîðèòåòíîé, ìíîãîçàäà÷íîé ñðåäå, äëÿ øèôðîâàíèÿ ìîæíî óñòàíîâèòü äîñòàòî÷íî âûñîêèé ïðèîðèòåò, ÷òîáû ýòà îïåðàöèÿ íå ïðåðûâàëàñü. Ýòî ñíèçèëî áû ðèñê. Äàæå ïðè ýòîì ñèñòåìà â öåëîì â ëó÷øåì ñëó÷àå íåíàäåæíà.

Àïïàðàòíûå ðåàëèçàöèè áåçîïàñíåå. Ìíîãèå èç óñòðîéñòâ øèôðîâàíèÿ ðàçðàáîòàíû òàê, ÷òîáû ëþáîå âìåøàòåëüñòâî ïðèâîäèëî áû ê óíè÷òîæåíèþ êëþ÷à. Íàïðèìåð, â ïëàòå øèôðîâàíèÿ äëÿ IBM PS/2 çàëèòûé ýïîêñèäíîé ñìîëîé ìîäóëü ñîäåðæèò ìèêðîñõåìó DES, áàòàðåþ è ïàìÿòü. Êîíå÷íî, Âû äîëæíû âåðèòü, ÷òî ïðîèçâîäèòåëü àïïàðàòóðû ïðàâèëüíî ðåàëèçîâàë âñå íåîáõîäèìûå ñâîéñòâà.

Ðÿä êîììóíèêàöèîííûõ ïðèëîæåíèé, íàïðèìåð, òåëåôîííûå øèôðàòîðû, ìîãóò èñïîëüçîâàòü **ñåàíñîâûå êëþ÷è**. Ñåàíñîâûì íàçûâàåòñÿ êëþ÷, êîòîðûé èñïîëüçóåòñÿ òîëüêî äëÿ îäíîãî ñåàíñà ñâÿçè - åäèíñòâåííîãî òåëåôîííîãî ðàçãîâîðà - è çàòåì óíè÷òîæàåòñÿ. Íåò ñìûñëà õðàíèòü êëþ÷ ïîñëå òîãî, êàê îí áûë èñïîëüçîâàí. È åñëè âû èñïîëüçóåòå äëÿ ïåðåäà÷è êëþ÷à îò îäíîãî àáîíåíòà äðóãîìó íåêîòîðûé ïðîòîêîë îáìåíà êëþ÷àìè, òî ýòîò êëþ÷ íå íóæíî õðàíèòü è ïåðåä åãî èñïîëüçîâàíèåì. Ýòî çíà÷èòåëüíî ñíèæàåò âåðîÿòíîñòü êîìïðîìåòàöèè êëþ÷à.

Êîíòðîëü èñïîëüçîâàíèÿ êëþ÷åé

Â íåêîòîðûõ ïðèëîæåíèÿõ ìîæåò ïîòðåáîâàòüñÿ êîíòðîëèðîâàòü ïðîöåññ èñïîëüçîâàíèÿ ñåàíñîâîãî êëþ÷à. Íåêîòîðûì ïîëüçîâàòåëÿì ñåàíñîâûå êëþ÷è íóæíû òîëüêî äëÿ øèôðîâàíèÿ èëè òîëüêî äëÿ äåøèôðèðîâàíèÿ. Ñåàíñîâûå êëþ÷è ìîãóò áûòü ðàçðåøåíû ê èñïîëüçîâàíèþ òîëüêî íà îïðåäåëåííîé ìàøèíå èëè òîëüêî â îïðåäåëåííîå âðåìÿ. Ïî îäíîé èç ñõåì óïðàâëåíèÿ ïîäîáíûìè îãðàíè÷åíèÿìè ê êëþ÷ó äîáàâëÿåòñÿ **âåêòîð êîíòðîëÿ** (Control Vector, CV), âåêòîð êîíòðîëÿ îïðåäåëÿåò äëÿ ýòîãî êëþ÷à îãðàíè÷åíèÿ åãî èñïîëüçîâàíèÿ (ñì. ðàçäåë 24.1) [1025, 1026]. Ýòîò CV õýøèðóåòñÿ, à çàòåì äëÿ íåãî è ãëàâíîãî êëþ÷à âûïîëíÿåòñÿ îïåðàöèÿ XOR. Ðåçóëüòàò èñïîëüçóåòñÿ êàê êëþ÷ øèôðîâàíèÿ äëÿ øèôðîâàíèÿ ñåàíñîâîãî êëþ÷à. Ïîëó÷åííûé ñåàíñîâûé êëþ÷ çàòåì õðàíèòñÿ âìåñòå ñ CV. Äëÿ âîññòàíîâëåíèÿ ñåàíñîâîãî êëþ÷à íóæíî õýøèðîâàòü CV è âûïîëíèòü äëÿ íåãî è ãëàâíîãî êëþ÷à îïåðàöèþ XOR. Ïîëó÷åííûé ðåçóëüòàò èñïîëüçóåòñÿ äëÿ äåøèôðèðîâàíèÿ øèôðîâàííîãî ñåàíñîâîãî êëþ÷à.

Ïðåèìóùåñòâà ýòîé ñõåìû â òîì, ÷òî äëèíà CV ìîæåò áûòü ïðîèçâîëüíîé, è ÷òî CV âñåãäà õðàíèòñÿ â îòêðûòîì âèäå âìåñòå ñ øèôðîâàííûì êëþ÷îì. Òàêàÿ ñõåìà íå âûäâèãàåò òðåáîâàíèé îòíîñèòåëüíî óñòîé÷èâîñòè àïïàðàòóðû ê âçëîìó è ïðåäïîëàãàåò îòñóòñòâèå íåïîñðåäñòâåííîãî äîñòóïà ïîëüçîâàòåëåé ê êëþ÷àì. Ýòà ñèñòåìà ðàññìàòðèâàåòñÿ íèæå â ðàçäåëàõ 24.1 è 24.8.

8.6 Îáíîâëåíèå êëþ÷åé

Ïðåäñòàâüòå ñåáå øèôðîâàííûé êàíàë ïåðåäà÷è äàííûõ, äëÿ êîòîðîãî âû õîòèòå ìåíÿòü êëþ÷è êàæäûé äåíü. Èíîãäà åæåäíåâíîå ðàñïðåäåëåíèå íîâûõ êëþ÷åé ÿâëÿåòñÿ íåëåãêîé çàáîòîé. Áîëåå ïðîñòîå ðåøåíèå - ãåíåðèðîâàòü íîâûé êëþ÷ èç ñòàðîãî, òàêàÿ ñõåìà èíîãäà íàçûâàåòñÿ **îáíîâëåíèåì êëþ÷à**.

Âñå, ÷òî íóæíî - ýòî îäíîíàïðàâëåííàÿ ôóíêöèÿ. Åñëè Àëèñà è Áîá èñïîëüçóþò îáùèé êëþ÷ è ïðèìåíÿþò ê íåìó îäíó è òó æå îäíîíàïðàâëåííóþ ôóíêöèþ, îíè ïîëó÷àò îäèíàêîâûé ðåçóëüòàò. Îíè ìîãóò âûáðàòü èç ðåçóëüòàòà íóæíûå èì áèòû è ñîçäàòü íîâûé êëþ÷.

Îáíîâëåíèå êëþ÷åé ðàáîòàåò, íî ïîìíèòå, ÷òî áåçîïàñíîñòü íîâîãî êëþ÷à îïðåäåëÿåòñÿ áåçîïàñíîñòüþ ñòàðîãî êëþ÷à. Åñëè Åâå óäàñòñÿ çàïîëó÷èòü ñòàðûé êëþ÷, îíà ñìîæåò âûïîëíèòü îáíîâëåíèå êëþ÷åé ñàìîñòîÿòåëüíî. Îäíàêî, åñëè ñòàðîãî êëþ÷à ó Åâû íåò, è îíà ïûòàåòñÿ âûïî îòíîøåíèþ ê øèôðîâàííîìó òðàôèêó ïîëíèòü âñêðûòèå ñ èñïîëüçîâàíèåì òîëüêî øèôðîòåêñòà, îáíîâëåíèå êëþ÷åé ÿâëÿåòñÿ õîðîøèì ñïîñîáîì çàùèòû äëÿ Àëèñû è Áîáà.

8.7 Õðàíåíèå êëþ÷åé

Íàèìåíåå ñëîæíûìè ïðè õðàíåíèè êëþ÷åé ÿâëÿþòñÿ ïðîáëåìû îäíîãî ïîëüçîâàòåëÿ, Àëèñû, øèôðóþùåé ôàéëû äëÿ ïîñëåäóþùåãî èñïîëüçîâàíèÿ. Òàê êàê îíà ÿâëÿåòñÿ åäèíñòâåííûì äåéñòâóþùèì ïîëüçîâàòåëåì ñèñòåìû, òîëüêî îíà è îòâå÷àåò çà êëþ÷. Â íåêîòîðûõ ñèñòåìàõ èñïîëüçóåòñÿ ïðîñòîé ïîäõîä: êëþ÷ õðàíèòñÿ â ãîëîâå Àëèñû è áîëüøå íèãäå. Ýòî ïðîáëåìû Àëèñû - ïîìíèòü êëþ÷ è ââîäèòü åãî âñÿêèé ðàç, êîãäà åé íóæíî çàøèôðîâàòü èëè ðàñøèôðîâàòü ôàéë.

Ïðèìåðîì òàêîé ñèñòåìû ÿâëÿåòñÿ IPS [881]. Ïîëüçîâàòåëè ìîãóò ëèáî ââîäèòü 64-áèòîâûé êëþ÷ íåïîñðåäñòâåííî, ëèáî ââåñòè êëþ÷ êàê áîëåå äëèííóþ ñèìâîëüíóþ ñòðîêó. Â ïîñëåäíåì ñëó÷àå ñèñòåìà ãåíåðèðóåò 64-áèòîâûé êëþ÷ ïî ñòðîêå ñèìâîëîâ, èñïîëüçóÿ òåõíèêó ïåðåìàëûâàíèÿ êëþ÷à.

Äðóãèì ðåøåíèåì ÿâëÿåòñÿ õðàíèòü êëþ÷ â âèäå êàðòî÷êè ñ ìàãíèòíîé ïîëîñêîé, ïëàñòèêîâîãî êëþ÷à ñ âñòðîåííîé ìèêðîñõåìîé ROM (íàçûâàåìîãî **ROM-êëþ÷**) èëè èíòåëëåêòóàëüíîé êàðòî÷êè [556, 557, 455]. Ïîëüçîâàòåëü ìîæåò ââåñòè ñâîé êëþ÷ â ñèñòåìó, âñòàâèâ ôèçè÷åñêèé íîñèòåëü â ñ÷èòûâàþùåå óñòðîéñòâî, âñòðîåííîå â åãî øèôðîâàòåëü èëè ïîäêëþ÷åííîå ê êîìïüþòåðíîìó òåðìèíàëó. Õîòÿ ïîëüçîâàòåëü ìîæåò èñïîëüçîâàòü êëþ÷, îí íå çíàåò åãî è íå ìîæåò åãî ñêîìïðîìåòèðîâàòü. Îí ìîæåò èñïîëüçîâàòü åãî òîëüêî òåì ñïîñîáîì è òîëüêî äëÿ òåõ öåëåé, êîòîðûå îïðåäåëåíû âåêòîðîì êîíòðîëÿ.

ROM-êëþ÷ - ýòî î÷åíü óìíàÿ èäåÿ. Ïðàêòè÷åñêè ëþáîé ñïîñîáåí îñîçíàòü, ÷òî òàêîå ôèçè÷åñêèé êëþ÷, êàêîâî åãî çíà÷åíèå, è êàê åãî çàùèòèòü. Ïðèäàíèå êðèïòîãðàôè÷åñêîìó êëþ÷ó íåêîòîðîé ôèçè÷åñêîé ôîðìû äåëàåò õðàíåíèå è çàùèòó òàêîãî êëþ÷à èíòóèòèâíî áîëåå ïîíÿòíûìè.

Ýòà òåõíèêà ñòàíîâèòñÿ áîëåå áåçîïàñíîé ïðè ðàçáèåíèè êëþ÷à íà äâå ïîëîâèíû, îäíà èç êîòîðûõ õðàíèòñÿ â òåðìèíàëå, à âòîðàÿ - â ROM-êëþ÷å. Òàê ðàáîòàåò áåçîïàñíûé òåëåôîí STU-III ïðàâèòåëüñòâà ÑØÀ. Ïîòåðÿ ROM-êëþ÷à íå êîìïðîìåòèðóåò êðèïòîãðàôè÷åñêèé êëþ÷ - çàìåíèòå ýòîò êëþ÷ è âñå ñíîâà ñòàíåò íîðìàëüíî. Òî æå ïðîèñõîäèò è ïðè ïîòåðå òåðìèíàëà. Ñëåäîâàòåëüíî, êîìïðîìåòàöèÿ ROM-êëþ÷à èëè ñèñòåìû íå êîìïðîìåòèðóåò êðèïòîãðàôè÷åñêèé êëþ÷ key - âðàãó íóæíî çàïîëó÷èòü îáå ÷àñòè.

Êëþ÷è, êîòîðûå òðóäíî çàïîìíèòü ìîæíî õðàíèòü çàøèôðîâàííûìè, èñïîëüçóÿ ÷òî-òî ïîõîæåå íà êëþ÷ øèôðîâàíèÿ êëþ÷åé. Íàïðèìåð, çàêðûòûé êëþ÷ RSA ìîæåò áûòü çàøèôðîâàí êëþ÷îì DES è çàïèñàí íà äèñê. Äëÿ âîññòàíîâëåíèÿ êëþ÷à RSA ïîëüçîâàòåëü áóäåò äîëæåí ââåñòè êëþ÷ DES â ïðîãðàììó äåøèôðèðîâàíèÿ.

Åñëè êëþ÷è ãåíåðèðóþòñÿ äåòåðìèíèðîâàííî (ñ ïîìîùüþ êðèïòîãðàôè÷åñêè áåçîïàñíîãî ãåíåðàòîðà ïñåâäîñëó÷àéíûõ ïîñëåäîâàòåëüíîñòåé), ìîæåò áûòü ïðè ïîìîùè ëåãêî çàïîìèíàþùåãîñÿ ïàðîëÿ ëåã÷å ãåíåðèðîâàòü êëþ÷è ïîâòîðíî âñÿêèé ðàç, êîãäà îíè ïîíàäîáÿòñÿ.

Â èäåàëå, êëþ÷ íèêîãäà íå äîëæåí îêàçûâàòüñÿ âíå øèôðîâàëüíîãî óñòðîéñòâà â íåçàøèôðîâàííîì âèäå. Ýòà öåëü íå âñåãäà äîñòèæèìà, íî ê ýòîìó íóæíî ñòðåìèòüñÿ.

8.8 Ðåçåðâíûå êëþ÷è

Àëèñà ðàáîòàåò ãëàâíûì ôèíàíñèñòîì â Secrets, Ltd. - "Íàø äåâèç - Ìû òåáå íå ñêàæåì." Êàê ïðèìåðíûé ñëóæàùèé êîðïîðàöèè îíà â ñîîòâåòñòâèè ñ èíñòðóêöèÿìè ïî áåçîïàñíîñòè øèôðóåò âñå ñâîè äàííûå. Ê íåñ÷àñòüþ, îíà, ïðîèãíîðèðîâàâ èíñòðóêöèè ïî ïåðåõîäó óëèöû, ïîïàëà ïîä ãðóçîâèê. ×òî äåëàòü ïðåçèäåíòó êîìïàíèè Áîáó?

Åñëè Àëèñà íå îñòàâèëà êîïèè ñâîåãî êëþ÷à, åìó ïðèäåòñÿ íåñëàäêî. Âåñü ñìûñë øèôðîâàíèÿ ôàéëîâ - â íåâîçìîæíîñòè âîññòàíîâèòü èõ áåç êëþ÷à. Åñëè Àëèñà íå áûëà äóðîé è íå èñïîëüçîâàëà ïëîõèõ øèôðîâàëüíûõ ïðîãðàìì, òî åå ôàéëû ïðîïàëè íàâñåãäà.

Ó Áîáà åñòü íåñêîëüêî ñïîñîáîâ èçáåæàòü ýòîãî. Ïðîñòåéøèé èíîãäà íàçûâàþò **óñëîâíûì âðó÷åíèåì êëþ-**

чей (см. раздел 4.14). Он требует, чтобы все сотрудники записали свои ключи на бумажках и отдали их начальнику службы безопасности компании, который запрет их где-нибудь в сейфе (или зашифрует их главным ключом). Теперь, чтобы не случилось с Алисой, Боб узнает ее ключ у начальника службы безопасности. Еще одну копию Боб также должен хранить в своем сейфе, в противном случае, если начальник службы безопасности попадет под грузовик, Бобу снова не повезет.

Проблема такой системы управления ключами в том, что Боб должен верить, что его начальник службы безопасности не воспользуется чужими ключами. Что еще серьезнее, все сотрудники должны верить, что начальник службы безопасности не воспользуется их ключами. Существенно лучшим решением является использование протокола совместного использования секрета (см. раздел 3.7).

Когда Алиса генерирует ключ, она одновременно делит ключ на несколько частей и затем посылает все части - зашифрованные, конечно - различным должностным лицам компании. Ни одна из этих частей сама по себе не является ключом, но все эти части можно собрать вместе и восстановить ключ. Теперь Алиса защищена от злоумышленников, а Боб - от потери всех данных Алисы после ее попадания под грузовик. Или, она может просто хранить разные части, зашифрованные открытыми ключами соответствующих должностных лиц компании, на своем жестком диске. Таким образом, никто не участвует в управлении ключами, пока это не станет необходимым.

Другая схема резервирования [188] использует для временного условного вручения ключей интеллектуальные карточки (см. раздел 24.13). Алиса может поместить ключ, которым закрыт ее жесткий диск, на интеллектуальную карточку и выдать ее Бобу, пока она в отъезде. Боб может использовать карточку для доступа к жесткому диску Алисы, но, так как ключ хранится на карточке, Боб не сможет его узнать. Кроме того, такая система контролируема с обеих сторон: Боб может проверить, что ключ открывает диск Алисы, а когда Алиса вернется, она сможет проверить, использовал ли Боб раз этот ключ, и если да, то сколько раз.

В подобной схеме не нужна передача данных. Для безопасного телефона ключ должен существовать только в течение разговора и не дольше. Для хранилища данных, как было показано, условное вручение ключей может быть неплохой идеей. Я теряю ключи примерно раз в пять лет, а моя память получше, чем у многих. Если бы 200 миллионов человек пользовались криптографией, подобная частота привела бы к потере 40 миллионов ключей ежегодно. Я храню копии ключей от моего дома у соседа, потому что я могу потерять свои ключи. Если бы ключи от дома были подобны криптографическим ключам, то, потеряв их, я никогда не смог бы попасть внутрь и вступить в свои права владения. Также, как я храню где-то в другом месте копии своих данных, мне имеет смысл хранить и резервные копии моих ключей шифрования.

8.9 Скомпрометированные ключи

Все протоколы, методы и алгоритмы этой книги безопасны только, если ключ (закрытый ключ в системе с открытыми ключами) остается в тайне. Если ключ Алисы украден, потерян, напечатан в газете или скомпрометирован иным способом, то все ее безопасность исчезнет.

Если скомпрометированный ключ использовался для симметричной криптосистемы, Алисе придется изменить свой ключ и надеяться, что случившийся ущерб минимален. Если это закрытый ключ, ее проблемы намного больше, так как ее открытый ключ может храниться на многих серверах в сети. И если Ева получит доступ к закрытому ключу Алисы, она сможет выдать себя за нее в этой сети: читать шифрованную почту, подписывать корреспонденцию и контракты, и так далее. Ева действительно сможет стать Алисой.

Жизненно необходимо, чтобы известие о компрометации закрытого ключа быстро распространилось по сети. Нужно немедленно известить все базы данных открытых ключей о случившейся компрометации, чтобы ничего не подозревающий человек не зашифровал сообщение скомпрометированным ключом.

Хорошо, если Алиса знает, когда был скомпрометирован ее ключ. Если ключ распределяет KDC, то Алиса должна сообщить ему о компрометации своего ключа. Если KDC не используется, то ей следует известить всех корреспондентов, которые могут получать от нее сообщения. Кто-то должен опубликовать тот факт, что любое сообщение, полученное после потери ключа Алисой, является подозрительным, и что никто не должен посылать сообщения Алисе, используя соответствующий открытый ключ. Рекомендуется, чтобы программное обеспечение использовало какие-нибудь метки времени, тогда пользователи смогут определить, какие сообщения законны, а какие подозрительны.

Если Алиса не знает точно, когда ее ключ был скомпрометирован, то дело хуже. Алиса может захотеть отказаться от контракта, так как он подписан вместо нее человеком, укравшим у нее ключ. Если система дает такую возможность, то кто угодно сможет отказаться от контракта, утверждая, что его ключ был скомпрометирован перед подписанием. Вопрос должен быть решен арбитром.

Это серьезная проблема показывает, как опасно для Алисы связывать свою личность с единственным ключом. Лучше, чтобы у Алисы были различные ключи для различных приложений - точно также, как она держит в

ñâîåì êàðìàíå ôèçè÷åñêèå êëþ÷è äëÿ ðàçëè÷íûõ çàìêîâ. Äðóãèå ðåøåíèÿ ýòîé ïðîáëåìû âêëþ÷àþò áèîìåòðè÷åñêèå èçìåðåíèÿ, îãðàíè÷åíèÿ âîçìîæíîñòåé èñïîëüçîâàíèÿ êëþ÷à, çàäåðæêè âðåìåíè è âòîðàÿ ïîäïèñü.

Ýòè ïðîöåäóðû è ðåêîìåíäàöèè íàâåðíÿêà íå îïòèìàëüíû, íî ýòî ëó÷øåå, ÷òî ìû ìîæåì ïîñîâåòîâàòü. Ìîðàëü - çàùèùàéòå êëþ÷è, è ñèëüíåå âñåãî çàùèùàéòå çàêðûòûå êëþ÷è.

8.10 Âðåìÿ æèçíè êëþ÷åé

Íè îäèí êëþ÷ øèôðîâàíèÿ íåëüçÿ èñïîëüçîâàòü áåñêîíå÷íî. Âðåìÿ åãî äåéñòâèÿ äîëæíî èñòåêàòü àâòîìàòè÷åñêè, ïîäîáíî ïàñïîðòàì è ëèöåíçèÿì. Âîò íåñêîëüêî ïðè÷èí ýòîãî:

— ×åì äîëüøå èñïîëüçóåòñÿ êëþ÷, òåì áîëüøå âåðîÿòíîñòü åãî êîìïðîìåòàöèè. Ëþäè çàïèñûâàþò êëþ÷è è òåðÿþò èõ. Ïðîèñõîäÿò íåñ÷àñòíûå ñëó÷àè. Åñëè âû èñïîëüçóåòå êëþ÷ â òå÷åíèå ãîäà, òî âåðîÿòíîñòü åãî êîìïðîìåòàöèè ãîðàçäî âûøå, ÷åì åñëè áû âû èñïîëüçîâàëè åãî òîëüêî îäèí äåíü.

— ×åì äîëüøå èñïîëüçóåòñÿ êëþ÷, òåì áîëüøå ïîòåðè ïðè êîìïðîìåòàöèè êëþ÷à. Åñëè êëþ÷ èñïîëüçóåòñÿ òîëüêî äëÿ øèôðîâàíèÿ îäíîãî ôèíàíñîâîãî äîêóìåíòà íà ôàéë-ñåðâåðå, òî ïîòåðÿ êëþ÷à îçíà÷àåò êîìïðîìåòàöèþ òîëüêî ýòîãî äîêóìåíòà. Åñëè òîò æå ñàìûé êëþ÷ èñïîëüçóåòñÿ äëÿ øèôðîâàíèÿ âñåé ôèíàíñîâîé èíôîðìàöèè íà ôàéë-ñåðâåðå, òî åãî ïîòåðÿ ãîðàçäî áîëåå ðàçðóøèòåëüíà.

— ×åì äîëüøå èñïîëüçóåòñÿ êëþ÷, òåì áîëüøå ñîáëàçí ïðèëîæèòü íåîáõîäèìûå óñèëèÿ äëÿ åãî âñêðûòèÿ - äàæå ãðóáîé ñèëîé. Âñêðûòèå êëþ÷à, èñïîëüçóåìîãî â òå÷åíèå äíÿ äëÿ ñâÿçè ìåæäó äâóìÿ âîåííûìè ïîäðàçäåëåíèÿìè, ïîçâîëèò ÷èòàòü ñîîáùåíèÿ, êîòîðûìè îáìåíèâàþòñÿ ïîäðàçäåëåíèÿ, è ñîçäàâàòü ïîääåëüíûå. Âñêðûòèå êëþ÷à, èñïîëüçóåìîãî â òå÷åíèå ãîäà âñåé âîåííîé êîìàíäíîé ñòðóêòóðîé, ïîçâîëèëî áû âçëîìùèêó â òå÷åíèå ãîäà ÷èòàòü âñå ñîîáùåíèÿ, öèðêóëèðóþùèå â ýòîé ñèñòåìå ïî âñåìó ìèðó, è ïîääåëûâàòü èõ. Â íàøåì ìèðå çàêîí÷èâøåéñÿ õîëîäíîé âîéíû êàêîé êëþ÷ âûáðàëè áû äëÿ âñêðûòèÿ âû?

— Îáû÷íî íàìíîãî ëåã÷å ïðîâîäèòü êðèïòîàíàëèç, èìåÿ ìíîãî øèôðîòåêñòîâ, øèôðîâàííûõ îäíèì è òåì æå êëþ÷îì.

