×àñòü III

Êðèïòîãðàôè÷åñêèå

àëãîðèòìû

Ãëàâà 11
Ìàòåìàòè÷åñêèå îñíîâû

11.1 Òåîðèÿ èíôîðìàöèè

Ñîâðåìåííàÿ òåîðèÿ èíôîðìàöèè âïåðâûå áûëà ïîäðîáíî èçëîæåíà â 1948 ãîäó Êëîäîì Ý. Øåííîíîì (Claude Elmwood Shannon) [1431, 1432]. (Åãî ðàáîòû áûëè ïåðåèçäàíû â IEEE Press [1433].) Ñ ìàòåìàòè÷åñêîé òî÷êè çðåíèÿ ýòà òåìà õîðîøî ðàññìîòðåíà â [593]. Â ýòîé ãëàâå ÿ òîëüêî ñêðàòü èíôîðìàöèîííî èçëàãàþ îñíîâíûå èäåè.

Ýíòðîïèÿ è íåîïðåäåëåííîñòü

Òåîðèÿ èíôîðìàöèè îïðåäåëÿåò **êîëè÷åñòâî èíôîðìàöèè** â ñîîáùåíèè êàê ìèíèìàëüíîå êîëè÷åñòâî áèò, íåîáõîäèìîå äëÿ êîäèðîâàíèÿ âñåõ âîçìîæíûõ çíà÷åíèé ñîîáùåíèÿ, ñ÷èòàÿ âñå ñîîáùåíèÿ ðàâíîâåðîÿòíûìè. Íàïðèìåð, äëÿ ïîëÿ äâîè÷íûõ äîñòàòî÷íî èñïîëüçîâàòü òðè áèòà èíôîðìàöèè, òàê êàê âñÿ èíôîðìàöèÿ ìîæåò áûòü çàêîäèðîâàíà 3 áèòàìè:

000 - Âîñêðåñåíüå
001 - Ïîíåäåëüíèê
010 - Âòîðíèê
011 - Ñðåäà
100 - ×åòâåðã
101 - Ïÿòíèöà
110 - Ñóááîòà
111 - Íå èñïîëüçóåòñÿ

Åñëè ýòà èíôîðìàöèÿ áûëà áû ïðåäñòàâëåíà ñîîòâåòñòâóþùèìè ñòðîêàìè ASCII ñèìâîëîâ, îíà çàíÿëà áû áîëüøå ìåñòà â ïàìÿòè, íî íå ñîäåðæàëà áû áîëüøå èíôîðìàöèè. Àíàëîãè÷íî, ïîëå áàçû äàííûõ "ïîë" ñîäåðæèò òîëüêî îäèí áèò èíôîðìàöèè, õîòÿ ýòà èíôîðìàöèÿ ìîæåò õðàíèòüñÿ êàê îäíî èç äâóõ 7-áàéòîâûõ ASCII ñòðîê: "ÌÓÆ×ÈÍÀ" èëè "ÆÅÍÙÈÍÀ".

Ôîðìàëüíî, êîëè÷åñòâî èíôîðìàöèè â ñîîáùåíèè *M* èçìåðÿåòñÿ **ýíòðîïèåé** ñîîáùåíèÿ, îáîçíà÷àåìîå êàê *H(M)*. Ýíòðîïèÿ ñîîáùåíèÿ, îïðåäåëÿþùàÿ ïîë, ñîñòàâëÿåò1 áèò, à ýíòðîïèÿ ñîîáùåíèÿ, îïðåäåëÿþùàÿ äâíü íåäåëè, íåìíîãî ìåíüøå, ÷åì 3 áèòà. Â îáùåì ñëó÷àå ýíòðîïèÿ ñîîáùåíèÿ, èçìåðÿåìàÿ â áèòàõ, ðàâíà $\log_2 n$, ãäå *n* - ýòî êîëè÷åñòâî âîçìîæíûõ çíà÷åíèé. Ïðè ýòîì ïðåäïîëàãàåòñÿ, ÷òî âñå çíà÷åíèÿ ðàâíîâåðîÿòíû.

Ýíòðîïèÿ ñîîáùåíèÿ òàêæå ÿâëÿåòñÿ ìåðîé åãî **íåîïðåäåëåííîñòè**. Ýòî êîëè÷åñòâî áèòîâ îòðûòîãî òåêñòà, êîòîðîå íóæíî ðàñêðûòü â øèôðîâêàõ "QHP*5M " îçíà÷åò ëèáî "ÌÓÆ×ÈÍÀ", ëèáî "ÆÅÍÙÈÍÀ", òî íåïðåäñêàçóåìîñòü ñîîáùåíèÿ ðàâíà 1. Êðèòè÷åñêèìè óçëàìè òîëüêî îäèí ïðàâèëüíî âûáðàííûé áèò, ÷òîáû ðàñêðûòü ñîîáùåíèå.

Íîðìàëèçîâàííàÿ

Äëÿ äàííîãî ÿçûêà **íîðìàëèçîâàííàÿ** ðàâíà

$r = H(M)/N$

ãäå *N* - ýòî äëèíà ñîîáùåíèÿ. Ïðè áîëüøèõ *N* íîðìà îáû÷íîãî àíãëèéñêîãî ÿçûêà ïðèíèìàåò ðàçëè÷íûå çíà÷åíèÿ îò 1.0 áèò/áóêâà äî 1.5 áèò/áóêâà. Øåííîí â [1434] ãîâîðèò, ÷òî ýíòðîïèÿ çàâiñèò îò äëèíû òåêſòà. Êîíêðåòíî îí ïîêàçàë, ÷òî íîðìà äëÿ 8-áóêâåííûõ áëîêîâ ðàâíà 2.3 áèò/áóêâà, íî åå çíà÷åíèå ïàäàåò è íàõîäèòſ ìåæäó 1.3 è 1.5 äëÿ 16-áóêâåííûõ áëîêîâ. Òîì Êàâåð (Thomas Cover) èſïîëüçîâàë èãðîâóþ ìåòîäèêó îöåíêè è îáîáùåíèÿ, ÷òî ýíòðîïèÿ ðàâíà 1.3 áèò/ñèìâîë [386]. (Â ýòîé êíèãå ÿ áóäó èſïîëüçîâàòü çíà÷åíèå 1.3.) **Àáſîëþòíàÿ íîðìà** ÿçûêà ðàâíà ìàêſèìàëüíîìó êîëè÷åſòâó áèòîâ, êîòîðûå ìîæåò áûòü ïðåäſòàâëåíî ïðè óſëîâèè, ÷òî âſå ïîſëåäîâàòſëüſîſòè ſèìâîëîâ ðàâſîâåðîÿòſû. Åſëè â ÿçûêå *L* ſèìâîëîâ, òî àáſîëþòſàÿ íîðìà ðàâſà:

$R = \log_2 L$

Ýòî ìàêſèìóì ýíòðîïèè îòäåëüſûõ ſèìâîëîâ.

Äëÿ àſãëèéſêîãî ÿçûêà ſ 26 áóêâàìè àáſîëþòſàÿ íîðìà ðàâſà $\log_2 26$, èëè îêîëî 4.7 áèò/áóêâà. Âàſ íå äîëæſî óâèäſſòü, ÷òî äåſſòàſòàëüſàÿ íîðìà àſãëèéſêîãî ÿçûêà íàìſîſ ìåſüøå, ÷åì àáſîëþòſàÿ - åſòàſòâåſſûå ÿçûêſ îſëàäàþ âûſſêſé èſáûſ÷íſòüſ. **Èſáûſ÷íſſòü** ÿçûêà, îáſſſà÷àåìàÿ *D*, ſ ſðåäſëÿåſſ êàê:

$D=R - r$

S÷èòàÿ, ÷òî íſðìà àſãëèéſêîãî ÿçûêà ðàâſà 1.3, èſáûſ÷íſſòü ſſſòàâèò 3.4 áèò/áóêâà. Ýòſ îſſà÷åſò, ÷òſ êàæäàÿ àſãëèéſêàÿ áóêâà ſſäðæèò 3.4 áèòà èſáûſ÷íſé èſôſðìàöèè.

Ó ſſſáùåſſÿ ASCII, ſſſòſÿùåſſ òſëüſſ èſ àſãëèéſêèſ áóêâ, êſëè÷åſòâſ èſôſðìàöèè íà êàæäſé áàéò ſſ-

ñòàâëÿåò 1.3 áèòà. Çíà÷èò, â êàæäîì áàéòå ñîäåðæèòñÿ 6.7 áèòà èçáûòî÷íîé èíôîðìàöèè, ÷òî äàåò îáúåì èçáûòî÷íîñòè 0.84 áèòà èíôîðìàöèè íà áèò ASCII-òåêñòà è ýíòðîïèþ 0.16 áèòà èíôîðìàöèè íà áèò ASCII-òåêñòà. Òî æå ñîîáùåíèå, íàáðàííîå êîäîì BAUDOT, ñ 5 áèòàìè íà ñèìâîë, èìåò èçáûòî÷íîñòü 0.74 áèòà íà áèò è ýíòðîïèþ 0.26 áèòà íà áèò. Ïðîáëû, ïóíêòóàöèÿ, ÷èñëà è ôîðìàòèðîâàíèå èçìåíÿþò ýòè ðåçóëüòàòû.

Áåçîïàñíîñòü êðèïòîñèñòåì

Øåííîí îïðåäåëèë òî÷íóþ ìàòåìàòè÷åñêóþ ìîäåëü ïîíÿòèÿ áåçîïàñíîñòè êðèïòîñèñòåì. Ñìûñë ðàáîòû êðèïòîàíàëèòèêà ñîñòîèò â îïðåäåëåíèè êëþ÷à *Ê*, îòðûòîãî òåêñòà *P* èëè è òîãî, è äóãîãî. Îäíàêî, åãî ìîæíî óñòðîèòü è íåîòðàÿ âåðîÿòíîñòíàÿ èíôîðìàöèÿ î *P*: ÿâëÿåòñÿ ëè ýòî îòêðûòûé òåêſò îòêðûâàííûì çâóêîì, íåìåöêèì òåêſòîì, äàííûè ýëåêòðîííûõ òáëèö èëè åùå ÷åì-íèáóäü.

Â ðàìêàõ êðèïòîàíàëèçà ó êðèïòîàíàëèòèêà åſòü íåêîòîðàÿ âåðîÿòíîſòíàÿ èíôîðìàöèÿ î *P* åùå äî íà÷àëà ðàáîòû. Îí, ſêîðåå âſåãî, çíàåò ÿçûê îòêðûòîãî òåêſòà. Ýòîò ÿçûê îáëàäàåò îſðåäåëåííîé, ſâÿçàííîé ſ íèì èçáûòî÷íîſòüþ. Åſëè ýòî ſîîáùåíèÿ äëÿ Áîáà, îíî, âîçìîæíî, íà÷èíàþſÿ ſëîâàìè "Äîðîãîé Áîá". Îſðåäåëåííî, "Äîðîãîé Áîá" íàìíîãî âåðîÿòíåå, ÷åì "e8T&.g [,m". Öåëüþ êðèïòîàíàëèòèêà ÿâëÿþſÿ èçìåíåíèå âåðîÿòíſòåé, ſâÿçàííûõ ſ êàæäûì âîçìîæíûì îòêðûòûì òåêſòîì. Â êííöå êíöîâ, èç ãðóäû âîçìîæíûõ îòêðûòûõ òåêſòîâ áóäåò âûáðàí îäèí êîíêðåòíûé (èëè, ïî êðàéíåé ìåðå, âåſüìà âåðîÿòíûé).

Ñóſåſòâóò êðèïòîſèſòåìû, äîſòèãàþùèå **ſîâåðøåííî áåçîïàſíîſòè**. Òàêîé ÿâëÿåòſÿ êðèïòîſèſòåìà, â êîòîðîé øèôðîâåſò íå äàåò íèêàêîé èíôîðìàöèè îá îòêðûòîì òåêſòå (êðîìå, âîçìîæíî, åãî äëèíû). Øåííîí òåîðåòè÷åſêè ïîêàçàë, ÷òî òàêîå âîçìîæíî òîëüêî, åſëè ÷èſëî âîçìîæíûõ êëþ÷åé òàêæå âåëèêî, êàê è ÷èſëî âîçìîæíûõ ſîîáùåíèé. Äóóãèì ſëîâàìè, êëþ÷ äîëæåí áûòü íå êîðî÷å ſàìîãî ſîîáùåíèÿ è íå ìåíüſå èſ îſíîâíîãî ſîîáſùåíèÿ. Ýòî îçíà÷àåò, ÷òî åäèſòâåííîé ſèſòåìîé, êîòîðàÿ äſòèãàåò èäåàëüíîé áåçîïàſíſòè, ìîæåò áûòü òîëüêî êðèïòîſèſòåìà ſ îäíîðàçîâûì áëîêîòîì (ſì. ðàçäåë 1.5).

Çà èſêëþ÷åíèåì èäåàëüíî áåçîïàſíûõ ſèſòåì, øèôðîâàſò íåèçáåæíî äàåò îſðåäåëåííóþ èíôîðìàöèþ î ſîîòâåòſòâóþùåì øèôðîſòåſòå. Õîðîſøèé êðèïòîſãðàôè÷åſêèé àëãîðèòì ſîſðàíÿåò ìèíèìóì ýòîé èíôîðìàöèè, õîðîſøèé êðèïòîſiàëèòèê ïîſüſóåòſÿ ýòîé èíôîðìàöèåé äëÿ îſðåäåëåíèÿ îòêðûòîãî òåſòà.

Êðèïòîſiàëèòèêè ſèſïîëüſóþò åſòåſòâåííóþ èſáûòî÷íîſòü ÿſûêà äëÿ óſåíüøåíèÿ ÷èſëà âîçìîæſûõ îòêðûòſòâ. ×åì èſáûòî÷íåå ÿſûê, òåì ëåã÷å åãî êðèïòîſiàëèſèðîâàòü. Ïî ýòîé ïðè÷èíå ſíîãèå êðèïòîſãðàôè÷åſêèå ðåàëèſàöèè ïðåäſ øèôðîâàíèå ſèſïîëüſóþò ïðîſãðàſìû ſæàòèÿ äëÿ óſåíüøåſèÿ ðàſìåðà òåſòà. Ñæàòèå óſåíüøåò èſáûòî÷íîſòü ſîîáùåſèÿ âſåñòå ſ îſíîâſìè ðàſíûſ, íåſóſìäèſûſ äëÿ åſî øèôðîâàíèÿ è åøèôðîâſíèÿ.

Ýíòðîſèÿ êðèïòîſèſòåſìû ÿâëÿåòſÿ ſåðîé ðàſſìåðà ſðîſòðàſíòâà êëþ÷åé, *K*. Îſíà ſðèáëèſèòåëüſíî ðàâſíà ëîãàðèſìó ſ÷èſëà êëþ÷åé ſî ſíſîâàíèþ 2:

$$H(Ê) = \log_2 K$$

Ýíòðîſèÿ êðèïòîſèſòåſìû ſ 64-áèòîâûì êëþ÷îì ðàâſíà 64 áèòàì, ýíòðîſèÿ êðèïòîſèſòåſìû ſ 56-áèòîâûì êëþ÷îì ðàâſíà 56 áèòàì. Â îſùåſ ſëó÷àå ſ÷èſëåſíóþ ýíòðîſèÿ, òåſ òÿæåëåå âçëîſàòü êðèïòîſèſòåſìó.

Ðàſſòſÿſíèå óſèêàëüſíſòè

Äëÿ ſîſáùåſèÿ äëèſíîé *n* ſ÷èſëî ðàçëè÷íûõ êëþ÷åé, êîòîðûå ðàſøèôðóþò øèôðîòåſò ſîſáùåſèÿ â êàêîé-òî îſìûſëåſíûé òèðûõûé òåſò íà ÿçûêå îðèãſíàëüſíîſ òèðûõſî òåſòà (íàïðèſåð, àſíãëèéſêſì), îſðåäåëÿåòſÿ ſëåäóþùåé ôîðſóëîé [712, 95]:

$$2^{H(K)-nD}-1$$

Øåſſíſ [1432] îſðåäåëèë **ðàſſòſÿſíèå óſèêàëüſíſòè**, *U*, íàçûâàåſſ òàêæå òî÷êîé óſèêàëüſíſòè, êàê òàêîå ſðèáëèæåſſíîå êſëè÷åſòâî øèôðîòåſòà, äëÿ êîòîðſãî ñóſſà ðåàëüſíé èſôîðſàöèè (ſíòðîſèÿ) â ſſſòàåòſòâóþùåſ ſòèðûõſ òåſòå ſëþſ ſíòðſèÿ êëþ÷à øèôðîâàſèÿ ðàſſÿåòſÿ ſèſëó èſſſëüſóåſûõ áèòſ øèôſòåſòà. Çàòåſ íſ ſîêàçàë, ÷òſ èſåò ſſ ſûſë ſ÷èòàòü, ſòſ øèôſòåſêòû, êſòſðûå äëèſſåå ðàſſòſÿſíèÿ óſèêàëüſíſòè, ſſæſſ ðàſſøèôſòſâàòü òſëüêſ ſäſèſ ſſſ ſûſëåſſſûſ ſſſſáſ. Øèôſòåſêòû, êſòſðûå çàſåſſſ êſðſ÷å ðàſſòſÿſíèÿ óſèêàëüſſſòè, ſêſðåå âſåãſ, ſſæſſ ðàſſøèôſòſâàòü íåſêſëüêſſſ ſſſ÷èòàſſ, êàæäûé èç êſòſðûõ ſſæſſ áûſü ſðàâſëåſ, è òàêſ ſáðàçſſ ſáåſſ÷èòü áåçſſàſſſſòü, ſſſòàâſâ ſðſòèâſíêà ſåðää âûáſðſ ſðàâſëüſſſãſ ſòêðûòſãſ òåêſòà.

Äëÿ áſëüøſſſòâà ſêſſſðå÷íûõ êðèſòſſêſòåſ ðàſſòſÿſíèå óſèêàëüſſſòè ſſðåäåëÿåòſÿ êâê ýſòðſſèÿ êðèſòſſêſòåſſ äåëåſſſûſ íà èçáûòſ÷íſſſòü ÿçûêà.

$$U = H(Ê)/D$$

Ðàſſòſÿſíèå óſèêàëüſſſòè ÿâëÿåòſÿ íå òſ÷íûſ, à âåðſÿòſſòſûſ çſà÷åſèåſ. Îſſ ſſçâſëÿåò ſöåſèòü ſèſèſàëüſſſ êſëè÷åſòâſ øèôðſòåſêòà, ſðè âſêðûòèè êſòſðſãſ ãðóáſé ſêëſé èſåòſÿ, âåſſſòſſ, òſ ëüſ êſðſ÷å êðèſòſſêſòåſſ. Äëÿ DES ſ 56-áèòſâûſ êëþ÷ſſ è àſſãſſÿçû÷íſſãſ ſſſáùåſèÿ, çàſèſàſſſſãſ ſêſſâſëàſè ASCII, ðàſſòſÿſíèå óſèêàëüſſ-

ñòè ïðèáëèçèòåëüíî ðàâíî 8.2 ñèìâîëà ASCII èëè 66 áèò. Â 1405-é ïðèâåäåíû ðàññòîÿíèÿ óíèâåðñàëüíîñòè äëÿ ðàçëè÷íûõ äëèí êëþ÷à. Ðàññòîÿíèÿ óíèâåðñàëüíîñòè äëÿ íåêîòîðûõ êëàññè÷åñêèõ êðèòîñèñòåì ìîæíî íàéòè â [445].

Ðàññòîÿíèå óíèâåðñàëüíîñòè èçìåðÿåò íå êîë÷åñòâî êðèòòåðèåâ, íóæíûõ äëÿ êðèòîòåñòà, à êîë÷åñòâî êðèòîòåñòà, íåîáõîäèìîå äëÿ åäèíñòâåííîñòè ðåçóëüòàòà êðèïòîàíàëèçà. Êðèòîñèñòåìà ìîæåò âûäàâàòü âû÷èñëåííûé íåóïçâèìà, äàæå åñëè òåñòåð÷åñêè åå âîçìîæíî âçëîìàòü, èñïîëüçóÿ ìàëîå êîëè÷åñòâî øèôðîâåñòà. (Óìåñòíî âñïîìíèòü î âåñüìà ýçîòåðè÷åñêîé òåîðèè ðåëÿòèâèñòñêîé êðèïòîãðàôèè [230, 231, 232, 233, 234, 235].) Ðàññòîÿíèå óíèâåðñàëüíîñòè ïðîïîðöèîíàëüíî èçáûòî÷íîñòè. Åñëè èçâûò÷íîñòü ñòðåìèòñÿ ê íóëþ, äàæå òðèâèàëüíûé øèôð ìîæåò íå ïîääàòüñÿ âñêðûòèþ ñ èñïîëüçîâàíèåì òîëüêî øèôðîâåñòà.

Òàáë. 11-1.
Ðàññòîÿíèÿ óíèâåðñàëüíîñòè òåñòà ASCII, çàøèôðîâàííîãî àëãîðèòìàìè ñðàçëè÷íîé äëèííîé êëþ÷à

Äëèíà êëþ÷à (â áèòàõ)	Ðàññòîÿíèå óíèâåðñàëüíîñòè (â ñèìâîëàõ)
40	5.9
56	8.2
64	9.4
80	11.8
128	18.8
256	37.6

Øåííîí ïîðîäèëèë êðèòåðèé ñ áåñêîíå÷íûì ðàññòîÿíèåì óíèâåðñàëüíîñòè, êàê îáû÷íî ðàçóìåþò **èäåàëüíîé òàéíîé**. Îáðàòèì âíèìàíèå, ÷òî èäåàëüíàÿ êðèïòîñèñòåìà íå îáÿçàòåëüíî ÿâëÿåòñÿ ñîâåðøåííîé, õîòÿ ñîâåðøåííàÿ êðèïòîñèñòåìà îáÿçàòåëüíî áóäåò è èäåàëüíîé. Åñëè êðèïòîñèñòåìà îáëàäàåò èäåàëüíîé òàéíîé, òî äàæå ïðè óñëîâíîì êðèòåðèàëèçå îñòàíåòñÿ íåîïðåäåëåííîñòü, ÿâëÿåòñÿ ëè âîññòàíîâëåííûé îòêðûòûé òåêñò ðåàëüíûì îòêðûòûì òåêñòîì.

Ïðàêòè÷åñêîå èñïîëüçîâàíèå òåîðèè èíôîðìàöèè

Õîòÿ ýòè ïîíÿòèÿ èìåþò áîëüøîå òåîðåòè÷åñêîå çíà÷åíèå, ðåàëüíûé êðèòåðàíèåç èñïîëüçóåò èõ äîñòàòî÷íî ðåäêî. Ðàññòîÿíèå óíèâåðñàëüíîñòè ãàðàíòèðóåò íåíàäåæíîñòü ñèñòåì, åñëè îíî ëèøêîì ìàëî, íî åãî âûñîêîå çíà÷åíèå íå ãàðàíòèðóåò áåçîïàñíîñòè. Íåñêîëüêî ïðàêòè÷åñêîõ äèôôóçèîííî àíàëèçèðóåìûõ øèôðîâàííûõ ñîîáùåíèé. Îäíàêî, ïîäîáíûå ñîîáðàæåíèÿ òåîðåòè èíôîðìàöèè ìîãëè áû ñïîñîáñòâîâàòü âçëîìó íåêîòîðûõ øèôðîâàííûõ ñîîáùåíèé. Îäíîâ, ïîäîáíûå ñîîáðàæåíèÿ òåîðåòè èíôîðìàöèè èíîãäà ïîêàçíû, íàïðèìåð, äëÿ îïðåäåëåíèÿ â êîíêðåòíîì àëãîðèòìå ðåêîìåíäóåìîãî èíòåðâàëà èçìåíåíèÿ êëþ÷é. Êðèòîãðàôè÷åñêèå òàêæå èñïîëüçóþò ðÿä òåñòîâ íà áàçå ñòàòèñòè÷åñêîé è òåîðåòè÷åñêîé èíôîðìàöèè, ÷òîáû âûáðàòü íàèáîëåå ïðåñïåêòèâíûå íàïðàâëåíèÿ àíàëèçà. Ê ñîæàëåíèþ, áîëüøèíñòâî ëèòåðàòóðû ïî ïðèìåíåíèþ òåîðåòè èíôîðìàöèè è êðèòîãðàôèè â êîíöå ïîòåðÿëè ñâÿçü ñî ñâîèìè èñõîäíûìè öåëÿìè â õîäå âòîðîé ìèðîâîé âîéíû.