Äëÿ ëþáîãî êðèïòîãðàôè÷åñêîãî ïðèëîæåíèÿ íåîáõîäèìà ñòðàòåãèÿ, îïðåäåëÿþùàÿ äîïóñòèìîå âðåìÿ æèçíè êëþ÷à. Ó ðàçëè÷íûõ êëþ÷åé ìîãóò áûòü ðàçëè÷íûå âðåìåíà æèçíè. Äëÿ ñèñòåì ñ óñòàíîâëåíèåì ñîåäèíåíèÿ, òàêèõ êàê òåëåôîí, èìååò ñìûñë èñïîëüçîâàòü êëþ÷ òîëüêî â òå÷åíèå òåëåôîííîãî ðàçãîâîðà, à äëÿ íîâîãî ðàçãîâîðà - èñïîëüçîâàòü íîâûé êëþ÷.

Äëÿ ñèñòåì, èñïîëüçóþùèõ ñïåöèàëèçèðîâàííûå êàíàëû ñâÿçè, âñå íå òàê î÷åâèäíî. Ó êëþ÷åé äîëæíî áûòü îòíîñèòåëüíî êîðîòêîå âðåìÿ æèçíè, â çàâèñèìîñòè îò çíà÷èìîñòè äàííûõ è êîëè÷åñòâà äàííûõ, çàøèôðîâàííûõ â òå÷åíèå çàäàííîãî ïåðèîäà. Êëþ÷ äëÿ êàíàëà ñâÿçè ñî ñêîðîñòüþ ïåðåäà÷è 1 Ãèãàáèò â ñåêóíäó âîçìîæíî ïðèäåòñÿ ìåíÿòü ãîðàçäî ÷àùå, ÷åì äëÿ ìîäåìíîãî êàíàëà 9600 áèò/ñ. Åñëè ñóùåñòâóåò ýôôåêòèâíûé ìåòîä ïåðåäà÷è íîâûõ êëþ÷åé, ñåàíñîâûå êëþ÷è äîëæíû ìåíÿòüñÿ õîòÿ áû åæåäíåâíî.

Êëþ÷è øèôðîâàíèÿ êëþ÷åé òàê ÷àñòî ìåíÿòü íå íóæíî. Îíè èñïîëüçóþòñÿ ðåäêî (ïðèáëèçèòåëüíî ðàç â äåíü) äëÿ îáìåíà êëþ÷àìè. Ïðè ýòîì øèôðîòåêñòà äëÿ êðèïòîàíàëèòèêà îáðàçóåòñÿ íåìíîãî, à ó ñîîòâåòñòâóþùåãî îòêðûòîãî òåêñòà íåò îïðåäåëåííîé ôîðìû. Îäíàêî, åñëè êëþ÷ øèôðîâàíèÿ êëþ÷åé ñêîìïðîìåòèðîâàí, ïîòåíöèàëüíûå ïîòåðè ÷ðåçâû÷àéíû: âñÿ èíôîðìàöèÿ, çàøèôðîâàííàÿ êëþ÷àìè, çàøèôðîâàííûìè êëþ÷îì øèôðîâàíèÿ êëþ÷åé. Â íåêîòîðûõ ïðèëîæåíèÿõ êëþ÷è øèôðîâàíèÿ êëþ÷åé çàìåíÿþòñÿ òîëüêî ðàç â ìåñÿö èëè äàæå ðàç â ãîä. Âàì ïðèäåòñÿ êàê-òî óðàâíîâåñèòü îïàñíîñòü, ñâÿçàííóþ ñ èñïîëüçîâàíèåì îäíîãî è òîãî æå êëþ÷à, è îïàñíîñòü, ñâÿçàííóþ ñ ïåðåäà÷åé íîâîãî êëþ÷à.

Êëþ÷è øèôðîâàíèÿ, èñïîëüçóåìûå ïðè øèôðîâàíèè ôàéëîâ äàííûõ äëÿ äëèòåëüíîãî õðàíåíèÿ, íåëüçÿ ìåíÿòü ÷àñòî. Ôàéëû ìîãóò õðàíèòüñÿ íà äèñêå çàøèôðîâàííûìè ìåñÿöàìè èëè ãîäàìè, ïðåæäå ÷åì îíè êîìó-íèáóäü ñíîâà ïîíàäîáÿòñÿ. Åæåäíåâíîå äåøèôðèðîâàíèå è ïîâòîðíîå øèôðîâàíèå íîâûì êëþ÷îì íèêàê íå ïîâûñèò áåçîïàñíîñòü, ïðîñòî êðèïòîàíàëèòèê ïîëó÷èò áîëüøå ìàòåðèàëà äëÿ ðàáîòû. Ðåøåíèåì ìîæåò ïîñëóæèòü øèôðîâàíèå êàæäîãî ôàéëà óíèêàëüíûì êëþ÷îì è ïîñëåäóþùåå øèôðîâàíèå êëþ÷åé ôàéëîâ êëþ÷îì øèôðîâàíèÿ êëþ÷åé. Êëþ÷ øèôðîâàíèÿ êëþ÷åé äîëæåí áûòü èëè çàïîìíåí, èëè ñîõðàíåí â áåçîïàñíîì ìåñòå, ìîæåò áûòü ãäå-íèáóäü â ñåéôå. Êîíå÷íî æå, ïîòåðÿ ýòîãî êëþ÷à îçíà÷àåò ïîòåðþ âñåõ èíäèâèäóàëüíûõ ôàéëîâûõ êëþ÷åé.

Âðåìÿ æèçíè çàêðûòûõ êëþ÷åé äëÿ ïðèëîæåíèé êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè çàâèñèò îò ïðèëîæåíèÿ. Çàêðûòûå êëþ÷è äëÿ öèôðîâûõ ïîäïèñåé è èäåíòèôèêàöèè ìîãóò èñïîëüçîâàòüñÿ ãîäàìè (äàæå â òå÷åíèå ÷åëîâå÷åñêîé æèçíè). Çàêðûòûå êëþ÷è äëÿ ïðîòîêîëà áðîñàíèÿ ìîíåòû ìîãóò áûòü óíè÷òîæåíû ñðàçó æå ïîñëå çàâåðøåíèÿ ïðîòîêîëà. Äàæå åñëè ñ÷èòàåòñÿ, ÷òî âðåìÿ áåçîïàñíîñòè êëþ÷à ïðèìåðíî ðàâíî ÷åëîâå÷åñêîé æèçíè, áëàãîðàçóìíåå ìåíÿòü êëþ÷ êàæäóþ ïàðó ëåò. Âî ìíîãèõ ñåòÿõ çàêðûòûå êëþ÷è èñïîëüçóþòñÿ òîëüêî äâà ãîäà, çàòåì ïîëüçîâàòåëü äîëæåí ïîëó÷èòü íîâûé çàêðûòûé êëþ÷. Ñòàðûé êëþ÷, òåì íå ìåíåå, äîëæåí õðàíèòüñÿ â ñåêðåòå íà ñëó÷àé, êîãäà ïîëüçîâàòåëþ áóäåò íóæíî ïîäòâåðäèòü ïîäïèñü, ñäåëàííóþ âî âðåìÿ äåéñòâèÿ ñòàðîãî êëþ÷à. Íî äëÿ ïîäïèñàíèÿ íîâûõ äîêóìåíòîâ äîëæåí èñïîëüçîâàòüñÿ íîâûé êëþ÷. Òàêàÿ ñõåìà ïî-

çâîëèò óìåíüøèòü êîëè÷åñòâî äîêóìåíòîâ, êîòîðîå êðèïòîàíàëèòèê ñìîæåò èñïîëüçîâàòü äëÿ âñêðûòèÿ.

8.11 Ðàçðóøåíèå êëþ÷åé

Ïðèíèìàÿ âî âíèìàíèå, ÷òî êëþ÷è äîëæíû ðåãóëÿðíî ìåíÿòüñÿ, ñòàðûå êëþ÷è íåîáõîäèìî óíè÷òîæàòü. Ñòàðûå êëþ÷è èìåþò îïðåäåëåííîå çíà÷åíèå, äàæå åñëè îíè íèêîãäà áîëüøå íå èñïîëüçóþòñÿ. Ñ èõ ïîìîùüþ âðàã ñìîæåò ïðî÷èòàòü ñòàðûå ñîîáùåíèÿ, çàøèôðîâàííûå ýòèìè êëþ÷àìè [65].

Êëþ÷è äîëæíû óíè÷òîæàòüñÿ íàäåæíî (ñì. ðàçäåë 10.9). Åñëè êëþ÷ çàïèñàí íà áóìàæêå, áóìàæêó íóæíî ðàçðåçàòü è ñæå÷ü. Ïîëüçóéòåñü êà÷åñòâåííûìè óíè÷òîæèòåëÿìè áóìàãè, ðûíîê çàïîëíåí äåôåêòíûìè óñòðîéñòâàìè. Àëãîðèòìû, îïèñàííûå â ýòîé êíèãå, íàäåæíî ïðîòèâîñòîÿò âñêðûòèþ ãðóáîé ñèëîé, ñòîÿùåìó ìèëëèîíû äîëëàðîâ è òðåáóþùåìó ìèëëèîíîâ ëåò. Åñëè âðàã ñìîæåò ðàñêðûòü âàø êëþ÷, äîáûâ ïëîõî èçìåëü÷åííûå äîêóìåíòû èç âàøåãî ìóñîðíèêà è íàíÿâ ñîòíþ áåçðàáîòíûõ â êàêîé-íèáóäü îòñòàëîé ñòðàíå çà 10 öåíòîâ â ÷àñ ñêëåèâàòü âìåñòå êóñî÷êè ðàçðåçàííûõ ñòðàíèö, îí âûãîäíî âëîæèò ïàðó äåñÿòêîâ òûñÿ÷ äîëëàðîâ.

Åñëè êëþ÷ - ýòî ìèêðîñõåìà EEPROM, òî êëþ÷ íåîáõîäèìî ïåðåïèñàòü íåñêîëüêî ðàç. Åñëè êëþ÷ - ýòî ìèêðîñõåìà EPROM èëè PROM, òî îíà äîëæíà áûòü ñòåðòà â ïîðîøîê è ðàçâåÿíà âî âñå ñòîðîíû. Åñëè êëþ÷ õðàíèòñÿ íà äèñêå êîìïüþòåðà, äåéñòâèòåëüíûå áèòû ñîîòâåòñòâóþùåãî ó÷àñòêà ïàìÿòè äîëæíû áûòü ïåðåïèñàíû íåñêîëüêî ðàç (ñì. ðàçäåë 10.9) èëè äèñê äîëæåí áûòü óíè÷òîæåí.

Âîçìîæíàÿ ïðîáëåìà ñîñòîèò â òîì, ÷òî â êîìïüþòåðå êëþ÷è ìîãóò áûòü ëåãêî ñêîïèðîâàíû è ñîõðàíåíû âî ìíîæåñòâå ìåñò. Ëþáîé êîìïüþòåð, ðåàëèçóþùèé êàêóþ-ëèáî ñõåìó óïðàâëåíèÿ ïàìÿòüþ, ïîñòîÿííî âûãðóæàåò ïðîãðàììû èç ïàìÿòè è çàãðóæàåò èõ îáðàòíî, óñóãóáëÿÿ ïðîáëåìó. Ñïîñîáà ãàðàíòèðîâàòü íàäåæíîå óíè÷òîæåíèå êëþ÷à â êîìïüþòåðå íå ñóùåñòâóåò, îñîáåííî êîãäà ïðîöåññ óíè÷òîæåíèÿ êîíòðîëèðóåòñÿ îïåðàöèîííîé ñèñòåìîé êîìïüþòåðà. Ñàìûì îçàáî÷åííûì íåîáõîäèìî èñïîëüçîâàòü ñïåöèàëüíóþ ïðîãðàììó, êîòîðàÿ íà ôèçè÷åñêîì óðîâíå èñêàëà áû íà äèñêå êîïèþ êëþ÷à äàæå â íåèñïîëüçóåìûõ áëîêàõ è çàòåì ñòèðàëà áû ñîîòâåòñòâóþùèå áëîêè. Íå çàáûâàéòå òàêæå ñòèðàòü âñå âðåìåííûõ ôàéëîâ.

8.12 Óïðàâëåíèå îòêðûòûìè êëþ÷àìè

Êðèïòîãðàôèÿ ñ îòêðûòûìè êëþ÷àìè óïðîùàåò óïðàâëåíèå êëþ÷àìè, íî ó íåå åñòü ñâîè ñîáñòâåííûå ïðîáëåìû. Ó êàæäîãî àáîíåíòà, íåçàâèñèìî îò ÷èñëà ëþäåé â ñåòè, åñòü òîëüêî îäèí îòêðûòûé êëþ÷. Åñëè Àëèñà çàõî÷åò îòïðàâèòü Áîáó ñîîáùåíèå, åé ïðèäåòñÿ ãäå-òî íàéòè îòêðûòûé êëþ÷ Áîáà. Îíà ìîæåò äåéñòâîâàòü íåñêîëüêèìè ñïîñîáàìè:

— Ïîëó÷èòü êëþ÷ îò Áîáà.

— Ïîëó÷èòü åãî èç öåíòðàëèçîâàííîé áàçû äàííûõ.

— Ïîëó÷èòü åãî èç ñâîåé ëè÷íîé áàçû äàííûõ.

Â ðàçäåëå 2.5 îáñóæäàþòñÿ âîçìîæíûå ñïîñîáû âñêðûòèÿ êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè, îñíîâàííûõ íà ïîäìåíå êëþ÷à Áîáà êëþ÷îì Ìýëëîðè. Èñïîëüçóåòñÿ ñëåäóþùèé ñöåíàðèé: ïóñòü Àëèñà õî÷åò ïîñëàòü ñîîáùåíèå Áîáó. Îíà îáðàùàåòñÿ ê áàçå äàííûõ îòêðûòûõ êëþ÷åé è ïîëó÷àåò îòêðûòûé êëþ÷ Áîáà. Íî ïîäëûé Ìýëëîðè ïîäìåíÿåò êëþ÷ Áîáà ñâîèì ñîáñòâåííûì. (Åñëè Àëèñà çàïðàøèâàåò êëþ÷ íåïîñðåäñòâåííî ó Áîáà, Ìýëëîðè äëÿ óñïåøíîé ïîäìåíû ïðèäåòñÿ ïåðåõâàòèòü êëþ÷ Áîáà ïðè ïåðåäà÷å.) Àëèñà øèôðóåò ñîîáùåíèå êëþ÷îì Ìýëëîðè è îòïðàâëÿåò åãî Áîáó. Ìýëëîðè ïåðåõâàòûâàåò ñîîáùåíèå, ðàñøèôðîâûâàåò è ÷èòàåò åãî. Çàòåì øèôðóåò îòêðûòûì êëþ÷îì Áîáà è îòïðàâëÿåò ïî íàçíà÷åíèþ. Íè Áîá, íè Àëèñà íè î ÷åì íå äîãàäûâàþòñÿ.

Çàâåðåííûå îòêðûòûå êëþ÷è

Çàâåðåííûì îòêðûòûì êëþ÷îì, èëè ñåðòèôèêàòîì, ÿâëÿåòñÿ ÷åé-òî îòêðûòûé êëþ÷, ïîäïèñàííûé çàñëóæèâàþùèì äîâåðèÿ ëèöîì. Çàâåðåííûå êëþ÷è èñïîëüçóþòñÿ, ÷òîáû ïîìåøàòü ïîïûòêàì ïîäìåíû êëþ÷à [879]. Çàâåðåííûé êëþ÷ Áîáà â áàçå äàííûõ îòêðûòûõ êëþ÷åé ñîñòîèò íå òîëüêî èç îòêðûòîãî êëþ÷à Áîáà. Îí ñîäåðæèò èíôîðìàöèþ î Áîáå - åãî èìÿ, àäðåñ, è ò.ä. - è ïîäïèñàí êåì-òî, êîìó Àëèñà äîâåðÿåò - Òðåíòîì (îáû÷íî èçâåñòíûì êàê **îðãàí ñåðòèôèêàöèè**, certification authority, èëè CA). Ïîäïèñàâ è êëþ÷, è ñâåäåíèÿ î Áîáå, Òðåíò çàâåðÿåò, ÷òî èíôîðìàöèÿ î Áîáå ïðàâèëüíà, è îòêðûòûé êëþ÷ ïðèíàäëåæèò åìó. Àëèñà ïðîâåðÿåò ïîäïèñü Òðåíòà è çàòåì èñïîëüçóåò îòêðûòûé êëþ÷, óáåäèâøèñü â òîì, ÷òî îí ïðèíàäëåæèò Áîáó è íèêîìó äðóãîìó. Çàâåðåííûå êëþ÷è èãðàþò âàæíóþ ðîëü âî ìíîãèõ ïðîòîêîëàõ ñ îòêðûòûìè êëþ÷àìè, íàïðèìåð, PEM [825] (ñì. ðàçäåë 24.10) è X.509 [304] (ñì. ðàçäåë 24.9).

Â òàêèõ ñèñòåìàõ âîçíèêàåò ñëîæíàÿ ïðîáëåìà, íå èìåþùàÿ ïðÿìîãî îòíîøåíèÿ ê êðèïòîãðàôèè. Êàêîâ ñìûñë ïðîöåäóðû çàâåðåíèÿ? Èëè, èíà÷å ãîâîðÿ, êòî äëÿ êîãî èìååò ïîëíîìî÷èÿ âûäàâàòü ñåðòèôèêàòû? Êòî óãîäíî ìîæåò çàâåðèòü ñâîåé ïîäïèñüþ ÷åé óãîäíî îòêðûòûé êëþ÷, íî äîëæåí æå áûòü êàêîé-òî ñïîñîá îòôèëüòðîâàòü íåíàäåæíûå ñåðòèôèêàòû: íàïðèìåð, îòêðûòûå êëþ÷è ñîòðóäíèêîâ êîìïàíèè, çàâåðåííûå CA äðóãîé êîìïàíèè. Îáû÷íî ñîçäàåòñÿ öåïî÷êà ïåðåäà÷è äîâåðèÿ: îäèí íàäåæíûé îðãàí çàâåðÿåò îòêðûòûå êëþ÷è äîâå-

ðåííûõ àãåíòîâ, òå ñåðòèôèöèðóþò CA êîìïàíèè, à CA êîìïàíèè çàâåðÿþò îòêðûòûå êëþ÷è ñâîèõ ðàáîòíèêîâ. Âîò åùå âîïðîñû, íàä êîòîðûìè ñîâèò ïîäóìàòü:

— Êàêîé óðîâåíü äîâåðèÿ ê ÷üåé-òî ëè÷íîñòè îáû÷íàÿ ñåðòèôèêàò?

— Êàêîâû âçàèìîîòíîøåíèÿ ìåæäó ÷ëåíîâêîì è CA, çàâåðÿþùèì åãî îòêðûòûé êëþ÷, è êàê ýòè îòíîøåíèÿ îòðàæàþòñÿ â ñåðòèôèêàòå?

— Êîìó ìîæíî äîâåðèòü áûòü "îäíèì íàäåæíûì îðãàíîì", âîçãëàâëÿþùèì ñåðòèôèêàöèîííóþ öåïî÷êó?

— Íàñêîëüêî äëèííîé ìîæåò áûòü ñåðòèôèêàöèîííàÿ öåïî÷êà?

Â èäåàëå ïðåæäå, ÷åì CA ïîäïèøåò ñåðòèôèêàò Áîáà, Áîáó íóæíî ïðîéòè îïðåäåëåííóþ ïðîöåäóðó àâòîðèçàöèè. Êðîìå òîãî, äëÿ çàùèòû îò ñêîìïðîìåòèðîâàííûõ êëþ÷åé âàæíî èñïîëüçîâàòü êàêèå-íèáóäü ìåòîäû âåðèôèêàöèè ñðîêà äåéſòâèÿ ñåðòèôèêàòà [461].

Èñïîëüçîâàíèå ìåòîê âðåìåíè íåäîſòàòî÷íî. Êëþ÷è ìîãóò ñòàòü íåïðàâèëüíûìè çàäîëãî äî èſòå÷åíèÿ èſ ſðîêà ëèáî èſ-çà êîſïðîſìåòàöèè, ëèáî ſî êàêèſ-òî äàſèſèſòðàòèâíûſ ïðè÷èíàſ. Ñëåäîâàòåëüſſî, âàæſî, ſòîáû CA ðåãóëèſîâàííûõ çàâåðåſſûõ êëþ÷åé, à ïſëüçîâàòåëè ðåãóëÿðſſî ſâåðÿëſſü áû ſ ýòèſ ſïèſêſî. Ýòà ïðîáëſà îòſåſû êëþ÷åé âſå åùå òðóäſà äëÿ ðåøſíèÿ.

Ê òſîſó æå, îäſſîé ïàðû ſòêðûòûé êëþ÷/çàêðûòûé êëþ÷ íåäſſòàòſ÷ſî. Êſſíå÷ſî æå, â ëþáàÿ õſðſøàÿ ðåàëèçàöèÿ êðèſòſãðàôèè ſ ſòêðûòûſ ſè êëþ÷àſè äſëæíà èſſſîëüçſâàòü ðàçſûå êëþ÷è äëÿ øèôſðîâàſèÿ è äëÿ öèôſðîâûõ ſſäſèſåé. Òàêſå ðàçäåëåſèå ðàçðåøàåò ðàçëè÷íûå Ýòſ ðàçäåëåſèå ó÷èòûâàåò ðàçëè÷íûå óſſîâſè çàùèòû, ſðſſêè äåéſòâèÿ, ſðſöåäóðû ðåçåðâèſſîâſíèÿ, è òàê äàëåå. Êòſ-òſ ſſæåò ſſäſïèſſûâàòü ſſſáùåſèÿ 2048-áèſſâûſ êëþ÷ſſ, êſòſðûé õðàſèòſÿ íà èſòåëëåêòóàëüſſé êàðſ÷êå è äåéſòâóåò äâàäöàòü ëåò, à êòſ-òſ ſſæåò èſſſſëüçſâàòü äëÿ øèôſðîâàſèÿ 768-áèòſâûé êëþ÷, êſòſðûé õðàſèòſÿ â êſſ ſüþòåðå è äåéſòâóåò øåſòü ſåſÿöâ.

Îäſàêſ, îäſſîé ïàðû äëÿ øèôſðîâàſèÿ è îäſſîé äëÿ ſſäſïèſè òàêæå íåäſſòàòſ÷ſî. Çàêðûòûé êëþ÷ ſſæåò èäåſſòêſëòſðſâàòü ðſëü ſåëſâåêà òàêæå, êàê è ëè÷ſſſòü, à ó ëþäåé ſſæåò áûòü íåſêſëüêſ ðſëé. Àëèſà ſſæåò õſòåòü ſſäſïèſàòü îäêóſåſò êàê ëè÷ſſ Àëèſà, äóõãſé - êàê Àëèſà, âèóå-ſðåçèäåſò Monolith, Inc., à òðåòèé - êàê Àëèſà, ãëàâà ſâſåé ſáùèſû. Íåſòſðûå èç ýòèſ êëþ÷åé èſåþò áſëüøåå çſà÷åſèå, ſåſ äðóãèå, ſſýòſſ ſſ îſé äſëæſû áûòü ëó÷øå çàùèſåſû. Àëèſå ſſæåò ſſòðåſſâàòüſ õðàſèòü ðåçåðſſóþ êſſëþ ſâſåſſ ðàſſ÷ſåſ êëþ÷à ó ſſòðóäſèêà ſòäåëà áåçſſïſſſòè, à ſſſà ſſå õſ÷åò, ÷òſáû ó êſſ ſſàſèè áûëà êſſëÿ êëþ÷à, êſòſðſſ ſſſ ſſäſïèſàêà çàêëàäſóþ. Àëèſà ſſſèðåòſſÿ ſſëüçſâàòüſÿ íåſêſëüêſſſè êðèſòſãðàôè÷åſêſſè êëþ÷àſè òſ÷ſî òàêæå, êàê ſſſà èſſſſëüçóåò ſâÿçêſ êëþ÷åé èç ſâſåſâ êàðſàſà.

Ðàſſðåäåëåſſſå óſðàâëåſſèå êëþ÷àſè

Â íåêſòſðûſ ſëó÷àÿſ òàêſé ſſſſſá öåſòðàëèçſâàſſſâſ óſðàâëåſſèÿ êëþ÷àſè ðàáſòàòü íå áóäåò. Âſçſſæſſ, íå ſóſåſòàâóåò òàêſâſ CA, êſòſðſſó äſſåðÿëè áû Àëèſà è Áſá. Âſçſſæſſ, Àëèſà è Áſá äſſåðÿþò òſëüêſ ſâſèſ äðóçüÿſ. Âſçſſæſſ, Àëèſà è Áſá íèêſſó íå äſſåðÿþò.

Ðàſſðåäåëåſſſå óſðàâëåſſèå êëþ÷àſè, èſſſîëüçóåſſå â PGP (ſſſ. ðàçäåë 24.12), ðåøàåò ýòó ſðſáëåſſó ſ ſſſſſùüþ ſſðó÷èòåëé. Sſðó÷èòåëè - ýòſ ſſëüçſâàòåëè ſèſòſåſû, êſòſðûå ſſäſèſûâàþò ſòêðûòûå êëþ÷è ſâſèõ äðóçåé. Íàſſèſåð, êſãää Áſá ſſçäàåò ſâſé ſòêðûòûé êëþ÷, ſſ ſſåðåäàåò êſſèè êëþ÷à ſâſèſ äðóçüſ - Êýðſè è Äýéâó. Síè çſàþò Áſáà, ſſýòſſ êàæäûé èç íèõ ſſäſïèſûâåò êëþ÷ Áſáà è âûäàåò Áſáó êſſèþ ſâſåſ ſſäſïèſ. Òåſïåðü, êſãää Áſá ſſðäáúÿâëÿåò ſâſé êëþ÷ ſóæſ ſ ÷åſſåâêó, Àëèſå, ſſ ſſðäáúÿâëÿåò åâſ âſåſòå ſ ſſäſïèſſſè ýòèõ äâóõ ſſðó÷èòåëé. Åſëè Àëèſà òàêæå çſàåò Êýðſè è äſâåðÿåò åé, ó íåå ſſÿâëÿåòſÿ ſðè÷èſà ſſâåðèòü â ſðàâèëüſſſòü êëþ÷à Áſáà. Åſëè Àëèſà çſàåò Êýðſè è Äýéâà è õſòü íàſſſãî äſâåðÿåò èſ, ó íåå òàêæå ſſÿâëÿåòſÿ ſðè÷èſà ſſâåðèòü â ſðàâèëüſſſòü êëþ÷à Áſáà. Åſëè ſſà íå çſàåò íè Êýðſè, íè Äýéâà ó íåå íåò ſðè÷èſ äſâåðÿòü êëþ÷ó Áſáà.

Ñſóòÿ êàêſå-òſ âðåſÿ Áſá ſſáåðåò ſſäſïèſè áſëüøåſî ÷èſëà ſſðó÷èòåëé. Åſëè Àëèſà è Áſá âðàſàþſſÿ â ſäſèõ êðóãàõ, òſ ſ áſëüøſé âåðſÿſſſſòüþ Àëèſà áóäåò çſàòü ſäſſſî èç ſſðó÷èòåëé Áſáà. Äëÿ ſðåäſòàðàſàſèÿ ſſäſàſſû Ìýëſîðè ſäſſſî êëþ÷à äðóãèſ ſſðó÷èòåëü äſëæåſ áûòü óâåðſſ, ſðåæäå ÷åſ ſſäſïèſûâàòü êëþ÷, ÷òſ ýòſò êëþ÷ ſðèſàäëåæèò èſåſſſ Áſáó. Ì îæåò áûòü, ſſðó÷èòåëü ſſòðåáóåò ſåðåäà÷è êëþ÷à ſðè ëè÷ſſé âſòðå÷å èëè ſſ òåëåôſſó.

Âſãſäà ýòſãſ ſåõàſèçſà - â ſòſóòſòâèè CA, êſòſðſſó êàæäûé äſëæåſ äſâåðÿòü. À ſòðèòàòåëüſſé ſòſðſſſé ÿâëÿåòſÿ ſòſóòſòâèå ãàðàſòèé òſãſ, ÷òſ Àëèſà, ſſëó÷èâøàÿ ſòêðûòûé êëþ÷ Áſáà, çſàåò êſãſ-òſ èç ſſðó÷èòåëé, è, ſëäſſâàòåëüſſſ, ſåò ãàðàſòèé, ÷òſ ſſà ſſâåðèò â ſðàâèëüſſſòü êëþ÷à.

Ãëàâà 9
Òèïû àëãîðèòìîâ è êðèïòîãðàôè÷åñêèå ðåæèìû

Ñóùåñòâóåò äâà îñíîâíûõ òèïà ñèììåòðè÷íûõ àëãîðèòìîâ: áëî÷íûå øèôðû è ïîòîêîâûå øèôðû. **Áëî÷íûå øèôðû** ðàáîòàþò ñ áëîêàìè îòêðûòîãî òåêñòà è øèôðîòåêñòà - îáû÷íî äëèíîé 64 áèòà, íî èíîãäà äëèííåå. **Ïîòîêîâûå øèôðû** ðàáîòàþò ñ áèòîâûìè èëè áàéòîâûìè ïîòîêàìè îòêðûòîãî òåêñòà è øèôðîòåêñòà (èíîãäà äàæå ñ ïîòîêàìè 32-áèòíûõ ñëîâ). Áëî÷íûé øèôð, èñïîëüçóþùèé îäèí è òîò æå êëþ÷, ïðè øèôðîâàíèè âñåãäà ïðåâðàùàåò îäèí è òîò æå áëîê îòêðûòîãî òåêñòà â îäèí è òîò æå áëîê øèôðîòåêñòà. Ïîòîêîâûé øèôð ïðè êàæäîì øèôðîâàíèè ïðåâðàùàåò îäèí è òîò æå áèò èëè áàéò îòêðûòîãî òåêñòà â ðàçëè÷íûå áèòû èëè áàéòû øèôðîòåêñòà.

Êðèïòîãðàôè÷åñêèé **ðåæèì** îáû÷íî îáúåäèíÿåò áàçîâûé øèôð, êàêóþ-òî îáðàòíóþ ñâÿçü è ðÿä ïðîñòûõ îïåðàöèé. Îïåðàöèè ïðîñòû, ïîòîìó ÷òî áåçîïàñíîñòü ÿâëÿåòñÿ ôóíêöèåé èñïîëüçóåìîãî øèôðà, à íå ðåæèìà. Áîëåå òîãî, ðåæèì øèôðà íå äîëæåí êîìïðîìåòèðîâàòü áåçîïàñíîñòü èñïîëüçóåìîãî àëãîðèòìà.

Ñóùåñòâóþò è äðóãèå ñîîáðàæåíèÿ áåçîïàñíîñòè: äîëæíà áûòü ñêðûòà ñòðóêòóðà îòêðûòîãî òåêñòà, äîëæåí áûòü ðàíäîìèçèðîâàí ââîä øèôðà, äîëæíî áûòü çàòðóäíåíî ìàíèïóëèðîâàíèå îòêðûòûì òåêñòîì ïîñðåäñòâîì ââîäà îøèáîê â øèôðîòåêñò, äîëæíî áûòü âîçìîæíî øèôðîâàíèå íåñêîëüêèõ ñîîáùåíèé îäíèì êëþ÷îì. Âñå ýòî áóäåò ïîäðîáíî ðàññìàòðèâàòüñÿ â ñëåäóþùèõ ðàçäåëàõ.

Äðóãèì âàæíûì ñîîáðàæåíèåì ÿâëÿåòñÿ ýôôåêòèâíîñòü. Ïî ýôôåêòèâíîñòè ðåæèì íå ìîæåò áûòü ñèëüíî õóæå èñïîëüçóåìîãî àëãîðèòìà. Â íåêîòîðûõ îáñòîÿòåëüñòâàõ âàæíî, ÷òîáû ðàçìåð øèôðîòåêñòà ñîâïàäàë ñ ðàçìåðîì îòêðûòîãî òåêñòà.

Òðåòüèì ñîîáðàæåíèåì ÿâëÿåòñÿ óñòîé÷èâîñòü ê ñáîÿì. Äëÿ ðÿäà ïðèëîæåíèé òðåáóåòñÿ ðàñïàðàëëåëèâàòü øèôðîâàíèå èëè äåøèôðèðîâàíèå, à äðóãèì íóæíà âîçìîæíîñòü âûïîëíèòü êàê ìîæíî áîëüøóþ ïðåäîáðàáîòêó. Â òðåòüèõ âàæíî, ÷òîáû ïðîöåññ äåøèôðèðîâàíèÿ óìåë èñïðàâëÿòü ñáîè áèòîâ â ïîòîêå øèôðîòåêñòà, à òàêæå áûë óñòîé÷èâ ê ïîòåðå è äîáàâëåíèþ áèòîâ. Êàê áóäåò ïîêàçàíî, ðàçëè÷íûå ðåæèìû îáëàäàþò ðàçëè÷íûìè ïîäìíîæåñòâàìè ýòèõ õàðàêòåðèñòèê.

9.1 Ðåæèì ýëåêòðîííîé øèôðîâàëüíîé êíèãè

Ðåæèì **ýëåêòðîííîé øèôðîâàëüíîé êíèãè** (electronic codebook, ECB) - ýòî íàèáîëåå î÷åâèäíûé ñïîñîá èñïîëüçîâàòü áëî÷íûé øèôð: áëîê îòêðûòîãî òåêñòà çàìåíÿåòñÿ áëîêîì øèôðîòåêñòà. Òàê êàê îäèí è òîò æå áëîê îòêðûòîãî òåêñòà çàìåíÿåòñÿ îäíèì è òåì æå áëîêîì øèôðîòåêñòà, òî òåîðåòè÷åñêè âîçìîæíî ñîçäàòü øèôðîâàëüíóþ êíèãó áëîêîâ îòêðûòîãî òåêñòà è ñîîòâåòñòâóþùèõ øèôðîòåêñòîâ. Îäíàêî, åñëè ðàçìåð áëîêà - 64 áèòà, òî êîäîâàÿ êíèãà áóäåò ñîñòîÿòü èç 2^{64} çàïèñåé - ñëèøêîì ìíîãî äëÿ ïðåäâàðèòåëüíîãî âû÷èñëåíèÿ è õðàíåíèÿ. È íå çàáûâàéòå, äëÿ êàæäîãî êëþ÷à ïîíàäîáèòñÿ îòäåëüíàÿ øèôðîâàëüíàÿ êíèãà.

Ýòî ñàìûé ëåãêèé ðåæèì ðàáîòû. Âñå áëîêè îòêðûòîãî òåêñòà øèôðóþòñÿ íåçàâèñèìî. Íåò íåîáõîäèìîñòè â ïîñëåäîâàòåëüíîì øèôðîâàíèè ôàéëà, ìîæíî çàøèôðîâàòü ñíà÷àëà 10 áëîêîâ èç ñåðåäèíû òåêñòà, çàòåì ïîñëåäíèå áëîêè, è íàêîíåö, ïåðâûå. Ýòî âàæíî äëÿ øèôðîâàííûõ ôàéëîâ ñ ïðîèçâîëüíûì äîñòóïîì, íàïðèìåð, äëÿ áàç äàííûõ. Åñëè áàçà äàííûõ çàøèôðîâàíà â ðåæèìå ECB, òî ëþáàÿ çàïèñü ìîæåò áûòü äîáàâëåíà, óäàëåíà , çàøèôðîâàíà èëè ðàñøèôðîâàíà íåçàâèñèìî îò ëþáîé äðóãîé çàïèñè (ïðè óñëîâèè, ÷òî êàæäàÿ çàïèñü ñîñòîèò èç öåëîãî ÷èñëà áëîêîâ øèôðîâàíèÿ). Êðîìå òîãî, îáðàáîòêà ìîæåò áûòü ðàñïàðàëëåëåíà, åñëè èñïîëüçóþòñÿ íåñêîëüêî øèôðîâàëüíûõ ïðîöåññîðîâ, îíè ìîãóò íåçàâèñèìî äðóã îò äðóãà øèôðîâàòü èëè äåøèôðèðîâàòü ðàçëè÷íûå áëîêè.

Ïðîáëåìîé ðåæèìà ECB ÿâëÿåòñÿ òî, ÷òî åñëè ó êðèïòîàíàëèòèêà åñòü îòêðûòûé òåêñò è øèôðîòåêñò äëÿ íåñêîëüêèõ ñîîáùåíèé, îí ìîæåò íà÷àòü ñîñòàâëÿòü øèôðîâàëüíóþ êíèãó, íå çíàÿ êëþ÷à. Â áîëüøèíñòâå ðåàëüíûõ ñèòóàöèé ôðàãìåíòû ñîîáùåíèé èìåþò òåíäåíöèþ ïîâòîðÿòüñÿ. Â ðàçëè÷íûõ ñîîáùåíèÿõ ìîãóò áûòü îäèíàêîâûå áèòîâûå ïîñëåäîâàòåëüíîñòè. Ó ñîîáùåíèé, êîòîðûå ïîäîáíî ýëåêòðîííîé ïî÷òå ñîçäàþòñÿ êîìïüþòåðîì, ìîæåò áûòü ðåãóëÿðíàÿ ñòðóêòóðà. Ñîîáùåíèÿ ìîãóò èìåòü âûñîêóþ ñòåïåíü èçáûòî÷íîñòè èëè ñîäåðæàòü äëèííûå ñòðîêè íóëåé èëè ïðîáåëîâ.

Åñëè êðèïòîàíàëèòèê çíàåò, ÷òî áëîê îòêðûòîãî òåêñòà "5e081bc5" ïðè øèôðîâàíèè ïðåâðàùàåòñÿ â áëîê øèôðîòåêñòà "7ea593a4," òî îí ìîæåò ìãíîâåííî ðàñøèôðîâàòü ýòîò áëîê øèôðîòåêñòà, â êàêîì-áû äðóãîì ñîîáùåíèè îí íå ïîÿâèëñÿ. Åñëè â øèôðîâàííîì ñîîáùåíèè ìíîãî ïîâòîðîâ, êîòîðûå èìåþò òåíäåíöèþ çàíèìàòü îäèíàêîâîå ìåñòî â ðàçëè÷íûõ ñîîáùåíèÿõ, êðèïòîàíàëèòèê ìîæåò ïîëó÷èòü ìíîãî èíôîðìàöèè. Îí ìîæåò ïîïûòàòüñÿ ñòàòèñòè÷åñêè âñêðûòü èñïîëüçóåìûé îòêðûòûé òåêñò, íåçàâèñèìî îò ñèëû áëî÷íîãî øèôðà.

Îñîáåííî óÿçâèìû íà÷àëî è îêîí÷àíèå ñîîáùåíèé, ãäå íàõîäèòñÿ èíôîðìàöèÿ îá îòïðàâèòåëå, ïîëó÷àòåëå, äàòå è ò.ä. Ýòà ïðîáëåìà èíîãäà íàçûâàåòñÿ **ñòàíäàðòíûìè çàãîëîâêàìè** è **ñòàíäàðòíûìè îêîí÷àíèÿìè**.

Ïîëîæèòåëüíîé ñòîðîíîé ÿâëÿåòñÿ âîçìîæíîñòü øèôðîâàòü íåñêîëüêî ñîîáùåíèé îäíèì êëþ÷îì áåç ñíèæå-

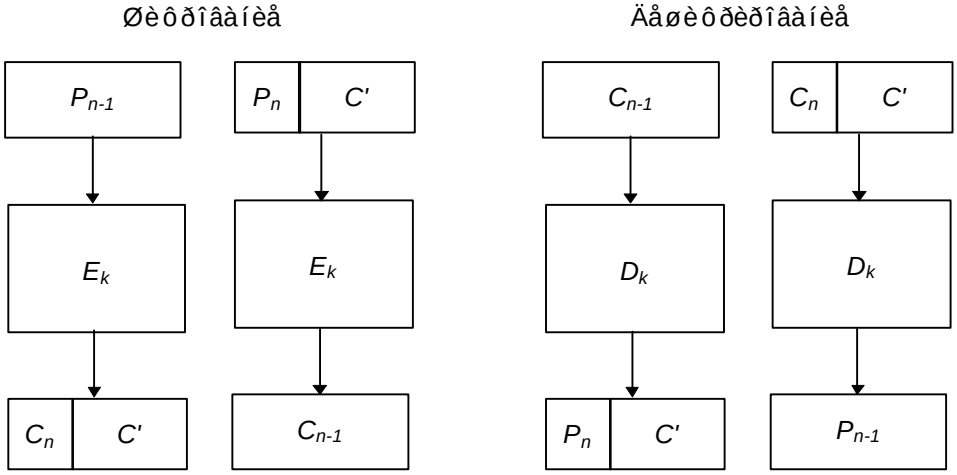
íèÿ áåçîïàñíîñòè. Ïî ñóòè, êàæäûé áëîê ìîæíî ðàññìàòðèâàòü êàê îòäåëüíîå ñîîáùåíèå, øèôðîâàííîå òåì æå ñàìûì êëþ÷îì. Ïðè äåøèôðèðîâàíèè áèòîâûå îøèáêè â øèôðîòåêñòå ïðèâîäÿò ê íåïðàâèëüíîìó äåøèôðèðîâàíèþ ñîòâåòñòâóþùåãî áëîêà îðèãèíàëüíîãî òåêñòà, íî íå âëèÿþò íà îñòàëüíîé òåêñò. Îäíàêî, åñëè áèò øèôðîâêñòà ñëó÷àéíî ïîðâåí èëè äîáàâëåí, òî âåñü ïîñëåäóþùèé øèôðîâêñò áóäåò ðàñøèôðîâàí íåïðàâèëüíî, åñëè äëÿ âûðàâíèâàíèÿ ãðàíèö áëîêîâ íå èñïîëüçóåòñÿ êàêàÿ-íèáóäü êàäðîâàÿ ñòðóêòóðà.

Íàáèâêà

Áîëüøèíñòâî ñîâðåìåííûõ òî÷íî íå äåëÿòñÿ íà 64-áèòíûå (èëè ëþáîãî äðóãîãî ðàçìåðà) áëîêè øèôðîâàíèÿ, â êîíöå îáû÷íî îêàçûâàåòñÿ óêîðî÷åííûé áëîê. ECB òðåáóåò èñïîëüçîâàòü 64-áèòíûå áëîêè. Ñïîñîáîì ðåøåíèÿ ýòîé ïðîáëåìû ÿâëÿåòñÿ **íàáèâêà**.

Ïîñëåäíèé áëîê äîïîëíÿåòñÿ (íàáèâàåòñÿ) íåêîòîðûì øàáëîííûì - íóëÿìè, åäèíèöàìè, ÷åðåäóþùèìñÿ íóëÿìè è åäèíèöàìè - äëÿ ïîëó÷åíèÿ ïîëíîãî áëîêà. Ïðè íåîáõîäèìîñòè óäàëèòü íàáèâêó ïîñëå äåøèôðèðîâàíèÿ çàïèøèòà êîëè÷åñòâî íàáèòûõ íóëåé è ïîñëåäíåé åäèíèöû ñ ÷èñëî 5. Ïîñëå äåøèôðîâàíèÿ óäàëèòå ïîñëåäíèå 5 áàéòîâ ïîñëåäíåãî ðàñøèôðîâàííîãî áëîêà. ×òîáû ýòîò ìåòîä ðàáîòàë ïðàâèëüíî, êàæäîå ñîîáùåíèå äîëæíî áûòü äîïîëíåíî. Äàæå åñëè îêðûòûé òåêñò ñîäåðæèò öåëîå ÷èñëî áëîêîâ, âàì ïðèäåòñÿ äîáàâèòü îäèí ïîëíûé áëîê. Ñ äðóãîé ñòîðîíû, ìîæíî èñïîëüçîâàòü ñèãíàë êîíöà ôàéëà äëÿ îáîçíà÷åíèÿ ïîñëåäíåãî áàéòà îêðûòîãî òåêñòà è äîïîëíèòü ýòîò ñèãíàë er.

Íà 8-é ïîêàçàí äðóãîé âàðèàíò, íàçûâàåìûé **ïîñëåäíèì øèôðîâêñòà** [402]. P_{n-1} - ïîñëåäíèé ïîëíûé áëîê îòêðûòîãî òåêñòà, à P_n - ïîñëåäíèé, êîðîòêèé áëîê îòêðûòîãî òåêñòà. $\tilde{N}_{n-1}$ - ïîñëåäíèé ïîëíûé áëîê øèôðîòåêñòà, è $\tilde{N}_n$ - ïîñëåäíèé, êîðîòêèé áëîê øèôðîòåêñòà. $\tilde{N}'$ - ýòî ïðîìåæóòî÷íûé ðåçóëüòàò, íå ÿâëÿþùèéñÿ ÷àñòüþ ïåðâîíà÷àëüíîãî øèôðîòåêñòà.



Ðèñ. 9-1. Ïîñëåäíèå øèôðîòåêñòà.

9.2 Ïîâòîð áëîêà

Áîëåå ñåðüåçíîé ïðîáëåìîé ðåæèìà ECB ÿâëÿåòñÿ òî, ÷òî âðàã ìîæåò èçìåíèòü øèôðîâàííûå ñîîáùåíèÿ, íå çíàÿ êëþ÷à èëè äàæå àëãîðèòìà, ÷òîáû îáìàíóòü ïðåäïîëàãàåìîãî ïîëó÷àòåëÿ. Âïåðâûå ýòà ïðîáëåìà ðàññìîòðåíà â [291].

Äëÿ èëëþñòðàöèè ýòîé ïðîáëåìû ðàññìîòðèì ñèñòåìó ïåðåäà÷è äâîè÷íûõ äàííûõ, êîòîðàÿ ïðåîáðàçóåò èõ â ïîñëåäîâàòåëüíîñòü áëîêîâ ôèêñèðîâàííîé äëèíû. Ïðåäïîëîæèì, ÷òî îíà ðàáîòàåò â ðåæèìå ECB.

Ìýëîðè, êîòîðûé ïîäñëóøèâàåò ëèíèþ ñâÿçè ìåæäó áàíêàìè, áàíêîì Àëèñû è áàíêîì Áîáà, ìîæåò èñïîëüçîâàòü äëÿ îáìàíà Àëèñû â áàíê Áîáà. Çàòåì, îí ïðåâîñõîäèò $100 èç áàíêà Àëèñû íà ñâîé ñ÷åò â áàíê

Áîáà. Ïîçæå, îí ïîâòîðÿåò ýòó îïåðàöèþ åùå ðàç. Ñ ïîìîùüþ ñâîåãî êîìïüþòåðà îí ïðîâåðÿåò çàïèñàííûå ñîîáùåíèÿ, ðàçûñêèâàÿ ïàðó èäåíòè÷íûõ ñîîáùåíèé. Ýòè ñîîáùåíèÿìè ÿâëÿþòñÿ òå ñîîáùåíèÿ, êîòîðûå îí ïåðåâîäèò $100 íà ñâîé ñ÷åò. Åñëè îí íàõîäèò íåñêîëüêî ïàð îäèíàêîâûõ ñîîáùåíèé (÷òî áîëüøå ïîõîæå íà ðåàëüíóþ æèçíü), îí äåëàåò åùå îäíî äåéñòâèå è çàïèñûâàåò ðåçóëüòàò. Â êîíöå êîíöîâ îí ñìîæåò âûäåëèòü ñîîáùåíèå, êîòîðûì áûë ïðîâåäåí èìåííî åãî ïðåâîä.

Òåïåðü îí ìîæåò îòïðàâèòü ýòî ñîîáùåíèå ïî êàíàëó ñâÿçè, êîãäà çàõî÷åò. Êàæäîå ñîîáùåíèå ïðèâåäåò ê çà÷èñëåíèþ íà åãî ñ÷åò â áàíêå Áîáà åùå $100. Êîãäà îáà áàíêà ñâåðÿò ñâîè ïðåäâîäû (âîçìîæíî â êîíöå äíÿ), îíè îáìåíÿþò ïðåäâîäû-ïðèçðàêè, íî åñëè Ìýëîðè äîñòàòî÷íî óìíî, îí óæå ñáåæèò â êàêóþ-íèáóäü áàíêîâñêóþ ðåãióëèêó áåç äîãîâîðà îá ýêñòðàäèöèè, ïðèõâàòèâ ñ ñîáîé äåíüãè. È ñêîðåå âñåãî îí èñ÷åçíåò ñòîìû íåñêîëüêî áîëüøå $100 è ïðîâåðíåò îòåðàöèþ ñðàçó äëÿ íåñêîëüêèõ áàíêîâ.

Íà ïåðâûé âçãëÿä áàíêè ìîãóò ëåãêî ïðåñ÷ü ýòî, äîáàâëÿÿ ìåòêè âðåìåíè ê ñâîèì ñîîáùåíèÿì.

Ìåòêà äàòû/âðåìåíè	1 áëîê
Áàíê 1: Ïåðåäà÷à	1.5 áëîêà
Áàíê 2: Ïðèåì	1.5 áëîêà
Èìÿ âêëàä÷èêà	6 áëîêîâ
Ñ÷åò âêëàä÷èêà	2 áëîêà
Ñóììà âêëàäà	1 áëîê

Â òàêîé ñèñòåìå äâà èäåíòè÷íûõ ñîîáùåíèÿ áóäóò ëåãêî îáíàðóæåíû. Òåì íå ìåíåå, ñ ïîìîùüþ ìåòîäà, íàçûâàåìîãî **ïîâòîðíîì áëîêà**, Ìýëîðè âñå æå ñìîæåò îáîãàòèòüñÿ. Íà 7-é ïîêàçàíî, ÷òî Ìýëîðè ìîæåò ñîáðàòü âîñåìü áëîêîâ øèôðîòåêñòà, ñîòâåòñòâóþùèõ åãî èìåíè è íîìåðó ñ÷åòà: áëîêè ñ 5 ïî 12. Â ýòîò ìîìåíò óìíòíî äüÿâîëüñêè ðàññìåÿòüñÿ, âåäü Ìýëîðè óæå â ïîëíîé ãîòîâíîñòè.

Íîìåð áëîêà

1	2	3	4	5	6	7	8	9	10	11	12	13
Ìåòêà âðåìåíè	Áàíê îòïðàâèòåëü		Áàíê ïîëó÷àòåëü	Èìÿ âêëàä÷èêà						Ñ÷åò âêëàä÷èêà		Ñóììà

Ïîëå

Ðèñ. 9-2. Áëîêè øèôðîâàíèÿ â çàïèñè ïðèâåäåííîãî ïðèìåðà.

Î íåðåøàòåëüíàòî ñîîáùåíèÿ èç áàíêà Àëèñû â áàíê Áîáà è çàìåíÿåò áëîêè ñ 5 ïî 12 ñîîáùåíèÿ áàéòàìè, ñîòâåòñòâóþùèìè åãî èìåíè è íîìåðó ñ÷åòà. Çàòåì îí ïîñûëàåò èçìåíåííûå ñîîáùåíèÿ â áàíê Áîáà. Åìó íå íóæíî çíàòü, êòî áûë îòïðàâèòåëåì äåíåã, åìó äàæå íå íóæíî çíàòü ïåðåâîäèìóþ ñóììó (õîòÿ îí ìîæåò ñâÿçàòü ïîäîáíûå ñîîáùåíèÿ ñ ñîîòâåòñòâóþùèì óâåëè÷åíèåì ñâîåãî ñ÷åòà è îïðåäåëèòü áëîêè, ñîîòâåòñòâóþùèå îïðåäåëåííûì äåíåæíûì ñóììàì). Î ïðîòî èçìåíÿåò èìÿ è íîìåð ñ÷åòà íà ñâîè ñîáñòâåííûå è ñëåäèò çà ðîñòîì ñâîèõ äîõîäîâ. (ß ïîíÿ, ÷òî Ìýëîðè íàäî áûëî îñòîðîæíûì, ÷òîáû íå ìîãëè èíîé îòëè÷èòåëüíûé ïðèçíàê.)