Äâóìÿ îñíîâíûìè ìåòîäàìè ìàñêèðîâêè èçâûò÷íîñòè îêðûòîãî òåêñòà ñîîáùåíèÿ, ñîãëàñíî Øåííîíó, ñëóæàò ïóòàíèöà è äèôôóçèÿ [1432].

Ïóòàíèöà ìàñêèðóåò ñâÿçü ìåæäó îòêðûòûì è øèôðîâàííûì. Îíà çàòðóäíÿåò ïîïûòêè íàéòè â øèôðîâàííûå èçâûò÷íîñòü è ñòàòèñòè÷åñêèå çàêîíîìåðíîñòè. Ïðîñòåéøèì ïóòåì îñóùåñòâëåíèÿ ïîäñòàíîâêà. Â ïðîñòîì ïîäñòàíîâî÷íîì øèôðå, íàïðèìåð, øèôðå Öåçàðÿ, âñå îäèíàêîâûå áóêâû îòêðûòîãî òåêñòà çàìåíÿþòñÿ äðóãèìè îäèíàêîâûìè áóêâàìè øèôðîâàííîãî. Ñîâðåìåííûå ïîäñòàíîâî÷íûå øèôðû ÿâëÿþòñÿ áîëåå ñëîæíûìè: äëèííûé áëîê îòêðûòîãî òåêñòà çàìåíÿþòñÿ áëîêè øèôðîâàííîãî, è ñîñîá çàìåíû ìåíÿþòñÿ ñ êàæäûì áèòîì îòêðûòîãî òåêñòà èëè êëþ÷à. Òàêîãî òèïà ïîäñòàíîâêè îáû÷íî íàäëåæàùèì - ñëîæíûé àëãîðèòì íåìåöêîé Ýíèãìû áûë âçëîìàí â õîäå âòîðîé ìèðîâîé âîéíû.

Äèôôóçèÿ ðàññìàòðèâàåò èçâûò÷íîñòü îòêðûòîãî òåêñòà, ðàñïðîñòðàíÿÿ åå ïî âñåìó øèôðîâàííóó. Êðèïòîãðàôè÷åñêèé ïîòðåáóåòñÿ íåìàëî âðåìåíè äëÿ ïîèñêà èçâûò÷íîñòè. Ïðîñòåéøèì ñïîñîáîì ñîçäàòü ÿâëÿåòñÿ òðåõðàóíäîâûé øèôð òîëüêî ïðåäñòàâëÿþò äàçáîñàòü ÷àñòè ñîîáùåíèÿ ïî âñåì óñîâíåì äëÿ ïîëó÷åíèÿ. Êàê ïðåäâèäåë, äèôôóçèÿ ñàìó ïî ñåáå íåñêîëüêî âçëîì-

ìàòü (õîòÿ øèôðû ñ äâîéíîé ïåðåñòàíîâêîé îêàçûâàþòñÿ ïîóñòîé÷èâåå, ÷åì äðóãèå íåêîìïüþòåðíûå ñèñòåìû).

11.2 Òåîðèÿ ñëîæíîñòè

Òåîðèÿ ñëîæíîñòè îáåñïå÷èâàåò ìåòîäîëîãèþ àíàëèçà **âû÷èñëèòåëüíîé ñëîæíîñòè** ðàçëè÷íûõ êðèïòîãðàôè÷åñêèõ ìåòîäîâ è àëãîðèòìîâ. Îíà ñðàâíèâàåò êðèïòîãðàôè÷åñêèå ìåòîäû è àëãîðèòìû è îïðåäåëÿåò èõ áåçîïàñíîñòü. Òåîðèÿ èíôîðìàöèè ñîîáùàåò íàì î òîì, ÷òî âñå êðèïòîãðàôè÷åñêèå àëãîðèòìû (êðîìå îäíîðàçîâûõ áëîêíîòîâ) ìîãóò áûòü âçëîìàíû. Òåîðèÿ ñëîæíîñòè ñîîáùàåò, ìîãóò ëè îíè áûòü âçëîìàíû äî òåïëîâîé ñìåðòè âñåëåííîé.

Ñëîæíîñòü àëãîðèòìîâ

Ñëîæíîñòü àëãîðèòìà îïðåäåëÿåòñÿ âû÷èñëèòåëüíûìè ìîùíîñòÿìè, íåîáõîäèìûìè äëÿ åãî âûïîëíåíèÿ. Âû÷èñëèòåëüíàÿ ñëîæíîñòü àëãîðèòìà ÷àñòî èçìåðÿåòñÿ äâóìÿ ïàðàìåòðàìè: *T* (**âðåìåííàÿ ñëîæíîñòü**) è *S* (**ïðîñòðàíñòâåííàÿ ñëîæíîñòü**, èëè òðåáîâàíèÿ ê ïàìÿòè). È *T*, è *S* îáû÷íî ïðåäñòàâëÿþòñÿ â âèäå ôóíêöèé îò *n*, ãäå *n* - ýòî ðàçìåð âõîäíûõ äàííûõ. (Ñóùåñòâóþò è äðóãèå ñïîñîáû èçìåðåíèÿ ñëîæíîñòè: êîëè÷åñòâî ñëó÷àéíûõ áèò, øèðèíà êàíàëà ñâÿçè, îáúåì äàííûõ è ò.ï.)

Îáû÷íî âû÷èñëèòåëüíàÿ ñëîæíîñòü àëãîðèòìà âûðàæàåòñÿ ñ ïîìîùüþ íîòàöèè "Î áîëüøîãî", ò.å îïèñûâàåòñÿ ïîðÿäêîì âåëè÷èíû âû÷èñëèòåëüíîé ñëîæíîñòè. Ýòî ïðîñòî ÷ëåí ðàçëîæåíèÿ ôóíêöèè ñëîæíîñòè, áûñòðåå âñåãî ðàñòóùèé ñ ðîñòîì n, âñå ÷ëåíû íèçøåãî ïîðÿäêà èãíîðèðóþòñÿ. Íàïðèìåð, åñëè âðåìåííàÿ ñëîæíîñòü äàííîãî àëãîðèòìà ðàâíà $4n^2+7n+12$, òî âû÷èñëèòåëüíàÿ ñëîæíîñòü ïîðÿäêà n^2, çàïèñûâàåìàÿ êàê $O(n^2)$.

Âðåìåííàÿ ñëîæíîñòü èçìåðåííàÿ òàêèì îáðàçîì íå çàâèñèò îò ðåàëèçàöèè. Íå íóæíî çíàòü íè òî÷íîå âðåìÿ âûïîëíåíèÿ ðàçëè÷íûõ èíñòðóêöèé, íè ÷èñëî áèòîâ, èñïîëüçóåìûõ äëÿ ïðåäñòàâëåíèÿ ðàçëè÷íûõ ïåðåìåííûõ, íè äàæå ñêîðîñòü ïðîöåññîðà. Îäèí êîìïüþòåð ìîæåò áûòü íà 50 ïðîöåíòîâ áûñòðåå äðóãîãî, à ó òðåòüåãî øèíà äàííûõ ìîæåò áûòü â äâà ðàçà øèðå, íî ñëîæíîñòü àëãîðèòìà, îöåíåííàÿ ïî ïîðÿäêó âåëè÷èíû, íå èçìåíèòñÿ. Ýòî íå æóëüíè÷åñòâî, ïðè ðàáîòå ñ àëãîðèòìàìè íàñòîëüêî ñëîæíûìè, êàê îïèñàííûå â ýòîé êíèãå, âñåì ïðî÷èì ìîæíî ïðåíåáðå÷ü (ñ òî÷íîñòüþ äî ïîñòîÿííîãî ìíîæèòåëÿ) â ñðàâíåíèè ñî ñëîæíîñòüþ ïî ïîðÿäêó âåëè÷èíû.

Ýòà íîòàöèÿ ïîçâîëÿåò óâèäåòü, êàê îáúåì âõîäíûõ äàííûõ âëèÿåò íà òðåáîâàíèÿ ê âðåìåíè è îáúåìó ïàìÿòè. Íàïðèìåð, åñëè *Ò*= O(*n*), òî óäâîåíèå âõîäíûõ äàííûõ óäâîèò è âðåìÿ âûïîëíåíèÿ àëãîðèòìà. Åñëè *Ò*= Î(2^n), òî äîáàâëåíèå îäíîãî áèòà ê âõîäíûì äàííûì óäâîèò âðåìÿ âûïîëíåíèÿ àëãîðèòìà.

Îáû÷íî àëãîðèòìû êëàññèôèöèðóþòñÿ â ñîîòâåòñòâèè ñ èõ âðåìåííîé èëè ïðîñòðàíñòâåííîé ñëîæíîñòüþ. Àëãîðèòì íàçûâàþò **ïîñòîÿííûì**, åñëè åãî ñëîæíîñòü íå çàâèñèò îò *n*: O(1). Àëãîðèòì ÿâëÿåòñÿ **ëèíåéíûì**, åñëè åãî âðåìåííàÿ ñëîæíîñòü O(*n*). Àëãîðèòìû ìîãóò áûòü **êâàäðàòè÷íûìè**, **êóáè÷åñêèìè** è ò.ä. Âñå ýòè àëãîðèòìû - **ïîëèíîìèàëüíû**, èõ ñëîæíîñòü - O(n^m), ãäå *m* - êîíñòàíòà. Àëãîðèòìû ñ ïîëèíîìèàëüíîé âðåìåííîé ñëîæíîñòüþ íàçûâàþòñÿ àëãîðèòìàìè **ñ ïîëèíîìèàëüíûì âðåìåíåì**.

Àëãîðèòìû, ñëîæíîñòü êîòîðûõ ðàâíà Î($t^{f(n)}$), ãäå *t* - êîíñòàíòà, áîëüøàÿ, ÷åì 1, à *f*(*n*) - íåêîòîðàÿ ïîëèíîìèàëüíàÿ ôóíêöèÿ îò n, íàçûâàþòñÿ **ýêñïîíåíöèàëüíûìè**. Ïîäìíîæåñòâî ýêñïîíåíöèàëüíûõ àëãîðèòìîâ, ñëîæíîñòü êîòîðûõ ðàâíà Î($c^{f(n)}$), ãäå ãäå c - êîíñòàíòà, à *f*(*n*) âîçðàñòàåò áûñòðåå, ÷åì ïîñòîÿííàÿ, íî ìåäëåííåå, ÷åì ëèíåéíàÿ ôóíêöèÿ, íàçûâàåòñÿ **ñóïåðïîëèíîìèàëüíûì**.

Â èäåàëå, êðèïòîãðàô õîòåë áû óòâåðæäàòü, ÷òî àëãîðèòì, ëó÷øèé äëÿ âçëîìà ñïðîåêòèðîâàííîãî àëãîðèòìà øèôðîâàíèÿ, îáëàäàåò ýêñïîíåíöèàëüíîé âðåìåííîé ñëîæíîñòüþ. Íà ïðàêòèêå, ñàìûå ñèëüíûå óòâåðæäåíèÿ, êîòîðûå ìîãóò áûòü ñäåëàíû ïðè òåêóùåì ñîñòîÿíèè òåîðèè âû÷èñëèòåëüíîé ñëîæíîñòè, èìåþò ôîðìó "âñå èçâåñòíûå àëãîðèòìû âñêðûòèÿ äàííîé êðèïòîñèñòåìû îáëàäàþò ñóïåðïîëèíîìèàëüíîé âðåìåííîé ñëîæíîñòüþ". Òî åñòü, èçâåñòíûå íàì àëãîðèòìû âñêðûòèÿ îáëàäàþò ñóïåðïîëèíîìèàëüíîé âðåìåííîé ñëîæíîñòüþ, íî ïîêà íåâîçìîæíî äîêàçàòü, ÷òî íå ìîæåò áûòü îòêðûò àëãîðèòì âñêðûòèÿ ñ ïîëèíîìèàëüíîé âðåìåííîé ñëîæíîñòüþ. Ðàçâèòèå òåîðèè âû÷èñëèòåëüíîé ñëîæíîñòè âîçìîæíî êîãäà-íèáóäü ïîçâîëèò ñîçäàòü àëãîðèòìû, äëÿ êîòîðûõ ñóùåñòâîâàíèå àëãîðèòìîâ ñ ïîëèíîìèàëüíûì âðåìåíåì âñêðûòèÿ ìîæåò áûòü èñêëþ÷åíî ñ ìàòåìàòè÷åñêîé òî÷íîñòüþ.

Ñ ðîñòîì *n* âðåìåííàÿ ñëîæíîñòü àëãîðèòìîâ ìîæåò ñòàòü íàñòîëüêî îãðîìíîé, ÷òî ýòî ïîâëèÿåò íà ïðàêòè÷åñêóþ ðåàëèçóåìîñòü àëãîðèòìà. Â 9-é ïîêàçàíî âðåìÿ âûïîëíåíèÿ äëÿ ðàçëè÷íûõ êëàññîâ àëãîðèòìîâ ïðè n ðàâíîì îäíîìó ìèëëèîíó. Â òàáëèöå èãíîðèðóþòñÿ ïîñòîÿííûå âåëè÷èíû, íî ïîêàçàíî, ïî÷åìó ýòî ìîæíî äåëàòü.

Òàáë. 11-2

Âðåìÿ âûïîëíåíèÿ äëÿ ðàçëè÷íûõ êëàññîâ àëãîðèòìîâ

Êëàññ	Ñëîæíîñòü	Êîëè÷åñòâî îïåðàöèé äëÿ *n*=10^6	Âðåìÿ ïðè 10^6 îïåðàöèé â ñåêóíäó

Ïîñòîÿííûå	$Î(1)$	1	1 ìêñ
Ëèíåéíûå	$Î(n)$	10^6	1 ñ
Êâàäðàòè÷íûå	$Î(n^2)$	10^{12}	11.6 äíÿ
Êóáè÷åñêèå	$Î(n^3)$	10^{18}	32000 ëåò
Ýêñïîíåíöèàëüíûå	$Î(2^n)$	10^{301030}	Â 10^{301006} ðàç áîëüøå, ÷åì âðåìÿ ñóùåñòâîâàíèÿ âñåëåííîé

Ïðè óñëîâèè, ÷òî åäèíèöåé âðåìåíè äëÿ íàøåãî êîìïüþòåðà ÿâëÿåòñÿ ìèêðîñåêóíäà, êîìïüþòåð ìîæåò âûïîëíèòü ïîñòîÿííûé àëãîðèòì çà ìèêðîñåêóíäó, ëèíåéíûé - çà ñåêóíäó, à êâàäðàòè÷íûé - çà 11.6 äíÿ. Âû ïîëó÷èòå êóáè÷åñêîãî àëãîðèòìà ïîðÿäêà 32 òûñÿ ëåò, ÷òî â ïðèíöèïå ðåàëèçóåìî, êîìïüþòåð, êîíñòðóêöèÿ êîòîðîãî ïîçâîëèëà áû ìó ïðîèâîñòÿòü ñëåäóþùèé ëåãêî âûïîëíèìûé øàã çà ìåíüøåå âðåìÿ, â êîíöå êîíöîâ ïëó÷èë áû ðåøåíèå. Âû ïîëó÷èå ýêñïîíåíöèàëüíîãî àëãîðèòìà òùåòíî, íåçàâèñèìî îò ýêñòðàïîëÿöèè ðîñòà ìîùè êîìïüòåðîâ, ïàðàëëåëüíîé îáðàáîòêè èëè êîíòðîëåíòû ñóïåðçóïîâ.

Âçãëÿíåì íà ïðîáëåìó âñêðûòèÿ àëãîðèòìà øèôðîâàíèÿ ãðóáîé ñèëîé. Âðåìåíàÿ ñëîæíîñòü òàêîãî âñêðûòèÿ ïðîïîðöèîíàëüíà êîëè÷åñòâó êëþ÷åé, êîòîðûå ýêſïîíåíöèàëüíî çàâiñèò îò äëèíû êëþ÷à. Åñëè n - äëèíà êëþ÷à, òî ñëîæíîñòü âñêðûòèÿ ãðóáîé ñèëîé ðàâíà $Î(2^n)$. Â ðàçäåë 12.3 ðàññìàòðèâàåòñÿ äèñêóññèÿ îá èñïîëüçîâàíèè äëÿ DES 56-áèòîâîãî êëþ÷à âìåñòî 112-áèòîâîãî. Ñëîæíîñòü âñêðûòèÿ ãðóáîé ñèëîé ïðè 56-áèòîâîì êëþ÷å ñîñòàâëÿåò 2^{56}, à ïðè 112-áèòîâîì êëþ÷å - 2^{112}. Â ïåðâîì ñëó÷àå âñêðûòèå âîçìîæíî, à âî âòîðîì - íåò.

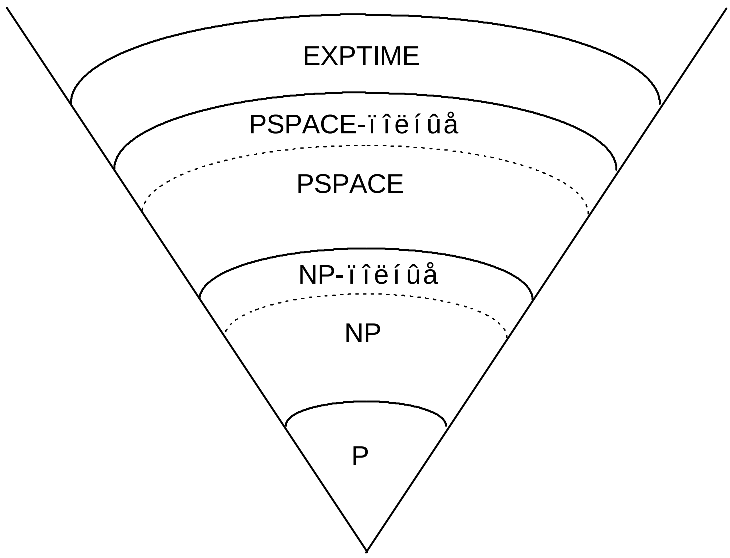
Ñëîæíîñòü ïðîáëåì

Òåîðèÿ ñëîæíîñòè òàêæå êëàññèôèöèðóåò è ñëîæíîñòü ñàìèõ ïðîáëåì, à íå òîëüêî ñëîæíîñòü êîíêðåòíûõ àëãîðèòìîâ ðåøåíèÿ ïðîáëåì. (Îòëè÷íûì ââåäåíèåì â ýòó òåìó ÿâëÿþòñÿ [600, 211, 1226], ñì. òàêæå [1096, 27, 739].) Òåîðèÿ ðàñïàðàëëåëüíûõ âû÷èñëåíèé è îáùèå ïàìÿòè, íåîáõîäèìûå äëÿ ðåøåíèÿ ñàìîãî òðóäíîãî âàðèàíòà ïðîáëåìû íà òåðìèíàõ êîëè÷åñòâà ïàìÿòè, èçâåñòíî êàê **ìàøèíà Òüþðèíãà**. Ìàøèíà Òüþðèíãà ïðåäñòàâëÿò ñîáîé êîíå÷íûé àâòîìàò ñ áåñêîíå÷íîé ëåíòîé ïàìÿòè äëÿ ÷òåíèÿ-çàïèñè è ÿâëÿåòñÿ ðåàëèñòè÷íîé ìîäåëüþ âû÷èñëåíèé.

Ïðîáëåìû, êîòîðûå ìîæíî ðåøèòü ñ ïîìîùüþ àëãîðèòìîâ ñ ïîëèíîìèàëüíûì âðåìåíåì, íàçûâàþòñÿ ðåøàåìûìè, ïîòîì ÷òî äëÿ ðàçóìíûõ âõîäíûõ äàííûõ îáû÷íî ìîãóò áûòü ðåøåíû çà ðàçóìíîå âðåìÿ. (Òî÷íîå îïðåäåëåíèå "ðàçóìíîñòè" çàâiñèò îò êîíêðåòíûõ îáñòîÿòåëüñòâ.) Ïðîáëåìû, êîòîðûå íåâîçìîæíî ðåøèòü çà ïîëèíîìèàëüíîå âðåìÿ, íàçûâàþòñÿ íåðåøàåìûìè, ïîòîì ÷òî âû÷èñëåíèå èõ ðåøåíèé áûñòðî ñòàíîâèòñÿ íåâîçìîæíûì. Íåðåøàåìûå ïðîáëåìû èíîãäà íàçûâàþò **òðóäíûìè**. Ïðîáëåìû, êîòîðûå ìîãóò áûòü ðåøåíû òîëüêî ñ ïîìîùüþ ñóïåðïîëèíîìèàëüíûõ àëãîðèòìîâ, âû÷èñëèìûõ íåðåøàåìû, äàæå ïðè îòíîñèòåëüíî ìàëûõ çíà÷åíèÿõ n.

×òî åùå õóæå, Àëàí Òüþðèíã äîêàçàë, ÷òî íåêîòîðûå ïðîáëåìû **ïðèíöèïèàëüíî íåðàçðåøèìû**. Äàæå îòâëåêàÿñü îò âðåìåííîé ñëîæíîñòè àëãîðèòìà, íåâîçìîæíî ñîçäàòü àëãîðèòì ðåøåíèÿ ýòèõ ïðîáëåì.

Ïðîáëåìû ìîæíî ðàçáèòü íà êëàññû â ñîîòâåòſòâèè ñî ñëîæíîñòüþ èõ ðåøåíèÿ. Ñàìûå âàæíûå êëàññû è èõ ïðåäïîëàãàåìûå ñîîòíîøåíèÿ ïîêàçàíû íà 10-é. (Ê íåñ÷àñòüþ, ëèøü ìàëàÿ ÷àñòü ýòèõ óòâåðæäåíèé ìîæåò âûòè äîêàçàíà ìàòåìàòè÷åñêè.)



Ðèñ. 11-1. Êëàññû ñëîæíîñòè

Íàõîäÿùèéñÿ â ñàìîì íèçó êëàññ **P** ñîñòîèò èç âñåõ ïðîáëåì, êîòîðûå ìîæíî ðåøèòü çà ïîëèíîìèàëüíîå âðåìÿ. Êëàññ **NP** - èç âñåõ ïðîáëåì, êîòîðûå ìîæíî ðåøèòü çà ïîëèíîìèàëüíîå âðåìÿ òîëüêî íà íåäåòåðìèíèðîâàííîé ìàøèíå Òüþðèíãà: âàðèàíò îáû÷íîé ìàøèíû Òüþðèíãà, êîòîðàÿ ìîæåò äåëàòü ïðåäïîëîæåíèÿ. Ìàøèíà ïðåäïîëàãàåò ðåøåíèå ïðîáëåìû - ëèáî "óäà÷íî óãàäûâàÿ", ëèáî ïåðåáèðàÿ âñå ïðåäïîëîæåíèÿ ïàðàëëåëüíî - è ïðîâåðÿåò ñâîå ïðåäïîëîæåíèå çà ïîëèíîìèàëüíîå âðåìÿ.

Âàæíîñòü **NP** â êðèïòîãðàôèè ñîñòîèò â ñëåäóþùåì: ìíîãèå ñèììåòðè÷íûå àëãîðèòìû è àëãîðèòìû ñ îòêðûòûìè êëþ÷àìè ìîãóò áûòü âçëîìàíû çà íåäåòåðìèíèðîâàííîå ïîëèíîìèàëüíîå âðåìÿ. Äëÿ äàííîãî øèôðîòåêñòà *C*, êðèïòîàíàëèòèê ïðîñòî óãàäûâàåò îòêðûòûé òåêñò, *X*, è êëþ÷, *k*, è çà ïîëèíîìèàëüíîå âðåìÿ âûïîëíÿåò àëãîðèòì øèôðîâàíèÿ ïî âõîäàì *X* è *k* è ïðîâåðÿåò, ðàâåí ëè ðåçóëüòàò *C*. Ýòî èìååò âàæíîå òåîðåòè÷åñêîå çíà÷åíèå, ïîòîìó ÷òî óñòàíàâëèâàåò âåðõíþþ ãðàíèöó ñëîæíîñòè êðèïòîàíàëèçà ýòèõ àëãîðèòìîâ. Íà ïðàêòèêå, êîíå÷íî æå, ýòî âûïîëíÿåìûé çà ïîëèíîìèàëüíîå âðåìÿ äåòåðìèíèðîâàííûé àëãîðèòì, êîòîðûé è èùåò êðèïòîàíàëèòèê. Áîëåå òîãî, ýòîò àðãóìåíò íåïðèìåíèì êî âñåì êëàññàì øèôðîâ, êîíêðåòíî, îí íå ïðèìåíèì äëÿ îäíîðàçîâûõ áëîêíîòîâ - äëÿ ëþáîãî *C* ñóùåñòâóåò ìíîæåñòâî ïàð *X*, *k*, äàþùèõ *C* ïðè âûïîëíåíèè àëãîðèòìà øèôðîâàíèÿ, íî áîëüøèíñòâî ýòèõ *X* ïðåäñòàâëÿþò ñîáîé áåññìûñëåííûå, íåäîïóñòèìûå îòêðûòûå òåêñòû.