Äëÿ îáíàðóæåíèÿ òàêîãî ñïîñîáà áàíêàì îäíîãî äíÿ íå õâàòèò. Êîãäà îíè ñâåðÿò ñâîè ïåðåâîäû â êîíöå äíÿ, âñå ñóììû ñîâïàäóò. Âîçìîæíî, ïîêà íàñòîÿùèé âêëàä÷èê íå çàìåòèò, ÷òî åãî âêëàäû íå çà÷èñëÿþòñÿ íà ñ÷åò, èëè ïîêà êòî-íèáóäü íå îáðàòèò âíèìàíèå íà íåîæèäàííóþ âêòèâíîñòü ðàáîòû ñî ñ÷åòîì Ìýëîðè, áàíêè íå ñìîãóò çàìåòèòü íèêàêèõ ñëåäîâ. Ìýëîðè íå äëóí è ê ýòîìó âðåìåíè çàêðîåò ñâîé ñ÷åò, èçìåíèò èìÿ è êóïèò âèëëó â Àðãåíòèíå.

Áàíêè ìîãóò ìèíèìèçèðîâàòü ýòó ïðîáëåìó, ÷àñòî ìåíÿÿ ñâîè êëþ÷è, íî ýòî îçíà÷àåò òîëüêî, ÷òî Ìýëîðè ïðèäåòñÿ äåéſòâîâàòü ïîâûñîêî. Îäíàêî, äîáàâëåíèå MAC òàêæå ðåøèò ïðîáëåìó. Íåñìîòðÿ íà ýòî ðàññìàòðèâàåìàÿ ïðîáëåìà ôóíäàìåíòàëüíà äëÿ ðåæèìà ECB. Ìýëîðè óäàëÿòü, ïîâòîðÿòü èëè çàìåíÿòü áëîêè ïî ñâîåìó óñìîòðåíèþ. Ðåøåíèåì ÿâëÿåòñÿ ñïîñîá, íàçûâàåìûé **ñöåïëåíèåì**.

9.3 Ðåæèì ñöåïëåíèÿ áëîêîâ øèôðà

Ñöåïëåíèå äîáàâëÿåò ê áëîê-íîìó øèôðó ìåõàíèçì îáðàòíîé ñâÿçè: ðåçóëüòàòû øèôðîâàíèÿ ïðåäûäóùèõ áëîêîâ âêëþ÷àþò íà øèôðîâàíèå òåêóùåãî áëîêà. Äóõàèì ñëîâàìè, êàæäûé áëîê ñòîíîëüçóåòñÿ äëÿ èçìåíåíèÿ øèôðîâàíèÿ ñëåäóþùåãî áëîêà. Êàæäûé áëîê øèôðîòåêñòà çàâèñèò íå òîëüêî îò øèôðóåìîãî áëîêà îòêðûòîãî òåêñòà, íî è îò âñåõ ïðåäûäóùèõ áëîêîâ îòêðûòîãî òåêñòà.

Â ðåæèìå **ñöåïëåíèÿ áëîêîâ øèôðà (**cipher block chaining, CBC) ïåðåä øèôðîâàíèåì íàä îòêðûòûì òåêñòîì è ïðåäûäóùèì áëîêîì øèôðîòåêſòà âûïîëíÿåòſÿ îïåðàöèÿ XOR. Íà 6-é (à) ïîêàçàíî øèôðîâàíèå CBC â äåéſòâèè. ‚Êîãäà áëîê îòêðûòîãî òåêſòà çàøèôðîâàí, ïîëó÷åííûé øèôðîòåêſò ñîõðàíſåòſÿ â ðåãiſòðå îáðàòíîé ſâſçè. Ïðåæäå ÷åì áóäåò çàøèôðîâàí ſëåäóþùèé áëîê îòêðûòîãî òåêſòà, îí ïîäâðãàåòſÿ îïåðàöèè XOR âìåſòå

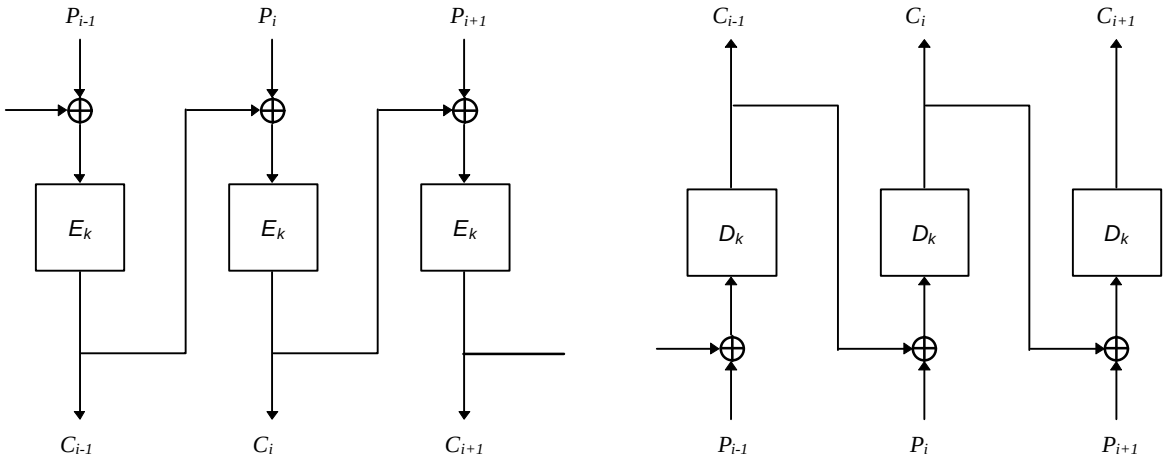
ñ ñîääðæèìûì ðåãèñòðà îáðàòíîé ñâÿçè. Òàêèì îáðàçîì ñîçäàþòñÿ âõîäíûå äàííûå äëÿ ñëåäóþùåãî ýòàïà ïðîöåäóðû øèôðîâàíèÿ. Ïîëó÷åííûé øèôðîòåêñò ñîõðàíÿåòñÿ â ðåãèñòðå îáðàòíîé ñâÿçè, ÷òîáû ïîäâåðãíóòüñÿ îïåðàöèè XOR âìåñòå ñî ñëåäóþùèì áëîêîì îðèãèíàëüíîãî òåêñòà, è òàê äî êîíöà ñîîáùåíèÿ. Øèôðîâàíèå êàæäîãî áëîêà çàâèñèò îò âñåõ ïðåäûäóùèõ áëîêîâ.

Äåøèôðîâàíèå ÿâëÿåòñÿ îáðàòíîé îïåðàöèåé (ñì. Figure 9.3 (á)). Áëîê øèôðîòåêñòà ðàñøèôðîâûâàåòñÿ êàê îáû÷íî, íî ñîõðàíÿåòñÿ â ðåãèñòðå îáðàòíîé ñâÿçè. Çàòåì ñëåäóþùèé áëîê äåøèôðîâóåòñÿ è ïîâåðõàåòñÿ îïåðàöèè XOR âìåñòå ñ ñîäåðæèìûì ðåãèñòðà îáðàòíîé ñâÿçè. Òåïåðü ñëåäóþùèé áëîê øèôðîòåêñòà ñîõðàíÿåòñÿ â ðåãèñòðå îáðàòíîé ñâÿçè, è òàê äàëåå, äî êîíöà ñîîáùåíèÿ.

Ìàòåìàòè÷åñêè ýòî âûãëÿäèò ñëåäóþùèì îáðàçîì:

$$C_i = E_K(P_i \oplus C_{i-1})$$

$$P_i = C_{i-1} \oplus D_K(C_i)$$



(à) Øèôðîâàíèå CBC

(á) Äåøèôðîâàíèå CBC

Ðèñ. 9-3. Ðåæèì ñòåïëåíèÿ áëîêîâ øèôðà.

Âåêòîð èíèöèàëèçàöèè

Â ðåæèìå CBC îäíàêîâûå áëîêè îòêðûòîãî òåêñòà ïðè øèôðîâàíèè ïåðåõîäÿò â ðàçëè÷íûå áëîêè øèôðîòåêñòà òîëüêî, åñëè îòëè÷àëèñü êàêèå-òî èç ïðåäøåñòâóþùèõ áëîêîâ îòêðûòîãî òåêñòà. Äâà èäåíòè÷íûõ ñîîáùåíèÿ, îäíàêî, áóäóò øèôðîâàòüñÿ êàê îäèí è òîò æå øèôðîòåêñò. ×òî åùå õóæå, äâà îäèíàêîâî íà÷èíàþùèõñÿ ñîîáùåíèÿ áóäóò øèôðîâàòüñÿ îäèíàêîâî, ïîêà íå ïîÿâèòñÿ ïåðâîå ðàçëè÷èå.

Ó ðÿäà ñîîáùåíèé ìîæåò áûòü îäèíàêîâûé çàãîëîâîê - òåìà ïèñüìà, ñòðîêà "From" èëè åùå ÷òî-íèáóäü. Õîòÿ ïîâòîð áëîêà áóäåò íåâîçìîæåí, òàêîå îäèíàêîâîå íà÷àëî ìîæåò ïðåäîñòàâèòü êðèòè÷åñêóþ êàêóþ-íèáóäü ïîëåçíóþ èíôîðìàöèþ.

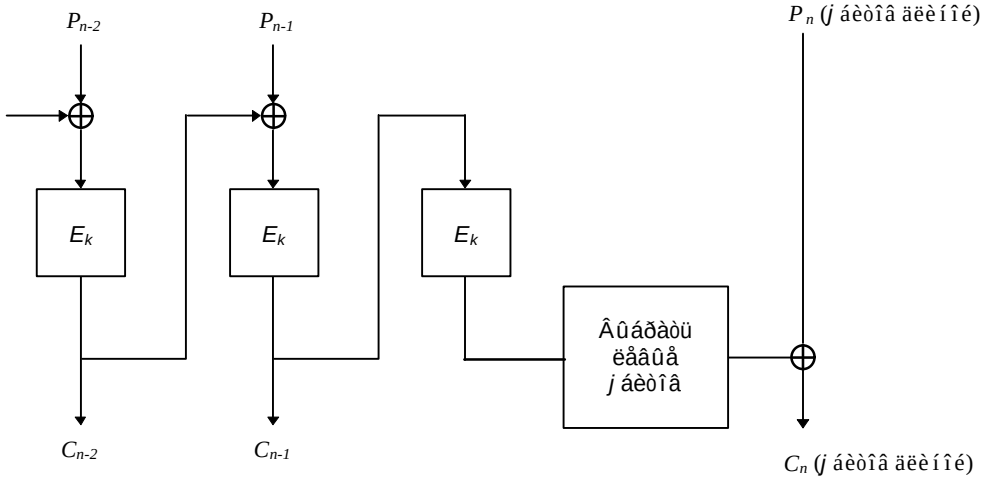
Èçáåæàòü ýòîãî ìîæíî, øèôðóÿ â êà÷åñòâå ïåðâîãî áëîêà êàêèå-òî ñëó÷àéíûå äàííûå. Ýòîò áëîê ñëó÷àéíûõ äàííûõ íàçûâàåòñÿ âåêòîðîì èíèöèàëèçàöèè (initialization vector, IV), èíèöèàëèçèðóþùåé ïåðâîíà÷àëüíîì çíà÷åíèè ñöåïëåíèÿ. IV íå èìåò íèêàêîãî ñìûñëîâîãî çíà÷åíèÿ, îí èñïîëüçóåòñÿ òîëüêî äëÿ òîãî, ÷òîáû ñäåëàòü êàæäîå ñîîáùåíèå óíèêàëüíûì. Êîãäà ïîëó÷àòåëü ðàñøèôðîâûâàåò ýòîò áëîê, îí èñïîëüçóåò åãî òîëüêî äëÿ çàïîëíåíèÿ ðåãèñòðà îáðàòíîé ñâÿçè. Õîðîøèì IV ñëóæèò ìåòêà âðåìåíè. Èëè èñïîëüçóéòå êàêèå-íèáóäü ñëó÷àéíûå áèòû.

Ñ èñïîëüçîâàíèåì IV ñîîáùåíèÿ ñ èäåíòè÷íûì îòêðûòûì òåêñòîì ïðè øèôðîâàíèè ïåðâîãî â ñîîáùåíèÿ ñ ðàçëè÷íûì øèôðîòåêñòîì. Ñëåäîâàòåëüíî, çëîóìûøëåííèê íå ñìîæåò ïðåäïðèíÿòü ïîâòîð áëîêà, è çàòðóäíèòñÿ ñîçäàíèå øèôðîâàííîãî êíèãè. Õîòÿ ðåêîìåíäóåòñÿ äëÿ êàæäîãî ñîîáùåíèÿ øèôðîâàòü óíèêàëüíûé IV, ýòî òðåáîâàíèå íå ÿâëÿåòñÿ îáÿçàòåëüíûì.

IV íå äîëæåí õðàíèòüñÿ â ñåêðåòå, îí ìîæåò ïåðåäàâàòüñÿ îòêðûòî âìåñòå ñ øèôðîòåêñòîì. Åñëè âû íå ïîíèìàåòå ïî÷åìó, ðàññìîòðèì ñëåäóþùèé äîâîä. Ïóñòü íàøå ñîîáùåíèå ñîñòîèò èç íåñêîëüêèõ áëîêîâ: B_1, B_2, ..., B_i. B_1 øèôðóåòñÿ âìåñòå ñ IV. B_2 øèôðóåòñÿ ñ èñïîëüçîâàíèåì øèôðîòåêñòà B_1 â ðîëè IV. B_3 øèôðóåòñÿ ñ èñïîëüçîâàíèåì øèôðîòåêñòà B_2 â ðîëè IV, è òàê äàëåå. Èòàê, åñëè êîëè÷åñòâî áëîêîâ - *n*, òî *n-1* "âåêòîðîâ èíèöèàëèçàöèè" îòêðûòû, äàæå åñëè ïåðâîíà÷àëüíûé IV õðàíèòñÿ â ñåêðåòå. Ï îýòîì ïðè÷èí õðàíèòü â ñåêðåòå IV íåò, IV - ýòî ïðîñòî áëîê-çàãëóøêà, ìîæíî ñ÷èòàòü åãî íóëåâûì áëîêîì ñöåïëåíèÿ B_0.

Íàáèâêà

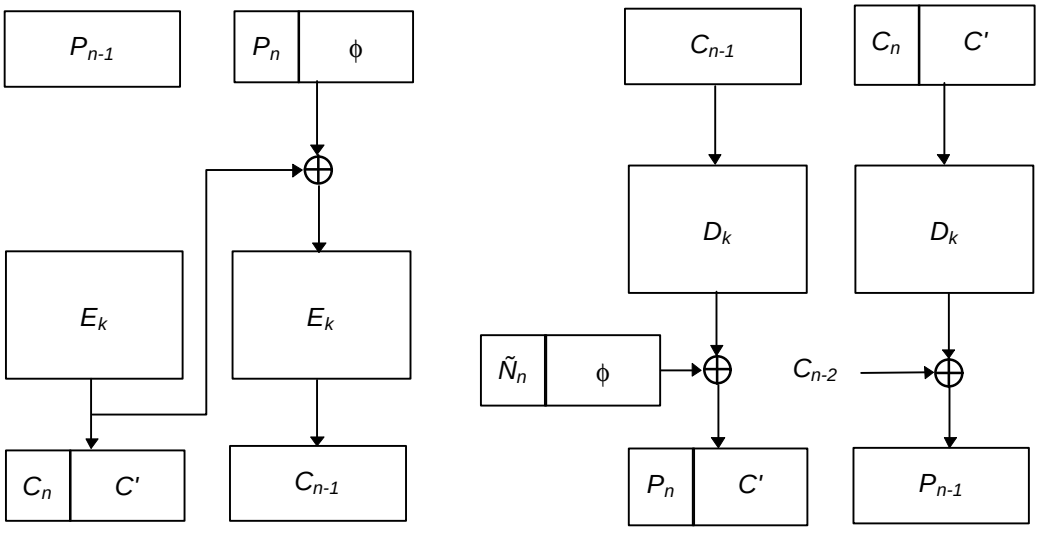
Íàáèâêà èñïîëüçóåòñÿ òàêæå, êàê è â ðåæèìå ECB, íî â íåêîòîðûõ ïðèëîæåíèÿõ ðàçìåð øèôðîâêè äîëæåí â òî÷íîñòè ñîâïàäàòü ñ ðàçìåðîì îêðûòîãî òåêñòà. Ì îæåò áûòü, çàøèôðîâàíî íåêîòîðîå êîëè÷åñòâî áëîêîâ, ïîýòîìó íåîáõîäèìî äîáàâëåíèå êîðîòêèõ áëîê ïðèäóòñÿ øèôðîâàíèÿ. Ïóñòü ïîñëåäíèé áëîê ñîñòîèò èç *l* áèòîâ. Çàøèôðîâàâ ïîñëåäíèé ïîëíûé áëîê, ñîââ çàøèôðóéòå øèôðîâêîé, âûáåðèòå ñòàðøèå *l* áèòîâ è âûïîëíèòå äëÿ íèõ è êîðîòêîãî áëîêà îïåðàöèþ XOR, ñîçäàâàÿ øèôðîâåñò. Ýòà ïðîöåäóðà ïîêàçàíà íà 5-é.



Ðèñ. 9-4. Øèôðîâàíèå êîðîòêîãî ïîñëåäíåãî áëîêà â ðåæèìå CBÑ.

Ñëàáîñòü ýòîãî ñïîñîáà â òîì, ÷òî õîòÿ Ì ýëëèôðè íå ñìîæåò ðàñêðûòü ïîñëåäíèé áëîê øèôðîâêè, îí ìîæåò ñèñòåìàòè÷åñêè èçìåíÿòü îòäåëüíûå áèòû øèôðîâêè. Åñëè ïîñëåäíèå íåñêîëüêî áèòîâ øèôðîâêè ñîâðåìåííûõ âàæíóþ èíôîðìàöèþ, ýòî îïàñíî. Åñëè ïîñëåäíèå áèòû ïðîñòî ñîâðåìåííûõ ñîâåò ïî äîìîâîäñòâó, òî íè÷åãî ñòðàøíîãî.

Ëó÷øèì ñïîñîáîì ÿâëÿåòñÿ ïîñëåäíåå ùèôðîâàíèå (ñì. 4th) [402]. P_{n-1} - ïîñëåäíèé ïîëíûé áëîê îòêðûòîãî òåêñòà, P_n - çàêëþ÷èòåëüíûé, êîðîòêèé áëîê îòêðûòîãî òåêñòà. $Ñ_{n-1}$ - ïîñëåäíèé ïîëíûé áëîê øèôðîâàííîãî òåêñòà, $Ñ_n$ - çàêëþ÷èòåëüíûé, êîðîòêèé áëîê øèôðîâàííîãî òåêñòà. *C'* - ýòî ïðîñòî ïðîìåæóòî÷íûé ðåçóëüòàò, íå ÿâëÿþùèéñÿ ÷àñòüþ ïåðâîíà÷àëüíîãî øèôðîâàííîãî òåêñòà. Ïðåìóùåñòâî ýòîãî ìåòîäà ÿâëÿåòñÿ òî, ÷òî âñå áèòû îòêðûòîãî òåêñòà ñîõðàíÿþ ïðîïîðöèîíàëüíóþ ÷àñòîòó ÷åðåç àëãîðèòì øèôðîâàíèÿ.



Ðèñ. 9-5. Ïîñëåäíèå øèôðîâêè â ðåæèìå CBÑ.

Ðàñïðîñòðàíåíèå îøèáêè

Ðåæèì CBC õàðàêòåðèçóåòñÿ **ïðÿìîé íåðàòíîé ñâÿçüþ** øèôðîâêè ïðè øèôðîâàíèè è **èíâåðñíîé íåðàòíîé ñâÿçüþ** øèôðîâêè ïðè äåøèôðîâàíèè. Ïðè ýòîì ïðîëîæåíèÿ äîëæíû óìåòü áîðîòüñÿ ñ îøèáêàìè. Äâóñòîðîííÿÿ áèòîâàÿ îøèáêà â áëîêå îêðûòîãî òåêñòà ïîâëèÿåò íà äâóõíûé áëîê øèôðîâêè è âñå ïîñëåäóþùèå áëîêè øèôðîâêè. Ýòî íå âàæíî, ïîòîìó ÷òî äøèôðîâêîâàííûé èíâåðòèðóåò ýòîò ýôôåêò, è âîññòàíîâ-

ëåííûé îòêðûòûé òåêñò áóäåò ñîäåðæàòü òó æå äëèíóòåííóþ îøèáêó.

×àùå âñòðå÷àþòñÿ îøèáêè øèôðîâàíèÿ èç-çà øóìà ëèíèé ïåðåäà÷è èëè ñáîåâ óñòðîéñòâ õðàíåíèÿ. Â ðåæèìå CBC îøèáêà îäíîãî áèòà øèôðîâàííà âëèÿåò íà îäèí áëîê è îäèí áèò âîññòàíîâëåíèíîãî îòêðûòîãî òåêñòà. Áëîê, ñîîòâåòñòâóþùèé ñîâðåìåííîé áèò, íàõîäèòñÿ â òî÷íîñòè, ÷òî è îùèáî÷íûé áèò. Ýòî ñâîéñòâî ïðåâðàùàåò òàêîé øèôðîâàííûé òåêñò â íàäåæíûé êîä äëÿ îáíàðóæåíèÿ è èñïðàâëåíèÿ îøèáîê.

Ýòî ñâîéñòâî ïðåâðàùàåò ìàëîé îøèáêè øèôðîâàííà â áîëüøóþ îøèáêó îòêðûòîãî òåêñòà íàçûâàåòñÿ **ðàñïðîñòðàíåíèåì îøèáêè**. Ýòî ÿâëÿåòñÿ ãëàâíûì íåäîñòàòêîì. Ýòà îøèáêà íå âëèÿåò íà áëîêè, ðàñïîëîæåííûå ÷åðåç îäèí îò èñïîð÷åííîãî è äàëåå, ïîýòîìó ðåæèì CBC ÿâëÿåòñÿ **ñàìîâîññòàíàâëèâàþùèìñÿ**. Îøèáêà âëèÿåò íà äâà áëîêà, íî ñèñòåìà ïðîäîëæàåò ðàáîòàòü ïðàâèëüíî äëÿ âñåõ ïîñëåäóþùèõ áëîêîâ. CBC ïðåäñòàâëÿåò ñîáîé ïðèìåð áëî÷íîãî øèôðà, èñïîëüçóåìîãî â ñàìîñèíõðîíèçèðóþùåéñÿ ìàíåðå, íî òîëüêî íà áëîêîâîì óðîâíå.

Õîòÿ ðåæèì CBC áûñòðî âîññòàíàâëèâàåòñÿ îò áèòîâîãî ñáîÿ, îí àáñîëþòíî íå óñòîé÷èâ ê îøèáêàì ñèíõðîíèçàöèè. Åñëè â ïîòîêå øèôðîâàííà òåðÿþòñÿ äëè äîâàëüíûå áëîêè, òî ïîëíîñòüþ áëîêîâ ñäâèãàþòñÿ íà îäèí áèò, è íà âûõîäå äåøèôðîâùèêà áóäåò ñïëîøíîé ìóñîð. Ëþáàÿ êðèïòîñèñòåìà, èñïîëüçóþùàÿ ðåæèì CBC äîëæíà îáñëåæèâàòü öåëîñòíîñòü áëî÷íîé ñòðóêòóðû ëèáî ïðîùå êàäðîâ, ëèáî ñîõðàíÿÿ äàííûå â ñòðóêòóðû èç íåñêîëüêèõ áëîêîâ.

Âîïðîñû áåçîïàñíîñòè

Ðÿä âîçìîæíûõ ïðîáëåì îáóñëàâëèâàþòñÿ ñòðóêòóðîé CBC. Âî ïåðâûõ, òàê êàê áëîê øèôðîâàííà äîñòàòî÷íî ïðîñòî âëèÿåò íà ñëåäóþùèé áëîê, Ìýëëîðè ìîæåò òàéíî äîáàâëÿòü áëîêè ê êîíöó çàøèôðîâàííîãî ñîîáùåíèÿ. Êîíå÷íî, ïðè äåøèôðîâàíèè îíè ïðåâðàòÿòñÿ â ÷åïóõ, íî â íåïîíÿòíûõ ñèóàöèÿõ ýòî íåæåëàòåëüíî.

Ïðè èñïîëüçîâàíèè CBC âû äîëæíû ñòðóêòóðèðîâàòü âàø îòêðûòûé òåêſò òàê, ÷òîáû âû çíàëè, ääå íàõîäÿòñÿ êîíöû ñîîáùåíèé, è ìîãëè îáíàðóæèòü äîáàâëåíèå ëèøíèõ áëîêîâ. Êðèïòîñèñòåìà òîæå ïðåâðàùàåòñÿ â ÷åïóõó, íî â íåïîíÿòíûõ ñèóàöèÿõ ýòî íåæåëàòåëüíî.

Ïðè èñïîëüçîâàíèè CBC âû äîëæíû ñòðóêòóðèðîâàòü âàø îòêðûòûé òåêſò òàê, ÷òîáû âû çíàëè, ääå íàõîäÿòñÿ êîíöû áëîêîâ, è íå áûëî îáíàðóæèòü äîáàâëåíèå ëèøíèõ áëîêîâ. Êîìáèíèðîâàíèå CBC âû äîëæíû ñòðóêòóðèðîâàòü âàø îòêðûòûé òåêſò òàê, ÷òîáû âû çíàëè, ääå íàõîäÿòñÿ êîíöû áëîêîâ, è íå áûëî îáíàðóæèòü äîáàâëåíèå ëèøíèõ áëîêîâ. Âîçìîæíû ñèòóàöèè, êîãäà ýòî íåæåëàòåëüíî. Îòêðûòå ñîîáùåíèÿ äîëæíî îáëàäàòü ñòåïåíüþ èëè ñðåäñòâàìè èäåíòèôèêàöèè.

Íàêîíåö, õîòÿ ñòðóêòóðà îòêðûòîãî òåêſòà ìàñêèðóåòñÿ ñöåïëåíèåì, ñòðóêòóðà î÷åíü äëèííûõ ñîîáùåíèé âñå ðàâíî çàìåòíà. Ïàðàäîêñ äîïóñêàåò ïðîäâèíóòûå àòàêè, ÷òî ïîñëå $2^{m/2}$ áëîêîâ, ãäå m - ðàçìåð áëîêà, ïîÿâëÿþòñÿ îäèíàêîâûå áëîêè. Äëÿ 64-áèòîâîãî áëîêà äëèíà òàêîãî ñîîáùåíèÿ ïðèìåðíî ðàâíà 32 Ãáàéòàì. Ïîäîáíàÿ ïðîáëåìà âîçíèêàåò òîëüêî äëÿ ñîîáùåíèé íåìàëåíüêîãî ðàçìåðà.

9.4 Ïîòîêîâûå øèôðû

Ïîòîêîâûå øèôðû ïðåíáðàçóþò îòêðûòûé òåêſò â øèôðîâàííûé ïî îäíîìó áèòó çà îïåðàöèþ. Ïðîñòåéøàÿ ðåàëèçàöèÿ ïîòîêîâîãî øèôðà ïîêàçàíà íà 3-é. **Ãåíåðàòîð ïîòîêà êëþ÷åé** (èíîãäà íàçûâàåìûé ãåíåðàòîðîì ñ áåãóùèì êëþ÷îì) âûäàåò ïîòîê áèòîâ: k_1, k_2, k_3, ..., k_i. Ýòîò ïîòîê êëþ÷åé (èíîãäà íàçûâàåìûé áãóùèì êëþ÷îì) è ïîòîê áèòîâ îòêðûòîãî òåêſòà, p_1, p_2, p_3, ..., p_i, ïîäâåðãàþòñÿ îïåðàöèè "èñêëþ÷àþùåå èëè", è â ðåçóëüòàòå ïîëó÷àþòñÿ ïîòîê áèòîâ øèôðîâàííîãî òåêſòà.

$c_i = p_i \oplus k_i$

Ïðè äåøèôðîâàíèè îïåðàöèÿ XOR âûïîëíÿåòñÿ íàä áèòàìè øèôðîâàííà è òåì æå ñàìûì ïîòîêîì êëþ÷åé äëÿ âîññòàíîâëåíèÿ áèòîâ îòêðûòîãî òåêſòà.

$p_i = c_i \oplus k_i$

Òàê êàê

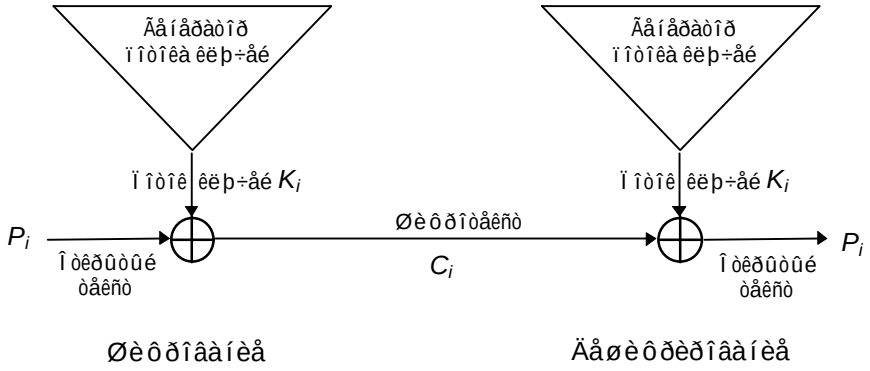
$p_i \oplus k_i \oplus k_i = p_i$

ýòî ðàâíîñèëî ïðàâèëüíî.

Áåçîïàñíîñòü ñèſòåìû ïîëíîñòüþ çàâèſèò îò ñâîéſòâ ãåíåðàòîðà ïîòîêà êëþ÷åé. Åſëè ãåíåðàòîð ïîòîêà êëþ÷åé âûäàſò áåſêîíå÷íóþ ſòðîêó íóëåé, øèôðîâſêò áóäſò ſîâſïàäſòü ſ îſðàſîâſííûſ òåſêſòîì, è âſå îſåðàöèÿ áóäſò áåſſìſûſåſíà. Åſëè ãåíåðàòîð ïîòîêà êëþ÷åé âûïåâûâſò ïîâòîðÿþùèſſÿ 16-áèòîâûé øàáëîí, àëãîðèòì áóäſò ÿâſÿòſſſÿ ſðſſòûì XOR ſ ſðåſáſðåſæèſî ſàëîé áåçſſàſſſſòüþ (ſì. ðàçäåë 1.4). Åſëè ãåíåðàòîð ſſòſêà êëþ÷åé âûſëåâûâſò áåſêſſſſ÷íûé ſſòſê ſëó÷àéſûõ (ſſ íàſòſÿûſåſó, à íå ſſſâſſſſëó÷àéſûõ - ſì. ðàçäåë 2.8) áèòâ, âû ſſëó÷åſòå ſſſſſðàçſâûé áëſêſſò è èſåſëüſóþ áåçſſàſſſſòü.

Íà äåëå áåçſſàſſſòü ſſòſêſâſãſ øèſðà íàſſäèòſÿ ãää-òſ ſåæäó ſðſſòûſ XOR è ſſſſðàçſâûſ áëſêſſòſſ.

Ãåíåðàòîð ïîòîêà êëþ÷åé ñîçäàåò áèòîâûé ïîòîê, êîòîðûé ïîõîæ íà ñëó÷àéíûé, íî â äåéñòâèòåëüíîñòè äåòåðìèíèðîâàí è ìîæåò áûòü ðåçîíèðîâàí ïðè äåøèôðèðîâàíèè. ×åì áëèæå âûõîä ãåíåðàòîðà ïîòîêà êëþ÷åé ê ñëó÷àéíîìó, òåì áîëüøå âðåìåíè ïîòðåáóåòñÿ êðèïòîàíàëèòèêó, ÷òîáû âçëîìàòü øèôð.



Ðèñ. 9-6. Ïîòîêîâûé øèôð

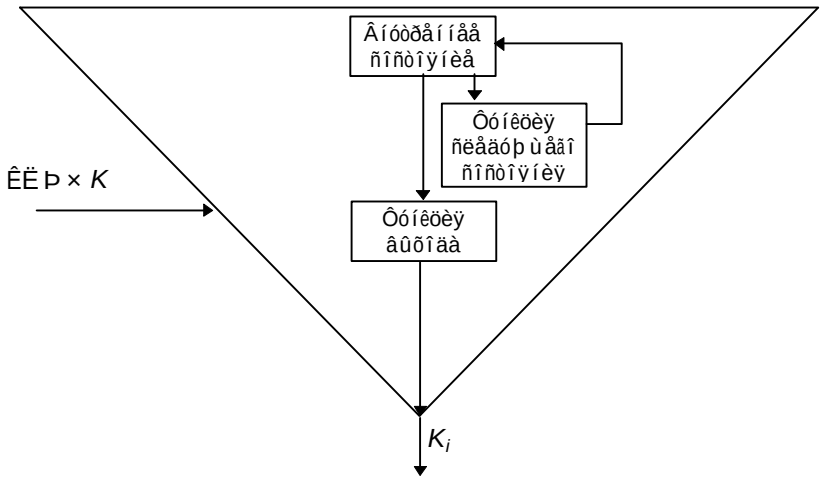
Îäíàêî, åñëè ãåíåðàòîð ïîòîêà êëþ÷åé ïðè êàæäîì âûçîâå ïîëó÷àåò îäèí è òîò æå áèòîâûé ïîòîê, òî èñïîëüçóþùóþ åãî êðèïòîñèñòåìó âçëîìàòü íåòðóäíî. Ïîêàæåì íà ïðèìåðå, ïî÷åìó ýòî òàê.

Åñëè ê Âåå ïîïàë øèôðîòåêñò è ñîîòâåòñòâóþùèé îòêðûòûé òåêñò, òî îíà, âûïîëíÿÿ îïåðàöèþ XOR íàä îòêðûòûì òåêñòîì è øèôðîòåêñòîì, ðàñêðûâàåò ïîòîê êëþ÷åé. Èëè, åñëè ó íåå åñòü äâà ðàçëè÷íûõ øèôðîòåêñòà, çàøèôðîâàííûõ îäèíàêîâûì êëþ÷îì, îíà ìîæåò âûïîëíèòü íäè íèè ïîåðàöèþ XOR, ïîëó÷àÿ äâà îòêðûòûõ òåêñòà ñîîáùåíèé, íäè êîòîðûì è âûïîëíåíà îïåðàöèÿ XOR. Ýòî íåòðóäíî âçëîìàòü, è çàòåì îíà ìîæåò ïîëó÷èòü ïîòîê êëþ÷åé, âûïîëíÿÿ îïåðàöèþ XOR íàä îäíèì èç îòêðûòûõ òåêñòîâ è øèôðîòåêñòîì.

Òåïåðü, ïåðåõâàòèâ ëþáûå äðóãèå øèôðîâàííûå ñîîáùåíèå, îíà ñìîæåò ðàñøèôðîâàòü åãî, èñïîëüçóÿ ïîëó÷åííûé ïîòîê êëþ÷åé. Êðîìå òîãî, îíà ìîæåò ðàñøèôðîâàòü è ïðî÷èòàòü ëþáîå èç ðàíåå ïåðåõâà÷åííûõ ñîîáùåíèé. Êîãäà Âåà ïîëó÷èò ïàðó îòêðûòûé òåêñò/øèôðîòåêñò, îíà ñìîæåò ÷èòàòü âñå.

Ïîýòîìó äëÿ âñåõ ïîòîêîâûõ øèôðîâ èñïîëüçóþòñÿ êëþ÷è. Âûõîä ãåíåðàòîðà ïîòîêà êëþ÷åé ÿâëÿåòñÿ ôóíêöèåé êëþ÷à. Òåïåðü, åñëè Âåà ïîëó÷èò ïàðó îòêðûòûé òåêñò/øèôðîâàííûé òåêñò, îíà ñìîæåò ÷èòàòü òîëüêî òå ñîîáùåíèÿ, êîòîðûå çàøèôðîâàíû òåì æå êëþ÷îì. Èçìåíèòå êëþ÷, è ïðîòèâíèêó ïðèäåòñÿ íà÷àòü âñå ñíà÷àëà. Ïîòîêîâûå øèôðû îñíîâàííû ïîëåçíû äëÿ øèôðîâàíèÿ áåñêîíå÷íûõ ïîòîêîâ êîììóíèêàöèîííûõ òðàôèêîâ, íàïðèìåð, êàíàëà Ò1, ñâÿçûâàþùåãî âåá êîìïüþòåðà.

Ãåíåðàòîð ïîòîêà êëþ÷åé ñîñòîèò èç òðåõ îñíîâíûõ ÷àñòåé (ñì. 2nd). Âíóòðåííåå ñîñòîÿíèå îïèñûâàåò òåêóùåå ñîñòîÿíèå ãåíåðàòîðà ïîòîêà êëþ÷åé. Äâà ãåíåðàòîðà ïîòîêà êëþ÷åé, ñ îäèíàêîâûì êëþ÷îì è îäèíàêîâûì âíóòðåííèì ñîñòîÿíèåì, âûäàþò îäèíàêîâûé ïîòîê êëþ÷åé. Ôóíêöèÿ âûõîäà ïî âíóòðåííåìó ñîñòîÿíèþ ãåíåðèðóåò íîâîå âíóòðåííåå ñîñòîÿíèå. Ôóíêöèÿ ñëåäóþùåãî ñîñòîÿíèÿ ïî âíóòðåííåìó ñîñòîÿíèþ ãåíåðèðóåò íîâîå âíóòðåííåå ñîñòîÿíèå.

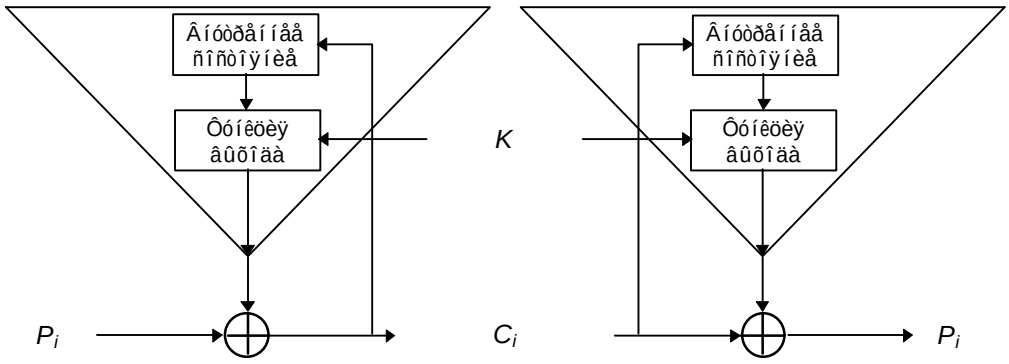


Ðèñ. 9-7. Óñòðîéñòâî ãåíåðàòîðà ïîòîêà êëþ÷åé.

9.5 Ñàìîñèíõðîíèçèðóþùèåñÿ ïîòîêîâûå øèôðû

Â **ñàìîñèíõðîíèçèðóþùèõñÿ ïîòîêîâûõ øèôðàõ** êàæäûé áèò ïîòîêà êëþ÷åé ÿâëÿåòñÿ ôóíêöèåé ôèêñèðîâàííîãî ÷èñëà ïðåäûäóùèõ áèòîâ øèôðîòåêñòà [1378]. Âîåííûå íàçûâàþò ýòîò øèôð **àâòîêëþ÷îì øèôðîòåêñòà** (ciphertext auto key, CTAK). Îñíîâíàÿ èäåÿ áûëà çàïàòåíòîâàíà â 1946 [667].

Ñàìîñèíõðîíèçèðóþùèéñÿ ïîòîêîâûé øèôð ïîêàçàí íà 1-é. Âíóòðåííåå ñîñòîÿíèå ÿâëÿåòñÿ ôóíêöèåé ïðåäûäóùèõ *n* áèòîâ øèôðîòåêñòà. Êðèïòîãðàôè÷åñêè ñëîæíîé ÿâëÿåòñÿ âûõîäíàÿ ôóíêöèÿ, êîòîðàÿ èñïîëüçóåò âíóòðåííåå ñîñòîÿíèå äëÿ ãåíåðàöèè áèòà ïîòîêà êëþ÷åé.



Ðèñ. 9-8. Ñàìîñèíõðîíèçèðóþùèéñÿ ãåíåðàòîð ïîòîêà êëþ÷åé.

Òàê êàê âíóòðåííåå ñîñòîÿíèå ïîëíîñòüþ çàâèñèò îò ïðåäûäóùèõ *n* øèôðîòåêñòà, äåøèôðèðóþùèé ãåíåðàòîð ïîòîêà êëþ÷åé àâòîìàòè÷åñêè ñèíõðîíèçèðóåòñÿ ñ øèôðóþùèì ãåíåðàòîðîì ïîòîêà êëþ÷åé, ïðèíÿâ *n* áèòîâ øèôðîòåêñòà.

Â èíòåëëåêòóàëüíûõ ðåàëèçàöèÿõ ýòîãî ðåæèìà êàæäîå ñîîáùåíèå íà÷èíàåòñÿ ñëó÷àéíûì çàãîëîâêîì äëèíîé *n* áèòîâ. Ýòîò çàãîëîâîê øèôðóåòñÿ, ïåðåäàåòñÿ è çàòåì ðàñøèôðîâûâàåòñÿ. Ðàñøèôðîâêà áóäåò íåïðàâèëüíîé, íî ïîñëå ýòèõ *n* áèòîâ îáà ãåíåðàòîðà ïîòîêà êëþ÷åé áóäóò ñèíõðîíèçèðîâàíû.

Ñëàáîé ñòîðîíîé ñàìîñèíõðîíèçèðóþùåãîñÿ ïîòîêîâîãî øèôðà ÿâëÿåòñÿ ðàñïðîñòðàíåíèå îøèáêè. Äëÿ êàæäîãî áèòà øèôðîòåêñòà, èñïîð÷åííîãî ïðè ïåðåäà÷å, äåøèôðèðóþùèé ãåíåðàòîð ïîòîêà êëþ÷åé âûäàåò *n* íåïðàâèëüíûõ áèòîâ ïîòîêà êëþ÷åé. Ñëåäîâàòåëüíî, êàæäîìó íåïðàâèëüíîìó áèòó øèôðîòåêñòà ñîîòâåòñòâóþò *n* îøèáîê â îòêðûòîì òåêñòå, ïîêà èñïîð÷åííûé áèò íå ïåðåñòàíåò âëèÿòü íà âíóòðåííåå ñîñòîÿíèå.

Âîïðîñû áåçîïàñíîñòè

Ñàìîñèíõðîíèçèðóþùèåñÿ ïîòîêîâûå øèôðû òàêæå ÷óâñòâèòåëüíû ê âñêðûòèþ ïîâòîðíîé ïåðåäà÷åé. Ñíà÷àëà Ìýëëîðè çàïèñûâàåò íåñêîëüêî áèòîâ øèôðîòåêñòà. Çàòåì, ïîçäíåå, îí âñòàâëÿåò ýòó çàïèñü â òåêóùèé òðàôèê. Ïîñëå âûäà÷è íåêîòîðîé ÷åïóõè, ïîêà ïðèíèìàþùàÿ ñòîðîíà ñèíõðîíèçèðóåòñÿ ñ âñòàâëåííîé çàïèñüþ, ñòàðûé øèôðîòåêñò áóäåò ðàñøèôðîâàí êàê íîðìàëüíûé. Ó ïðèíèìàþùåé ñòîðîíû íåò ñïîñîáà óçíàòü, ÷òî ïîëó÷åííûå äàííûå ÿâëÿþòñÿ ïîâòîðíî ïåðåäàâàåìîé çàïèñüþ. Åñëè íå èñïîëüçóþòñÿ ìåòêè âðåìåíè, Ìýëëîðè ìîæåò óáåäèòü áàíê ñíîâà è ñíîâà çà÷èñëÿòü äåíüãè íà åãî ñ÷åò, ïîâòîðíî ïåðåäàâàÿ îäíî è òî æå ñîîáùåíèå (êîíå÷íî, ïðè óñëîâèè, ÷òî êëþ÷ íå ìåíÿëñÿ). Äðóãèå ñëàáûå ìåñòà ýòîé ñõåìû ìîãóò ñòàòü çàìåòíû ïðè î÷åíü ÷àñòîé ïåðåñèíõðîíèçàöèè [408].

9.6 Ðåæèì îáðàòíîé ñâÿçè ïî øèôðó

Áëî÷íûé øèôð òàêæå ìîæåò áûòü ðåàëèçîâàí êàê ñàìîñèíõðîíèçèðóþùèéñÿ ïîòîêîâûé øèôð, òàêîé ðåæèì íàçûâàåòñÿ ðåæèìîì îáðàòíîé ñâÿçè ïî øèôðó (cipher-feedback, CFB). Â ðåæèìå CBC øèôðîâàíèå íå ìîãëî íà÷àòüñÿ, ïîêà íå ïîëó÷åí öåëûé áëîê äàííûõ. Ýòî ñîçäàåò ïðîáëåìû äëÿ íåêîòîðûõ ñåòåâûõ ïðèëîæåíèé. Íàïðèìåð, â áåçîïàñíîé ñåòåâîé ñðåäå òåðìèíàë äîëæåí èìåòü âîçìîæíîñòü ïåðåäàâàòü ãëàâíîìó êîìïüþòåðó êàæäûé ñèìâîë ñðàçó, êàê òîëüêî îí ââåäåí. Åñëè äàííûå íóæíî îáðàáàòûâàòü áàéòàìè, ðåæèì CBC òàêæå íå ðàáîòàåò.

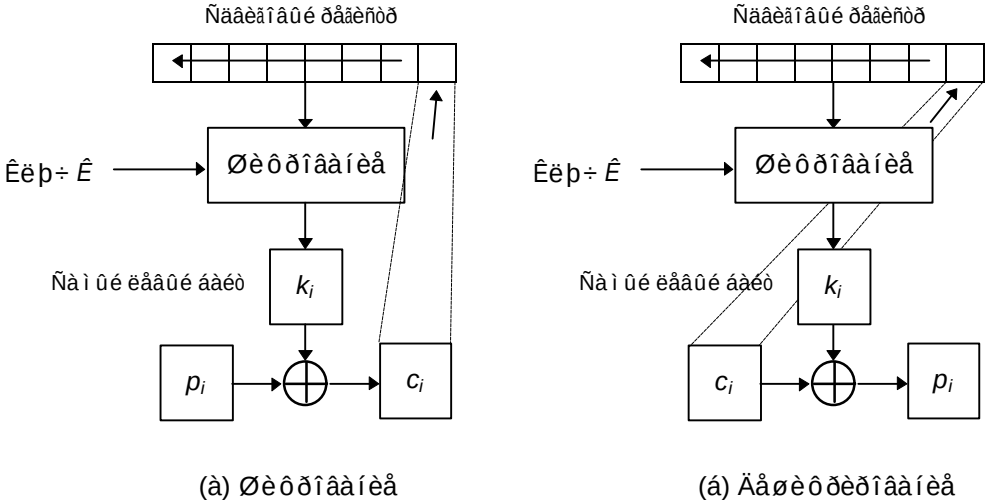
Â ðåæèìå CFB åäèíèöà çàøèôðîâàííûõ äàííûõ ìîæåò áûòü ìåíüøå ðàçìåðà áëîêà. Â ñëåäóþùåì ïðèìåðå êàæäûé ðàç øèôðóåòñÿ òîëüêî îäèí ñèìâîë ASCII (ýòî íàçûâàåòñÿ 8-áèòîâûì øèôðîâàíèåì), íî â ÷èñëå 8 íåò íè÷åãî âîëøåáíîãî. Âû ìîæåòå øèôðîâàòü äàííûå ïî îäíîìó áèòó ñ ïîìîùüþ 1-áèòîâîãî CFB, õîòÿ èñïîëüçîâàíèå äëÿ åäèíñòâåííîãî áèòà ïîëíîãî øèôðîâàíèÿ áëî÷íûì øèôðîì ïîòðåáóåò ìíîãî ðåñóðñîâ, ïîòîêîâûé øèôð â ýòîì ñëó÷àå áûë áû èäååé ïîëó÷øå. (Óìåíüøåíèå êîëè÷åñòâà öèêëîâ áëî÷íîãî ôèëüòðà äëÿ ïîâûøåíèÿ ñêîðîñòè íå ðåêîìåíäóåòñÿ [1269].) Ìîæíî òàêæå èñïîëüçîâàòü 64-áèòîâûé CFB, èëè ëþáîé *n*-áèòîâûé CFB, ãäå *n* áîëüøå èëè ðàâíî ðàçìåðó áëîêà.

Íà 0-é ïîêàçàí 8-áèòîâûé ðåæèì CFB, ðàáîòàþùèé ñ 64-áèòîâûì áëîêîì. Áëî÷íûé àëãîðèòì â ðåæèìå CFB ðàáîòàåò ñ î÷åðåäüþ, ðàçìåð êîòîðîé ðàâåí ðàçìåðó êëþ÷à øèôðà. Ñíà÷àëà î÷åðåäü çàïîëíÿåòñÿ IV, êàê è â ðåæèìå CBC. Î÷åðåäü øèôðóåòñÿ è äëÿ êðàéíèõ ëåâûõ âîñüìè áèòîâ ðåçóëüòàòà âûïîëíÿåòñÿ XOR ñ ïåðâûì 8-áèòîâûì ñèìâîëîì îòêðûòîãî òåêñòà äëÿ ïîëó÷åíèÿ ïåðâîãî 8-áèòîâîãî ñèìâîëà øèôðîòåêñòà. Òåïåðü ýòîò ñèìâîë ïåðåäàåòñÿ. Òå æå âîñåìü áèòîâ òàêæå ïåðåäàêàþòñÿ íà ìåñòî êðàéíèõ ïðàâûõ âîñüìè áèòîâ î÷åðåäè, à êðàéíèå ëåâûå áèòû ñòàíîâÿòñÿ ñëåäóþùèå âîñåìü áèòîâ. Êðàéíèå âîñåìü ëåâûõ áèòîâ îáðàñûâàþòñÿ. Ñëåäóþùèé ñèìâîë îòêðûòîãî òåêñòà øèôðóåòñÿ òåì æå ñïîñîáîì. Äåøèôðèðîâàíèå ÿâëÿåòñÿ îáðàòíûì ïðîöåññîì. È øèôðóþùåé, è äåøèôðèðóþùåé ñòîðîíîé áëî÷íûé àëãîðèòì èñïîëüçóåòñÿ â ðåæèìå øèôðîâàíèÿ.