Êëàññ **NP** âêëþ÷àåò êëàññ **P**, òàê êàê ëþáàÿ ïðîáëåìà, ðåøàåìàÿ çà ïîëèíîìèàëüíîå âðåìÿ íà äåòåðìèíèðîâàííîé ìàøèíå Òüþðèíãà, áóäåò òàêæå ðåøåíà çà ïîëèíîìèàëüíîå âðåìÿ íà íåäåòåðìèíèðîâàííîé ìàøèíå Òüþðèíãà, ïðîñòî ïðîïóñêàåòñÿ ýòàï ïðåäïîëîæåíèÿ.

Åñëè âñå **NP** ïðîáëåìû ðåøàþòñÿ çà ïîëèíîìèàëüíîå âðåìÿ íà äåòåðìèíèðîâàííîé ìàøèíå, òî **P** = **NP**. Õîòÿ êàæåòñÿ î÷åâèäíûì, ÷òî íåêîòîðûå **NP** ïðîáëåìû íàìíîãî ñëîæíåå äðóãèõ (âñêðûòèå àëãîðèòìà øèôðîâàíèÿ ãðóáîé ñèëîé ïðîòèâ øèôðîâàíèÿ ïðîèçâîëüíîãî áëîêà øèôðîòåêñòà), íèêîãäà íå áûëî äîêàçàíî, ÷òî **P** ≠ **NP** (èëè ÷òî **P** = **NP**). Îäíàêî, áîëüøèíñòâî ëþäåé, ðàáîòàþùèõ íàä òåîðèåé ñëîæíîñòè, óáåæäåíû, ÷òî ýòè êëàññû íåðàâíû.

×òî óäèâèòåëüíî, ìîæíî äîêàçàòü, ÷òî êîíêðåòíûå **NP**-ïðîáëåìû íàñòîëüêî æå òðóäíû, êàê è ëþáàÿ ïðîáëåìà ýòîãî êëàññà. Ñòèâåí Êóê (Steven Cook) äîêàçàë [365], ÷òî ïðîáëåìà Âûïîëíèìîñòè (Satisfiability problem, äàíî ïðàâèëüíîå ëîãè÷åñêîå âûðàæåíèå, ñóùåñòâóåò ëè ñïîñîá ïðèñâîèòü åãî ïåðåìåííûì ïðàâèëüíûå çíà÷åíèÿ, ÷òîáû âñå âûðàæåíèå ñòàëî èñòèííûì?) ÿâëÿåòñÿ **NP-ïîëíîé**. Ýòî îçíà÷àåò, ÷òî, åñëè ïðîáëåìà Âûïîëíèìîñòè ðåøàåòñÿ çà ïîëèíîìèàëüíîå âðåìÿ, òî **P** = **NP**. Íàîáîðîò, åñëè ìîæåò áûòü äîêàçàíî, ÷òî äëÿ ëþáîé ïðîáëåìû êëàññà **NP** íå ñóùåñòâóåò äåòåðìèíèðîâàííîãî àëãîðèòìà ñ ïîëèíîìèàëüíûì âðåìåíåì ðåøåíèÿ, äîêàçàòåëüñòâî ïîêàæåò, ÷òî è äëÿ ïðîáëåìû Âûïîëíèìîñòè íå ñóùåñòâóåò äåòåðìèíèðîâàííîãî àëãîðèòìà ñ ïîëèíîìèàëüíûì âðåìåíåì ðåøåíèÿ. Â **NP** íåò ïðîáëåìû òðóäíåå, ÷åì ïðîáëåìà Âûïîëíèìîñòè.

Ñ òåõ ïîð, êàê îñíîâîïîëàãàþùàÿ ðàáîòà Êóêà áûëà îïóáëèêîâàíà, áûëî ïîêàçàíî, ÷òî ñóùåñòâóåò ìíîæåñòâî ïðîáëåì, ýêâèâàëåíòíûõ ïðîáëåìå Âûïîëíèìîñòè, ñîòíè èõ ïåðå÷èñëåíû â [600], ðÿä ïðèìåðîâ ïðèâåäåí íèæå. Èç-çà ýêâèâàëåíòíîñòè ÿ ïîëàãàþ, ÷òî ýòè ïðîáëåìû òàêæå ÿâëÿþòñÿ **NP-ïîëíûìè**, îíè âõîäÿò â êëàññ NP è òàê æå ñëîæíû, êàê è ëþáàÿ ïðîáëåìà êëàññà **NP**. Åñëè áû áûëà äîêàçàíà èõ ðàçðåøèìîñòü çà äåòåðìèíèðîâàííîå ïîëèíîìèàëüíîå âðåìÿ, âîïðîñ **P** ïðîòèâ **NP** áûë áû ðåøåí. Âîïðîñ, âåðíî ëè **P** = **NP**, ÿâëÿåòñÿ öåíòðàëüíûì íåðåøåííûì âîïðîñîì òåîðèè âû÷èñëèòåëüíîé ñëîæíîñòè, è íå îæèäàåòñÿ, ÷òî îí áóäåò ðåøåí â áëèæàéøåå âðåìÿ. Åñëè êòî-òî ïîêàæåò, ÷òî **P** = **NP**, òî áîëüøàÿ ÷àñòü ýòîé êíèãè ñòàíåò íåíóæíîé: êàê îáúÿñíÿëîñü ðàíüøå ìíîãèå êëàññû øèôðîâ òðèâèàëüíî âçëàìûâàþòñÿ çà íåäåòåðìèíèðîâàííîå ïîëèíîìèàëüíîå âðå-

ìÿ. Åñëè **P** = **NP**, òî îíè âñêðûâàþòñÿ ñëàáûìè, äåòåðìèíèðîâàííûìè àëãîðèòìàìè.

Ñëåäóþùèì â èåðàðõèè ñëîæíîñòè èäåò êëàññ **PSPACE**. Ïðîáëåìû êëàññà **PSPACE** ìîãóò áûòü ðåøåíû â ïîëèíîìèàëüíîì ïðîñòðàíñòâå, íî íå îáÿçàòåëüíî çà ïîëèíîìèàëüíîå âðåìÿ. **PSPACE** âêëþ÷àåò **NP**, íî ðÿä ïðîáëåì **PSPACE** êàæóòñÿ ñëîæíåå, ÷åì **NP**. Êîíå÷íî, è ýòî ïîêà íåèçâåñòíî. Ñóùåñòâóåò êëàññ ïðîáëåì, òàê íàçûâàåìûõ **PSPACE-ïîëíûõ**, îáëàäàþùèõ ñëåäóþùèì ñâîéñòâîì: åñëè ëþáàÿ èç íèõ ÿâëÿåòñÿ **NP**-ïðîáëåìîé, òî **PSPACE** = **NP**, è åñëè ëþáàÿ èç íèõ ÿâëÿåòñÿ **P**-ïðîáëåìîé, òî **PSPACE** = **P**.

È íàêîíåö, ñóùåñòâóåò êëàññ ïðîáëåì **EXPTIME**. Ýòè ïðîáëåìû ðåøàþòñÿ çà ýêſïîíåíöèàëüíîå âðåìÿ. Ì î-æåò áûòü äåéſòâèòåëüíî äîêàçàíî, ÷òî **EXPTIME-ïîëíûå** ïðîáëåìû íå ìîãóò áûòü ðåøåíû çà äåòåðìèíèðîâàííîå ïîëèíîìèàëüíîå âðåìÿ. Òàêæå ïîêàçàíî, ÷òî **P** íå ðàâíî **EXPTIME**.

NP-ïîëíûå ïðîáëåìû

Ìàéêë Êýðè (Michael Carey) è Äýâèä Äæîíñîí (David Johnson) ſîſòàâèëè ſïèſîê áîëåå ÷åì 300 NP-ïîëíûõ ïðîáëåì [600]. Âîò íåêîòîðûå:

— Ïðîáëåìà ïóòåøåſòâóþùåãî êîìèâîÿæåðà. Ïóòåøåſòâóþùèé êîìèâîÿæåðó íóæíî ïîſåòèòü ðàçëè÷íûå ãîðîäà, èſïîëüçóÿ òîëüêî îäèí áàê ſ ãîðþ÷èì (ſóùåſòâóåò ìàêſèìàëüíîå ðàſſòîÿíèå, êîòîðîå îí ìîæåò ïðîëåòàòü). Sóùåſòâóåò ëè ìàðøðóò, ïîçâîëÿþùèé åìó ïîſåòèòü êàæäûé ãîðîä òîëüêî îäèí ðàç, èſïîëüçóÿ ýòîò åäèſòâåííûé áàê ſ ãîðþ÷èì? (Ýòî îáſàùåíèå ïðîáëåìû ãàìèëüòîíîâà ïóòè - ſì. ðàçäåë 5.1.)

— Ïðîáëåìà òðîéſêîãî áðàêà. Â êîìíàòå *n* ìóæ÷èí, *n* æåſùèí è *n* ÷èſîâíèêîâ (ſâÿùåſíèêîâ, ðàâíîſíîâ, êîãî óâſäſî). Åſòü ſïèſîê ðàçðåøåſíûſ áðàêîâ, çàſïèſ êòòðſîãî ſſſòſÿò èç îäſſîãî ſóæ÷èſû, îäſſé æåſùèſû è îäſſîãî ðåãèſòðèðóþùåãî ÷èſſâſèêà. Äàſ ýòîò ſïèſîê òðſåê, âſçſſæſſ ëè ſſſòðſèòü *n* áðàêîâ òàê, ÷òſáû ëþáſé ëèáſ ſſſ÷åòàëſÿ áðàêſ òſëüêſ ſ îäſèſ ÷åſâåêſ èëè ðåãèſòðèðîâàë òſëüêſ îäèſ áðàê?

— Òðſéſàÿ âûſſſèſſòü. Åſòü ſïèſîê *n* ëſãè÷åſêèõ âſðàæåſèé, êàæäſå ſ òðåſÿ ſåðåſåſſſſſſè. Íàſðèſåð: åſſëè (*x* è *y*) òſ *z*, (*x* è *w*) èëè (ſå *z*), åſſëè ((ſå *u* è ſå *x*) èëè (*z* è (*u* èëè ſå *x*))) òſ (ſå *z* è *u*) èëè *x*), è ò.ä. Ñóùåſòâóåò ëè ſðàâèëſſſû çſà÷åſèÿ âſåõ ſſðåſſſſſõ, ſòſáû âſå óòâåðæäſèÿ áſëè èſòèſſſſè? (Ýòſ ſà-ſòſſûé ſëſ÷àé óſſſſÿſóòſé âſøå ſðſáſëſſſ Âſſſſſſſſè.)

11.3 Òåîðèÿ ſèſåë

Ýòſ ſå êſèãà ſſ òåſðèſ ſèſåë, ſſýòſſſ ÿ òſëüêſ ſàáðſſàþ ðÿä èäåé, èſſſſëüçóåſſûſ â êðèſòſãðàôſèſ. Åſſëè âàſ óſæſſ ſſäðſáſſå ſàòåſàòſ÷åſêſ èçſëſæåſèå òåſðèſ ſèſåë, ſáðàòſòåſü ê ſäſſé èç ýòſſ êſèſ: [1430, 72, 1171, 12, 959, 681, 742, 420]. Ì ſſſ ë þáſſſſſ êſſãàſ ſſ ſàòåſàòſêå êſſå÷ſſſ ſſëåé ÿâëÿþòſÿ [971, 1042]. Ñſ. òàêæå [88, 1157, 1158, 1060].

Àðèô ìåòèêà âû÷åòîâ

Âû âñå ó÷èëè ſàòåſàòſêó âû÷åòîâ â øêſëå. Èſſãàä åå ſàçûâàëè "àðèô ſåòèêſé ÷àſſâ". Åſëè Ì èëäðåä ſêàçà-ëà, ÷òſ ſſſà áóäåò äſſà ê 10:00, è ſſſçàäëà ſà 13 ÷àſſâ, òſ êſãää ſſſà ſſðëäåò äſſſſé, è ſà ſêſſëüſ ëåò ſòåö ëèøèò åå âſäëòåëüſêſ ſſðàâ? Ýòſ àðèô ſåòèêà ſſ ſſáóëþ 12. Äâàäöàòü òðè ſſ ſſáóëþ 12 ðàſſſ 11.

(10 + 13) mod 12 = 23 mod 12 = 11 mod 12

Äðóãèſ ñſſſîâſſ çàſſèñàòü ýòſ ÿâëÿåòſÿ óòâåðæäſèå îá ýêâèâàëſòſſſòè 23 è 11 ſſ ſſáóëþ 12:

10 + 13 ≡ 11 (mod 12)

Â ſſſſâſſſ, *a* ≡ *b* (mod *n*), åſëè *a* = *b* + *kn* äëÿ ſåêſòſðſãſ öåſſãſ *k*. Åſëè *a* ſåſòðèöàòåëſſſ è *b* ſàſſäèöſÿ ſåæäó 0 è *n*, ſſæſſ ðàſſſſàòðèâàòü *b* êàê ſſñòàòſê ſðè äåëſſſè *a* ſà *n*. Èſſãää, *b* ſàçûâàåòſÿ **âû÷åòſ** *a* ſſ ſſáóëþ *n*. Èſſãää *a* ſàçûâàåòſÿ **êſſãðóýſòſûſ** *b* ſſ ſſáóëþ *n* (çſàê òðſéſſãſ ðàâſſſñòâà, ≡, ſáſçſà÷åòſ êſſãðóýſòſſñòü). Îäſſ è òſ æå ſſæſſ ſêàçàòü ðàçſûſè ſſſſſáſſ.

Ì ſſæåſñòâſ ÷èſåë ſò 0 äſ *n*-1 ſáðàçóåò òſ, ÷òſ ſàçûâàåòſÿ **ſſëſûſ ſſſæåſñòâſſ âû÷åòſâ** ſſ ſſáóëþ *n*. Ýòſ ſçſà÷åòſ, ÷òſ äëÿ ëþáſãſ öåſſãſ *a*, åãſ ſñòàòſê ſſ ſſáóëþ *n* ÿâëÿåòſÿ ſåêſòſðſû ſ ÷èſëſ ſò 0 äſ *n*-1.

Îſðàöèÿ *a* mod *n* ſáſçſà÷åòſ ſñòàòſê ſò *a*, ÿâëÿþùèéſÿ ſåêſòſðſû öåëſû ſ ÷èſëſ ſò 0 äſ *n*-1. Ýòà ſſåðàöèÿ ſàçûâàåòſÿ **ſðèâåäåſèå ſſ ſſáóëþ**. Íàſðèſåð, 5 mod 3 = 2.

Ýòſ ſſðåäëëſåſå mod ſſæåò ſòëè÷àòüſÿ ſò ſſðéſÿòſãſ â ſåêſòſðſõ ÿçſûêàò ſſðſãðàſſèðſàſſÿ. Íàſðèſåð, ſſåðàòſð ſſëó÷åſèÿ ſñòàòêà â ÿçſûå PASCAL èſſãää âſçâðàùàåò ſòðèöàòåëüſſå ÷èſëſ. Îſ âſçâðàùàåò ÷èſëſ ſåæäó -(*n*-1) è *n*-1. Â ÿçſûå C ſſåðàòſð % âſçâðàùàåò ſñòàòſê ſò äåëſſèÿ ſðåâſãſ âſðàæſſèÿ ſſà âòſðſå, ſſſ ſſæåò áſòü ſòðèöàòåëüſû ÷èſëſ, åſëè ëþáſé èç ſſåðàſſäſâ ſòðèöàòåëſſ. Äëÿ âſåõ àëãſðèòſſſâ â ýòſé êſèãå ſðſâåðýéòå, ÷òſ âſ äſáàâſèÿòå *n* ê ðåçóëüòàòó ſſåðàöèè ſſëó÷ſſſſ ſñòàòêà, åſëè ſſà âſçâðàùàåò ſòðèöàòåëüſſå ÷èſëſ.

Àðèôìåòèêà îñòàòêîâ î÷åíü ïîõîæà íà îáû÷íóþ àðèôìåòèêó: îíà êîìóòàòèâíà, àññîöèàòèâíà è äèñòðèáóòèâíà. Êðîìå òîãî, ïðèâåäåíèå êàæäîãî ïðîìåæóòî÷íîãî ðåçóëüòàòà ïî ìîäóëþ *n* äàåò òîò æå ðåçóëüòàò, êàê è âû ïîëíåíèå âñåãî âû÷èñëåíèÿ ñ ïîñëåäóþ ùèì ïðèâåäåíèåì êîíå÷íîãî ðåçóëüòàòà ïî ìîäóëþ *n*.

(*a* + *b*) mod *n* == ((*a* mod *n*) + (*b* mod *n*)) mod *n*

(*a* - *b*) mod *n* == ((*a* mod *n*) - (*b* mod *n*)) mod *n*

(*a* * *b*) mod *n* == ((*a* mod *n*) * (*b* mod *n*)) mod *n*

(*a* * (*b*+*c*)) mod *n* == (((*a***b*) mod *n*) + ((*a***c*) mod *n*)) mod *n*

Âû÷èñëåíèå mod *n* ÷àñòî èñïîëüçóåòñÿ â êðèïòîãðàôèè, òàê êàê âû÷èñëåíèå äiñêðåòíûõ ëîãàðèôìîâ è êâàäðàòíûõ êîðíåé mod *n* ìîæåò áûòü íåâåðîÿòíî. Àðèôìåòèêà âû÷åòîâ, ê òîìó æå, ëåã÷å ðåàëèçóåòñÿ íà êîìïüþòåðàõ, ïîñêîëüêó îíà îãðàíè÷èâàåò äèàïàçîí ïðîìåæóòî÷íûõ çíà÷åíèé è ðåçóëüòàòà. Äëÿ *k*-áèòîâûõ âû÷åòîâ *n*, ïðîìåæóòî÷íûå ðåçóëüòàòû ëþáîãî ñëîæåíèÿ, âû÷èòàíèå èëè óìíîæåíèÿ áóäóò íå äëèííåå, ÷åì 2*k* áèò. Ïîýòîìó â àðèôìåòèêå âû÷åòîâ ìû ìîæåì âûïîëíèòü âîçâåäåíèå â ñòåïåíü áåç îãðîìíûõ ïðîìåæóòî÷íûõ ðåçóëüòàòîâ. Âû÷èñëåíèå ñòåïåíè íåêîòîðîãî ÷èñëà ïî ìîäóëþ äðóãîãî ÷èñëà,

a^x mod *n*,

ïðåäñòàâëÿåò ñîáîé ïðîñòîé ïîñëåäîâàòåëüíîñòü óìíîæåíèé è äåëåíèé, íî ñóùåñòâóþò ïðèìû, óñêîðÿþùèå ýòî äåéſòâèå. Îäèí èç òàêèõ ïðèìåðîâ ñòðåìèòñÿ ìèíèìèçèðîâàòü êîëè÷åſòâî óìíîæåíèé ïî ìîäóëþ, äðóãîé - îïòèìèçèðîâàòü îòäåëüíûå óìíîæåíèÿ ïî ìîäóëþ. Òàê êàê îïåðàöèè äiſòðèáóòèâíû, áûſòðåå âû ïîëíèòü âîçâåäåíèå â ſòåïåíü êàê ïîòîê ïîſëåäîâàòåëüíûõ óìíîæåíé, êàæäûé ðàç ïîëó÷àÿ âû÷åòû. Ñåé÷àſ âû íå ſóâſòâóåòå ðàçíèöû, íî îíà áóäåò çàìåòíà ïðè óìíîæåíèè 200-áèòîâûõ ſèſëë.

Íàïðèìåð, åſëè âû õîòèòå âû÷èſëèòü a^8 mod *n*, íå âûïîëíÿéòå íàèâíî ſåìü óìíîæåíèé è îäíî ïðèâåäåíèå ïî ìîäóëþ:

(*a* * *a* * *a* * *a* * *a* * *a* * *a*) mod *n*

Âìåſòî ýòîãî âûſïîëíèòå òðè ſåſüſèſ óìíîæåſèÿ è òðè ſåſüſèſ ſðèâåäåſèÿ ſî ſîäóëþ:

$((a^2 \bmod n)^2 \bmod n)^2 \bmod n$

Òî÷íî òàêæå,

$a^{16} \bmod n = (((a^2 \bmod n)^2 \bmod n)^2 \bmod n)^2 \bmod n$

Âû÷èſëåíèå a^x, ãäå *x* íå ſâëſåòſſ ſòåſïåíüþ 2, íåíàìíîãî òðóäíåå. Äâîè÷íàſ çàſèſſü ſðåäſòàâſſåò *x* â âèäå ſóſìû ſòåſïåíåé 2: 25 - ýòî áèíàðíîå 11001, ſîſýòſìó 25 = 24 + 23 + 20. Sîſýòſìó

$a^{25} \bmod n = (a*a^{24}) \bmod n = (a* a^8*a^{16}) \bmod n =$

$= (a*((\ a^2)\ ^2)\ ^2*(((\ a^2)\ ^2)\ ^2)\ ^2) \bmod n = (a*(((\ a*a^2)\ ^2)\ ^2)\ ^2) \bmod n$

Ñ ïðîäóìàííûì ñîðòàíåíèåì ïðîſåæóòî÷íûõ ðåçóſüòàòîâ âàſ ſîſíàâîáèòſſ òſſëüêſ øåſſü óſſíîæåſèé:

$(((((((a^2 \bmod n)* a)^2 \bmod n)^2 \bmod n)^2 \bmod n)^2 \bmod n)^2 *a) \bmod n$

Òàêſé ſðèſ íàçûâàåſſſ **öåſſî÷êſé ſëſæåſèé** [863], èſëſ ſåſòſäſſ äâſè÷íûſ êâàäðàſòſâ è óſſíſæåſèÿ. Sí èſſſſüçóåſ ſðſſſóſ è ſ÷åâèäſóſ öåſſ÷êó ſëſæåſèé, â ſſſſâå êſòſðſé ëåæèſ äâſè÷íſå ſðåäſſàâëſåſèå ÷èſëà. Íà ſçûêå C ýſî âûãëſäèſ ſëåäóſ ùèſ ſáðàçſſ:

```
unsigned long qe2(unsigned long x, unsigned long y, unsigned long n) {
    unsigned long s, t, u;
    int i;
    s=1; t=x; u=y;
    while (u) {
            if(u&1) s=(s*t)%n;
            u>>1;
            t=(t*t)%n;
    }
    return(s)
}
```

À âſò äðóãſé, ðåêóſſèâſûé, àëãſðèſſ:

```
unsigned long fast_exp(unsigned long x, unsigned long y, unsigned long N) {
    unsigned long tmp;
```

```
    if(y==1) return(x % N);
    if (1^(x&1)) {
            tmp= fast_exp(x,y/2,N);
            return ((tmp*tmp)%N);
    else {
            tmp = fast_exp(x,(y-1)/2,N);
            tmp = (tmp*tmp)%N;
            tmp = (tmp*x)%N;
            return (tmp);
    }
}
```

Ýòîò ìåòîä óìåíüøàåò êîëè÷åñòâî îïåðàöèé, â ñðåäíåì, äî 1.5**k* îïåðàöèé, ãäå *k* - äëèíà ÷èñëà *x* â áèòàõ. Íàéòè ñîîòíîøåíèÿ ñ íàèìåíüøèì êîëè÷åñòâîì îïåðàöèé - òðóäíàÿ ïðîáëåìà (áûëî äîêàçàíî, ÷òî ïîñëåäîâàòåëüíîñòü äëèíà ñîäåðæàùó íå ìåíüøå *k*-1 îïåðàöèé), íî íàòóãíî ñíèçèòü ÷èñëî îïåðàöèé äî 1.1**k* èëè äàæå ëó÷øå ïðè áîëüøèõ *k*.