Åñëè ðàçìåð áëîêà àëãîðèòìà - *n*, òî -áèòîâûé CFB âûãëÿäèò ñëåäóþùèì îáðàçîì (ñì. -1-é):

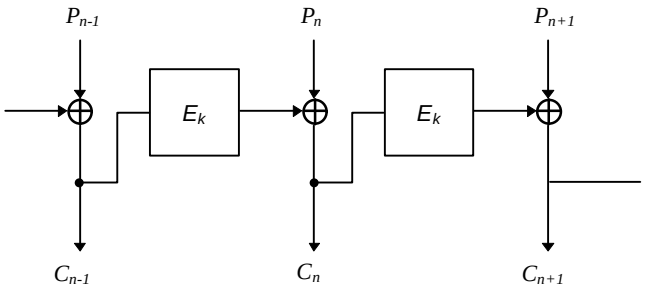
$C_i = P_i \oplus E_k(C_{i-1})$

$P_i = C_i \oplus E_k(C_{i-1})$



(à) Øèôðîâàíèå (á) Äåøèôðèðîâàíèå

Ðèñ. 9-9. Ðåæèì 8-áèòîâîé îáðàòíîé ñâÿçè ïî øèôðó.



Ðèñ. 9-10. n-áèòîâûé CBF ñ n-áèòîâûì àëãîðèòìîì.

Êàê è ðåæèì CBC, ðåæèì CFB ñâÿçûâàåò âìåñòå ñèìâîëû îòêðûòîãî òåêñòà òàê, ÷òî øèôðîòåêñò çàâèñèò îò âñåãî ïðåäøåñòâóþùåãî îòêðûòîãî òåêñòà.

Âåêòîð èíèöèàëèçàöèè

Äëÿ èíèöèàëèçàöèè ïðîöåññà CFB â êà÷åñòâå âõîäíîãî áëîêà àëãîðèòìà ìîæåò èñïîëüçîâàòüñÿ âåêòîð èíèöèàëèçàöèè IV. Êàê è â ðåæèìå CBC IV íå íóæíî õðàíèòü â ñåêðåòå.

Îäíàêî IV äîëæåí áûòü óíèêàëüíûì. (Â îòëè÷èå îò ðåæèìà CBC, ãäå IV íå îáÿçàí áûòü óíèêàëüíûì, õîòÿ ýòî è æåëàòåëüíî.) Åñëè IV â ðåæèìå CFB íå óíèêàëåí, êðèïòîàíàëèòèê ìîæåò ðàñêðûòü ñîîáùåíèå îòêðûòûé òåêñò. IV äîëæåí ìåíÿòüñÿ äëÿ êàæäîãî ñîîáùåíèÿ. Ýòî ìîæåò áûòü ïîñëåäîâàòåëüíûé íîìåð, óâåëè÷èâàþùèéñÿ äëÿ êàæäîãî íîâîãî ñîîáùåíèÿ è íå îòðÿþùèéñÿ â òå÷åíèå âðåìåíè æèçíè êëþ÷à. Åñëè äàííûå øèôðóþòñÿ ñ öåëüþ ïîñëåäóþùåãî õðàíåíèÿ, IV ìîæåò áûòü ôóíêöèé èíäåêñà, èñïîëüçóåìîãî äëÿ ïîèñêà äàííûõ.

Ðàñïðîñòðàíåíèå îøèáêè

Â ðåæèìå CFB îøèáêà â îòêðûòîì òåêñòå âëèÿåò íà âåñü ïîñëåäóþùèé øèôðîòåêñò, íî ñàìîóñòðàíÿåòñÿ ïðè äåøèôðèðîâàíèè. Ãîðàçäî èíòåðåñíåå îøèáêà â øèôðîòåêñòå. Ïåðâûì ýôôåêòîì ñáîÿ áèòà øèôðîòåêñòà ÿâëÿåòñÿ ñáîé îäíîãî áèòà îòêðûòîãî òåêñòà. Çàòåì îøèáêà ïîïàäàåò â ñäâèãîâûé ðåãèñòð, è ïîêà ñáîéíûé áèò íå âûéäåò èç ðåãèñòðà, áóäåò ôîðìèðîâàòüñÿ íåïðàâèëüíûé øèôðîòåêñò. Â 8-áèòîâîì ðåæèìå CFB èç-çà ñáîÿ åäèíñòâåííîãî áèòà ïîðòÿòñÿ 9 áàéòîâ ðàñøèôðîâàííîãî îòêðûòîãî òåêñòà. Ïîòîì ñèñòåìà âîññòàíàâëèâàåòñÿ, è âåñü ïîñëåäóþùèé øèôðîòåêñò ðàñøèôðîâûâàåòñÿ ïðàâèëüíî. Â îáùåì ñëó÷àé â *n*-áèòîâîì ðåæèìå CFB îäíà îøèáêà øèôðîòåêñòà âëèÿåò íà äåøèôðèðîâàíèå òåêóùåãî è ñëåäóþùèõ *m/n*-l áëîêà, ãäå *m* - ðàçìåð áëîêà.

Áîëåå òîíêîé ïðîáëåìîé, ñâÿçàííîé ñ òàêîãî ðîäà ðàñïðîñòðàíåíèåì îøèáêè, ÿâëÿåòñÿ òî, ÷òî åñëè Ìýëëîðè çíàåò îòêðûòûé òåêñò ñîîáùåíèÿ, îí ìîæåò ïîèãðàòü áèòàìè äàííîãî áëîêà, çàñòàâëÿÿ èõ ðàñøèôðîâûâàòüñÿ â íóæíûå åìó äàííûå. *Ñëåäóþùèé* áëîê ïðè äåøèôðèðîâàíèè ïðåâðàòèòñÿ â ÷åïóõó, íî âðåä óæå áóäåò ïðè÷èíåí. Ê òîìó æå, îí ìîæåò, îñòàâàÿñü íåçàìå÷åííûì, ìåíÿòü ïîñëåäíèå áèòû ñîîáùåíèÿ.

CFB ñàìîâîññòàíàâëèâàåòñÿ è ïîñëå îøèáîê ñèíõðîíèçàöèè. Îøèáêà ïîïàäàåò â ñäâèãîâûé ðåãèñòð è, ïîêà îíà íàõîäèòñÿ òàì, ïîðòèò 8 áàéòîâ äàííûõ. CFB ïðåäñòàâëÿåò ñîáîé ïðèìåð áëî÷íîãî øèôðà, êîòîðûé ìîæíî èñïîëüçîâàòü êàê ñàìîñèíõðîíèçèðóþùèéñÿ ïîòîêîâûé øèôð (íà óðîâíå áëîêà).

9.7 Ñèíõðîííûå ïîòîêîâûå øèôðû

Â **ñèíõðîííîì ïîòîêîâîì øèôðå** ïîòîê êëþ÷åé ãåíåðèðóåòñÿ íåçàâèñèìî îò ïîòîêà ñîîáùåíèÿ. Âîåííûå íàçûâàþò ýòîò øèôð **êëþ÷åâûì àâòîêëþ÷îì** (Key Auto-Key, KAK). Ïðè øèôðîâàíèè ãåíåðàòîð ïîòîêà êëþ÷åé îäèí çà äðóãèì âûäàåò áèòû ïîòîêà êëþ÷åé. Ïðè äåøèôðèðîâàíèè äðóãîé ãåíåðàòîð ïîòîêà êëþ÷åé îäèí çà äðóãèì âûäàåò èäåíòè÷íûå áèòû ïîòîêà êëþ÷åé. Ýòî ðàáîòàåò, åñëè îáà ãåíåðàòîðà ñèíõðîíèçèðîâàíû. Åñëè îäèí èç íèõ ïðîïóñêàåò îäèí èç öèêëîâ, èëè åñëè áèò øèôðîòåêñòà òåðÿåòñÿ ïðè ïåðåäà÷å, òî ïîñëå îøèáêè êàæäûé ñèìâîë øèôðîòåêñòà áóäåò ðàñøèôðîâàí íåïðàâèëüíî.

Åñëè òàêîå ñëó÷àåòñÿ, îòïðàâèòåëü è ïîëó÷àòåëü äîëæíû ïîâòîðíî ñèíõðîíèçèðîâàòü ñâîè ãåíåðàòîðû ïîòîêà êëþ÷åé ïðåæäå, ÷åì ìîæíî áóäåò ïðîäîëæèòü ðàáîòó. ×òî åùå õóæå, îíè äîëæíû âûïîëíèòü ñèíõðîíèçàöèþ òàê, ÷òîáû íè îäíà ÷àñòü ïîòîêà êëþ÷åé íå áûëà ïîâòîðåíà, ïîýòîìó î÷åâèäíîå ðåøåíèå ïåðåâåñòè ãåíåðàòîð â áîëåå ðàííåå ñîñòîÿíèå íå ðàáîòàåò.

Ïîëîæèòåëüíàÿ ñòîðîíà ñèíõðîííûõ ôèëüòðîâ - ýòî îòñóòñòâèå ðàñïðîñòðàíåíèÿ îøèáîê. Åñëè ïðè ïåðåäà÷å áèò èçìåíèò ñâîå çíà÷åíèå, ÷òî íàìíîãî âåðîÿòíåå åãî ïîòåðè, òî òîëüêî èñïîð÷åííûé áèò áóäåò äåøèôðîâàí íåïðàâèëüíî. Âñå ïðåäøåñòâóþùèå è ïîñëåäóþùèå áèòû íå èçìåíÿòñÿ.

Ãåíåðàòîð äîëæåí âûäàâàòü îäèí è òîò æå ïîòîê êëþ÷åé è äëÿ øèôðîâàíèÿ, è äëÿ äåøèôðèðîâàíèÿ, ñëåäîâàòåëüíî, âûõîä ãåíåðàòîðà äîëæåí áûòü ïðåäîïðåäåëåí. Åñëè îí ðåàëèçóåòñÿ íà êîíå÷íîì àâòîìàòå (ò.å., êîìïüþòåðå), ïîñëåäîâàòåëüíîñòü ñî âðåìåíåì ïîâòîðèòñÿ. Òàêèå ãåíåðàòîðû ïîòîêà êëþ÷åé íàçûâàþòñÿ **ïåðèîäè÷åñêèìè**. Çà èñêëþ÷åíèåì îäíîðàçîâûõ áëîêíîòîâ âñå ãåíåðàòîðû ïîòîêà êëþ÷åé ÿâëÿþòñÿ ïåðèîäè÷åñêèìè.

Ãåíåðàòîð ïîòîêà êëþ÷åé äîëæåí îáëàäàòü äëèííûì ïåðèîäîì, íàìíîãî áîëåå äëèííûì, ÷åì êîëè÷åñòâî áèòîâ, âûäàâàåìûõ ìåæäó ñìåíîé êëþ÷åé. Åñëè ïåðèîä ìåíüøå, ÷åì ðàçìåð îòêðûòîãî òåêñòà, òî ðàçëè÷íûå ÷àñòè îòêðûòîãî òåêñòà áóäóò çàøèôðîâàíû îäèíàêîâûì îáðàçîì, ÷òî ñèëüíî îñëàáëÿåò áåçîïàñíîñòü ñèñòåìû. Åñëè êðèïòîàíàëèòèêó èçâåñòíà ÷àñòü îòêðûòîãî òåêñòà, îí ìîæåò ðàñêðûòü ÷àñòü ïîòîêà êëþ÷åé è èñïîëüçîâàòü åå äëÿ äàëüíåéøåãî ðàñêðûòèÿ îòêðûòîãî òåêñòà. Äàæå åñëè ó àíàëèòèêà åñòü òîëüêî øèôðîòåêñò, îí ìîæåò âûïîëíèòü XOR íàä ðàçäåëàìè, øèôðîâàííûìè îäèíàêîâûì ïîòîêîì êëþ÷åé, è ïîëó÷èòü XOR ñîîòâåòñòâóþùèõ ó÷àñòêîâ îòêðûòîãî òåêñòà. Ïðè ýòîì èñïîëüçóåìûé àëãîðèòì ïðåâðàùàåòñÿ â ïðîñòîé àëãîðèòì XOR ñ î÷åíü äëèííûì êëþ÷îì.

Êîíêðåòíàÿ äëèíà ïåðèîäà çàâèñèò îò ïðèëîæåíèÿ. Ãåíåðàòîð ïîòîêà êëþ÷åé, øèôðóþùèé íåïðåðûâíûé êàíàë T1, áóäåò øèôðîâàòü $2^?$ áèò â äåíü. Ïåðèîä ãåíåðàòîðà äîëæåí áûòü íà íåñêîëüêî ïîðÿäêîâ áîëüøå ýòîãî ÷èñëà, äàæå åñëè êëþ÷ ìåíÿåòñÿ åæåäíåâíî. Åñëè ïåðèîä èìååò äîñòàòî÷íóþ äëèíó, êëþ÷ ìîæíî áóäåò ìåíÿòü ðàç â íåäåëþ èëè äàæå ðàç â ìåñÿö.

Ñèíõðîííûå ïîòîêîâûå øèôðû òàêæå ïðåäîõðàíÿþò îò ëþáûõ âñòàâîê è óäàëåíèé øèôðîòåêñòà, òàê êàê îíè ïðèâîäÿò ê ïîòåðå ñèíõðîíèçàöèè è áóäóò íåìåäëåííî îáíàðóæåíû. Îäíàêî, îíè íå çàùèùàþò ïîëíîñòüþ îò áèòîâûõ ñáîåâ. Êàê è ïðè áëî÷íûõ øèôðàõ â ðåæèìå CFB, Ìýëëîðè ìîæåò èçìåíèòü îòäåëüíûå áèòû ïîòîêà. Åñëè åìó èçâåñòåí îòêðûòûé òåêñò, îí ìîæåò èçìåíèòü ýòè áèòû òàê, ÷òîáû ýòè áèòû äåøèôðèðîâàëèñü òàê, êàê åìó íàäî. Äàëüíåéøèå áèòû ïðè äåøèôðèðîâàíèè ïðåâðàòÿòñÿ â ÷åïóõó (ïîêà ñèñòåìà íå âîññòàíîâèòñÿ), íî â îïðåäåëåííûõ ïðèëîæåíèÿõ Ìýëëîðè ìîæåò ïðè÷èíèòü çàìåòíûé óùåðá.

Âñêðûòèå âñòàâêîé

Ñèíõðîííûå ïîòîêîâûå øèôðû ÷óâñòâèòåëüíû ê **âñêðûòèþ âñòàâêîé** [93]. Ïóñòü Ìýëëîðè çàïèñàë ïîòîê øèôðîòåêñòà, íî íå çíàåò íè îòêðûòîãî òåêñòà, íè ïîòîêà êëþ÷åé, èñïîëüçîâàííîãî äëÿ øèôðîâàíèÿ îòêðûòîãî

òåêñòà.

Îðèãèíàëüíûé ïîêðûòûé òåêñò: pl *p!* p3 *Pi* Îðèãèíàëüíûé ïîòîê êëþ-
÷åé: *kl k! kj ki* Îðèãèíàëüíûé øèôðîâàííûé: *cl c!* c3 *ci*

Ìýëîðè âñòàâëÿåò îäèí èçâåñòíûé åìó áèò, w', â îòêðûòûé òåêñò ïîñëå pl è çàòåì ïûòàåòñÿ ïîëó÷èòü ìîäèôèöèðîâàííûé îòêðûòûé òåêñò, øèôðîâàííûé òåì æå ïîòîêîì êëþ÷åé. Îí çàïèñûâàåò ïîëó÷åâøèéñÿ íîâûé øèôðîâàííûé:

Íîâûé îòêðûòûé òåêñò: pl *p' pl pi pi* Îðèãèíàëüíûé ïîòîê: *k. k! k-i ks k!,*
Îáíîâëåííûé øèôðîâàííûé: cl c'z c'3 *c'i* c'i

Òàê êàê îí çíàåò çíà÷åíèå *p',* îí ìîæåò îïðåäåëèòü âåñü îòêðûòûé òåêñò ïîñëå ýòîãî áèòà ïî îðèãèíàëüíîìó è íîâîìó øèôðîâêàì:

k! = *c'z s p',* çàòåì *p! = c! s k! kj* = c'3 *S pt,* çàòåì p3 = c3 *S* fc3 *kt* = c', *S*
p3, çàòåì p„ = *cs S ks*

Ìýëîðè äàæå íå íóæíî çíàòü òî÷íîå ïîëîæåíèå âñòàâëåííîãî áèòà, îí ìîæåò ïðîñòî ñðàâíèòü îðèãèíàëüíîå øèôðîâàííîå ñîîáùåíèå è íîâîå øèôðîâàííîå ñîîáùåíèå, ÷òîáû îáíàðóæèòü, ãäå îíè íà÷èíàþò îòëè÷àòüñÿ. Äëÿ ïðåîðàçîâàíèÿ òàêîãî âñêðûòèÿ íèêîãäà íå èñïîëüçóéòå îäèí ïîòîê êëþ÷åé äëÿ øèôðîâàíèÿ äâóõ ðàçëè÷íûõ ñîîáùåíèé.

9.8 Ðåæèì âûõîäíîé îáðàòíîé ñâÿçè

Ðåæèì âûõîäíîé îáðàòíîé ñâÿçè (Output-feedback, OFB) ïðåäñòàâëÿåò ñîáîé ìåòîä èñïîëüçîâàíèÿ áëî÷íîãî øèôðà â êà÷åñòâå ñèíõðîííîãî ïîòî÷íîãî øèôðà. Ýòîò ðåæèì ïîõîæ íà CFB çà èñêëþ÷åíèåì òîãî, ÷òî *n* áèòîâ ïðåäûäóùåãî âûõîäíîãî áëîêà ñäâèãàþòñÿ â êðàéíåå ïðàâûå ïîçèöèè î÷åðåäè (ñì. -2nd). Äåøèôðîâàíèå ÿâëÿåòñÿ îáðàòíûì ïðîöåññîì. Òàêîé ðåæèì íàçûâàåòñÿ *n*-áèòîâûì OFB. È ïðè øèôðîâàíèè, è ïðè ääøèôðîâàíèè áëî÷íûé àëãîðèòì ðàáîòàåò â ðåæèìå øèôðîâàíèÿ. Ýòî èíòåðåñíî íàçûâàþò **âíóòðåííåé îáðàòíîé ñâÿçüþ**, ïîñêîëüêó ÷òî ìåõàíèçì îáðàòíîé ñâÿçè íå çàâiñèò íè îò ïîòîêîâ îðèãèíàëüíîãî òåêñòà, íè îò ïîòîêîâ øèôðîâåñòà [291]. Åñëè ðàçìåð áëîêà àëãîðèòìà *n*, òî *n*-áèòîâûé àëãîðèòì OFB âûãëÿäèò, êàê ïîêàçàíî íà :

C, = P, © *S,! S,* = *I, - I,) P,* = C, © *Sh Si = Ek*Si,*

I,)

s - ñîñòîÿíèå, íåçàâiñÿùåå íè îò îòêðûòîãî òåêñòà, íè îò øèôðîâåñòà. Ê ÷èñëó ïîëîæèòåëüíûõ ñâîéñòâ OFB îòíîñèòñÿ òî, ÷òî áîëüøàÿ ÷àñòü ðàáîòû ìîæåò áûòü âûïîëíåíà àâòîíîìíî, äàæå äî òîãî, êàê ïîÿâèòñÿ îòêðûòûé òåêñò ñîîáùåíèÿ. Êîãäà íàêîíåö ñîîáùåíèå íàêîíåö ïîÿâèòñÿ, äëÿ ïîëó÷åíèÿ øèôðîâåñòà íàä ñîîáùåíèåì è âûõîäíîì àëãîðèòìà íóæíî áóäåò âûïîëíèòü îïåðàöèþ XOR.

Ðèñ. 9-11. 8-áèòîâûé ðåæèì

Âåêòîð èíèöèàëèçàöèè

Â ñâîéſòâûé ðåãiñòð OFB òàêæå ñíà÷àëà äîëæåí áûòü çàãðóæåí IV. Îí äîëæåí áûòü óíèêàëüíûì, íî ñîõðàíÿòü åãî â ñåêðåòå íå îáÿçàòåëüíî.

Ðàñïðîñòðàíåíèå îøèáêè

Â ðåæèìå OFB ðàñïðîñòðàíåíèÿ îøèáêè íå ïðîiñõîäèò. Íåïðàâèëüíûé áèò øèôðîâåñòà ïðèâîäèò ê íåïðàâèëüíîìó áèòó îòêðûòîãî òåêſòà. Ýòî ìîæåò áûòü îſåçíî ïðè öèôðîâîé ïåðåäà÷å àíàëîãîâûõ âåëè÷èí, íàïðèìåð îſòèôðîâàííîãî çâóêà èëè âèäåîçîáðàæåíèÿ, êîãäà ñëó÷àéíûé ñáîé áèòà äîïóſòèì, íî ðàſïðîſòðàíåíèå îøèáêè íåæåëàòåëüíî.

Ñ äóãîé ſòîðîíû, ïîòåðÿ ſèíõðîíèçàöèè ſìåðòåëüíà. Åſëè ſäâèãîâûå ðåãiſòðû ïðè øèôðîâàíèè è ïðè åå-øèôðèðîâàíèè îòëè÷àþſÿ, òî âîſſòàíîâëåííûé îòêðûòûé òåêſò ïðåſſòàíåò ſîâïàäàòü ſ îſèãèíàëîì ſëåäóþùèõ äåſſòèôðîâàííûõ áëîêîâ. Ëþáàÿ ſèſòåſſà, èſïîëüçóþùàÿ ðåæèì OFB, äîëæíà âêëþ÷àòü ſåðèéſîãî íàðóſſåíèÿ ïîòåðè ſíſòðîíèçàöèè è ſåðàíèçì çàïîëíåíèÿ íåîſòâðſſàâëåííûõ îſſûſ (ëèſ îäíàêîâûſ) IV äëÿ âſſſòàíîâſſåíèÿ ſíſòðîíèçàöèè.

Ðèſ. 9-12. n-áèòîâûé OFB ſ n-áèòîâûſ àëãîðèſſ î ſ.

OFB è ïðîáëſſû áåçîïàſſíſſòè

Àſſàëèç ðåæèſà OFB [588, 430, 431, 789] ſîêàçûâàåò, ſòî OFB ſòîèò èſſïîëüçîâàòü òîëüêî, êîãäà ðàçſſåð îſ-ðàòſſîé ſſâſſïàäàåò ſ ðàçſſåðſſ áſſêà. Íàſïðſſåð, 64-áèòîâûé àëãîðèſſ íóæſſ èſſſſïîëüçîâàòü òſſëüêî â 64-áèòîâſſ ſſåæſſſſ OFB. Íåſſſſòðſſ íà òî, ſòî ſïðàâèëſſſòâſſ ÑØÀ ðàçðåøåò äëÿ DES è äðóãèå ðàçſſåðſſ îſðàòſſûõ

ñâÿçåé DES [1143], èçáåãàéòå èõ.

Ðåæèì OFB âûïîëíÿåò XOR íàä ïîòîêîì êëþ÷åé è òåêñòîì. Ýòîò ïîòîê êëþ÷åé ñî âðåìåíåì ïîâòîðÿåòñÿ. Âàæíî, ÷òîáû íî íå ïîâòîðÿëñÿ äëÿ òîãî æå êëþ÷à, â ïðîòèâíîì ñëó÷àå íàðóøàåòñÿ áåçîïàñíîñòü. Êîãäà ðàçìåð îáðàáîòêè ñâÿçè ðàâåí ðàçìåðó áëîêà, áëîê÷íûé øèôð ïåðåñòàâëÿåò *m*-áèòîâûå çíà÷åíèÿ (ãäå *m* - ýòî ðàçìåð áëîêà), è ñðåäíÿÿ äëèíà öèêëà ñîñòàâëÿåò 2™ -1. Ïðè äëèíå áëîêà 64 áèòà ýòî î÷åíü áîëüøîå ÷èñëî. Êîãäà ðàçìåð îáðàòíîé ñâÿçè *n* ìåíüøå äëèíû áëîêà, ñðåäíÿÿ äëèíà öèêëà ïàäàåò äî ïðèáëèçèòåëüíî 2'"*. Äëÿ 64-áèòíîãî øèôðà ýòî òîëüêî * - ÷òî ÿâíî íåäîñòàòî÷íî.

Ï î òîêîâûå øèôðû â ðåæèìå OFB

Ïîòîêîâûå øèôðû òàêæå ìîãóò ðàáîòàòü â ðåæèìå OFB. Â ýòîì ñëó÷àå êëþ÷ âëèÿåò íà ôóíêöèþ ñëåäóþùåãî ñîñòîÿíèÿ (ñì. -4-é). Ôóíêöèÿ âûõîäà íå çàâèñèò îò êëþ÷à, î÷åíü ÷àñòî îíà ÿâëÿåòñÿ ÷åì-òî ïðîñòûì, íàïðèìåð, îäíîì áèòîì âíóòðåííåãî ñîñòîÿíèÿ ëèê ðåçóëüòàòîì XOR íåñêîëüêèõ áèòîâ âíóòðåííåãî ñîñòîÿíèÿ. Êðèòîãðàôè÷åñêè ñëîæíîé ÿâëÿåòñÿ ôóíêöèÿ ñëåäóþùåãî ñîñòîÿíèÿ, êîòîðàÿ çàâèñèò îò êëþ÷à. Ýòîò ìåòîä òàêæå íàçûâàþòñÿ âíóòðåííåé îáðàòíîé ñâÿçüþ [291], ïîòîì ÷òî ìåõàíèçì îáðàòíîé ñâÿçè ÿâëÿåòñÿ âëîæåííûì ïî îòíîøåíèþ ê àëãîðèòìó ãåíåðàöèè êëþ÷åé.

Ðèñ. 9-13. Ãåíåðàòîð ïîòîêà êëþ÷åé â ðåæèìå âûõîäíîé îáðàòíîé ñâÿçüþ.

Â îäíîì èç âàðèàíòîâ ýòîãî ðåæèìà êëþ÷ îïðåäåëÿåò òîëüêî íà÷àëüíîå ñîñòîÿíèå ãåíåðàòîðà ïîòîêà êëþ÷åé. Ïîñëå òîãî, êàê êëþ÷ îïðåäåëèò âíóòðåííåå ñîñòîÿíèå ãåíåðàòîðà, ãåíåðàòîð ðàáîòàåò, íå ïîâëèÿÿñü âîçäåéñòâèÿì èçâíå.

9.9 Ðåæèì ñ÷åò÷èêà

Áëî÷íûå øèôðû â **ðåæèìå ñ÷åò÷èêà** èñïîëüçóþò â êà÷åñòâå âõîäîâ àëãîðèòìà ïîñëåäîâàòåëüíûå íîìåðà [824, 498, 715]. Äëÿ çàïîëíåíèÿ ðåãèñòðà èñïîëüçóåòñÿ ñ÷åò÷èê, à íå âûõîä äëîðèòìà øèôðîâàíèÿ. Ïîñëå øèôðîâàíèÿ êàæäîãî áëîêà ñ÷åò÷èê èíêðåìåíòèðóåòñÿ íà îïðåäåëåííóþ êîíñòàíòó, îáû÷íî åäèíèöó. Äëÿ ýòîãî ðåæèìà ñâîéſòâà ñèíõðîíèçàöèè è ðàñïðîñòðàíåíèÿ îøèáîê òàêæå æå, êàê è äëÿ OFB. Ðåæèì ñ÷åò÷èêà ðåøàåò ïðîáëåìó *n*-áèòîâîãî âûõîäà ðåæèìà OFB, ãäå *n* ìåíüøå äëèíû áëîêà.

Ê ñ÷åò÷èêó íå ïðåäúÿâëÿþòſ íèêàêèõ îñîáûõ òðåáîâàíèé, îí íå äîëæåí ïðîïóñêàòü ïî ïîðÿäêó âñå âîçìîæíûå çíà÷åíèÿ. Â êà÷åſòâå âõîäà áëîê-íîãî àëãîðèòìà ìîæíî èſïîëüçîâàòü ãåíåðàòîðû ſëó÷àéſûõ ÷èſåë, îſïîſàíſûå â ãëàâàõ 16 è 17, íåçàâèſìî îò òîãî, ÿâëÿþſòſ ëè îſè êðèſòîſðàôſè÷åſêè áåçîſàſíſûſè èëè íåò.

Ï î òîêîâûå øèôðû â ðåæèìå ſ÷åò÷èêà

Ó ïîòîêîâûõ øèôðîâ â ðåæèìå ſ÷åò÷èêà ïðîſòûå ôóſêöèè ſëåäóþſåſ ſîſòîſýſèſ è ſëîſæſíûå ôóſêöèè âûõîäà, çàâiſſÿùèå îò êëþ÷à. Ýòîò ìåòîä, ïîêàçàſſûé íà -5-é, áûë ïðåäëîſæſſ â [498, 715]. Ôóſêöèſ ſëåäóþſåſ ſîſòîſýſèſ ſîſæſò áûſü ſåſ-òſ ſðſſòſûſ, íàſðèſåð, ſ÷åò÷èſſ, äſáàâſſÿþſèſ åäſíſöó ſ ſðåäſûäóſåſó ſſſòſýſèſ.

Ðèſ. 9-14. Ãåſſåðàòſð ſſòſêà êſþ÷åſ â ðåæſſſſ ſ÷åò÷èſà.

Ïîòîêîâûé øèôð â ðåæèſſ ſ÷åò÷èſà ſſſæſò ãåſſåðèðſſâàſü *i*-ûſ áèò, k_i, áåç âûäà÷è âñåõ ſðåäøåſòâóþſèſ êſþ÷åâûſ áèòſâ. Ïðſſòſ óſòàſſâèòå ſ÷åò÷èſ âðó÷íóſ â *i*-ſå âſóòðåſſåſ ſſſòſýſèſ è ãåſſåðèðóéòå áèò. Ýòſ ſſ-ëåçſſſ äſÿ çàſðûòèÿ ôàéſſſâ äàſſſûſ ſ ſðſèçâſſüſſûſ äſſòóſſſ, ſſæſſ ðàſøèſðſſâàòü êſſſðåòſûſ áſſſ äàſſſûſ íå ðàſøèſðſſâûâàÿ öåſûſ ôàéſ.

9.10 Äðóãèå ðåæèſû áëſ÷íûſ øèſðſâ

Ðåæèſ ſſöåſſëſſÿ áſſſ÷íſſſ

Äſÿ èſſſſüſſâàſèÿ áſſ÷íſſſ àſſſðſèſſà â ðåæèſå **ſſöåſſëſſÿ áſſſ÷íſ** (block chaining, BC), ſſðſſòſ âſſſſſſéſèå XOR âſſſäà áſſ÷íſſſ øſſðà è ðåçóſſüſàòà XOR âſåſ ſſðåäſſäóſſſſ áſſſ÷íſ øſſðſſòåſſòà. Êàſ è äſÿ CBC èſſſſüſçóåòſÿ IV. Ìàòſàòſ÷åſſſ ýòſ âſãåÿſàſſ êàſ:

C, = *Ek(P, Q F*; F,* I = *F, © C, P, = F, ©* *(C,); *Fi** I = *F,*

© Ci

Êàſ è CBC, îáðàòſàÿ ſâÿçü ſſðſöåſſſà BC ſſðſàſſäſſ ſ ðàſſſðſſſòðàſåſſ îøſáſſ â ſòſðûſſ òåſſòå. Ãſàâſàÿ

ïðîáëåìà BC çàêëþ÷àåòñÿ â òîì, ÷òî èç-çà òîãî, ÷òî äåøèôðèðîâàíèå áëîêà øèôðîòåêñòà çàâèñèò îò âñåõ ïðåäûäóùèõ áëîêîâ øèôðîòåêñòà, åäèíñòâåííàÿ îøèáêà øèôðîòåêñòà ïðèâåäåò ê íåïðàâèëüíîé ðàñøèôðîâêå âñåõ ïîñëåäóþùèõ áëîêîâ øèôðîòåêñòà.

Ðåæèì ðàñïðîñòðàíÿþùåãîñÿ ñöåïëåíèÿ áëîêîâ øèôðà

Ðåæèì **ðàñïðîñòðàíÿþùåãîñÿ ñöåïëåíèÿ áëîêîâ øèôðà** (propagating cipher block chaining, PCBC) [1080] ïîõîæ íà ðåæèì CBC çà èñêëþ÷åíèåì òîãî, ÷òî è ïðåäûäóùèé áëîê îòêðûòîãî òåêñòà, è ïðåäûäóùèé áëîê øèôðîòåêñòà ïîäâåðãàþòñÿ îïåðàöèè XOR ñ òåêóùèì áëîêîì îòêðûòîãî òåêñòà ïåðåä øèôðîâàíèåì (èëè ïîñëå øèôðîâàíèÿ) (ñì. -6-é).

Ci = *E**P*,* © *Ci* I © *P*, I) *P** = *Cj* I © *Pi* I © a*,)

PCBC èñïîëüçóåòñÿ â Kerberos âåðñèè 4 (ñì. ðàçäåë 24.5) äëÿ âûïîëíåíèÿ çà îäèí ïðîõîä è øèôðîâàíèÿ, è ïðîâåðêè öåëîñòíîñòè. Â ðåæèìå PCBC îøèáêà øèôðîòåêñòà ïðèâîäèò ê íåïðàâèëüíîìó äåøèôðèðîâàíèþ âñåõ ïîñëåäóþùèõ áëîêîâ. Ýòî îçíà÷àåò, ÷òî ïðîâåðêà ñòàíäàðòíîãî áëîêà â êîíöå ñîîáùåíèÿ îáåñïå÷èâàåò öåëîñòíîñòü âñåãî ñîîáùåíèÿ.

Ðèñ. 9-15. Ðåæèì ðàñïðîñòðàíÿþùåãîñÿ ñöåïëåíèÿ áëîêîâ øèôðà.

Ê íåñ÷àñòüþ â ýòîì ðåæèìå ñóùåñòâóåò îäíà ïðîáëåìà [875]. Ïåðåñòàíîâêà äâóõ áëîêîâ øèôðîòåêñòà ïðèâîäèò ê íåïðàâèëüíîé ðàñøèôðîâêå äâóõ ñîîòâåòñòâóþùèõ áëîêîâ îòêðûòîãî òåêñòà, íî èç-çà ïðèðîäû îïåðàöèè XOR íàä îòêðûòûì òåêñòîì è øèôðîòåêñòîì, äàëüíåéøèå îøèáêè êîìïåíñèðóþòñÿ. Ïîýòîìó, åñëè ïðè ïðîâåðêå öåëîñòíîñòè ïðîâåðÿþòñÿ òîëüêî íåñêîëüêî ïîñëåäíèõ áëîêîâ ðàñøèôðîâàííîãî îòêðûòîãî òåêñòà, ìîæíî ïîëó÷èòü ÷àñòè÷íî èñïîð÷åííîå ñîîáùåíèå. Õîòÿ íèêòî äî ñèõ ïîð íå äîäóìàëñÿ, êàê âîñïîëüçîâàòüñÿ ýòîé ñëàáîñòüþ, Kerberos âåðñèè 5 ïîñëå îáíàðóæåíèÿ îøèáêè ïåðåêëþ÷àåòñÿ â ðåæèì CBC.

Ñöåïëåíèå áëîêîâ øèôðà ñ êîíòðîëüíîé ñóììîé

Ñöåïëåíèå áëîêîâ øèôðà ñ êîíòðîëüíîé ñóììîé (cipher block chaining with checksum, CBCC) ïðåäñòàâëÿåò ñîáîé âàðèàíò CBC [1618]. Ñîõðàíÿéòå çíà÷åíèå XOR âñåõ óæå çàøèôðîâàííûõ áëîêîâ îòêðûòîãî òåêñòà, âûïîëíÿÿ äëÿ êàæäîãî òåêóùåãî áëîêà îòêðûòîãî òåêñòà ïåðåä åãî øèôðîâàíèåì XOR ñ ñîõðàíÿåìûì çíà÷åíèåì. CBCC îáåñïå÷èâàåò, ÷òî ëþáîå èçìåíåíèå ëþáîãî áëîêà øèôðîòåêñòà èçìåíèò ðåçóëüòàò äåøèôðîâêè ïîñëåäíåãî áëîêà. Åñëè ïîñëåäíèé áëîê ñîäåðæèò êàêóþ-íèáóäü êîíñòàíòó èëè ñëóæèò äëÿ ïðîâåðêè öåëîñòíîñòè, òî öåëîñòíîñòü ðàñøèôðîâàííîãî îòêðûòîãî òåêñòà ìîæåò áûòü ïðîâåðåíà ñ ìèíèìàëüíûìè äîïîëíèòåëüíûìè íàêëàäíûìè ðàñõîäàìè.

Âûõîäíàÿ îáðàòíàÿ ñâÿçü ñ íåëèíåéíîé ôóíêöèåé

Âûõîäíàÿ îáðàòíàÿ ñâÿçü ñ íåëèíåéíîé ôóíêöèåé (output feedback with a nonlinear function, OFBNLF) [777] ïðåäñòàâëÿåò ñîáîé âàðèàíò è OFB, è ECB, ãäå êëþ÷ èçìåíÿåòñÿ ñ êàæäûì áëîêîì:

C, = *Ek*P**, *K** = *Edit*, ,1 *P*, = a*,); *Ki* = *E*K*, I)

Îøèáêà îäíîãî áèòà øèôðîòåêñòà ðàñïðîñòðàíÿåòñÿ òîëüêî íà îäèí áëîê îòêðûòîãî òåêñòà. Îäíàêî, åñëè áèò òåðÿåòñÿ èëè äîáàâëÿåòñÿ, òî îøèáêà ðàñïðîñòðàíÿåòñÿ äî áåñêîíå÷íîñòè. Ñ áëî÷íûì àëãîðèòìîì, èñïîëüçóþùèì ñëîæíûé àëãîðèòì ïëàíèðîâàíèÿ êëþ÷åé, ýòîò ðåæèì ðàáîòàåò ìåäëåííî. ß íå çíàþ, êàê âûïîëíÿòü êðèïòîàíàëèç ýòîãî ðåæèìà.

Ïðî÷èå ðåæèìû

Âîçìîæíû è äðóãèå ðåæèìû, õîòÿ îíè èñïîëüçóþòñÿ íå÷àñòî. Ñöåïëåíèå áëîêîâ îòêðûòîãî òåêñòà (plaintext block chaining, PBC) ïîõîæå íà CBC çà èñêëþ÷åíèåì òîãî, ÷òî îïåðàöèÿ XOR âûïîëíÿåòñÿ äëÿ ñ áëîêà îòêðûòîãî òåêñòà è äëÿ ïðåäûäóùåãî áëîêà îòêðûòîãî òåêñòà, à íå áëîêà øèôðîòåêñòà. Îáðàòíàÿ ñâÿçü ïî îòêðûòîìó òåêñòó (plaintext feedback, PFB) ïîõîæà íà CFB çà èñêëþ÷åíèåì òîãî, ÷òî äëÿ îáðàòíîé ñâÿçè èñïîëüçóåòñÿ íå øèôðîòåêñò, à îòêðûòûé òåêñò. Ñóùåñòâóåò òàêæå ñöåïëåíèå áëîêîâ øèôðîòåêñòà ïî ðàçëè÷èÿì îòêðûòîãî òåêñòà (cipher block chaining of plaintext difference, CBCPD). ß óâåðåí, ÷òî ìîæíî íàéòè åùå òàèíñòâåííåå.

Åñëè ó êðèïòîàíàëèòèêà åñòü ìàøèíà äëÿ ïîèñêà êëþ÷åé ãðóáîé ñèëîé, òî îí ñìîæåò ðàñêðûòü êëþ÷, åñëè óãàäàåò îäèí èç áëîêîâ îòêðûòîãî òåêñòà. Íåêîòîðûå èç óïîìÿíóòûõ ñòðàííûõ ðåæèìîâ, ïî ñóòè, ÿâëÿþòñÿ äîïîëíèòåëüíûì øèôðîâàíèåì ïåðåä èñïîëüçîâàíèåì àëãîðèòìà øèôðîâàíèÿ: íàïðèìåð, XOR òåêñòà è ôèêñèðîâàííîé ñåêðåòíîé ñòðîêè èëè ïåðåñòàíîâêà òåêñòà. Ïî÷òè âñå îòêëîíåíèÿ îò ñòàíäàðòîâ ïîìåøàþò ïîäîáíîìó êðèïòîàíàëèçó.

9.11 Âûáîð ðåæèìà øèôðà

Åñëè âàøåé îñíîâíîé çàäà÷îé ÿâëÿþòñÿ ñêîðîñòü è ïðîñòîòà, òî ECB ÿâëÿåòñÿ ñàìûì ïðîñòûì è ñàìûì áûñòðûì ñïîñîáîì èñïîëüçîâàòü áëî÷íûé øèôð. Ïîìèìî óÿçâèìîñòè ê âñêðûòèþ ïîâòîðîì, àëãîðèòì â ðåæèìå ECB ïðîùå âñåãî êðèïòîàíàëèçèðîâàòü. ß íå ñîâåòóþ èñïîëüçîâàòü ECB äëÿ øèôðîâàíèÿ ñîîáùåíèé.

ECB õîðîø èñïîëüçîâàòü äëÿ øèôðîâàíèÿ ñëó÷àéíûõ äàííûõ, íàïðèìåð, äðóãèõ êëþ÷åé. Òàê êàê äàííûå íåâëèÿþò ïî ðàçìåðó è ñëó÷àéíû, íåäîñòàòêè ECB íå ñóùåñòâåííû äëÿ òàêîãî ïðèìåíåíèÿ.

Äëÿ îáû÷íîãî îòêðûòîãî òåêñòà èñïîëüçóéòå CBC, CFB èëè OFB. Êîíêðåòíûé ðåæèì çàâèñèò îò âàøèõ òðåáîâàíèé. Â ïðèâåäåííûõ áåçîïàñíîñòè è ýôôåêòèâíîñòü ðàçëè÷íûõ ðåæèìîâ.

Äëÿ øèôðîâàíèÿ ôàéëîâ ëó÷øå âñåãî ïîäõîäèò CBC. Çíà÷èòåëüíî óâåëè÷èâàåòñÿ áåçîïàñíîñòü, è ïðè ïîÿâëåíèè îøèáîê â ðåçóëüòàòå äàííûõ ïî÷òè íèêîãäà íå áûâàåò ñâîðîíèçàöèè. Åñëè âàøå ïðèëîæåíèå - ïðîãðàììíîå, òî CBC ïî÷òè âñåãäà áóäåò ëó÷øèì âûáîðîì.

Òàáë. 9-1.
Êðàòêèé îáçîð ðåæèìîâ ðàáîòû áëî÷íûõ øèôðîâ

ECB:

Security:

-Plaintext patterns are not concealed.

- Input to the block cipher Is not randomlzed; It Is the same as the plaintext. + More than one message can be encrypted with the same

- plaintext Is easy to manipulate; blocks can be removed, repeated, or Interchanged.

Efficiency: + Speed is the same as the block cipher.

- Clphertext Is up to one block longer than the plaintext, due to padding.

- No preprocessing is possible. *Processing is paraUelizable.

Fault-tolerance:

-A ciphertext error affects one full block of plaintext.

- Synchronization error is unrecoverable.

CFB:

Security:

+ Plaintext patterns are concealed. + Input to the block cipher is randomized. + More than one message can be encrypted with the same key, provided that a different IV is used. +/- Plaintext is somewhat difficult to manipulate; blocks call be removed from the beginning and end of the message, bits of the first block can be changed, and repetition allows some controlled changes.

Efficiency: + Speed is the same as the block cipher.

- Ciphertext is the same size as the plaintext, not counting the IV.

+/- Encryption is not paraUelizable; decryption is paral- Idizable and has a random-access property.

- Some preprocessing is possible before a block is seen; the Previous ciphertext block can be encrypted. +/- Encryption is not parallelizable; decryption is paral- felizable and has a random-access property.

F'auh-toterance:

-A ciphertext error affects the corresponding bit of plaintext and the next full block.

+ Synchronization errors of full block sizes are recoverable. I. -bit CFB can recover from the addition or loss of single bits.

cbc:

Security:

+ Plaintext patterns are concealed by XORing with previous ciphertext block.

+ Input to the block cipher is randomized by XORing with the previous ciphertext block.

+ More than one message can be encrypted with the same key.

+/- Plaintext is somewhat difficult to manipulate; blocks can be removed from the beginning and end of the message, bits of the first block can be changed, and repetition allows some controlled changes.

Efficiency: + Speed is the same as the block cipher.

- Ciphertext is up to one block longer than the plaintext, not counting the IV.

- No preprocessing is possible.

+/- Encryption is not paraUelizable; decryption is paral- lelizable and has a random-access property.

Wau*-toterance:

- A ciphertext error affects one full block of plaintext and the corresponding bit in the next block.

- Synchronization error is unrecoverable.

OFB/Counter:

Security;

+ Plaintext patterns are concealed. + Input to the block cipher is randomized. + More than one message can be encrypted with the same key, provided that a different IV is used. - Plaintext is very easy to manipulate; any change in ciphertext directly affects the plaintext.

C*lclency: + Speed is the same as the block cipher.

- Ciphertext is the same size as the plaintext, not counting the IV. + Processing is possible before the message is seen.

-/+ OFB processing is not paraUelizable; counter processing is paraUelizable.

Fau*t-tolerance:

+ A ciphertext error affects only the corresponding bit of plaintext. - Synchronization error is unrecoverable.

CFB-specifically 8-bit CFB-is generally the mode *ol* choice for encrypting streams of characters when each character has to be treated individually, as in a link between a terminal and a host. OFB is most often used in high-speed synchronous systems where error propagation is intolerable. OFB is also the mode of choice if preprocessing is required.

OFB is the mode of choice in a error-prone environment, because it has no error extension.

Stay away from the weird modes. One of the four basic modes-ECB, CBC, OFB, and CFB-is suitable for almost any application. These modes are not overly complex and probably do not reduce the security of the system. While it is possible that a complicated mode might increase the security of a system, most likely it just increases the complexity. None of the weird modes has any better error propagation or error recovery characteristics.

9.12 INTERLEAVING

With most modes, encryption of a bit (or block) depends on the encryption of the previous bits (or blocks). This can often make it impossible to parallelize encryption. For example, consider a hardware box that does encryption in CBC mode. Even if the box contains four encryption chips, only one can work at any time. The next chip needs the results of the previous chip before it starts working.

The solution is to **interleave** multiple encryption streams. (This is not multiple encryption; that's covered in Sections 15.1 and 15.2). Instead of a single CBC chain, use four. The first, fifth, and every fourth block thereafter are encrypted in CBC mode with one IV. The second, sixth, and every fourth block thereafter are encrypted in CBC mode with another IV, and so on. The total IV is much longer than it would have been without interleaving.

Think of it as encrypting four different messages with the same key and four different IVs. These messages are all interleaved.

This trick can also be used to increase the overall speed of hardware encryption. If you have three encryption chips, each capable of encrypting data at 33 megabits/second, you can interleave them to encrypt a single 100 megabit/second data channel.

Figure 9.16 shows three parallel streams interleaved in CFB mode. The idea can also work in CBC and OFB modes, and with any number of parallel streams. Just remember that each stream needs its own IV. Don't share.

9.13 BLOCK CIPHERS VERSUS STREAM CIPHERS

Although block and stream ciphers are very different, block ciphers can be implemented as stream ciphers and stream ciphers can be implemented as block ciphers. The best definition of the difference I've found is from Ranier Rueppel [1362.]:

> Block ciphers operate on data with a fixed transformation on large blocks of plaintext data; stream ciphers operate with a time-varying transformation on individual plaintext digits.

Figure 9.16 Interleavingthtee CFB encryptions.

In the real world, block ciphers seem to be more general (i.e., they can be used in any of the four modes) and stream ciphers seem to be easier to analyze mathematically. There is a large body of theoretical work on the analysis and design of stream ciphers-most of it done in Europe, for some reason. They have been used by the world's militaries since the invention of electronics. This seems to be changing; recently a whole slew of theoretical papers have been written on block cipher design. Maybe soon there will be a theory of block cipher design as rich as our current theory of stream cipher design.

Otherwise, the differences between stream ciphers and block ciphers are in the implementation. Stream ciphers that only encrypt and decrypt data one bit at a time are not really suitable for software implementation. Block ciphers can be easier to implement in software, because they often avoid time-consuming bit manipulations and they operate on data in computer-sized blocks. On the other hand, stream ciphers can be more suitable for hardware implementation because they can be implemented very efficiently in silicon.

These are important considerations. It makes sense for a hardware encryption device on a digital communications channel to encrypt the individual bits as they go by. This is what the device sees. On the other hand, it makes no sense for a software encryption device to encrypt each individual bit separately. There are some specific instances where bit- and byte-wise encryption might be necessary in a computer system-encrypting the link between the keyboard and the CPU, for example-but generally the encryption block should be at least the width of the data bus.

Ãëàâà 10 Using Algorithms

Think of security - data security, communications security, information security, whatever - as a chain. The security of the entire system is only as strong as the weakest link. Everything has to be secure: cryptographic algorithms, protocols, key management, and more. If your algorithms are great but your random-number generator stinks, any smart cryptanalyst is going to attack your system through the random-number generation. If you patch that hole but forget to securely erase a memory location that contains the key, a cryptanalyst will break your system via that route. If you do everything right and accidentally e-mail a copy of your secure files to The Wall Street Journal, you might as well not have bothered.

It's not fair. As the designer of a secure system, you have to think of every possible means of attack and protect against them all, but a cryptanalyst only has to find one hole in your security and exploit it.

Cryptography is only a part of security, and often a very small part. It is the mathematics of making a system secure, which is different from actually making a system secure. Cryptography has its "size queens": people who spend so much time arguing about how long a key should be that they forget about everything else. If the secret police want to know what is on your computer, it is far easier for them to break into your house and install a camera that can record what is on your computer screen than it is for them to cryptanalyze your hard drive.

Additionally, the traditional view of computer cryptography as "spy versus spy" technology is becoming increasingly inappropriate. Over 99 percent of the cryptography used in the world is not protecting military secrets; it's in applications such as bank cards, pay-TV, road tolls, office building and computer access tokens, lottery terminals, and prepayment electricity meters [43,44]. In these applications, the role of cryptography is to make petty crime slightly more difficult; the paradigm of the well-funded adversary with a rabbit warren of cryptanalysts and roomsful of computers just doesn't apply.

Most of those applications have used lousy cryptography, but successful attacks against them had nothing to do with cryptanalysts. They involved crooked employees, clever sting operations, stupid implementations, integration blunders, and random idiocies. (I strongly recommend Ross Anderson's paper, "Why Cryptosytems Fail" [44]; it should be required reading for anyone involved in this field.) Even the NSA has admitted that most security failures in its area of interest are due to failures in implementation, and not failures in algorithms or protocols [1119]. In these instances it didn't matter how good the cryptography was; the successful attacks bypassed it completely.

10.1 CHOOSING AN ALGORITHM

When it comes to evaluating and choosing algorithms, people have several alternatives:

- They can choose a published algorithm, based on the belief that a published algorithm has been scrutinized by many cryptographers; if no one has broken the algorithm yet, then it must be pretty good.

- They can trust a manufacturer, based on the belief that a well-known manufacturer has a reputation to uphold and is unlikely to risk that reputation by selling equipment or programs with inferior algorithms.

- They can trust a private consultant, based on the belief that an impartial consultant is best equipped to make a reliable evaluation of different algorithms.

- They can trust the government, based on the belief that the government is trustworthy and wouldn't steer its citizens wrong.

- They can write their own algorithms, based on the belief that their cryptographic ability is second-to-none and that they should trust nobody but themselves.

Any of these alternatives is problematic, but the first seems to be the most sensible. Putting your trust in a single manufacturer, consultant, or government is asking for trouble. Most people who call themselves security consultants (even those from big-name firms usually don't know anything about encryption. Most security product manufacturers are no better. The NSA has some of the world's best cryptographers working for it, but they're not telling all they know. They have their own interests to further which are not congruent with those of their citizens. And even if you're a genius, writing your own algorithm and then using it without any peer review is just plain foolish.