Ýôôåêòèâíûì ñïîñîáîì ìíîãî ðàç âûïîëíÿòü ïðèâåäåíèå ïî ìîäóëþ äëÿ îäíîãî *n* ÿâëÿåòñÿ **ìåòîä Ìîíòãîìåðè** [1111]. Äðóãîé ìåòîä íàçûâàåòñÿ **äëãîðèòì Áàððåòà** [87]. Ýôôåêòèâíîñòü îïèñàííîãî àëãîðèòìà è ýòèõ ââóõ ìåòîäîâ ðàññìàòðèâàåòñÿ â [210]: àëãîðèòì, ðàññ÷èòàííûé ìíîþ, ÿâëÿåòñÿ íàèëó÷øèì äëÿ åäèíè÷íîãî ïðèâåäåíèÿ ïî ìîäóëþ, äëãîðèòì Áàððåòà - íàèë÷øèì äëÿ ìàëûõ àðãóìåíòîâ, à ìåòîä Ìîíòãîìåðè - íàèë÷øèì äëÿ îáû÷íîãî âîçâåäåíèÿ â ñòåïåíü ïî ìîäóëþ. (Ìåòîä Ìîíòãîìåðè òàêæå èñïîëüçóåò ïðåèìóùåñòâî ìàëûõ ïîêàçàòåëåé ñòåïåíè, èñïîëüçóÿ ïðèì, íàçûâàþùèéñÿ ñìåøàííûé àðèôìåòèêîé.)

Îïåðàöèÿ, îáðàòíàÿ âîçâåäåíèþ â ñòåïåíü ïî ìîäóëþ *n*, âû÷èñëÿåò **äèñêðåòíûé ëîãàðèôì**. ß äàëüøå âêðàòöå ðàññìîòðþ ýòó îïåðàöèþ.

Ïðîñòûå ÷èñëà

Ïðîñòûì íàçûâàåòñÿ öåëîå ÷èñëî, áîëüøåå åäèíèöû, åäèíñòâåííûìè íîæèòåëÿìè êîòîðîãî ÿâëÿåòñÿ 1 è îíî ñàìî: îíî íå äåëèòñÿ íè íà îäíî äðóãîå ÷èñëî. Äâà - ýòî ïðîñòîå ÷èñëî. Ïðîñòûìè ÿâëÿþòñÿ è 73, 2521, 2365347734339 è 2^{756839}-1. Ñóùåñòâóåò áåñêîíå÷íî ìíîãî ïðîñòûõ ÷èñåë. Êðèòåðèé, îñíîâíîé êðèòåðèé ñ îòðûòûìè êëþ÷àìè, ÷àñòî èñïîëüçóåò áîëüøèå ïðîñòûå ÷èñëà (512 áèò è äàæå áîëüøå).

Åâàíãåëîñ Êðàíàêèñ (Evangelos Kranakis) íàïèñàë îöåíêó êîëè÷åñòâà ïðîñòûõ ÷èñåë, ïðîñòûì ÷èñëàì è èõ ïðèìåíåíèþ â êðèïòîãðàôèè [896]. Ïàóëà Ðèáåíáîéì (Paula Ribenboim) íàïèñàëà âåñü îòëè÷íûõ ðàáîò ïî ïðîñòûì ÷èñëàì âîîáùå [1307, 1308].

Íàèáîëüøèé îáùèé äåëèòåëü

Äâà ÷èñëà íàçûâàþòñÿ **âçàèìíî ïðîñòûìè**, åñëè ó íèõ íåò îáùèõ ìíîæèòåëåé êðîìå 1. Èíûìè ñëîâàìè, åñëè **íàèáîëüøèé îáùèé äåëèòåëü** *a* è *n* ðàâåí 1. Ýòî çàïèñûâàþòñÿ êàê:

НОД(*a*,*n*)=1

Âçàèìíî ïðîñòû ÷èñëà 15 è 28. 15 è 27 íå ÿâëÿþòñÿ âçàèìíî ïðîñòûìè, à 13 è 500 - ÿâëÿþòñÿ. Ïðîñòîå ÷èñëî âçàèìíî ïðîñòî ñî âñåìè äóãèìè ÷èñëàìè, êðîìå ÷èñåë, êðàòíûõ äâóì ïðîñòîìó ÷èñëó.

Îäíî èç ñïîñîáîâ âû÷èñëèòü íàèáîëüøèé îáùèé äåëèòåëü äâóõ ÷èñåë ÿâëÿåòñÿ **àëãîðèòì Ýâêëèäà**. Ýâêëèä ïîëüçîâàë ýòîò àëãîðèòì â ñâîåé êíèãå, *Ýëåìåíòû*, íàïèñàííîé â 300 ãîäó äî íàøåé ýðû. Îí íå èçîáðåë åãî. Èñòîðèêè ñ÷èòàþò, ÷òî ýòîò àëãîðèòì ëåò íà 200 ñòàðøå. Ýòî ñàìûé äðåâíèé íåòðèâèàëüíûé àëãîðèòì, êîòîðûé äîøåë äî íàøèõ äíåé, è îí âñå åùå õîðîø. Êíóò îïèñàë àëãîðèòì è åãî ñîâðåìåííûå ìîäèôèêàöèè â [863]. Íà ÿçûêå C:

```
/* âîçâðàùàåò ÍÎÄ (gcd) x è y */
int gcd (int x, int y) {
    int g;
    if (x < 0)
            x = -x;
    if (y < 0)
            y = -y;
    if (x + y == 0 )
            ERROR ;
```

```
        g = y;
        while (x > 0) {
                g = x;
                x = y % x;
                y = g;
        }
        return g;
}
```

Ýòîò àëãîðèòì ìîæíî îáîáùèòü äëÿ ïîëó÷åíèÿ Í ÎÄ ìàññèâà *m* ÷èñåë:

```
/* âîçâðàùàåò ÍÎÄ (gcd) xl, x2...xm */
int multiple_gcd (int m, int *x) {
        slze_t i;
        int g;
        if (m < 1)
                return 0;
        g = x [0];
        for (i=l; i<m; ++i) {
                g = gcd(g, x[i]);
/* îïòèìèçàöèÿ, òàê êàê äëÿ ñëó÷àéíûõ x[i], g==l â 60% ñëó÷àåâ: */
                if (g == 1)
                return 1;
        }
        return g;
}
```

Îáðàòíûå çíà÷åíèÿ ïî ìîäóëþ

Ïîìíèòå, ÷òî òàêîå îáðàòíûå çíà÷åíèÿ? Îáðàòíûå çíà÷åíèÿ äëÿ 4 - 1/4, ïîòîìó ÷òî 4*1/4 =1. Â ìèðå âû÷èòîâ ïðîáëåìà óñëîæíÿåòñÿ:

$4*x = 1 \pmod 7$

Ýòî óðàâíåíèå ýêâèâàëåíòíî îáðàòíîé x è k, òàêèõ ÷òî

$4x = 7k + 1$

ãäå *x* è *k* - öåëûå ÷èñëà. Îáùàÿ çàäà÷à ñîñòîèò â íàõîæäåíèè x, òàêîãî ÷òî

$1 = (a*x) \bmod n$

Ýòî òàêæå ìîæíî çàïèñàòü êàê

$a^{-1} \equiv x \pmod n$

Ïðîáëåìó îáðàòíûõ çíà÷åíèé ïî ìîäóëþ ðåøèòü íåëåãêî. Èíîãäà ó íåå åñòü ðåøåíèå, èíîãäà íåò. Íàïðèìåð, îáðàòíîå çíà÷åíèå 5 ïî ìîäóëþ 14 ðàâíî 3. Ñ äðóãîé ñòîðîíû ó ÷èñëà 2 íåò îáðàòíîãî çíà÷åíèÿ ïî ìîäóëþ 14.

Â îáùåì ñëó÷àå ó óðàâíåíèÿ $a^{-1} \equiv x \pmod n$ ñóùåñòâóåò åäèíñòâåííîå ðåøåíèå, åñëè *a* è *n* âçàèìíî ïðîñòû. Åñëè *a* è *n* íå ÿâëÿþòñÿ âçàèìíî ïðîñòûìè, òî $a^{-1} \equiv x \pmod n$ íå èìåò ðåøåíèé. Åñëè n ÿâëÿåòñÿ ïðîñòûì ÷èñëîì, òî ëþáîå ÷èñëî îò 1 äî *n* -1 âçàèìíî ïðîñòî ñ *n* è èìåò â òî÷íîñòè îäíî îáðàòíîå çíà÷åíèå ïî ìîäóëþ *n*.

Òàê, õîðîøî. À òåïåðü êàê âû ñîáèðàåòåñü èñêàòü îáðàòíîå çíà÷åíèå *a* ïî ìîäóëþ *n*? Ñóùåñòâóåò äâà ïóòè. Îáðàòíîå çíà÷åíèå a ïî ìîäóëþ *n* ìîæíî âû÷èñëèòü ñ ïîìîùüþ àëãîðèòìà Ýâêëèäà. Èíîãäà ýòî íàçûâàåòñÿ ðàñøèðåííûì àëãîðèòìîì Ýâêëèäà.

Âîò ýòîò àëãîðèòì íà ÿçûêå C++:

```
#define isEven(x) ((x & 0x01) == 0)
#define isOdd(x)  (x& 0x01)
#define swap(x,y) (x^= y, y^= x, x^= y)
void ExtBinEuclid(int *u, int *v, int *u1, int *u2, int *u3) {
        // ïðåäóïðåæäåíèå: u è v áóäóò ïåðåñòàâëåíû, åñëè u<v
int k, tl, t2, t3;
```

```
if (*u < *v) swap(*u<,*v);
for (k = 0; isEven(*u) && isEven(*v); ++k) {
*u>>=1; *v >>1;
}
*u1 = 1; *u2 = 0; *u3 = *u; t1 = *v; t2 = *u - 1; t3 = *v;
do {
do {
if (isEven(*u3)) {
if (isOdd(*ul) || isOdd(*u2)) {
*u1 += *v; *u2 += *u;
                            }
*ul >>* 1; *u2 >>= 1; *u3 >>= 1;
                    }
if (isEven(t3) || *u3 < t3) {
swap(*ul,tl); smap(*u2,t2); smap(*u3,t3);
                    }
} while (isEven(*u3));
while (*ul < tl || *u2 < t2) {
*ul += *v; *u2 += *u;
            }
            ul -= tl; *u2 -= t2; *u3 -= t3;
} while (t3 > 0);
while (*ul >= *v && *u2 >= *u) {
*ul>l -= *v; *u2 -= *u;
     }
*u <<= k; *v <<= k; *u3 << k;
}
main(int argc, char **argv) {
int a, b, gcd;
if (argc < 3) {
cerr << "êàê èñïîëüçîâàòü: xeuclid u v" << end1;
return -1;
     }
     int u = atoi(argv[1]);
int v = atoi(argv[2]);
if (u <= 0 || v <= 0 ) {
     cerr << "Àðãóìåíò äîëæåí áûòü ïîëîæèòåëåí!" << end1;
return -2;
     }
// ïðåäóïðåæäåíèå: u è v áóäóò ïåðåñòàâëåíû åñëè u < v
ExtBinEuclid(&u, &v, &a, &b, &gcd);
cout << a <<" * " << u << " + (-"
<< b << ") * " << v << " = " << gcd << end1;
if (gcd == 1)
cout << "Îáðàòíîå çíà÷åíèå " << v << " mod " << u << " is: "
<< u - b << end1;
return 0;
}
```

ß íå ñîáèðàþñü äîêàçûâàòü, ÷òî ýòî ðàáîòàåò, èëè ïðèâîäèòü òåîðåòè÷åñêîå îáîñíîâàíèå. Ïîäðîáíîñòè ìîæíî íàéòè â [863] èëè â ëþáîé èç ïðèâåäåííûõ ðàíåå ðàáîò ïî òåîðèè ÷èñåë.

Àëãîðèòì èòåðàòèâåí è äëÿ áîëüøèõ ÷èñåë ìîæåò ðàáîòàòü ìåäëåííî. Êíóò ïîêàçàë, ÷òî ñðåäíåå ÷èñëî âû-

ïîëíÿåì ûõ àëãîðèòìîì äåëåíèé ðàâíî:

$0.843*\log_2(n) + 1.47$

Ðåøåíèå äëÿ êîýôôèöèåíòîâ

Àëãîðèòì Ýâêëèäà ìîæíî èñïîëüçîâàòü è äëÿ ðåøåíèÿ ñëåäóþùèõ ïðîáëåì: äàí ìàññèâ èç m ïåðåìåííûõ $x_1, x_2, ..., x_m$, íàéòè ìàññèâ m êîýôôèöèåíòîâ, $u_1, u_2, ..., u_m$, òàêèõ ÷òî

$u_1 * x_1+...+ u_m * x_m, = 1$

Ìàëàÿ òåîðåìà Ôåðìà

Åñëè m - ïðîñòîå ÷èñëî, è a íå êðàòíî m, òî **ìàëàÿ òåîðåìà Ôåðìà** óòâåðæäàåò

$a^{m-1} \equiv 1 \pmod m$

(Ïüåð äå Ôåðìà (Pierre de Fermat), ôðàíöóçñêèé ìàòåìàòèê, æèë ñ 1601 ïî 1665 ãîä. Ýòà òåîðåìà íå èìåò íè÷åãî îáùåãî ñ åãî çíàìåíèòîé òåîðåìîé.)

Ôóíêöèÿ Ýéëåðà

Ñóùåñòâóåò äóãîé ñïîñîá âû÷èñëèòü îáðàòíûå çíà÷åíèÿ ïî ìîäóëþ n, íî åãî íå âñåãäà âîçìîæíî èñïîëüçîâàòü. **Ïðèâåäåííûì ìíîæåñòâîì** mod n íàçûâàþòñÿ ïîäìíîæåñòâî ïîëíîãî ìíîæåñòâà îñòàòêîâ, ÷üå-íû êîòîðîãî âçàèìíî ïðîñòû ñ n. Íàïðèìåð, ïðèâåäåííûå îñòàòêîâ mod 12 - ýòî {1, 5, 7, 11}. Åñëè n - ïðîñòîå ÷èñëî, òî ïðèâåäåííûé ìíîæåñòâî îñòàòêîâ mod n - ýòî ìíîæåñòâî âñåõ ÷èñåë îò 1 äî n-1. Äëÿ ëþáîãî n, íå ðàâíîãî 1,÷èñëî 0 íèêîãäà íå âõîäèò â ïðèâåäåííûé ìíîæåñòâî îñòàòêîâ.

Ôóíêöèÿ Ýéëåðà, êîòîðóþ àâçæå íàçûâàþò ôóíêöèåé ôè Ýéëåðà è çàïèñûâàþò êàê $\phi(n)$, - ýòî êîëè÷åñòâî ýëåìåíòîâ â ïðèâåäåííîì ìíîæåñòâå îñòàòêîâ ïî ìîäóëþ n. Èíûìè ñëîâàìè, $\phi(n)$ - ýòî êîëè÷åñòâî ïîëîæèòåëüíûõ öåëûõ ÷èñåë, ìåíüøèõ n è âçàèìíî ïðîñòûõ ñ n (äëÿ ëþáîãî n, áîëüøåãî 1). (Ëåîíàðä Ýéëåð (Leonhard Euler), øâåéöàðñêèé ìàòåìàòèê, æèë ñ 1707 ïî 1783 ãîä.)

Åñëè n - ïðîñòîå ÷èñëî, òî $\phi(n) = n$-1. Åñëè $n = pq$, ãäå p è q -ïðîñòûå ÷èñëà, òî $\phi(n)= (p - 1)(q - 1)$. Ýòè ÷èñëà ïîÿâëÿþñÿ â íåêîòîðûõ àëãîðèòìàõ ñ îêðûòûì êëþ÷àìè, è âîò ïî÷åìó. Â ñîîòâåòñòâèè ñ îáùåèçâåñòíîé Ýéëåðà ìàëîé òåîðåìîé Ôåðìà, åñëè Í ÎÄ$(a,n) = 1$, òî

$a^{\phi(n)} \bmod n = 1$

Òåïåðü ëåãêî âû÷èñëèòü $a^{-1} \bmod n$:

$x = a^{\phi(n)-1} \bmod n$

Íàïðèìåð, êàêîå ÷èñëî ÿâëÿåòñÿ îáðàòíûì äëÿ 5 ïî ìîäóëþ 7? Òàê êàê 7 - ïðîñòîå ÷èñëî, $\phi(7) = 7 - 1 = 6$. Èòàê, ÷èñëî, îáðàòíîå ê 5 ïî ìîäóëþ 7, ðàâíî

$5^{6-1} \bmod 7 = 5^5 \bmod 7 = 3$

Ýòè ìåòîäû âû÷èñëåíèÿ îáðàòíûõ çíà÷åíèé ìîæíî ðàñøèðèòü äëÿ áîëåå îáùèé ïðîáëåìû íàõîæäåíèÿ x (åñëè Í ÎÄ$(a,n) = 1$):

$(a*x) \bmod n = b$

Èñïîëüçóÿ îáîáùåíèå Ýéëåðà, ðåøåì

$x = (b* a^{\phi(n)-1}) \bmod n$

Èñïîëüçóÿ àëãîðèòì Ýâêëèäà, íàõîäèì

$x = (b* (a^{-1} \bmod n)) \bmod n$

Â îáùåì ñëó÷àå äëÿ âû÷èñëåíèÿ îáðàòíûõ çíà÷åíèé àëãîðèòì Ýâêëèäà áûñòðåå, ÷åì îáîáùåíèå Ýéëåðà, îñîáåííî äëÿ ÷èñåë äëèííîé ïîðÿäêà 500 áèò. Åñëè Í ÎÄ$(a,n) \neq 1$, íå âñå ïîðîæäåíî. Â ýòîì îáùåì ñëó÷àå $(a*x) \bmod n=b$, ìîæåò èìåòü èëè íåñêîëüêî ðåøåíèé, èëè íè îäíîãî.

Êèòàéñêàÿ òåîðåìà îá îñòàòêàõ

Åñëè èçâåñòíî ðàçëîæåíèå ÷èñëà n íà ïðîñòûå ñîìíîæèòåëè, òî äëÿ ðåøåíèÿ ïîëíîé ñèñòåìû óðàâíåíèé ìîæíî âîñïîëüçîâàòüñÿ Êèòàéñêîé òåîðåìîé îá îñòàòêàõ. Îñíîâíîé âàðèàíò ýòîé òåîðåìû áûë îòêðûò â ïåðâîì âåêå êèòàéñêèì ìàòåìàòèêîì Ñóí Öçå.

Â îáùåì ñëó÷àå, åñëè ðàçëîæåíèå ÷èñëà n íà ïðîñòûå ñîìíîæèòåëè ïðåäñòàâëÿåò ñîáîé $p_1*p_2*...*p_t$, òî ñèñòåìà óðàâíåíèé

($x \bmod p_i$) = a_i, ãäå i = 1, 2, . . . , t

èìååò åäèíñòâåííîå ðåøåíèå, x, ìåíüøåå n. (Îáðàòèòå âíèìàíèå, ÷òî íåêîòîðûå ïðîñòûå ÷èñëà ìîãóò ïîÿâëÿòüñÿ íåñêîëüêî ðàç. Íàïðèìåð, p_1 ìîæåò áûòü ðàâíî p_2.) Äðóãèì ñëîâàìè, ÷èñëî (ìåíüøåå, ÷åì ïðîèçâåäåíèå íåñêîëüêèõ ïðîñòûõ ÷èñåë) îäíîçíà÷íî îïðåäåëÿåòñÿ ñâîéñòâàìè îò äâóõ ïðîñòûå ÷èñëà.

Íàïðèìåð, âîçüìåì ïðîñòûå ÷èñëà 3 è 5, è 14 â êà÷åñòâå çàäàííîãî ÷èñëà. 14 mod 3 = 2, è 14 mod 5 = 4. Ñóùåñòâóåò åäèíñòâåííîå ÷èñëî, ìåíüøåå 3*5 = 15, ñ òàêèìè îñòàòêàìè: 14. Äâà îñòàòêà îäíîçíà÷íî îïðåäåëþò ÷èñëî.

Ïîýòîìó äëÿ ïðîèçâîëüíîãî $a < p$ è $b < q$ (ãäå p è q - ïðîñòûå ÷èñëà), ñóùåñòâóåò åäèíñòâåííîå ÷èñëî x, ìåíüøåå pq, òàêîå ÷òî

$x \equiv a \pmod p$, è $x \equiv b \pmod q$

Äëÿ ïîëó÷åíèÿ x ñíà÷àëà âîñïîëüçóåìñÿ àëãîðèòìîì Ýâêëèäà, ÷òîáû íàéòè u, òàêîå ÷òî

$u*q \equiv 1 \pmod p$

Çàòåì âû÷èñëèì:

$x = (((a - b) *u) \bmod p) * q + b$

Âîò êàê âûãëÿäèò Êèòàéñêàÿ òåîðåìà íà ïñåâäîêîäå C:

```
/* r - ýòî êîëè÷åñòâî ýëåìåíòîâ â ìàññèâàõ m and u;
m - ýòî ìàññèâ (ïîïàðíî âçàèìíî ïðîñòûõ) ìîäóëåé
u - ýòî ìàññèâ êîýôôèöèåíòîâ
âîçâðàùàåò çíà÷åíèå n, òàêîå ÷òî n == u[k]%m[k] (k=0..r-1) è
n < [m[0]*m[l]*...*m[r-1]
*/
/* Ïîëó÷åíèå ôóíêöèè Ýéëåðà (totient) îñòàåòñÿ óïðàæíåíèåì äëÿ ÷èòàòåëÿ. */
int Chinese_remainder (size_t r, int *m, int *u) {
size_t i;
int modulus;
int n;
modulus=1;
for (i=0; i<r; ++i)
modulus*=m[i];
n=0;
for (i=0; i<r; ++i) {
n+=u[i] * modexp(modulus/m[i]*totient(m[i]),m[i]);
n %= modulus;
     }
return n;
}
```

Îáðàùåíèå Êèòàéñêîé òåîðåìû îá îñòàòêàõ ìîæåò áûòü èñïîëüçîâàíî äëÿ ðåøåíèÿ ñëåäóþùåé ïðîáëåìû: åñëè p è q - ïðîñòûå ÷èñëà, è p ìåíüøå q, òî ñóùåñòâóåò åäèíñòâåííîå x, ìåíüøåå, ÷åì pq, òàêîå ÷òî

$a \equiv x \pmod p$, è b ≡ x (mod q)

Åñëè $a \geq b \bmod p$, òî

$x = (((a - (b \bmod p)) * u) \bmod p) * q + b$

Åñëè $a < b \bmod p$, òî

$x = (((a + p - (b \bmod p))*u) \bmod p)*q + b$

Êâàäðàòè÷íûå âû÷åòû

Åñëè p - ïðîñòîå ÷èñëî, è a áîëüøå 0, íî ìåíüøå p, òî a ïðåäñòàâëÿåò ñîáîé êâàäðàòè÷íûé âû÷åò ïî ìîäóëþ p, åñëè

$x^2 \equiv a \pmod p$, äëÿ íåêîòîðûõ x

Íå âñå çíà÷åíèÿ *a* ñîîòâåòñòâóþò ýòîìó òåîðåìå. ×òîáû *a* áûëî êâàäðàòè÷íûì âû÷åòîì ïî *n*, îíî äîëæíî áûòü êâàäðàòè÷íûì âû÷åòîì ïî ìîäóëþ âñåõ ïðîñòûõ ñîìíîæèòåëåé *n*. Íàïðèìåð, åñëè *p* = 7, êâàäðàòè÷íûìè âû÷åòàìè ÿâëÿþòñÿ ÷èñëà 1, 2, è 4:

$1^2 = 1 \equiv 1 \pmod 7$

$2^2 = 4 \equiv 4 \pmod 7$

$3^2 = 9 \equiv 2 \pmod 7$

$4^2 = 16 \equiv 2 \pmod 7$

$5^2 = 25 \equiv 4 \pmod 7$

$6^2 = 36 \equiv 1 \pmod 7$

Çàìåòüòå, ÷òî êàæäûé êâàäðàòè÷íûé âû÷åò äâàæäû ïîÿâëÿåòñÿ â ýòîì ñïèñêå. Çíà÷åíèé *x*, óäîâëåòâîðÿþùèõ ëþáîìó èç ñëåäóþùèõ óðàâíåíèé, íå ñóùåñòâóåò:

$x^2 \equiv 3 \pmod 7$

$x^2 \equiv 5 \pmod 7$

$x^2 \equiv 6 \pmod 7$

Ýòè ÷èñëà - 3, 5 è 6 - íå ÿâëÿþòñÿ êâàäðàòè÷íûìè âû÷åòàìè ïî ìîäóëþ 7.