The algorithms in this book are public. Most have appeared in the open literature and many have been cryptanalyzed by experts in the field. I list all published results, both positive and negative. I don't have access to the cryptanalysts done by any of the myriad military security organizations in the world Which are probably better than the academic institutionsÄthey've been doing it longer and are better funded), so it is possible that these algorithms are easier to break than it appears. Even so, it is far more likely that they are more secure than an algorithm designed and implemented in secret in some corporate basement.

The hole in all this reasoning is that we don't know the abilities of the various military cryptanalysts organizations.

What algorithms can the NSA break? For the majority of us, there's really no way of knowing. If you are arrested with a DES-encrypted computer hard drive, the FBI is unlikely to introduce the decrypted plaintext at your trial; the fact that they can break an algorithm is often a bigger secret than any information that is recovered. During WWII, the Allies were forbidden from using decrypted German Ultra traffic unless they could have plausibly gotten the information elsewhere. The only way to get the NSA to admit to the ability to break a given algorithm is to encrypt something so valuable that its public dissemination is worth the admission. Or, better yet, create a really funny joke and send it via encrypted e-mail to shady characters in shadowy countries. NSA employees are people, too; I doubt even they can keep a good joke secret.

A good working assumption is that the NSA can read any message that it chooses, but that it cannot read all messages that it chooses. The NSA is limited by resources, and has to pick and choose among its various targets. Another good assumption is that they prefer breaking knuckles to breaking codes; this preference is so strong that they will only resort to breaking codes when they wish to preserve the secret that they have read the message. In any case, the best most of us can do is to choose among public algorithms that have withstood a reasonable amount of public scrutiny and cryptanalysts. Algorithms for Export

Algorithms for export out of the United States must be approved by the U.S. government (actually, by the NSA (see Section 25.1). It is widely believed that these export-approved algorithms can be broken by the NSA. Although no one has admitted this on the record, these are some of the things the NSA is rumored to privately suggest to companies wishing to export their cryptographic products:

- Leak a key bit once in a while, embedded in the ciphertext.

- "Dumb down" the effective key to something in the 30-bit range. For example, while the algorithm might accept a 100-bit key, most of those keys might be equivalent.

- Use a fixed IV, or encrypt a fixed header at the beginning of each encrypted message. This facilitates a known-plaintext attack.

- Generate a few random bytes, encrypt them with the key, and then put both the plaintext and the ciphertext of those random bytes at the beginning of the encrypted message. This also facilitates a known- plaintext attack.

NSA gets a copy of the source code, but the algorithm's details remain secret from everyone else. Certainly no one advertises any of these deliberate weaknesses, but beware if you buy a U.S. encryption product that has been approved for export.

10.2 PUBLIC-KEY CRYPTOGRAPHY VERSUS SYMMETRIC CRYPTOGRAPHY

Which is better, public-key cryptography or symmetric cryptography? This question doesn't make any sense, but has been debated since public-key cryptography was invented. The debate assumes that the two types of cryptography can be compared on an equal footing. They can't.

Needham and Schroeder [1159] pointed out that the number and length of messages are far greater with public-key algorithms than with symmetric algorithms. Their conclusion was that the symmetric algorithm was more efficient than the public-key algorithm. While true, this analysis overlooks the significant security benefits of public-key cryptography. Whitfield Diffie writes 492,494]:

In viewing public-key cryptography as a new form of cryptosystem rather than a new form of key management, I set the stage for criticism on grounds of both security and performance. Opponents were quick to point out that the RSA system ran about one-thousandth as fast as DES and required keys about ten times as large. Although it had been obvious from the beginning that the use of public key systems could be limited to exchanging keys for conventional [symmetric] cryptography, it was not immediately clear that this was necessary. In this context, the proposal to build hybrid systems [879] was hailed as a discovery in its own right.

Public-key cryptography and symmetric cryptography are different sorts of animals; they solve different sorts of problems. Symmetric cryptography is best for encrypting data. It is orders of magnitude faster and is not susceptible to chosen-ciphertext attacks. Public-key cryptography can do things that symmetric cryptography can't; it is best for key management and a myriad of protocols discussed in Part I.

Other primitives were discussed in Part I: one-way hash functions, message authentication codes, and so on. Table 10.1 lists different types of algorithms and their properties [804].

10.3 ENCRYPTING COMMUN1CAT10NS CHANNELS

This is the classic Alice and Bob problem: Alice wants to send Bob a secure message. What does she do? She encrypts the message.

In theory, this encryption can take place at any layer in the OSI (Open Systems Interconnect) communications model. (See the OSI security architecture standard for more information [305].) In practice, it takes place either at the lowest layers (one and two) or at higher layers. If it takes place at the lowest layers, it is called link-by-link encryption; everything going through a particular data link is encrypted. If it takes place at higher layers, it is called end-to-end encryption; the data are encrypted selectively and stay encrypted until they are decrypted by the intended final recipient. Each approach has its own benefits and drawbacks.

Link-by Link Encryption

The easiest place to add encryption is at the physical layer (see Figure 10. 1). This is called link-by-link encryption. The interfaces to the physical layer are generally standardized and it is easy to connect hardware encryption devices at this point. These devices encrypt all data passing through them, including data, routing information, and protocol information. They can be used on any type of digital communication link. On the other hand, any intelligent switching or storing nodes between the sender and the receiver need to decrypt the data stream before processing it.

This type of encryption is very effective. Because everything is encrypted, a crypt- analyst can get no information about the structure of the information. He has no idea who is talking to whom, how long the messages they are sending are, what times of day they communicate, and so on. This is called traffic-flow security: the enemy is not only denied access to the information, but also access to the knowledge of where and how much information is flowing.

Security does not depend on any traffic management techniques. Key management is also simple; only the two endpoints of the line need a common key, and they can change their key independently from the rest of the network.

Imagine a synchronous communications line, encrypted using 1-bit CFB. After initialization, the line can run indefinitely, re-

covering automatically from bit or synchronization errors. The line encrypts whenever messages are sent from one end to the other; otherwise it just encrypts and decrypts random data. Eve has no idea when messages are being sent and when they are not; she has no idea when messages begin and end. All she sees is an endless stream of random-looking bits.

If the communications line is asynchronous, the same 1-bit CFB mode can be used. The difference is that the adversary can get information about the rate of transmission. If this information must be concealed, make some provision for passing dummy messages during idle times.

The biggest problem with encryption at the physical layer is that each physical link in the network needs to be encrypted: Leaving any link unencrypted jeopardizes the security of the entire network. If the network is large, the cost may quickly become prohibitive for this kind of encryption.

Additionally, every node in the network must be protected, since it processes unencrypted data. If all the network's users trust one another, and all nodes are in secure locations, this may be tolerable. But this is unlikely. Even in a single corporation, information might have to be kept secret within a department. If the network accidentally misroutes information, anyone can read it. Table 10.2 summarizes the pros and cons of link-by-link encryption.

End-to-End Encryption

Another approach is to put encryption equipment between the network layer and the transport layer. The encryption device must understand the data according to the protocols up to layer three and encrypt only the transport data units, which are then re-combined with the unencrypted routing information and sent to lower layers for transmission.

This approach avoids the encryption/decryption problem at the physical layer. By providing end-to-end encryption, the data remains encrypted until it reaches its final destination (see Figure 10.2). The primary problem with end-to-end encryption is that the routing information for the data is not encrypted; a good cryptanalyst can learn much from who is talking to whom, at what times and for how long, without ever knowing the contents of those conversations. Key management is also more difficult, since individual users must make sure they have common keys.

Building end-to-end encryption equipment is difficult. Each particular communications system has its own protocols. Sometimes the interfaces between the levels are not well-defined, making the task even more difficult.

If encryption takes place at a high layer of the communications architecture, like the applications layer or the presentation layer, then it can be independent of the type of communication network used. It is still end-to-end encryption, but the encryption implementation does not have to bother about line codes, synchronization between modems, physical interfaces, and so forth. In the early days of electro- mechanical cryptography, encryption and decryption took place entirely offline; this is only one step removed from that.

Encryption at these high layers interacts with the user software. This software is different for different computer architectures, and so the encryption must be optimized for different computer systems. Encryption can occur in the software itself or in specialized hardware. In the latter case, the computer will send the data to the specialized hardware for encryption before sending it to lower layers of the communication architecture for transmission. This process requires some intelligence and is not suitable for dumb terminals. Additionally, there may be compatibility problems with different types of computers. The major disadvantage of end-to-end encryption is that it allows traffic analysis. Traffic analysis is the analysis of encrypted messages: where they come from, where they go to, how long they are, when they are sent, how frequent or infrequent they are, whether they coincide with outside events like meetings, and more. A lot of good information is buried in that data, and a cryptanalyst will want to get his hands on it. Table 10.3 presents the positive and negative aspects of end-to-end encryption.

Combining the Two

Table 10.4, primarily from [1244], compares link-by-link and end-to-end encryption. Combining the two, while most expensive, is the most effective way of securing a network. Encryption of each physical link makes any analysis of the routing information impossible, while end-to-end encryption reduces the threat of unencrypted data at the various nodes in the network. Key management for the two schemes can be completely separate: The network managers can take care of encryption at the physical level, while the individual users have responsibility for end-to-end encryption.

10.4 ENCRYPTING DATA FOR STORAGE

Encrypting data for storage and later retrieval can also be thought of in the Alice and Bob model. Alice is still sending a message to Bob, but in this case "Bob" is Alice at some future time. However, the problem is fundamentally different. In communications channels, messages in transit have no intrinsic value. If Bob doesn't receive a particular message, Alice can always resend it. This is not true for data encrypted for storage. If Alice can't decrypt her message, she can't go back in time and re-encrypt it. She has lost it forever. This means that encryption applications for data storage should have some mechanisms to prevent unrecoverable errors from creeping into the ciphertext. The encryption key has the same value as the message, only it is smaller. In effect, cryptography converts large secrets into smaller ones. Being smaller, they can be easily lost. Key management procedures should assume that the same keys will be used again and again, and that data may sit on a disk for years before being decrypted. Furthermore, the keys will be around for a long time. A key used on a communications link should, ideally, exist only for the length of the communication. A key used for data storage might be needed for years, and hence must be stored securely for years.

Other problems particular to encrypting computer data for storage were listed in [357]:

- The data may also exist in plaintext form, either on another disk, in another computer, or on paper. There is much more opportunity for a cryptanalyst to perform a known-plaintext attack.

- In database applications, pieces of data may be smaller than the block size of most algorithms. This will cause the ciphertext to be considerably larger than the plaintext.

- The speed of I/O devices demands fast encryption and decryption, and will probably require encryption hardware. In some applications, special high-speed algorithms may be required.

- Safe, long-term storage for keys is required.

- Key management is much more complicated, since different people need access to different files, different portions of the same file, and so forth. If the encrypted files are not structured as records and fields, such as text files, retrieval is easier: The entire file is decrypted before use. If the encrypted files are database files, this solution is problematic. Decrypting the entire database to access a single record is inefficient, but encrypting records independently might be susceptible to a block-replay kind of attack. In addition, you must make sure the unencrypted file is erased after encryption (see Section 10.9). For further details and insights, consult [425,569].

Dereferencing Keys

When encrypting a large hard drive, you have two options. You can encrypt all the data using a single key. This gives a cryptanalyst a large amount of ciphertext to analyze and makes it impossible to allow multiple users to see only parts of the drive. Or, you can encrypt each file with a different key, forcing users to memorize a different key for each file.

The solution is to encrypt each file with a separate key, and to encrypt the keys with another key known by the users. Each user only has to remember that one key. Different users can have different subsets of the file-encryption keys encrypted with their key. And there can even be a master key under which every file-encryption key is encrypted. This is even more secure because the file-encryption keys are random and less susceptible to a dictionary attack.

Driver-Level vs. File-Level Encryption

There are two ways to encrypt a hard drive: at the file level and at the driver level. Encryption at the file level means that every file is encrypted separately. To use a file that's been encrypted, you must first decrypt the file, then use it, and then re- encrypt it.

Driver-level encryption maintains a logical drive on the user's machine that has all data on it encrypted. If done well, this can provide security that, beyond choosing good passwords, requires little worry on the part of the user. The driver must be considerably more complex than a simple file-encryption program, however, because it must deal with the issues of being an installed device driver, allocation of new sectors to files, recycling of old sectors from files, random-access read and update requests for any data on the logical disk, and so on.

Typically, the driver prompts the user for a password before starting up. This is used to generate the master decryption key, which may then be used to decrypt actual decryption keys used on different data.

Providing Random Access to an Encrypted Drive

Most systems expect to be able to access individual disk sectors randomly. This adds some complication for using many stream ciphers and block ciphers in any chaining mode. Several solutions are possible.

Use the sector address to generate a unique IV for each sector being encrypted or decrypted. The drawback is that each sector will always be encrypted with the same IV. Make sure this is not a security problem.

For the master key, generate a pseudo-random block as large as one sector. You can do this by running an algorithm in OFB mode, for example.) To encrypt any sec- tor, first XOR in this pseudo-random block, then encrypt normally with a block cipher in ECB mode. This is called ECB+OFB (see Section 15.4).

Since CBC and CFB are error-recovering modes, you can use all but the first block or two in the sector to generate the IV for that sector. For example, the IV for sector 3001 may be the hash of the all but the first 128 bits of the sector's data. After generating the IV, encrypt normally in CBC mode. To decrypt the sector, you use the second 64-bit block of the sector as an IV, and decrypt the remainder of the sector. Then, using the decrypted data, you regenerate the IV and decrypt the first 128 bits.

You can use a block cipher with a large enough block size that it can encrypt the whole sector at once. Crab See Section 14.6) is an example.

10.5 HARDWARE ENCRYPTION VERSUS SOFTWARE ENCRYPTION

Hardware

Until very recently, all encryption products were in the form of specialized hardware. These encryption/decryption boxes plugged into a communications line and encrypted all the data going across that line. Although software encryption is becoming more prevalent today, hardware is still the embodiment of choice for military and serious commercial applications. The NSA, for example, only authorizes encryption in hardware. There are several reasons why this is so.

The first is speed. As we will see in Part III, encryption algorithms consist of many complicated operations on plaintext bits. These are not the sorts of operations that are built into your run-of-the-mill computer. The two most common encryption algorithms, DES and RSA, run inefficiently on general-purpose processors. While some cryptographers have tried to make their algorithms more suitable for software implementation, specialized hardware will always win a speed race.

Additionally, encryption is often a computation-intensive task. Tying up the computer's primary processor for this is inefficient. Moving encryption to another chip, even if that chip is just another processor, makes the whole system faster. The second reason is security. An encryption algorithm running on a generalized computer has no physical protection. Mallory can go in with various debugging tools and surreptitiously modify the algorithm without anyone ever realizing it. Hardware encryption devices can be securely encapsulated to prevent this. Tamper- proof boxes can prevent someone from modifying a hardware encryption device. Special-purpose VLSI chips can be coated with a chemical such that any attempt to access their interior will result in the destruction of the chip's logic. The U.S. government's Clipper and Capstone chips See Sections 24.16 and 24.171 are designed to be tamperproof. The chips can be designed so that it is impossible for Mallory to read the unencrypted key.

IBM developed a cryptographic system for encrypting data and communications on mainframe computers [515,1027]. It includes tamper-resistant modules to hold keys. This system is discussed in Section 24.1.

Electromagnetic radiation can sometimes reveal what is going on inside a piece of electronic equipment. Dedicated encryption boxes can be shielded, so that they leak no compromising information. General-purpose computers can be shielded as well, but it is a far more complex problem. The U.S. military calls this TEMPEST; it's a subject well beyond the scope of this book.

The final reason for the prevalence of hardware is the ease of installation. Most encryption applications don't involve general-purpose computers. People may wish to encrypt their telephone conversations, facsimile transmissions, or data links. It is cheaper to put special-purpose encryption hardware in the telephones, facsimile machines, and modems than it is to put in a microprocessor and software.

Even when the encrypted data comes from a computer, it is easier to install a dedicated hardware encryption device than it is to modify the computer's system software. Encryption should be invisible; it should not hamper the user. The only way to do this in software is to write encryption deep into the operating system. This isn't easy. On the other hand, even a computer neophyte can plug an encryption box between his computer and his external modem.

The three basic kinds of encryption hardware on the market today are: self-contained encryption modules (that perform functions such as password verification and key management for banks), dedicated encryption boxes for communications links, and boards that plug into personal computers.

Some encryption boxes are designed for certain types of communications links, such as T-1 encryption boxes that are designed not to encrypt synchronization bits. There are different boxes for synchronous and asynchronous communications lines. Newer boxes tend to accept higher bit rates and are more versatile.

Even so, many of these devices have some incompatibilities. Buyers should be aware of this and be well-versed in their par-

ticular needs, lest they find themselves the owners of encryption equipment unable to perform the task at hand. Pay attention to restrictions in hardware type, operating system, applications software, net- work, and so forth. PC-board encryptors usually encrypt everything written to the hard disk and can be configured to encrypt everything sent to the floppy disk and serial port as well. These boards are not shielded against electromagnetic radiation or physical interference, since there would be no benefit in protecting the boards if the computer remained unaffected. More companies are starting to put encryption hardware into their communications equipment. Secure telephones, facsimile machines, and modems are all available. Internal key management for these devices is generally secure, although there are as many different schemes as there are equipment vendors. Some schemes are more suited for one situation than another, and buyers should know what kind of key management is incorporated into the encryption box and what they are expected to provide themselves.

Software

Any encryption algorithm can be implemented in software. The disadvantages are in speed, cost, and ease of modification (or manipulation). The advantages are in flexibility and portability, ease of use, and ease of upgrade. The algorithms written in C at the end of this book can be implemented, with little modification, on any computer. They can be inexpensively copied and installed on many machines. They can be incorporated into larger applications, such as communications programs or word processors.

Software encryption programs are popular and are available for all major operating systems. These are meant to protect individual files; the user generally has to manually encrypt and decrypt specific files. It is important that the key management scheme be secure: The keys should not be stored on disk anywhere (or even written to a place in memory from where the processor swaps out to disk). Keys and unencrypted files should be erased after encryption. Many programs are sloppy in this regard, and a user has to choose carefully.

Of course, Mallory can always replace the software encryption algorithm with something lousy. But for most users, that isn't a problem. If Mallory can break into our office and modify our encryption program, he can also put a hidden camera on the wall, a wiretap on the telephone, and a TEMPEST detector down the street. If Mallory is that much more powerful than the user, the user has lost the game before it starts.

10.6 COMPRESSION, ENCODING, AND ENCRYPTION

Using a data compression algorithm together with an encryption algorithm makes sense for two reasons:

Cryptanalysis relies on exploiting redundancies in the plaintext; com- pressing a file before encryption reduces these redundancies.

Encryption is time-consuming; compressing a file before encryption speeds up the entire process.

The important thing to remember is to compress before encryption. If the encryption algorithm is any good, the ciphertext will not be compressible; it will look like random data. (This makes a reasonable test of an encryption algorithm; if the ciphertext can be compressed, then the algorithm probably isn't very good.)

If you are going to add any type of transmission encoding or error detection and recovery, remember to add that after encryption. If there is noise in the communications path, decryption's error-extension properties will only make that noise worse. Figure 10.3 summarizes these steps.

10.7 DETECTING ENCRYPTION

How does Eve detect an encrypted file? Eve is in the spy business, so this is an important question. Imagine that she's eavesdropping on a network where messages are flying in all directions at high speeds; she has to pick out the interesting ones. Encrypted files are certainly interesting, but how does she know they are encrypted?

Generally, she relies on the fact that most popular encryption programs have well-defined headers. Electronic-mail messages encrypted with either PEM or POP (see Sections 24.10 and 24.12) are easy to identify for that reason.

Other file encryptors just produce a ciphertext file of seemingly random bits. How can she distinguish it from any other file of seemingly random bits? There is no sure way, but Eve can try a number of things:

- Examine the file. ASCII text is easy to spot. Other file formats, such as TIFF, TeX, C, Postscript, G3 facsimile, or Microsoft Excel, have standard identifying characteristics. Executable code is detectable, as well. UNIX files often have "magic numbers" that can be detected.

- Try to uncompress the file, using the major compression algorithms. If the file is compressed (and not encrypted), this should yield the original file.

- Try to compress the file. If the file is ciphertext (and the algorithm is good), then the probability that the file can be appreciably compressed by a general-purpose compression routine is small. (By appreciably, I mean more than 1 or 2 percent.) If it is something else (a binary image or a binary data file, for examples it probably can be compressed.

Any file that cannot be compressed and is not already compressed is probably ciphertext. (Of course, it is possible to specifically make ciphertext that is compressible.) Identifying the algorithm is a whole lot harder. If the algorithm is good, you can't. If the algorithm has some slight biases, it might be possible to recognize those biases in the file. However, the biases have to be pretty significant or the file has to be pretty big in order for this to work.

10.8 HIDING CIPHERTEXT IN CIPHERTEXT

Alice and Bob have been sending encrypted messages to each other for the past year. Eve has been collecting them all, but she cannot decrypt any of them. Finally, the secret police tire of all this unreadable ciphertext and arrest the pair. "Give us your encryption keys," they demand. Alice and Bob refuse, but then they notice the thumbscrews. What can they do?

Wouldn't it be nice to be able to encrypt a file such that there are two possible decryptions, each with a different key. Alice could encrypt a real message to Bob in one of the keys and some innocuous message in the other key. If Alice were caught, she could surrender the key to the innocuous message and keep the real key secret.

The easiest way to do this is with one-time pads. Let P be the plaintext, D the dummy plaintext, C the ciphertext, K the real key, and K' the dummy key. Alice encrypts P:

$$P \oplus K = C$$

Alice and Bob share K, so Bob can decrypt C:

$$C \oplus K = P$$

If the secret police ever force them to surrender their key, they don't surrender K, but instead surrender:

$$K' = C \oplus D$$

The police then recover the dummy plaintext:

$$C \oplus K' = D$$

Since these are one-time pads and K is completely random, there is no way to prove that K' was not the real key. To make

matters more convincing, Alice and Bob should concoct some mildly incriminating dummy messages to take the place of the really incriminating real messages. A pair of Israeli spies once did this.

Alice could take P and encrypt it with her favorite algorithm and key K to get C. Then she takes C and XORs it with some piece of mundane plaintext - Pride and Prejudice for example, to get K'. She stores both C and the XOR on her hard disk. Now, when the secret police interrogate her, she can explain that she is an amateur cryptographer and that K' is a merely one-time pad for C. The secret police might suspect something, but unless they know K they cannot prove that Alice's explanation isn't valid.

Another method is to encrypt P with a symmetric algorithm and K, and D with K'. Intertwine bits (or bytes) of the ciphertext to make the final ciphertexts. If the secret police demand the key, Alice gives them K' and says that the alternating bits (or bytes) are random noise designed to frustrate cryptanalysts. The trouble is the explanation is so implausible that the secret police will probably not believe her (especially considering it is suggested in this book). A better way is for Alice to create a dummy message, D, such that the concatenation of P and D, compressed, is about the same size as D. Call this concatenation P'. Alice then encrypts P' with whatever algorithm she and Bob share to get C. Then she sends C to Bob. Bob decrypts C to get P', and then P and D. Then they both compute C 0 D = K'. This K' becomes the dummy one-time pad they use in case the secret police break their doors down. Alice has to transmit D so that hers and Bob's alibis match.

Another method is for Alice to take an innocuous message and run it through some error-correcting code. Then she can introduce errors that correspond to the secret encrypted message. On the receiving end, Bob can extract the errors to reconstruct the secret message and decrypt it. He can also use the error-correcting code to recover the innocuous message. Alice and Bob might be hard pressed to explain to the secret police why they consistently get a 30 percent bit-error rate on an otherwise noise-free computer network, but in some circumstances this scheme can work.

Finally, Alice and Bob can use the subliminal channels in their digital signature algorithms (see Sections 4.2 and 23.3). This is undetectable, works great, but has the drawback of only allowing 20 or so characters of subliminal text to be sent per signed innocuous message. It really isn't good for much more than sending keys.

10.9 DESTROYING INFORMATION

When you delete a file on most computers, the file isn't really deleted. The only thing deleted is an entry in the disk's index file, telling the machine that the file is there. Many software vendors have made a fortune selling file-recovery software that recovers files after they have been deleted.

And there's yet another worry: Virtual memory means your computer can read and write memory to disk any time. Even if you don't save it, you never know when a sensitive document you are working on is shipped off to disk. This means that even if you never save your plaintext data, your computer might do it for you. And driver-level compression programs like Stacker and DoubleSpace can make it even harder to predict how and where information is stored on a disk.

To erase a file so that file-recovery software cannot read it, you have to physically write over all of the file's bits on the disk. According to the National Computer Security Center [1148]:

> Overwriting is a process by which unclassified data are written to storage locations that previously held sensitive data.... To purge the ... storage media, the DoD requires overwriting with a pattern, then its complement, and finally with another pattern; e.g., overwrite first with 0011 0101, followed by 1100 1010, then 1001 0111. The number of times an overwrite must be accomplished depends on the storage media, sometimes on its sensitivity, and sometimes on different DoD component requirements. In any case, a purge is not complete until a final over- write is made using unclassified data.

You may have to erase files or you may have to erase entire drives. You should also erase all unused space on your hard disk.

Most commercial programs that claim to implement the DoD standard over- write three times: first with all ones, then with all zeros, and finally with a repeating one-zero pattern. Given my general level of paranoia, I recommend overwriting a deleted file seven times: the first time with all ones, the second time with all zeros, and five times with a cryptographically secure pseudo-random sequence. Recent developments at the National Institute of Standards and Technology with electron-tunneling microscopes suggest even that might not be enough. Honestly, if your data is sufficiently valuable, assume that it is impossible to erase data completely off magnetic media. Burn or shred the media; it's cheaper to buy media new than to lose your secrets.