Õîòÿ ÿ ýòîãî è íå äåëàë, íåñëîæíî äîêàçàòü, ÷òî êîãäà *p* íå÷åòíî, ñóùåñòâóåò â òî÷íîñòè (*p* - 1)/2 êâàäðàòè÷íûõ âû÷åòîâ ïî ìîäóëþ *p*, è ñòîëüêî æå ÷èñåë, íå ÿâëÿþùèõñÿ êâàäðàòè÷íûìè âû÷åòàìè ïî ìîäóëþ *p*. Êðîìå òîãî, åñëè *a* - ýòî êâàäðàòè÷íûé âû÷åò ïî ìîäóëþ *p*, òî ó *a* â òî÷íîñòè äâà êâàäðàòíûõ êîðíÿ, îäèí ìåæäó 0 è (*p*-1)/2, à âòîðîé - ìåæäó (*p* - 1)/2 è (*p* - 1). Îäèí èç ýòèõ êâàäðàòíûõ êîðíåé îäíîâðåìåííî ÿâëÿåòñÿ êâàäðàòè÷íûì ÷òàòåëåì ïî ìîäóëþ *p*, îí íàçûâàåòñÿ **ãëàâíûì êâàäðàòíûì êîðíåì**.

Åñëè *n* ÿâëÿåòñÿ ïðîèçâåäåíèåì äâóõ ïðîñòûõ ÷èñåë, *p* è *q*, òî ñóùåñòâóåò ðîâíî (*p* - l)(*q* - 1)/4 êâàäðàòè÷íûõ âû÷åòîâ ïî ìîäóëþ *n*. Êâàäðàòè÷íûé âû÷åò ïî ìîäóëþ *n* ÿâëÿåòñÿ ñîâðåííûì êâàäðàòîì ïî ìîäóëþ *n*, ïîòîìó ÷òî äëÿ òîãî, ÷òîáû áûòü êâàäðàòîì ïî ìîäóëþ *n*, âû÷åò äîëæåí áûòü êâàäðàòîì ïî ìîäóëþ *p* è êâàäðàòîì ïî ìîäóëþ *q*. Íàïðèìåð, ñóùåñòâóåò îäèííàäöàòü êâàäðàòè÷íûõ îñòàòêîâ mod 35: 1, 4, 9, 11, 15, 16, 21, 25, 29 è 30. Ó êâàäðàòè÷íîãî âû÷åòà ðîâíî ÷åòûðå êâàäðàòíûõ êîðíÿ.

Ñèìâîë Ëåæàíäðà

Ñèìâîë Ëåæàíäðà, L(*a*,*p*), îïðåäåëåí, åñëè *a* - ýòî ëþáîå öåëîå ÷èñëî, à *p* - ïðîñòîå ÷èñëî, áîëüøåå, ÷åì 2. Î í ðàâåí 0, 1 èëè -1.

L(*a*,*p*) = 0, åñëè a äåëèòñÿ íà p.

L(*a*,*p*) = 1, åñëè a - êâàäðàòè÷íûé âû÷åò ïî ìîäóëþ *p*.

L(*a*,*p*) = -1, åñëè a íå ÿâëÿåòñÿ êâàäðàòè÷íûì âû÷åòîì ïî ìîäóëþ *p*.

L(*a*,*p*) ìîæíî ðàññ÷èòàòü ñëåäóþùèì îáðàçîì:

L(*a*,*p*) = $a^{(p-1)/2} \bmod p$

Èëè ìîæíî âîñïîëüçîâàòüñÿ ñëåäóþùèì àëãîðèòìîì:

1. Åñëè a = 1, òî L(*a*,*p*) = 1
2. Åñëè a ÷åòíî, òî L(*a*,*p*) = L(*a*/2,*p*) * $(-1)^{(p^2-1)/8}$
3. Åñëè a íå÷åòíî (è ≠ 1), òî L(*a*,*p*)= L(*p* mod *a*, *p*)*$(-1)^{(a-1)(p-1)/4}$

Îáðàòèòå âíèìàíèå, ÷òî ýòîò ìåòîä òàêæå ÿâëÿåòñÿ ýôôåêòèâíûì ñïîñîáîì îïðåäåëèòü, ÿâëÿåòñÿ ëè *a* êâàäðàòè÷íûì âû÷åòîì ïî ìîäóëþ *p* (äëÿ ïðîñòîãî ÷èñëà *p*).

Ñèìâîë ßêîáè

Ñèìâîë ßêîáè, J(*a*,*n*), ïðåäñòàâëÿåò ñîáîé îáîáùåíèå ñèìâîëà Ëåæàíäðà íà ñîñòàâíûå ìîäóëè, îí îïðåäåëÿåòñÿ äëÿ ëþáîãî öåëîãî *a* è ëþáîãî íå÷åòíîãî öåëîãî *n*. Ôóíêöèÿ óäîáíà ïðè ïðîâåðêå íà ïðîñòîòó. Ñèìâîë ßêîáè ÿâëÿåòñÿ ôóíêöèåé íà ìíîæåñòâå ïîëó÷íûõ âû÷åòîâ äâóõ ÷èñåë *n* è ìîæåò áûòü âû÷èñëåí ïî ðàçëè÷íûì ôîðìóëàì [1412]. Âîò îäèí èç ñïîñîáîâ:

Î ïðåäåëåíèå 1: J(*a*,*n*) îïðåäåëåí, òîëüêî åñëè *n* íå÷åòíî.

Î ïðåäåëåíèå 2: J(0,*n*) = 0.

Î ïðåäâåëåíèå 3: Åñëè n - ïðîñòîå ÷èñëî, òî ñèìâîë ßêîáè J(a,n) = 0, åñëè a äåëèòñÿ íà n.

Î ïðåäâåëåíèå 4: Åñëè n - ïðîñòîå ÷èñëî, òî ñèìâîë ßêîáè J(a,n) = 1, åñëè a - êâàäðàòè÷íûé âû÷åò ïî ìîäóëþ n.

Î ïðåäâåëåíèå 5: Åñëè n - ïðîñòîå ÷èñëî, òî ñèìâîë ßêîáè J(a,n) = -1, åñëè a íå ÿâëÿåòñÿ êâàäðàòè÷íûì âû÷åòîì ïî ìîäóëþ n.

Î ïðåäâåëåíèå 6: Åñëè n - ñîñòàâíîå ÷èñëî, òî ñèìâîë ßêîáè J(a,n) = J(a,p_1)* ... * J(a,p_m), ãäå p_1, ... , p_m - ýòî ðàçëîæåíèå n íà ïðîñòûå ñîìíîæèòåëè.

Ñëåäóþùèé àëãîðèòì ðåêóðñèâíî ðàñ÷èòûâàåò ñèìâîë ßêîáè:

Ïðàâèëî 1: J(1,n) = 1

Ïðàâèëî 2: J(a*b,n) = J(a,n)* J(b,n)

Ïðàâèëî 3: J(2,n) =, åñëè (n^2-1) /8 íå÷åòíî, è -1 â ïðîòèâíîì ñëó÷àå

Ïðàâèëî 4: J(a,n)= J((a mod n),n)

Ïðàâèëî 5: J(a, b_1*b_2) = J(a, b_1)* J(a, b_2)

Ïðàâèëî 6: Åñëè íàèáîëüøèé îáùèé äåëèòåëü a è b = 1, à òàêæå a è b íå÷åòíû:

Ïðàâèëî 6a: J(a,b)= J(b, a), åñëè (a - l)(b - 1)/4 ÷åòíî

Ïðàâèëî 6b: J(a,b)= -J(b, a), åñëè (a - l)(b - 1)/4 íå÷åòíî

Âîò àëãîðèì íà ÿçûêå C:

```
/* Ýòîò àëãîðèì ðåêóðñèâíî âû÷èñëÿåò ñèìâîë ßêîáè */
int jacobi(int a, int b) {
int g;
     assert(odd(b));
     if (a >= b) a %= b; /* ïî ïðàâèëó 4 */
     if (a == 0) return 0; /* ïî îïðåäåëåíèþ 1 */
     if (a == 1) return 1; /* ïî ïðàâèëó 1 */
     if (a < 0)
             if ((b-l)/2 % 2 == 0)
                     return jacobi(-a,b);
             else
                     return -jacobi(-a,b);
     if (a % 2 == 0) /* a ÷åòíî */
             if (((b*b -1)/8) % 2 == 0)
                     return +jacobi(a/2,b);
             else
                     return -jacobi(a/2,b); /* ïî ïðàâèëàì 3 è 2 */
     g = gcd(a,b);
     assert(odd(a)); /* ýòî îáåñïå÷èâàåòñÿ ïðîâåðêîé (a % 2 == 0) */
     if (g == a) /* b äåëèòñÿ íà a */
             return 0; /* ïî ïðàâèëó 5 */
     else if (g != 1)
             return jacobi(g,b)*jacobi(a/g,b); /* ïî ïðàâèëó 2 */
     else if (((a-l)*(b-l)/4) % 2 == 0)
             return +jacobi(b,a); /* ïî ïðàâèëó 6a */
     else
             return -jacobi(b,a); /* ïî ïðàâèëó 6b */
}
```

Åñëè çàðàíåå èçâåñòíî, ÷òî n - ïðîñòîå ÷èñëî, âìåñòî èñïîëüçîâàíèÿ ïðåäûäóùåãî àëãîðèòìà ïðîñòî âû÷èñëèòü a((n-1)/2) mod n, â ýòîì ñëó÷åå J(a,n) ýêâèâàëåíòåí ñèìâîëó Ëåæàíäðà.

Ñèìâîë ßêîáè íåëüçÿ èñïîëüçîâàòü äëÿ îïðåäåëåíèÿ òîãî, ÿâëÿåòñÿ ëè a êâàäðàòè÷íûì âû÷åòîì ïî ìîäóëþ

n (åñëè, êîíå÷íî, n íå ÿâëÿåòñÿ ïðîñòûì ÷èñëîì). Îáðàòèìå âíèìàíèå, ÷òî åñëè J(a,n) = 1 è n - ñîñòàâíîå ÷èñëî, òî óòâåðæäåíèå, ÷òî a ÿâëÿåòñÿ êâàäðàòè÷íûì âû÷åòîì ïî ìîäóëþ n, íå îáÿçàòåëüíî áóäåò èñòèíîé. Íàïðèìåð:

J(7,143) = J(7,11)* J(7,13) = (-1)(-1) = 1

Îäíàêî íå ñóùåñòâóåò òàêèõ öåëûõ ÷èñåë x, ÷òî $x^2 \equiv 7 \pmod{143}$.

Öåëûå ÷èñëà Áëþ ìà

Åñëè p è q - äâà ïðîñòûõ ÷èñëà, êîíãðóýíòíûõ 3 ïî ìîäóëþ 4, òî $n = pq$ èíîãäà íàçûâàþò **öåëûì ÷èñëîì Áëþ ìà**. Åñëè n - ýòî öåëîå ÷èñëî Áëþ ìà, ó êâàäðàòè÷íîãî âû÷åòà ðîâíî ÷åòûðå êâàäðàòíûõ êîðíÿ, îäèí èç êîòîðûõ òàêæå ÿâëÿåòñÿ êâàäðàòè÷íûì - ýòî ãëàâíûé êâàäðàòíûé êîðåíü. Íàïðèìåð, ãëàâíûé êâàäðàòíûé êîðåíü 139 mod 437 - ýòî 24. Îñòàëüíûå òðè êîðíÿ - ýòî 185, 252 è 413.

Ãåíåðàòîðû

Åñëè p - ïðîñòîå ÷èñëî, è g ìåíüøå, ÷åì p, òî g íàçûâàþò **ãåíåðàòîðîì** ïî ìîäóëþ p, åñëè äëÿ êàæäîãî ÷èñëà b îò 1 äî p - 1 ñóùåñòâóåò íåêîòîðîå ÷èñëî a, ÷òî $g^a \equiv b \pmod{p}$.

Èíûìè ñëîâàìè, g ÿâëÿåòñÿ **ïðèìèòèâîì** ïî îòíîøåíèþ ê p. Íàïðèìåð, åñëè p = 11, òî 2 - ýòî ãåíåðàòîð ïî ìîäóëþ 11:

$2^{10} = 1024 \equiv 1 \pmod{11}$

$2^1 = 2 \equiv 2 \pmod{11}$

$2^8 = 256 \equiv 3 \pmod{11}$

$2^2 = 4 \equiv 4 \pmod{11}$

$2^4 = 16 \equiv 5 \pmod{11}$

$2^9 = 512 \equiv 6 \pmod{11}$

$2^7 = 128 \equiv 7 \pmod{11}$

$2^3 = 8 \equiv 8 \pmod{11}$

$2^6 = 64 \equiv 9 \pmod{11}$

$2^5 = 32 \equiv 10 \pmod{11}$

Êàæäîå ÷èñëî îò 1 äî 10 ìîæåò áûòü ïðåäñòàâëåíî êàê $2^a \pmod{p}$. Äëÿ p = 11 ãåíåðàòîðàìè ÿâëÿþòñÿ 2, 6, 7 è 8. Äðóãèå ÷èñëà íå ÿâëÿþòñÿ ãåíåðàòîðàìè. Íàïðèìåð, ãåíåðàòîðîì íå ÿâëÿåòñÿ ÷èñëî 3, ïîñêîëüêó ÷òî íå ñóùåñòâóåò ðåøåíèÿ äëÿ

$3^a \equiv 2 \pmod{11}$

Â îñíîâå ñëó÷àå ïðîâåðêè, ÿâëÿåòñÿ ëè äàííîå ÷èñëî ãåíåðàòîðîì, íåëåãêî. Îäíàêî çàäà÷à óïðîùàåòñÿ, åñëè èçâåñòíî ðàçëîæåíèå íà ìíîæèòåëè äëÿ p - 1. Ïóñòü q_1, q_2, ... , q_n - ýòî ðàçëè÷íûå ïðîñòûå ìíîæèòåëè p - 1. ×òîáû ïðîâåðèòü, ÿâëÿåòñÿ ëè ÷èñëî g ãåíåðàòîðîì ïî ìîäóëþ p, âû÷èñëèòå

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

äëÿ âñåõ çíà÷åíèé $q = q_1, q_2, \dots , q_n$.

Åñëè ýòî ÷èñëî ðàâíî 1 äëÿ íåêîòîðîãî q, òî g íå ÿâëÿåòñÿ ãåíåðàòîðîì. Åñëè äëÿ âñåõ çíà÷åíèé q ðàññ÷èòàííûå çíà÷åíèÿ íå ðàâíû 1, òî g - ýòî ãåíåðàòîð.

Íàïðèìåð, ïóñòü p = 11. Ïðîñòûå ìíîæèòåëè p - 1 = 10 - ýòî 2 è 5. Äëÿ ïðîâåðêè òîãî, ÿâëÿåòñÿ ëè ÷èñëî 2 ãåíåðàòîðîì, âû÷èñëèì:

$2^{(11-1)/5} \pmod{11} = 4$

$2^{(11-1)/2} \pmod{11} = 10$

Íè îäèí èç òàêèõ íå ðàâåí 1, ïîýòîìó 2 - ýòî ãåíåðàòîð.

Ïðîâåðèì, ÿâëÿåòñÿ ãåíåðàòîðîì ëè ÷èñëî 3:

$3^{(11-1)/5} \pmod{11} = 9$

$3^{(11-1)/2} \pmod{11} = 1$

Ñëåäîâàòåëüíî, 3 - ýòî íå ãåíåðàòîð.

Ïðè íåîáõîäèìîñòè îáíàðóæèòü ãåíåðàòîð ïî ìîäóëþ p ïðîñòî ñëó÷àéíî âûáèðàéòå ÷èñëî îò 1 äî p - 1 è ïðîâåðÿéòå, íå ÿâëÿåòñÿ ëè îíî ãåíåðàòîðîì. Ãåíåðàòîðîâ äîñòàòî÷íî, ïîýòîìó îäèí èç íèõ âû, ñêîðåå âñåãî, íàéäåòå áûñòðî.

Âû÷èñëåíèå â ïîëå Ãàëóà

Íå òðåâîæüòåñü, âñå ýòî ìû óæå äåëàëè. Åñëè n - ïðîñòîå ÷èñëî èëè ñòåïåíü áîëüøîãî ïðîñòîãî ÷èñëà, òî ìû ïîëó÷àåì òî, ÷òî ìàòåìàòèêè íàçûâàþò **êîíå÷íûì ïîëåì**. Â ÷åñòü ýòîãî ìû èñïîëüçóåì p âìåñòî n. Â äåéñòâèòåëüíîñòè ýòîò òèï êîíå÷íîãî ïîëÿ íàñòîëüêî çàìå÷àòåëåí, ÷òî ìàòåìàòèêè äàëè åìó ñîáñòâåííîå èìÿ - **ïîëå Ãàëóà**, îáîçíà÷àåìîå êàê GF(p). (Â ÷åñòü Ýâàðèñòà Ãàëóà, ôðàíöóçñêîãî ìàòåìàòèêà, æèâøåãî â äåâÿòíàäöàòîì âåêå è óñïåâøåãî çíà÷èòåëüíî ïðîäâèíóòü òåîðèþ ÷èñåë, ïðåæäå ÷åì â 20 ëåò îí áûë óáèò íà äóýëè.)

Â ïîëå Ãàëóà îïðåäåëåíû ñëîæåíèå, âû÷èòàíèå, óìíîæåíèå è äåëåíèå íà íåíóëåâûå ýëåìåíòû. Ñóùåñòâóåò íåéòðàëüíûé ýëåìåíò äëÿ ñëîæåíèÿ - 0 - è äëÿ óìíîæåíèÿ - 1. Äëÿ êàæäîãî íåíóëåâîãî ÷èñëà ñóùåñòâóåò åäèíñòâåííîå îáðàòíîå ÷èñëî (ýòî íå áûëî áû òàê, åñëè áû p íå áûëî ïðîñòûì ÷èñëîì). Âûïîëíÿþòñÿ êîììóòàòèâíûé, àññîöèàòèâíûé è äèñòðèáóòèâíûé çàêîíû.

Àðèôìåòèêà ïîëÿ Ãàëóà øèðîêî èñïîëüçóåòñÿ â êðèïòîãðàôèè. Â íåì ðàáîòàåò âñÿ òåîðèÿ ÷èñåë, ïîëå ñîäåðæèò òîëüêî ÷èñëà êîíå÷íîãî ðàçìåðà, ïðè äåëåíèè îòñóòñòâóþò îøèáêè îêðóãëåíèÿ. Ìíîãèå êðèïòîñèñòåìû îñíîâàíû íà GF(p), ãäå p - ýòî áîëüøîå ïðîñòîå ÷èñëî.

×òîáû åùå áîëåå óñëîæíèòü âîïðîñ, êðèïòîãðàôû òàêæå èñïîëüçóþò àðèôìåòèêó ïî ìîäóëþ **íåïðèâîäèìûõ** ìíîãî÷ëåíîâ ñòåïåíè n, êîýôôèöèåíòàìè êîòîðûõ ÿâëÿþòñÿ öåëûå ÷èñëà ïî ìîäóëþ q, ãäå q - ýòî ïðîñòîå ÷èñëî. Ýòè ïîëÿ íàçûâàþòñÿ GF(qn). Èñïîëüçóåòñÿ àðèôìåòèêà ïî ìîäóëþ $p(x)$, ãäå $p(x)$ - ýòî íåïðèâîäèìûé ìíîãî÷ëåí ñòåïåíè n.

Ìàòåìàòè÷åñêàÿ òåîðèÿ, ñòîÿùàÿ çà ýòèì, âûõîäèò äàëåêî çà ðàìêè ýòîé êíèãè, õîòÿ ÿ è îïèøó ðÿä êðèïòîñèñòåì, èñïîëüçóþùèõ åå. Åñëè âû õîòèòå ïîóïðàæíÿòüñÿ ñ íåïðèâîäèìûìè ìíîãî÷ëåíàìè, òî GF(2^3) âêëþ÷àåò ñëåäóþùèå ýëåìåíòû: 0, 1, x, $x + 1$, x^2, $x^2 + 1$, $x^2 + x$, $x^2 + x + 1$. Óäîáíûé äëÿ ïàðàëëåëüíîé ðåàëèçàöèè àëãîðèòì âû÷èñëåíèÿ îáðàòíûõ çíà÷åíèé â GF(2^n) ïðèâåäåí â [421].

Ïðè îáñóæäåíèè ïîëèíîìîâ òåðìèí "ïðîñòîå ÷èñëî" çàìåíÿåòñÿ òåðìèíîì "íåïðèâîäèìûé ìíîãî÷ëåí". Ïîëèíîì íàçûâàåòñÿ íåïðèâîäèìûì, åñëè åãî íåëüçÿ ïðåäñòàâèòü â âèäå äâóõ äðóãèõ ïîëèíîìîâ (êîíå÷íî æå, êðîìå 1 è ñàìîãî ïîëèíîìà). Ïîëèíîì $x^2 + 1$ íåïðèâîäèì íàä öåëûìè ÷èñëàìè, à ïîëèíîì $x^3 + 2x^2 + x$ íå ÿâëÿåòñÿ íåïðèâîäèìûì, îí ìîæåò áûòü ïðåäñòàâëåí êàê $x(x + l)(x + 1)$.

Ïîëèíîì, êîòîðûé â äàííîì ïîëå ÿâëÿåòñÿ ãåíåðàòîðîì, íàçûâàåòñÿ ïðèìèòèâíûì èëè áàçîâûì, âñå åãî êîýôôèöèåíòû âçàèìíî ïðîñòû. Ìû ñíîâà âåðíåìñÿ ê ïðèìèòèâíûì ïîëèíîìàì, êîãäà áóäåì ãîâîðèòü î ñäâèãîâûõ ðåãèñòðàõ ñ ëèíåéíîé îáðàòíîé ñâÿçüþ (ñì. ðàçäåë 16.2).

Âû÷èñëåíèÿ â GF(2^n) ìîãóò áûòü áûñòðî ðåàëèçîâàíû àïïàðàòíî ñ ïîìîùüþ ñäâèãîâûõ ðåãèñòðîâ ñ ëèíåéíîé îáðàòíîé ñâÿçüþ. Ïî ýòîé ïðè÷èíå âû÷èñëåíèÿ íàä GF(2^n) ÷àñòî áûñòðåå, ÷åì âû÷èñëåíèÿ íàä GF(p). Òàê êàê âîçâåäåíèå â ñòåïåíü â GF(2^n) ãîðàçäî ýôôåêòèâíåå, òî ýôôåêòèâíåå è âû÷èñëåíèå äèñêðåòíûõ ëîãàðèôìîâ [180, 181, 368, 379]. Äîïîëíèòåëüíóþ èíôîðìàöèþ îá ýòîì ìîæíî íàéòè â [140].

Äëÿ ïîëÿ Ãàëóà GF(2^n) êðèïòîãðàôû ëþáÿò èñïîëüçîâàòü â êà÷åñòâå ìîäóëåé òðåõ÷ëåíû $p(x) = x^n + x + 1$, òàê êàê äëèííàÿ ñòðîêà íóëåé ìåæäó êîýôôèöèåíòàìè ïðè x^n è x ïîçâîëÿåò ïðîñòî ðåàëèçîâàòü áûñòðîå óìíîæåíèå ïî ìîäóëþ [183]. Ïîëèíîì äîëæåí áûòü ïðèìèòèâíûì, â ïðîòèâíîì ñëó÷àå ìàòåìàòèêà íå áóäåò ðàáîòàòü. $x^n + x + 1$ ïðèìèòèâåí äëÿ ñëåäóþùèõ çíà÷åíèé n, ìåíüøèõ ÷åì 1000 [1649, 1648]:

1, 3, 4, 6, 9, 15, 22, 28, 30, 46, 60, 63, 127, 153, 172, 303, 471, 532, 865, 900

Ñóùåñòâóþò àïïàðàòíûå ðåàëèçàöèè GF(2^{127}), ãäå $p(x) = x^{127} + x + 1$ [1631, 1632, 1129]. Ýôôåêòèâíàÿ àðõèòåêòóðà àïïàðàòóðû âîçâåäåíèÿ â ñòåïåíü äëÿ GF(2^n) ðàññìàòðèâàåòñÿ â [147].

11.4 Ðàçëîæåíèå íà ìíîæèòåëè

Ðàçëîæèòü ÷èñëî íà ìíîæèòåëè - çíà÷èò íàéòè åãî ïðîñòûå ñîìíîæèòåëè.

10 = 2*5

60 = 2*2*3*5

252601 = 41*61*101

2113- 1 =3391*23279*65993*1868569*1066818132868207

Ðàçëîæåíèå íà ìíîæèòåëè ÿâëÿåòñÿ îäíîé èç äðåâíåéøèõ ïðîáëåì òåîðèè ÷èñåë. Ýòîò ïðîöåññ íåñëîæåí, íî òðåáóåò âðåìåíè. Ýòî ïîêà îñòàåòñÿ òàê, íî ðÿä ñäâèãîâ â ýòîì èñêóññòâå âñå æå ïðîèçîøåë. Ñåãîäíÿ ñàìûì ëó÷øèì àëãîðèòìîì ÿâëÿåòñÿ:

Ðåøåòî ÷èñëîâîãî ïîëÿ ÷èñåë (Number field sieve, **NFS**) [953] (ñì. òàêæå [952, 16, 279]). **Ðåøåòî îáùåãî ÷èñëîâîãî ïîëÿ** - ýòî ñàìûé áûñòðûé èç èçâåñòíûõ äëãîðåòì äëÿ ÷èñåë ðàçìåðîì 110 è áîëåå ðàçðÿäîâ [472, 635]. Â ñâîåì ïåðâîíà÷àëüíîì âèäå îí áûë ïðåäëîæåí, íî çà ïîñëåäíèå íåñêîëüêî ëåò îí áûë ïîñëåäîâàòåëüíî óëó÷øåí [953]. NFS âñå åùå ñëèøêîì íîâ, ÷òîáû áèòü ðåêîðäû ðàçëîæåíèÿ íà ìíîæèòåëè, íî ñêîðî âñå ïåðåíåñåíèòñÿ. Ðàíýý âåðñèÿ èñïîëüçîâàëàñü äëÿ ðàçëîæåíèÿ íà ìíîæèòåëè äââÿòîãî ÷èñëà Ôåðìà: 2512 + 1 [955,954].

Äðóãèå àëãîðèòìû, âûòåñíåííûå NFS:

Êâàäðàòè÷íîå ðåøåòî (Quadratic sieve, **QS**) [1257, 1617, 1259]. Ýòî ñàìûé áûñòðûé èç èçâåñòíûõ è ÷àùå âñåãî èñïîëüçîâàâøèéñÿ àëãîðèòì äëÿ ÷èñåë, äëèíà êîòîðûõ ìåíüøå 110 äåñÿòè÷íûõ ðàçðÿäîâ [440]. Áîëåå áûñòðàÿ âåðñèÿ ýòîãî àëãîðèòìà íàçûâàåòñÿ ìíîæåñòâåííûì ïîëèíîìèàëüíûì êâàäðàòè÷íûì ðåøåòîì [1453, 302]. Ñàìàÿ áûñòðàÿ âåðñèÿ íàçûâàåòñÿ äâîéíîé âàðèàöèåé ìíîæåñòâåííîãî ïîëèíîìèàëüíîãî êâàäðàòè÷íîãî ðåøåòà ñâîëüøèì ïðîñòûì ÷èñëîì.

Ìåòîä ýëëèïòè÷åñêîé êðèâîé (Elliptic curve method, **ECM**) [957, 1112, 1113]. Ýòîò ìåòîä èñïîëüçîâàëñÿ äëÿ ïîèñêà íå áîëåå, ÷åì 43-ðàçðÿäíûõ ìíîæèòåëåé.

Àëãîðèòì Ìîíòå-Êàðëî Ïîëëàðäà (Pollard's Monte Carlo algorithm) [1254, 248]. (Ýòîò àëãîðèòì òàêæå ïðèâåäåí ó Êíóòà â òîìå 2 [863].)

Àëãîðèòì íåïðåðûâíûõ äðîáåé (Continued fraction algorithm). Ñì. [1123, 1252, 863]. Ýòîò àëãîðèòì íå ïîäõîäèò ïî âðåìåíè âû÷èñëåíèÿ.

Ïðîáíîå äåëåíèå (Trial division). Ýòîò ñàìûé ñòàðûé àëãîðèòì ðàçëîæåíèÿ íà ìíîæèòåëè ñîñòîèò èç ïðîâåðêè êàæäîãî ïðîñòîãî ÷èñëà, ìåíüøåãî èëè ðàâíîãî êâàäðàòíîãî êîðíÿ èç ðàññëåäóåìîãî ÷èñëà.

Â êà÷åñòâå õîðîøåãî ââåäåíèÿ â ðàçëè÷íûå àëãîðèòìû ðàçëîæåíèÿ íà ìíîæèòåëè, êðîìå NFS, ìîæíî èñïîëüçîâàòü [251]. NFS ëó÷øå âñåãî ðàññìîòðåí â [953]. Áîëåå ñòàðûå ðîâáîòàìè ÿâëÿþòñÿ [505, 1602, 1258]. Ñâåäåíèÿ î ïàðàëëåëüíîì ðàçëîæåíèè íà ìíîæèòåëè ìîæíî íàéòè â [250].

Åñëè ÷èñëî n íà ìíîæèòåëè ðàñêëàäûâàþòñÿ, òî ýâðèñòè÷åñêîå âðåìÿ âûïîëíåíèÿ ñàìûõ áûñòðûõ âàðèàíòîâ QS àñèìïòîòè÷åñêè ðàâíî:

$$e^{(1+O(1))(\ln(n))^{1/2}(\ln((\ln(n)))^{1/2}}$$

NFS íàìíîãî áûñòðåå, îöåíêà åãî ýâðèñòè÷åñêîãî âðåìåíè âûïîëíåíèÿ:

$$e^{(1.923+O(1))(\ln(n))^{1/3}(\ln((\ln(n)))^{2/3}}$$

Â 1970 ãîäó áîëüøîé íîâîñòüþ ñòàëî ðàçëîæåíèå íà ìíîæèòåëè 41-ðàçðÿäíîãî òðóäíîãî ÷èñëà [1123]. ("Òðóäíûì" ÿâëÿåòñÿ òàêîå ÷èñëî, ó êîòîðîãî íåò ìàëåíüêèõ ìíîæèòåëåé, è êîòîðîå íå îäíàäàåò ñïåöèàëüíîé ôîðìîé, ïîçâîëÿþùåé óïðîñòèòü ïðîöåññ.) Äåñÿòü ëåò ñïóñòÿ ðàçëîæåíèå â äâà ðàç áîëåå äëèííîãî ÷èñëà çàíÿëî ëèøü íåñêîëüêî ÷àñîâ íà êîìïüþòåðå Cray [440].

Â 1988 ãîäó Êàðë Ïîìåðàíñ (Carl Pomerance), èñïîëüçóÿ îáû÷íûå ÑÁÈÑ, ñïðîåêòèðîâàë óñòðîéñòâî äëÿ ðàçëîæåíèÿ íà ìíîæèòåëè [1259]. Ðàçìåð ÷èñëà, êîòîðîå ìîæíî áûëî ðàçëîæèòü, çàâèñåë òîëüêî îò ðàçìåðîâ óñòðîéñòâà, êîòîðîå òàê è íå áûëî ïîñòðîåíî.

Â 1993 ãîäó ñ ïîìùüþ êâàäðàòè÷íîãî ðåøåòà áûëî ðàçëîæåíî íà ìíîæèòåëè 120-ðàçðÿäíîå òðóäíîå ÷èñëî. Ðàñ÷åò, ïîòðåáîâàâøèé 825 mips-ëåò, áûë âûïîëíåí çà òðè ìåñÿöà ðåàëüíîãî âðåìåíè [463]. Äðóãèå ðåçóëüòàòû ïðèâåäåíû â [504].

Ñåãîäíÿ äëÿ ðàçëîæåíèÿ íà ìíîæèòåëè èñïîëüçóþòñÿ êîìüþòåðíûå ñåòè [302, 955]. Äëÿ ðàçëîæåíèÿ 116_ðàçðÿäíîãî ÷èñëà Àðæåò Ëåíſòðà (Arjen Lenstra) è Ìàðê Ìàíàññ (Mark Manasse) â òå÷åíèå íåñêîëüêèõ ìåñÿöåâ èñïîëüçîâàëè ñâîáîäíûå âðåìÿ ìàññèâà êîìïüþòåðîâ, ðàçáðîñàííûõ ïî âñåìó ìèðó, - 400 mips-ëåò.

Â ìàðòå 1994 ãîäà ñ ïîìùüþ äâîéíîé âàðèàöèè ìíîæåñòâåííîãî ïîëèíîìèàëüíîãî QS [66] êîìàíäíé ìàòåìàòèêîâ ïîä ðóêîâîäñòâîì Ëåíſòðû áûëî ðàçëîæåíî íà ìíîæèòåëè 129-ðàçðÿäíîå (428-áèòîâîå) ÷èñëî. Âû÷èñëåíèÿ âûïîëíÿëèñü äîáðîâîëüíèêàìè â Internet - â òå÷åíèå âîñüìè ìåñÿöåâ òðóäèëèñü 600 ÷åëîâåê è 1600 êîìïüþòåðîâ, âîçìîæíî, ñàìûé áîëüøîé â èñòîðèè ìíîãîïðîöåññîðíûé êîíãëîìåðàò. Òðóäîåìêîñòü âû÷èñëåíèé áûëà â äèàïàçîíå îò 4000 äî 6000 mips-ëåò. Êîìïüþòåðû ñîåäèíÿëèñü ïî ýëåêòðîííîé ïî÷òå, ïåðåäàâàÿ ñâîè ðåçóëüòàòû â öåíòðàëüíîå õðàíèëèùå, äàâ âûïîëíÿëñÿ îêîí÷àòåëüíûé àíàëèç. Â ýòè âû÷èñëåíèÿõ èñïîëüçîâàëèñü QS è òåîðèÿ ïÿòèëåòíåé äâîéíîñòè, NFS ìîã áû óñêîðèòü âû÷èñëåíèå ðàñ÷åòîâ ðàç â äåñÿòü [949]. Â ñîîòâåòñòâèè ñ [66]: "Ì û äåëàì âûâîä, ÷òî øèðîêî èñïîëüçóåìûå 512-áèòîâûå ìîäóëè RSA ìîãóò áûòü îðãàíèçàöèåé, ãîòîâîé ïîðòàòèòü íåñêîëüêî ìèëëèîíîâ äîëëàðîâ è ïîäîæäàòü íåñêîëüêî ìåñÿöåâ." Ïî îöåíêàì àâòîðîâ ðàçëîæåíèå 512-áèòîâîãî ÷èñëà â 100 ðàç áîëåå òðóäîåìêî ïðè èñïîëüçîâàíèè òîé æå òåõíèêè è òîëüêî â 10 ñëîæíåå ïðè èñïîëüçîâàíèè NFS è ñîâðåìåííîé òåõíèêè [949].

Ñ öåëüþ ðàçâèòèÿ èñêóññòâà ðàçëîæåíèÿ íà ìíîæèòåëè RSA Data Security, Inc. â ìàðòå 1991 ãîäà îáúÿâèëî î

ïðîãðàì ìå RSA Factoring Challenge (ñîñòÿçàíèå RSA ïî ðàçëîæåíèþ íà ìíîæèòåëè) [532]. Ñîñòÿçàíèå ñîñòîèò â ðàçëîæåíèè íà ìíîæèòåëè ðÿäà òðóäíûõ ÷èñåë, êàæäîå èç êîòîðûõ ÿâëÿåòñÿ ïðîèçâåäåíèåì äâóõ ïðîñòûõ ÷èñåë ïðèìåðíî îäèíàêîâîãî ðàçìåðà. Êàæäîå ïðîñòîå ÷èñëî áûëî âûáðàíî êîíêóðåíòíûì 2 ïî ìîäóëþ 3. Âñåãî áûëî ïðåäëîæåíî 42 ÷èñëà, ïî îäíîìó ÷èñëó â äèàïàçîíå îò 100 äî 500 ðàçðÿäîâ ñ øàãîì 10 ðàçðÿäîâ (ïëþñ îäíî äîïîëíèòåëüíîå, 129-ðàçðÿäíîå ÷èñëî). Ê ìîìåíòó íàïèñàíèÿ ýòîé êíèãè RSA-100, RSA-110, RSA-120, è RSA-129 áûëè ðàçëîæåíû íà ìíîæèòåëè, âñå ñ ïîìîùüþ QS. Ñëåäóþùèì (ñ ïîìîùüþ NFS) ìîæåò áûòü RSA-130, èëè ÷åì ïèñîíû ïî ðàçëîæåíèþ íà ìíîæèòåëè ñðàçó âîçüìóòñÿ çà RSA -140.

Äàííàÿ îáëàñòü ðàçâèâàåòñÿ áûñòðî. Òåõíèêó ðàçëîæåíèÿ íà ìíîæèòåëè òðóäíî ýêñòðàïîëèðîâàòü, òàê êàê íåâîçìîæíî ïðåäñêàçàòü ìàòåìàòè÷åñêîé òåîðèè. Äî îòêðûòèÿ NFS íîâåå ñ÷èòàëè, ÷òî ëþáîé ìåòîä ðàçëîæåíèÿ íà ìíîæèòåëè íå ìîæåò äîñòè÷ü ñêîðîñòè, áîëüøåé, ÷åì ó ìåòîäà ïåðåáîðà äåëèòåëåé. Ïîñëå áûëè íàéäåíû.

Ïðåäñòîÿùåå ðàçâèòèå NFS, ïî âèäèìîìó, áóäåò ïðîèãðàíî â ôîðìå óìåíüøåíèÿ êîíñòàíòû: 1.923. Äëÿ ðÿäà ÷èñåë ñïåöèàëüíîé ôîðìû, òàêèõ êàê ÷èñëà Ôåðìà, êîíñòàíòà ïðèáëèæàåòñÿ ê 1.5 [955, 954]. Åñëè áû äëÿ òðóäíûõ ÷èñåë, èñïîëüçóåìûõ â ñåãîäíÿøíåé êðèïòîãðàôèè, êîíñòàíòó òîæå ìîæíî áûëî ñíèçèòü äî ýòîãî óðîâíÿ, òî 1024-áèòîâûå ÷èñëà ðàñêëàäûâàëèñü áû íà ìíîæèòåëè óæå ñåãîäíÿ. Îäíè èç ñîîáùåíèé êîíñòàíòó ÿâëÿåòñÿ îáíàðóæåíèå ëó÷øèõ ïîáî÷íûõ ïðåäñêàçàíèé ÷èñåë êâ îïèñûâàþùèõ ôóíêöèîíàëüíóþ ñâÿçü, íî âîçìîæíî ðåøàþùèé óñïåõ óæå áëèçîê [949].

Ïîñëåäíèå ðåçóëüòàòû ïðîãðàìì RSA Factoring Challenge ìîæíî óçíàòü, îòïðàâèâ çàïðîñ ïî ýëåêòðîííîé ïî÷òå ïî àäðåñó challenge-info@rsa.com.

Êâàäðàòíûå êîðíè ïî ìîäóëþ n

Åñëè *n* - ïðîèçâåäåíèå äâóõ ïðîñòûõ ÷èñåë, òî âîçìîæíîñòü âû÷èñëèòü êâàäðàòíûå êîðíè ïî ìîäóëþ *n* âû÷èñëèòåëüíî ýêâèâàëåíòíà âîçìîæíîñòè ðàçëîæèòü *n* íà ìíîæèòåëè [1283, 35, 36, 193]. Äðóãèì ñëîâàìè, òîò, êòî çíàåò ïðîñòûå ìíîæèòåëè ÷èñëà n, ìîæåò ëåãêî âû÷èñëèòü êâàäðàòíûå êîðíè ëþáîãî ÷èñëà ïî ìîäóëþ *n*, íî äëÿ ëþáîãî äðóãîãî âû÷èñëåíèå îêàæåòñÿ òàêèì æå òðóäíûì, êàê è ðàçëîæåíèå íà ïðîñòûå ìíîæèòåëè ÷èñëà *n*.

11.5 Ãåíåðàöèÿ ïðîñòîãî ÷èñëà

Äëÿ àëãîðèòìîâ ñ îòêðûòûìè êëþ÷àìè íóæíû ïðîñòûå ÷èñëà. Èõ íóæíî ìíîæåñòâî äëÿ ëþáîé äîñòàòî÷íî áîëüøîé ñåòè. Ïðåæäå, ÷åì îáñóæäàòü ìàòåìàòèêó ãåíåðàöèè ïðîñòîãî ÷èñëà, ÿ îòâå÷ó íà íåñêîëüêî î÷åâèäíûõ âîïðîñîâ.

Åñëè êàæäîìó ïîíàäîáèòñÿ ñâîå ïðîñòîå ÷èñëî, íå èñïÿêíåò ëè ó íàñ çàïàñ? Íåò. Â äåéñòâèòåëüíîñòè ñóùåñòâóåò ïðèáëèçèòåëüíî 10151 ïðîñòûõ ÷èñåë äëèíîé äî 512 áèò âêëþ÷èòåëüíî. Äëÿ ÷èñåë, áëèçêèõ *n*, âåðîÿòíîñòü òîãî, ÷òî ñëó÷àéíî âûáðàííîå ÷èñëî îêàæåòñÿ ïðîñòûì, ðàâíà 1/ln *n*. Ïîýòîìó ïîëíîå ÷èñëî ïðîñòûõ ÷èñåë, ìåíüøèõ n, ðàâíî *n*/(ln *n*). Âî âñåëåííîé âñåãî 10^{77} àòîìîâ. Åñëè áû äëÿ êàæäîãî àòîìà âî âñåëåííîé ñ íà÷àëà âðåìåí êàæäóþ ìèêðîñåêóíäó òðåõëèíâåëëèþ áû ìèëëèàðä ïðîñòûõ ÷èñåë, îïòèìèçèðîâàííûõ äëÿ òåñòîâ íà òåëëîâñêîì 10^{109} ïðîñòûõ ÷èñåë, îñòàëèñü áû åùå ïðèìåðíî 10^{151} ïðîñòûõ ÷èñåë.

×òî åñëè äàæå ÷åëîâåêà ñëó÷àéíî âûáðóò îäíî è òî æå ïðîñòîå ÷èñëî? Ýòîãî íå ñëó÷èòñÿ. Ïðè âûáîðå èç 10151 ïðîñòûõ ÷èñåë âåðîÿòíîñòü ñîâïàäåíèÿ âûáîðà çíà÷èòåëüíî ìåíüøå, ÷åì âåðîÿòíîñòü, ÷òî âàø êîìïüþòåð ñëó÷àéíî âñïûõíåò â òîò ñàìûé îíåíü, êîãäà âû âûáèðàåòå â ëîòåðåå.

Åñëè êòî-òî ñîçäàñò áàçó äàííûõ âñåõ ïðîñòûõ ÷èñåë, íå ñìîæåò ëè îí èñïîëüçîâàòü ýòó áàçó äàííûõ äëÿ âñêðûòèÿ äëãîâðåìåííûõ ñîâðåìåííûõ êëþ÷åé? Íåò. Åñëè áû âû õðàíèëè ïàëè "íåò" íà âîïðîñ "ßâëÿåòñÿ ëè ÷èñëî *n* ïðîñòûì?" ãîðàçäî ïðîùå, ÷åì îòâå÷àòü íà âîïðîñ "Êàêîâû ìíîæèòåëè *n*?"

Ãåíåðàöèÿ ñëó÷àéíûõ ÷èñåë ñ îïðåäåëåííûì ïîëîæåíèåì ðàçëîæåíèÿ èõ íà ìíîæèòåëè - ýòî íåïðàâäîïîäîáíî ïîñòîÿííî ïîèñêà ïðîñòûõ ÷èñåë. Ñóùåñòâóþò ðàçëè÷íûå âåðîÿòíîñòíûå ïðîâåðêè íà ïðîñòîòó ÷èñåë, îïðåäåëÿþùèå, ÿâëÿåòñÿ ëè ÷èñëî ïðîñòûì, ñ çàäàííîé ñòåïåíüþ äîñòîâåðíîñòè. Ïðè óñëîâèè, ÷òî ýòà "ñòåïåíü äîñòîâåðíîñòè" äîñòàòî÷íà âåëèêà, òàêèå ñïîñîáû ïðîâåðêè äîñòàòî÷íî õîðîøè. SS ñêàæó, ÷òî ïðîñòûå ÷èñëà, âåíåðåðîâàííûå òàêèì îáðàçîì íàçûâàþòñÿ "ïðîùëåííî ïðîñòûìè ÷èñëàìè": ýòè ÷èñëà âåðîÿòíî ÿâëÿþòñÿ ïðîñòûìè ñ êîíòðîëèðóåìîé âîçìîæíîñòüþ îøèáêè.

Ïðåäïîëîæèì, ÷òî îáíà ïðîâåðêà èç 2^{50} - îøèáî÷íà. Ýòî îçíà÷àåò, ÷òî ñ âåðîÿòíîñòüþ $1/10^{15}$ ïðîâåðêà îáúÿâèò ïðîñòûì ñîñòàâíîå ÷èñëî. (Ïðîñòîå ÷èñëî íèêîãäà íå áóäåò îáúÿâëåíî ñîñòàâíûì ïðè ïðîâåðêå.) Åñëè ïî

êàêîé-òî ïðè÷èíå ïîíàäîáèòñÿ áîëüøàÿ äîñòîâåðíîñòü ïðîñòîòû ÷èñëà, óðîâíþ îøèáêè ìîæíî ïîíèçèòü. Ñ äðóãîé ñòîðîíû, åñëè âû óòâåðæäàåòå âåðîÿòíîñòü òîãî, ÷òî ÷èñëî ÿâëÿåòñÿ ñîñòàâíûì, â 300 ìèëëèîíîâ ðàç ìåíüøåé, ÷åì âåðîÿòíîñòü âûèãðàòü ãëàâíûé ïðèç â ãîñóäàðñòâåííîé ëîòåðåå, âû ìîæåòå áîëüøå îá ýòîì íå âîëíîâàòüñÿ.

Îáîðû íåäàâíèõ èññëåäîâàíèé â ýòîé îáëàñòè ìîæíî íàéòè â [1256, 206]. Äðóãèìè âàæíûìè ðàáîòàìè ÿâëÿþòñÿ [1490, 384, 11, 19, 626, 651, 911].

Solovay-Strassen

Ðîáåðò Ñîëîâåé (Robert Solovay) è Ôîëüêåð Øòðàññåí (Volker Strassen) ðàçðàáîòàëè àëãîðèòì âåðîÿòíîñòíîé ïðîâåðêè ïðîñòîòû ÷èñëà [1490]. Äëÿ ïðîâåðêè ïðîñòîòû ÷èñëà p ýòîò àëãîðèòì èñïîëüçóåò ñèìâîë ßêîáè:

(1) Âûáåðèòå ñëó÷àéíî ÷èñëî a, ìåíüøåå p.

(2) Åñëè Í ÎÄ(a,p) (1, òî p íå ïðîõîäèò ïðîâåðêó è ÿâëÿåòñÿ ñîñòàâíûì.

(3) Âû÷èñëèòå $j = a^{(p-1)/2} \bmod p$.

(4) Âû÷èñëèòå ñèìâîë ßêîáè J(a,p).

(5) Åñëè $j \neq$ J(a,p), òî ÷èñëî p íàâåðíÿêà íå ÿâëÿåòñÿ ïðîñòûì.

(6) Åñëè $j =$ J(a,p), òî âåðîÿòíîñòü òîãî, ÷òî ÷èñëî p íå ÿâëÿåòñÿ ïðîñòûì, íå áîëüøå 50 ïðîöåíòîâ.

×èñëî a, êîòîðîå íå ïîêàçûâàåò, ÷òî p íàâåðíÿêà íå ÿâëÿåòñÿ ïðîñòûì ÷èñëîì, íàçûâàåòñÿ ñâèäåòåëåì. Åñëè p - ñîñòàâíîå ÷èñëî, âåðîÿòíîñòü ñëó÷àéíîãî ÷èñëà a áûò ñâèäåòåëåì íå íèæå 50 ïðöåíòîâ. Ïîâòîðèòå ýòó ïðîâåðêó t ðàç ñ t ðàçëè÷íûì çíà÷åíèåì a. Âåðîÿòíîñòü òîãî, ÷òî ñîñòàâíîå ÷èñëî ïðîéäåò âñå t ïðîâåðîê, íå ïðåâûøàåò $1/2^t$.

Lehmann

Äðóãîé, áîëåå ïðîñòîé òåñò áûë íåçàâèñèìî ðàçðàáîòàí Ëåìàíîì (Lehmann) [903]. Âîò ïîñëåäîâàòåëüíîñòü äåéñòâèé ïðè ïðîâåðêå ïðîñòîòû ÷èñëà p:

(1) Âûáåðèòå ñëó÷àéíî ÷èñëî a, ìåíüøåå p.

(2) Âû÷èñëèòå $a^{(p-1)/2} \bmod p$.

(3) Åñëè $a^{(p-1)/2} \neq 1$ èëè -1 (mod p), òî p íå ÿâëÿåòñÿ ïðîñòûì.

(4) Åñëè $a^{(p-1)/2} \equiv 1$ èëè -1 (mod p), òî âåðîÿòíîñòü òîãî, ÷òî ÷èñëî p íå ÿâëÿåòñÿ ïðîñòûì, íå áîëüøå 50 ïðöåíòîâ.

È ñíîâà, âåðîÿòíîñòü òîãî, ÷òî ñëó÷àéíîå ÷èñëî a áóäåò ñâèäåòåëåì ñîñòàâíîé ïðèðîäû ÷èñëà p, íå ìåíüøå 50 ïðöåíòîâ. Ïîâòîðèòå ýòó ïðîâåðêó t ðàç. Åñëè ðåçóëüòàò âû÷èñëåíèé ðàâåí 1 èëè -1, íî íå âñåãäà ðàâåí 1, òî p ÿâëÿåòñÿ ïðîñòûì ÷èñëîì ñ âåðîÿòíîñòüþ ïðåâûøàþùåé $1/2^t$.

Rabin-Miller

Ïîâñåìåñòíî èñïîëüçóåìûì ÿâëÿåòñÿ ïðîñòîé àëãîðèòì, ðàçðàáîòàííûé Ìàéêëîì Ðàáèíûì (Michael Rabin), ÷àñòè÷íî îñíîâàííûì íà èäåÿõ Ãýðè Ìèëëåðà [1093, 1284]. Ïî ñóòè, ýòî óïðîùåííàÿ âåðñèÿ àëãîðèòìà, ðåêîìåíäîâàííîãî â ïðåäëîæåíèè DSS proposal [1149, 1154].

Âûáåðèòå äëÿ ïðîâåðêè ñëó÷àéíîå ÷èñëî p. Âû÷èñëèòå b - ÷èñëî äëåíèé p - 1 íà 2 (ò.å., 2^b - ýòî íàèáîëüøàÿ ñòåïåíü 2, íà êîòîðîå äåëèòñÿ p - 1). Çàòåì âû÷èñëèòå m, òàêîå ÷òî $p = 1 + 2^b * m$.

(1) Âûáåðèòå ñëó÷àéíîå ÷èñëî a, ìåíüøåå p.

(2) Óñòàíîâèòå $j = 0$ è $z = am \bmod p$.

(3) Åñëè $z = 1$ èëè åñëè $z = p$ - 1, òî p ïðîõîäèò ïðîâåðêó è ìîæåò áûòü ïðîñòûì ÷èñëîì.

(4) Åñëè $j > 0$ è $z = 1$, òî p íå ÿâëÿåòñÿ ïðîñòûì ÷èñëîì.

(5) Óñòàíîâèòå $j = j + 1$. Åñëè $j < b$ è $z(p$ - 1, óñòàíîâèòå $z = z^2 \bmod p$ è âåðíèòåñü íà ýòàï (4). Åñëè $z = p$ - 1, òî p ïðîõîäèò ïðîâåðêó è ìîæåò áûòü ïðîñòûì ÷èñëîì.

(6) Åñëè $j = b$ è $z \neq p$ - 1, òî p íå ÿâëÿåòñÿ ïðîñòûì ÷èñëîì.

Â ýòîì òåñòå âåðîÿòíîñòü ïðîõîæäåíèÿ ïðîâåðêè ñîñòàâíûì ÷èñëîì óâû âàëî áûñòðåå, ÷åì â ïðåäûäóùèõ. Àäðàìñîí ïîêàçûâàåò, ÷òî òðè ÷åòâåðòè âîçìîæíûõ çíà÷åíèé a îêàæóòñÿ ñâèäåòåëÿìè. Ýòî îçíà÷àåò, ÷òî ñîñòàâíîå ÷èñëî ïðîñõîäèò ýòîò òåñò t ïðîâåðîê ñ âåðîÿòíîñòüþ íå áîëüøå $(1/4)^t$, ãäå t - ýòî ÷èñëî èòåðàöèé. Íà ñàìîì äåëå è ýòè îöåíêè ñëèøêîì ïåññèìèñòè÷íû. Äëÿ áîëüøèíñòâà ñëó÷àéíûõ ÷èñåë îêîëî 99.9 ïðöåíòîâ âîçìîæ-

íûõ çíà÷åíèé *a* ÿâëÿþòñÿ ñâèäåòåëÿìè [96].

Ñóùåñòâóþò áîëåå òî÷íûå îöåíêè [417]. Äëÿ *n*-áèòîâîãî êàíäèäàòà â ïðîñòûå ÷èñëà (ãäå *n* áîëüøå 100), âåðîÿòíîñòü îøèáêè â îäíîì òåñòå ìåíüøå, ÷åì $4n2^{(k/2)^{1/2}}$. È äëÿ 256-áèòîâîãî *n* âåðîÿòíîñòü îøèáêè â øåñòè òåñòàõ ìåíüøå, ÷åì $1/2^{51}$. Äîïîëíèòåëüíóþ òåîðèþ ìîæíî íàéòè â [418].

Ïðàêòè÷åñêèå ñîîáðàæåíèÿ

Â ðåàëüíûõ ïðèëîæåíèÿõ ãåíåðàöèÿ ïðîñòûõ ÷èñåë ïðîèñõîäèò áûñòðî.

(1) Ñãåíåðèðóéòå ñëó÷àéíîå *n*-áèòîâîå ÷èñëî *p*.

(2) Óñòàíîâèòå ñòàðøèé è ìëàäøèé áèòû ðàâíûìè 1. (Ñòàðøèé áèò ãàðàíòèðóåò òðåáóåìóþ äëèíó ïðîñòîãî ÷èñëà, à ìëàäøèé áèò îáåñïå÷èâàåò åãî íå÷åòíîñòü.)

(3) Óáåäèòåñü, ÷òî *p* íå äåëèòñÿ íà íåáîëüøèå ïðîñòûå ÷èñëà: 3, 5, 7, 11, è ò.ä. Âî ìíîãèõ ðåàëèçàöèÿõ ïðîâåðÿåòñÿ äåëèìîñòü *p* íà âñå ïðîñòûå ÷èñëà, ìåíüøèå 256. Íàèáîëåå ýôôåêòèâíîé ÿâëÿåòñÿ ïðîâåðêà íà äåëèìîñòü äëÿ âñåõ ïðîñòûõ ÷èñåë, ìåíüøèõ 2000 [949]. Ýòî ìîæåò áûòü ýôôåêòèâíî âûïîëíåíî ñ ïîìîùüþ êîëåñà [863].

(4) Âûïîëíèòå òåñò Rabin-Miller äëÿ íåêîòîðîãî ñëó÷àéíîãî *a*. Åñëè *p* ïðîõîäèò òåñò, ñãåíåðèðóéòå äðóãîå ñëó÷àéíîå *a* è ïîâòîðèòå ïðîâåðêó. Âûáèðàéòå íåáîëüøèå çíà÷åíèÿ *a* äëÿ óñêîðåíèÿ âû÷èñëåíèé. Âûïîëíèòå ïÿòü òåñòîâ [651]. (Îäíîãî ìîæåò ïîêàçàòüñÿ äîñòàòî÷íûì, íî âûïîëíèòå ïÿòü.) Åñëè *p* íå ïðîõîäèò îäíîé èç ïðîâåðîê, ñãåíåðèðóéòå äðóãîå *p* è ïîïðîáóéòå ñíîâà.

Èíà÷å, ìîæíî íå ãåíåðèðîâàòü p ñëó÷àéíûì îáðàçîì êàæäûé ðàç, íî ïîñëåäîâàòåëüíî ïåðåáèðàòü ÷èñëà, íà÷èíàÿ ñî ñëó÷àéíî âûáðàííîãî äî òåõ ïîð, ïîêà íå áóäåò íàéäåíî ïðîñòîå ÷èñëî.

Ýòàï (3) íå ÿâëÿåòñÿ îáÿçàòåëüíûì, íî ýòî õîðîøàÿ èäåÿ. Ïðîâåðêà, ÷òî ñëó÷àéíîå íå÷åòíîå *p* íå äåëèòñÿ íà 3, 5 è 7 îòñåêàåò 54 ïðîöåíòà íå÷åòíûõ ÷èñåë åùå äî ýòàïà (4). Ïðîâåðêà äåëèìîñòè íà âñå ïðîñòûå ÷èñëà, ìåíüøèå 100, óáèðàåò 76 ïðîöåíòîâ íå÷åòíûõ ÷èñåë, ïðîâåðêà äåëèìîñòè íà âñå ïðîñòûå ÷èñëà, ìåíüøèå 256, óáèðàåò 80 ïðîöåíòîâ íå÷åòíûõ ÷èñåë. Â îáùåì ñëó÷àå, äîëÿ íå÷åòíûõ êàíäèäàòîâ, êîòîðûå íå äåëÿòñÿ íè íà îäíî ïðîñòîå ÷èñëî, ìåíüøåå *n*, ðàâíà 1.12/ln *n*. ×åì áîëüøå ïðîâåðÿåìîå *n*, òåì áîëüøå ïðåäâàðèòåëüíûõ âû÷èñëåíèé íóæíî âûïîëíèòü äî òåñòà Rabin-Miller.

Îäíà èç ðåàëèçàöèé ýòîãî ìåòîäà íà Sparc II ñïîñîáíà íàõîäèòü 256-áèòîâûå ïðîñòûå ÷èñëà â ñðåäíåì çà 2.8 ñåêóíäû, 512-áèòîâûå ïðîñòûå ÷èñëà - â ñðåäíåì çà 24.0 ñåêóíäû, 768-áèòîâûå ïðîñòûå ÷èñëà - â ñðåäíåì çà 2.0 ìèíóòû, à 1024-áèòîâûå ïðîñòûå ÷èñëà - â ñðåäíåì çà 5.1 ìèíóòû [918].

Ñèëüíûå ïðîñòûå ÷èñëà

Åñëè *n* - ïðîèçâåäåíèå äâóõ ïðîñòûõ ÷èñåë, *p* è *q*, òî ìîæåò ïîíàäîáèòüñÿ èñïîëüçîâàòü â êà÷åñòâå *p* è *q* **ñèëüíûå ïðîñòûå ÷èñëà**. Òàêèå ïðîñòûå ÷èñëà îáëàäàþò ðÿäîì ñâîéñòâ, êîòîðûå óñëîæíÿþò ðàçëîæåíèå ïðîèçâåäåíèÿ *n* îïðåäåëåííûìè ìåòîäàìè ðàçëîæåíèÿ íà ìíîæèòåëè. Ñðåäè òàêèõ ñâîéñòâ áûëè ïðåäëîæåíû [1328, 651]:

Íàèáîëüøèé îáùèé äåëèòåëü *p* - 1 è *q* - 1 äîëæåí áûòü íåáîëüøèì.

È *p* - 1, è *q* - 1 äîëæíû èìåòü ñðåäè ñâîèõ ìíîæèòåëåé áîëüøèå ïðîñòûå ÷èñëà, ñîîòâåòñòâåííî *p′* è *q′*.

È *p′* - 1, è *q′* - 1 äîëæíû èìåòü ñðåäè ñâîèõ ìíîæèòåëåé áîëüøèå ïðîñòûå ÷èñëà.

È *p* + 1, è *q* + 1 äîëæíû èìåòü ñðåäè ñâîèõ ìíîæèòåëåé áîëüøèå ïðîñòûå ÷èñëà.

È (*p* - 1)/2, è (*q* - 1)/2 äîëæíû áûòü ïðîñòûìè [182). (Îáðàòèòå âíèìàíèå, ïðè âûïîëíåíèè ýòîãî óñëîâèÿ âûïîëíÿþòñÿ è äâà ïåðâûõ.)

Íàñêîëüêî ñóùåñòâåííî ïðèìåíåíèå èìåííî ñèëüíûõ ïðîñòûõ ÷èñåë, îñòàåòñÿ ïðåäìåòîì ïðîäîëæàþùèõñÿ ñïîðîâ. Ýòè ñâîéñòâà áûëè ðàçðàáîòàíû, ÷òîáû çàòðóäíèòü âûïîëíåíèå ðÿäà ñòàðûõ àëãîðèòìîâ ðàçëîæåíèÿ íà ìíîæèòåëè. Îäíàêî ñàìûå áûñòðûå àëãîðèòìû îäèíàêîâî áûñòðû ïðè ðàçëîæåíèè íà ìíîæèòåëè ëþáûõ ÷èñåë, êàê óäîâëåòâîðÿþùèõ ïðèâåäåííûì óñëîâèÿì, òàê è íåò [831].

ß ïðîòèâ ñïåöèàëüíîé ãåíåðàöèè ñèëüíûõ ïðîñòûõ ÷èñåë. Äëèíà ïðîñòûõ ÷èñåë ãîðàçäî âàæíåå èõ ñòðóêòóðû. Áîëåå òîãî, ñàìà ñòðóêòóðà óìåíüøàåò ñëó÷àéíîñòü ÷èñëà è ìîæåò ñíèçèòü óñòîé÷èâîñòü ñèñòåìû.

Íî âñå ìîæåò èçìåíèòüñÿ. Ìîãóò áûòü ñîçäàíû íîâûå ìåòîäû ðàçëîæåíèÿ íà ìíîæèòåëè, êîòîðûå ëó÷øå ðàáîòàþò ñ ÷èñëàìè, îáëàäàþùèìè îïðåäåëåííûìè ñâîéñòâàìè. Â ýòîì ñëó÷àå ñíîâà ìîãóò ïîòðåáîâàòüñÿ ñèëüíûå ïðîñòûå ÷èñëà. Çàãëÿäûâàéòå â æóðíàëû ïî òåîðåòè÷åñêîé ìàòåìàòèêå.

11.6 Äèñêðåòíûå ëîãàðèôìû â êîíå÷íîì ïîëå

Â êà÷åñòâå äóãîé îäíîíàïðàâëåííîé ôóíêöèè â êðèïòîãðàôèè ÷àñòî èñïîëüçóþòñÿ âîçâåäåíèå â ñòåïåíü ïî ìîäóëþ. Ëåãêî âû÷èñëèòü:

$a^x \bmod n$

Çàäà÷åé, îáðàòíîé âîçâåäåíèþ â ñòåïåíü ïî ìîäóëþ, ÿâëÿåòñÿ ïîèñê äèñêðåòíîãî ëîãàðèôìà. À ýòî óæå íåëåãêàÿ çàäà÷à:

Íàéòè x, äëÿ êîòîðîãî $a^x \equiv b \pmod n$.

Íàïðèìåð:

Åñëè $3^x \equiv 15 \bmod 17$, òî $x = 6$

Äåøåíèÿ ñóùåñòâóþò íå äëÿ âñåõ äèñêðåòíûõ ëîãàðèôìîâ (ïîìíèòå, ðå÷ü èäåò òîëüêî î öåëî÷èñëåííûõ ðåøåíèÿõ). Ëåãêî çàìåòèòü, ÷òî ñëåäóþùåå óðàâíåíèå íå èìåò ðåøåíèé

$3^x \equiv 7 \pmod{13}$

Åùå ñëîæíåå ðåøàòü ýòó çàäà÷ó äëÿ 1024-áèòîâûõ ÷èñåë.

Âû÷èñëåíèå äiñêðåòíûõ ëîãàðèôìîâ êîíå÷íîé ãðóïïå

Êðèïòîãðàôû èíòåðåñóþòñÿ äiñêðåòíûìè ëîãàðèôìàìè ñëåäóþùèõ òðåõ ãðóïï:

— Ìóëüòèïëèêàòèâíàÿ ãðóïïà ïîëåé ïðîñòîãî ÷èñëà: GF(p)

— Ìóëüòèïëèêàòèâíàÿ ãðóïïà êîíå÷íûõ ïîëåé ñòåïåíè 2: GF(2^n)

— Ãðóïïû ýëëèïòè÷åñêîé êðèâîé íàä êîíå÷íûìè ïîëÿìè F: EC(F)

Áåçîïàñíîñòü ìíîãèõ àëãîðèòìîâ ñ îòêðûòûìè êëþ÷àìè îñíîâàíà íà çàäà÷å ïîèñêà äiñêðåòíûõ ëîãàðèôìîâ, ïîýòîìó ýòà çàäà÷à áûëà ãëóáîêî èçó÷åíà. Õîðîøèé ïîäõîä ýòîé ïðîáëåìû è åå íàèëó÷øèå ðåøåíèÿ íà ñîôòâåðíîì óðîâíå ìîæíî íàéòè â [1189, 1039]. Ëó÷øåé ñîâðåìåííîé ñòàòüåé íà ýòó òåìó ÿâëÿåòñÿ [934].

Åñëè p ÿâëÿåòñÿ ïðîñòûì ÷èñëîì è èñïîëüçóåòñÿ â êà÷åñòâå ìîäóëÿ, òî ñëîæíîñòü ïîèñêà äiñêðåòíûõ ëîãàðèôìîâ â GF(p) ïî ñóùåñòâó ñîîòâåòñòâóåò ðàçëîæåíèþ íà ìíîæèòåëè ÷èñëà n òîãî æå ðàçìåðà, ãäå n - ýòî ïðîèçâåäåíèå äâóõ ïðîñòûõ ÷èñåë ïðèáëèçèòåëüíî ðàâíîé äëèíû [1378,934]. Òî åñòü:

$$e^{(1+O(1))(\ln(n))^{1/2}(\ln((\ln(n)))^{1/2}}$$

Ðåøåòî ÷èñëîâîãî ïîëÿ áûñòðåå, îöåíêà åãî ýêñïîíåíòû âûãëÿäèò:

$$e^{(1.923+O(1))(\ln(n))^{1/3}(\ln((\ln(n)))^{2/3}}$$

Ñòåâåí Ïîëèã (Stephen Pohlig) è Ìàðòèí Õåëëìàí íàøëè ñïîñîá áûñòðîãî âû÷èñëåíèÿ äiñêðåòíûõ ëîãàðèôìîâ â GF(p) ïðè óñëîâèè, ÷òî p - 1 ðàñêëàäûâàåòñÿ íà ìàëûå ïðîñòûå ìíîæèòåëè [1253]. Ïî ýòîé ïðè÷èíå â êðèïòîãðàôèè èñïîëüçóþòñÿ òîëüêî òàêèå ïîëÿ, äëÿ êîòîðûõ p - 1 îáÿçàòåëüíî õîòÿ áû îäíî áîëüøîå ïðîñòîå ìíîæèòåëü. Äðóãîé äëãîðèòì [14] âû÷iñëÿåò äiñêðåòíûå ëîãàðèôìû ñî ñêîðîñòüþ, ñðàâíèìîé ñ ðàçëîæåíèåì íà ìíîæèòåëè, îí áûë ðàñøèðåí íà ïîëÿ âèäà GF(p^n) [716]. Ýòîò àëãîðèòì áûë ïîäâåðãíóò êðèòèêå â [727] ïî ðÿäó òåõíè÷åñêèõ ìîìåíòîâ. Â äðóãèõ ñòàòüÿõ [1588] ìîæíî óêàçàòü, íàñêîëüêî íà ñàìîì äåëå òðóäíà ïðîáëåìà â öåëîì.

Âû÷iñëåíèå äiñêðåòíûõ ëîãàðèôìîâ òåñíî ñâÿçàíî ñ ðàçëîæåíèåì íà ìíîæèòåëè. Åñëè âû ìîæåòå ðåøèòü ïðîáëåìó äiñêðåòíîãî ëîãàðèôìà, òî âû ìîæåòå è ðàçëîæèòü íà ìíîæèòåëè. (Èñòèííîñòü îáðàòíîãî íåêîòîðûõ íå áûëà äîêàçàíà.) Â íàñòîÿùåå âðåìÿ ñóùåñòâóþò òðè ìåòîäà âû÷iñëåíèÿ äiñêðåòíûõ ëîãàðèôìîâ â ïîëå ïðîñòîãî ÷iñëà [370, 934, 648]: ëèíåéíîå ðåøåòî, ñðåäíå öåëûõ ÷iñëè Ãàóññà è ðåøåòî ÷iñëîâîãî ïîëÿ.

Ïðåäâàðèòåëüíîå, îáúåìíîå âû÷iñëåíèå äëÿ ïîëÿ äîëæíî áûòü âûïîëíåíî òîëüêî îäèí ðàç. Çàòåì, áûñòðî ìîæíî âû÷iñëÿòü îòäåëüíûå ëîãàðèôìû. Ýòî ìîæåò ñâðùåíî óùåíüøèòü áåçîïàñíîñòü ñèñòåì, îñíîâàííûõ íà òàêèõ ïîëÿõ. Âàæíî, ÷òîáû ðàçëè÷íûå ïðèìåíåíèÿ èñïîëüçîâàëè ðàçëè÷íûå ïîëÿ ïðîñòûõ ÷iñëè. Õîòÿ íåñêîëüêî ïðèëîæåíèé ìîãóò ïðèìåíÿòü îäíî è òî æå ïîëå, íî âî âñåì îñòàëüíîì íî õîðîø è ýôôåêòèâåí. Ðåàëèçàöèÿ ìåíåå ýôôåêòèâíîé âåðñèè ýòîãî æå àëãîðèòìà ïîñëå ñàìîé ïðîäâèíóòîé âû÷iñëåíèé òðàòèëà íà íàõîæäåíèå êàæäîãî äiñêðåòíîãî ëîãàðèôìà â ïîëå GF(2^{127}) ëèøü íåñêîëüêî

ñåêóíä [1130, 180]. (Ýòî êîíêðåòíûå ïîëå, êîãäà-òî èñïîëüçîâàâøåãî â íåêîòîðûõ êðèïòîñèñòåìàõ [142, 1631, 1632], íå ÿâëÿåòñÿ áåçîïàñíûì.) Îáçîð íåêîòîðûõ èç ýòèõ ðåçóëüòàòîâ ìîæíî íàéòè â [1189, 1039].

Ïîçäíåå áûëè âûïîëíåíû ïðåäâàðèòåëüíûå âû÷èñëåíèÿ äëÿ ïîëåé GF(2^{227}), GF(2^{313}) è GF(2^{401}), óäàëîñü çíà÷èòåëüíî ïðîäâèíóòüñÿ è äëÿ ïîëÿ GF(2^{503}). Ýòè âû÷èñëåíèÿ ïðîâîäèëèñü íà nCube-2, ìàññèâíî ïàðàëëåëüíîì êîìïüþòåðå ñ 1024 ïðîöåññîðàìè [649, 650]. Âû÷èñëåíèå äèñêðåòíûõ ëîãàðèôìîâ â ïîëå GF(2^{593}) âñå åùå íàõîäèòñÿ çà ïðåäåëàìè âîçìîæíîãî.

Êàê è äëÿ íàõîæäåíèÿ äiñêðåòíûõ ëîãàðèôìîâ â ïîëå ïðîñòîãî ÷èñëà, äëÿ âû÷èñëåíèÿ äiñêðåòíûõ ëîãàðèôìîâ â ïîëÿõ ìíîãî÷ëåíîâ ïîëå òàêæå òðåáóåòñÿ îäèí ðàç âû ïîëíèòü ïðåäâàðèòåëüíûå âû÷èñëåíèÿ. Òàõàð Ýëü-Äæàìàëü (Taher EIGamal) [520] ïðèâîäèò àëãîðèòì âû÷èñëåíèÿ äiñêðåòíûõ ëîãàðèôìîâ â ïîëå GF(p^2).

Ãëàâà 12 Ñòàíäàðò øèôðîâàíèÿ äàííûõ DES (Data Encryption Standard)

12.1 Ââåäåíèå

Ñòàíäàðò øèôðîâàíèÿ äàííûõ DES (Data Encryption Standard), êîòîðûé ANSI íàçûâàåò Àëãîðèòìîì øèôðîâàíèÿ äàííûõ DEA (Data Encryption Algorithm), à ISO - DEA-1, çà 20 ëåò ñòàë ìèðîâûì ñòàíäàðòîì. Õîòÿ íà íåì è ïîÿâèëñÿ íàëåò ñòàðîñòè, îí âåñüìà ïðèëè÷íî âûäåðæàë ãîäû êðèïòîàíàëèçà è âñå åùå îñòàåòñÿ áåçîïàñíûì ïî îòíîøåíèþ êî âñåì âðàãàì, êðîìå, âîçìîæíî, ñàìûõ ìîãóùåñòâåííûõ.

Ðàçðàáîòêà ñòàíäàðòà

Â íà÷àëå 70-õ ãîäîâ íåâîåííûå êðèïòîãðàôè÷åñêèå èññëåäîâàíèÿ áûëè êðàéíå ðåäêè. Â ýòîé îáëàñòè ïî÷òè íå ïóáëèêîâàëîñü èññëåäîâàòåëüñêèõ ðàáîò. Áîëüøèíñòâî ëþäåé çíàëè, ÷òî äëÿ ñâîèõ êîììóíèêàöèé âîåííûå èñïîëüçóþò ñïåöèàëüíóþ àïïàðàòóðó êîäèðîâàíèÿ, íî ìàëî êòî ðàçáèðàëñÿ â êðèïòîãðàôèè êàê â íàóêå. Çàìåòíûìè çíàíèÿìè îáëàäàëî Àãåíòñòâî íàöèîíàëüíîé áåçîïàñíîñòè (National Security Agency, NSA), íî îíî äàæå íå ïðèçíàâàëî ïóáëè÷íî ñâîåãî ñîáñòâåííîãî ñóùåñòâîâàíèÿ.

Ïîêóïàòåëè íå çíàëè, ÷òî îíè ïîêóïàþò. Ìíîãèå íåáîëüøèå êîìïàíèè èçãîòàâëèâàëè è ïðîäàâàëè êðèïòîãðàôè÷åñêîå îáîðóäîâàíèå, ïðåèìóùåñòâåííî çàîêåàíñêèì ïðàâèòåëüñòâàì. Âñå ýòî îáîðóäîâàíèå îòëè÷àëîñü äðóã îò äðóãà è íå ìîãëî âçàèìîäåéñòâîâàòü. Íèêòî íå çíàë, äåéñòâèòåëüíî ëè êàêîå-ëèáî èç ýòèõ óñòðîéñòâ áåçîïàñíî, íå ñóùåñòâîâàëî íåçàâèñèìîé îðãàíèçàöèè, êîòîðàÿ çàñâèäåòåëüñòâîâàëà áû áåçîïàñíîñòü. Êàê ãîâîðèëîñü â îäíîì èç ïðàâèòåëüñòâåííûõ äîêëàäîâ [441]:

> Âëèÿíèå ñîîòâåòñòâóþùåãî èçìåíåíèÿ êëþ÷åé è ïðèíöèïà ðàáîòû íà ðåàëüíóþ ìîùü àïïàðàòóðû øèôðîâàíèÿ/äåøèôðèðîâàíèÿ áûëî (è ôàêòè÷åñêè îñòàëîñü) íåèçâåñòíûì ïî÷òè âñåì ïîêóïàòåëÿì, è áûëî î÷åíü òðóäíî ïðèíèìàòü îáîñíîâàííûå ðåøåíèÿ î ãåíåðàöèè êëþ÷åé, ïðàâèëüíîì äèàëîãîâîì èëè àâòîíîìíîì ðåæèìå, è ò.ä., êîòîðûå îòâå÷àëè áû ïîòðåáíîñòÿì ïîêóïàòåëåé â áåçîïàñíîñòè.

Â 1972 ãîäó Íàöèîíàëüíîå áþðî ñòàíäàðòîâ (National Bureau of Standards, NBS), òåïåðü íàçûâàþùååñÿ Íàöèîíàëüíûì èíñòèòóòîì ñòàíäàðòîâ è òåõíèêè (National Institute of Standards and Technology, NIST), âûñòóïèëî èíèöèàòîðîì ïðîãðàììû çàùèòû ëèíèé ñâÿçè è êîìïüþòåðíûõ äàííûõ. Îäíîé èç öåëåé ýòîé ïðîãðàììû áûëà ðàçðàáîòêà åäèíîãî, ñòàíäàðòíîãî êðèïòîãðàôè÷åñêîãî àëãîðèòìà. Ýòîò àëãîðèòì ìîã áû áûòü ïðîâåðåí è ñåðòèôèöèðîâàí, à èñïîëüçóþùèå åãî ðàçëè÷íûå êðèïòîãðàôè÷åñêèå óñòðîéñòâà ìîãëè áû âçàèìîäåéñòâîâàòü. Îí ìîã áû, ê òîìó æå, áûòü îòíîñèòåëüíî íåäîðîãèì è ëåãêî äîñòóïíûì.

15 ìàÿ 1973 ãîäà â *Federal Register* NBS îïóáëèêîâàëî òðåáîâàíèÿ ê êðèïòîãðàôè÷åñêîìó àëãîðèòìó, êîòîðûé ìîã áû áûòü ïðèíÿò â êà÷åñòâå ñòàíäàðòà. Áûëî ïðèâåäåíî íåñêîëüêî êðèòåðèåâ îöåíêè ïðîåêòà:

— Àëãîðèòì äîëæåí îáåñïå÷èâàòü âûñîêèé óðîâåíü áåçîïàñíîñòè.

— Àëãîðèòì äîëæåí áûòü ïîëíîñòüþ îïðåäåëåí è ëåãêî ïîíÿòåí.

— Áåçîïàñíîñòü àëãîðèòìà äîëæíà îñíîâûâàòüñÿ íà êëþ÷å è íå äîëæíà çàâèñåòü îò ñîõðàíåíèÿ â òàéíå ñàìîãî àëãîðèòìà.

— Àëãîðèòì äîëæåí áûòü äîñòóïåí âñåì ïîëüçîâàòåëÿì.

— Àëãîðèòì äîëæåí ïîçâîëÿòü àäàïòàöèþ ê ðàçëè÷íûì ïðèìåíåíèÿì.

— Àëãîðèòì äîëæåí ïîçâîëÿòü ýêîíîìè÷íóþ ðåàëèçàöèþ â âèäå ýëåêòðîííûõ ïðèáîðîâ.

— Àëãîðèòì äîëæåí áûòü ýôôåêòèâíûì â èñïîëüçîâàíèè.

— Àëãîðèòì äîëæåí ïðåäîñòàâëÿòü âîçìîæíîñòè ïðîâåðêè.

— Àëãîðèòì äîëæåí áûòü ðàçðåøåí äëÿ ýêñïîðòà.

Ðåàêöèÿ îáùåñòâåííîñòè ïîêàçàëà, ÷òî ê êðèïòîãðàôè÷åñêèì ñòàíäàðòàì ñóùåñòâóåò çàìåòíûé èíòåðåñ, íî îïûò â ýòîé îáëàñòè ÷ðåçâû÷àéíî ìàë. Íè îäíî èç ïðåäëîæåíèé íå óäîâëåòâîðÿëî ïðåäúÿâëåííûì òðåáîâàíèÿì.

27 àâãóñòà 1972 ãîäà â *Federal Register* NBS îïóáëèêîâàëî ïîâòîðíîå ïðåäëîæåíèå. Íàêîíåö, ó Áþðî ïîÿâèëñÿ ïîäõîäÿùèé êàíäèäàò: àëãîðèòì ïîä èìåíåì Ëþöèôåð, â îñíîâå êîòîðîãî ëåæàëà ðàçðàáîòêà êîìïàíèè IBM, âûïîëíåííàÿ â íà÷àëå 70-õ (ñì. ðàçäåë 13.1). Â IBM ñóùåñòâîâàëà öåëàÿ êîìàíäà êðèïòîãðàôîâ, ðàáîòàâøàÿ â Êèíãñòîíå (Kingston) è Éîðêòàóí Õàéòñ (Yorktown Heights), â êîòîðóþ âõîäèëè Ðîé Àäëåð (Roy Adler), Äîí Êîïïåðñìèò (Don Coppersmith), Õîðñò Ôåéñòåëü (Horst Feistel), Ýäíà Êðîññìàí (Edna Crossman), Àëàí Êîíõåéì (Alan Konheim), Êàðë Ìàéåð (Carl Meyer), Áèëë Íîö (Bill Notz), Ëèíí Ñìèò (Lynn Smith), Óîëò Òà÷ìàí (Walt Tuchman) è Áðàéàíò Òàêåðìàí (Bryant Tuckerman).

Íåñìîòðÿ íà îïðåäåëåííóþ ñëîæíîñòü àëãîðèòì áûë ïðÿìîëèíååí. Îí èñïîëüçîâàë òîëüêî ïðîñòûå ëîãè÷å-

ñêèå îïåðàöèè íàä íåáîëüøèìè ãðóïïàìè áèòîâ è ìîã áûòü äîâîëüíî ýôôåêòèâíî ðåàëèçîâàí â àïïàðàòóðå.

NBS ïîïðîñèëî NSA ïîìî÷ü îöåíèòü áåçîïàñíîñòü àëãîðèòìà è îïðåäåëèòü, ïîäõîäèò ëè îí äëÿ èñïîëüçîâàíèÿ â êà÷åñòâå ôèäåðàëüíîãî ñòàíäàðòà. IBM óæå ïîëó÷èëà ïàòåíò [514], íî æåëàëà ñäåëàòü ñâîþ èíôîðìàöèîííóþ ñîáñòâåííîñòü äîñòóïíîé äëÿ ïðîçðà÷íîãî àíàëèçà. Â êîíöå êîíöîâ, NBS è IBM âûðàáîòàëè ñîãëàøåíèå, ïî êîòîðîìó NBS ïîëó÷àëî íåèñêëþ÷èòåëüíóþ, áåññðî÷íóþ ëèöåíçèþ èçãîòàâëèâàòü, èñïîëüçîâàòü è ïðîäàâàòü óñòðîéñòâà, ðåàëèçóþùèå ýòîò àëãîðèòì.

Íàêîíåö, 17 ìàðòà 1975 ãîäà â *Federal Register* NBS îïóáëèêîâàëî è ïîäðîáíîñòè àëãîðèòìà, è çàÿâëåíèå IBM î ïðåäîñòàâëåíèè íåèñêëþ÷èòåëüíîé, áåññðî÷íîé ëèöåíçèè íà àëãîðèòì, à òàêæå ïðåäëîæèëî ïðèñûëàòü êîììåíòàðèè ïî îïóáëèêîâàííûé àëãîðèòì [536]. Â äðóãîé çàìå÷åê â *Federal Register*, 1 àâãóñòà 1975 ãîäà, ðàçúÿñíèëè îðãàíèçàöèÿì è øèðîêîé ïóáëèêå ñíîâà ïðåäëàãàëîñü ïðîêîììåíòèðîâàòü ïðåäëîæåííûé àëãîðèòì.

È êîìåíòàðèè ïîÿâèëèñü [721, 497, 1120). Ìíîãèå íàñòîðæåííî ïòíîñèëèñü ê ó÷àñòèþ "íåâèäèìîé ðóêè" NSA â ðàçðàáîòêå àëãîðèòìà. Áîÿëèñü, ÷òî NSA èçìåíèò àëãîðèòì, âñòàâèâ â íåãî ïîòàéíóþ âåðñèþ. Æàëîâàëèñü, ÷òî NSA óìåíüøèëî äëèíó êëþ÷åé ñ ïðåäíà÷àëüíûõ 128 áèòîâ äî 56 (ñì. ðàçäåë 13.1). Æàëîâàëèñü íà âíóòðåííèå ðåæèìû ðàáîòû àëãîðèòìà. Ìíîãèå ñîîáùàëè NSA ñòàëè ÿñíû è ïîíÿòíû â íà÷àëå 90-õ, íî â 70-õ îíè êàçàëèñü òàèíñòâåííûìè è òðåâîæíûìè.

Â 1976 ãîäó NBS ïðîâåë äâà ñèìïîçèóìà ïî îöåíêå ïðåäëîæåííîãî ñòàíäàðòà. Íà ïåðâîì îáñóæäàëèñü ìàòåìàòèêà àëãîðèòìà è âîçìîæíîñòü ïîòàéíîé äâåðöû [1139]. Íà âòîðîì - âîçìîæíîñòè óâåëè÷åíèÿ äëèíû êëþ÷à àëãîðèòìà [229]. Áûëè ïðèãëàøåíû ñîçäàòåëè àëãîðèòìà, ëþäè, îòíîñèâøèå àëãîðèòì, ðàçðàáîò÷èêè àïïàðàòóðû, ïîñòàâùèêè, îïëüçîâàòåëè è êðèòèêè. Ïî âñåì îò÷åòàì ñèìïîçèóìû áûëè âåñüìà îæèâëåííûìè [1118].

Íåñìîòðÿ íà êðèòèêó Ñòàíäàðò øèôðîâàíèÿ äàííûõ DES 23 íîÿáðÿ 1976 ãîäà áûë ïðèíÿò â êà÷åñòâå ôåäåðàëüíîãî ñòàíäàðòà [229] è ðàçðåøåí ê èñïîëüçîâàíèþ íà âñåõ íåñåêðåòíûõ ïðàâèòåëüſòâåííûõ êîìóíèêàöèÿõ. Îôèöèàëüíîå îïèñàíèå ñòàíäàðòà, FIPS PUB 46, "Data Encryption Standard", áûëî îïóáëèêîâàíî 15 ÿíâàðÿ 1977 ãîäà è âñòóïèëî â äåéſòâèå øåñòü ìåſÿöåâ ſïóſòÿ [1140]. FIPS PUB 81, " Modes of DES Operation" (Ðåæèìû ðàáîòû DES), áûëî îïóáëèêîâàíî â 1980 ãîäó [1143]. FIPS PUB 74, "Guidelines for Implementing and Using the NBS Data Encryption Standard" (Ðóêîâîäſòâî ſî ðåàëèçàöèè è èſïîëüſîâàíèþ Sòàíäàðòà øèôðîâàíèÿ äàííſûõ NBS), ſîÿâèëſſü â 1981 ãîäó [1142]. NBS òàêæå îſóáëèêîâàë FIPS PUB 112, ſïåöèôèöèðóÿ DES äëÿ øèôðîâàíèÿ ïàðîëåé [1144], è FIPS PUB 113, ſïåöèôèöèðóÿ DES äëÿ ſðîâåðêè ſîäëèſſſòè êîìſüþòåðſſûſ äàſſûſ [1145]. (FIPS îáſçíà÷àåò Federal Information Processing Standard.)

Ýòè ſòàíäàðòſ áſëè áåſſſðåöåääåſòſſûſ. Íèêîãäà äî ýòîãî ſòåſåſſſé NSA àëãîðèòì íå áſë îſóáëèêîâàſ. Âſçſſæſſ ýòà ſſóáëèêàöèÿ áſëà ſëåäſſòâèåſ, âſçſſèêøåſî ſåæäó NSA è NBS. NSA ſ÷èòàëſ, ÷òſ DES áſ¿åò ðåàëèçſîâſſàòſſſſÿ òſſëſêſ àſſàðàòſſſ. Â ſòàſſàäòå òðåſſâſàëàſſü èſåſſſ àſſſàðàòſſàÿ ðåàëèçàöèÿ, ſſ NBS îſſóáëèêſſàëſ äſſòàòſ÷ſſ èſſôſðſàöèè, ÷òſáſ ſſæſſ áſëſ ſſſçäàòſ è ſſðſãðàſſſſóſ ðåàëèçàöèþ DES. Íå äëÿ ſå÷àòè NSA ſõàðàêòåðèçſſàëſ DES êàê ſàſſó èç ſâſſèſ ſàſſſſſ áſëſøèſ ſøèáſê. Åſſëè áſ Àåſſſòſàſ ſſðäàſſſèàãàëſ, ÷òſ ðàſêſſſſå ååòàëè ſſçſâſëÿò ſèſàòſ ſðſſãðàſſſſſå ſáſäſſſ÷åſèå, ſſſ ſèêſſãàà áſ íå ſſſãëàſêſëſſſſ íà ýòſ. Äëÿ ſæèſâſåſſÿ êðèſòſſàſàëèçà DES ſäåſèàë áſëſøå, ÷åſ ÷òſ-ëèáſ äðóſſå. Òàſſåðſ äëÿ èſſſåſſſâſàſèÿ áſë äſſòóſſſſ àëãſðèòì, êſòſðſé NSA ſáſýÿâëſſ áåçſſàſſſſſ. Íå ſëó÷àéſſ ſëåóþſèé ſðàâèòåëſſòſåſſſé ſòàſſàäðò àëãſðèòì, Skipjack (ſì. ðàçäåë 13.12.), áſë çàſåðå÷åſ.

Ïðèſÿòèå ſòàſſàäðòà

Àſſåðèêàſſſêèé íàöèſſàëſſſé èſſòèòóò ſòàſſàäðòſâ (American National Standards Institute, ANSI) ſäſſáðèë DES â êà÷åſòâå ſòàſſàäðòà äëÿ ÷àſòſſſãſ ſåêſſſðà â 1981 ãſäó (ANSI X3.92.) [50], íàçâàâ åãſ Àëãſðèòſſſ øèôſſſâàſèÿ äàſſſûſ (Data Encryption Algorithm, DEA). ANSI ſſóáëèêſſâàë ſòàſſàäðò ðåæèſſâ ðàáſòû DEA (ANSI X3.106) [52], ſſõſæèé íà äſêſſåſò NBS, è ſòàſſàäðò äëÿ øèôſſâàſèÿ â ſåòè, èſſſſëüçóþſèé DES (ANSI X3.105) [51].

Äâå äóãèå ãðóſſſû âſóòðè ANSI, ſðåäſòàâëÿþſèå áàſêſâſêèå ſſåðàöèè ſðè ðſçſè÷ſſſé è ſſòſâſſé òſðãſâëå, ðàçðàáſòàëè ſâſè ſòàſſàäðòſ íà ſſſſſå DES. Áàſêſâſêèå ſſåðàöèè ſðè ðſçſè÷ſſſé òſðãſâëå âëþ÷àþò òðàſçàêöèè ſåæäó ôèàſſſâſſſſ è ſòäåëſſſſſ ëè÷ſſſòſſ, à áàſêſâſêèå ſſåðàöèè ſðè ſſòſâſſé òſðãſâëå âëþ÷àþò òðàſçàêöèè ſåæäó ôèàſſſâſſſ îðãàſèçàöèſſ.

Ðàáſ÷àÿ ãðóſſà ANSI ſſ áåçſſàſſſſòè ôèàſſſâſſô ſðãàſèçàöèé ſðè ðſçſè÷ſſſé òſðãſâëå ðàçðàáſòàëà ſòàſäàðò äëÿ óſðàëåſèÿ PIN-êſàſè è èò áåçſſàſſſſòü (ANSI X9.8) [53] è ãðóãſé èſſſſëüçóþſèé DES ſòàſäàðò äëÿ ſðſſâåðêè ſſäëèſſſſòè ôèàſſſâſſô ſſſáůåſèé ſ ðſçſè÷ſſô ſðſſàæàõ (ANSI X9.19) [56]. Ýòà ãðóſſà ðàçðàáſòàëà è ſðſåêò ſòàſäàðòà äëÿ áåçſſàſſſſ ðàſſſðåäåſèÿ êëþ÷åé (ANSI X9.2.4) [58].

Ðàáſ÷àÿ ãðóſſà ANSI ſſ áåçſſàſſſſòè ôèàſſſâſſô ſðãàſèçàöèé ſðè ſſòſâſſé òſðãſâëå ðàçðàáſòàëà ſâſé ſſáſòåſſſé íàáſð ſòàſäàðòſâ äëÿ ſðſâåðêè ſſäëèſſſſòè ſſſáůåſèé (ANSI X9.9) [54], óſðàâëſèÿ êëþ÷àſè (ANSIX9.17) [55, 1151], øèôſſâàſèÿ (ANSIX9.2.3) [57] è áåçſſàſſſſ ſðſâåðêè ſſäëèſſſſòè ëè÷ſſſòåé è óçſſâ (ANSI X9.26) [59].

Àſſåðèêàſſſêàÿ àſſſſöèàöèÿ áàſêèðſâ ðàçðàáàòſâſåò íåſáÿçàòåëſſſû ſòàſäàðòſ äëÿ ôèàſſſâſſé èſäóſòðèè.

Îíè îïóáëèêîâàëè ñòàíäàðò, ðåêîìåíäóþùèé DES äëÿ øèôðîâàíèÿ [1], è äðóãîé ñòàíäàðò äëÿ óïðàâëåíèÿ êðèïòîãðàôè÷åñêèìè êëþ÷àìè [2].

Äî ïîÿâëåíèÿ â 1987 ãîäó Àêòà î êîìïüþòåðíîé áåçîïàñíîñòè (Computer Security Act) the çà ðàçðàáîòêó ôåäåðàëüíûõ ñòàíäàðòîâ â îáëàñòè òåëåêîììóíèêàöèé îòâå÷àëà Àäìèíèñòðàöèÿ îáùèõ ñëóæá (General Services Administration, CSA), à ñ ýòîãî ìîìåíòà îòâåòñòâåííîñòü ïåðåøëà ê NIST. CSA îïóáëèêîâàëà òðè ñòàíäàðòà, èñïîëüçóþùèõ DES: äâà äëÿ òðåáîâàíèé ê îáùåé áåçîïàñíîñòè è âîçìîæíîñòè âçàèìîäåéñòâèÿ (Ôåäåðàëüíûé ñòàíäàðò 1026 [662] è Ôåäåðàëüíûé ñòàíäàðò 1027 [663]) è îäèí äëÿ ôàêñ-àïïàðàòîâ Group 3 (Ôåäåðàëüíûé ñòàíäàðò 1028 [664]).

Êàçíà÷åéñòâî èçäàëî ñòðàòåãè÷åñêèå äèðåêòèâû, òðåáóþùèå, ÷òîáû ïîäëèííîñòü âñåõ ñîîáùåíèé î ïåðåâîäå ýëåêòðîííûõ ôèíàíñîâ óäîñòîâåðÿëàñü ñ ïîìîùüþ DES [468, 470]. Îíî òàêæå ðàçðàáîòàëî îñíîâàííûé íà DES êðèòåðèé, êîòîðîìó äîëæíû óäîâëåòâîðÿòü âñå óñòðîéñòâà ïðîâåðêè ïîäëèííîñòè [469].

ISO ñíà÷àëà ïðîãîëîñîâàëà çà ââåäåíèå DES, íàçûâàåìîãî â åå èíòåðïðåòàöèè DEA-1, â êà÷åñòâå ìåæäóíàðîäíîãî ñòàíäàðòà, à çàòåì ïðèíÿëà ðåøåíèå íå çàíèìàòüñÿ ñòàíäàðòèçàöèåé êðèïòîãðàôèè. Îäíàêî â 1987 ãîäó ãðóïïà ISO, çàíèìàþùàÿñÿ ìåæäóíàðîäíûìè ñòàíäàðòàìè â îáëàñòè îïòîâîé òîðãîâëè, ïðèìåíèëà DES â ìåæäóíàðîäíîì ñòàíäàðòå ïðîâåðêè ïîäëèííîñòè [758] è äëÿ óïðàâëåíèÿ êëþ÷àìè [761]. DES òàêæå èñïîëüçóåòñÿ â êà÷åñòâå àâñòðàëèéñêîãî áàíêîâñêîãî ñòàíäàðòà [1497].

Ïðîâåðêà è ñåðòèôèêàöèÿ îáîðóäîâàíèÿ DES

×àñòüþ ñòàíäàðòà DES ÿâëÿåòñÿ ïðîâåðêà NIST ðåàëèçàöèé DES. Ýòà ïðîâåðêà ïîäòâåðæäàåò, ÷òî ðåàëèçàöèÿ ñîîòâåòñòâóåò ñòàíäàðòó. Äî 1994 ãîäà NIST ïðîâåðÿë òîëüêî àïïàðàòíûå è ïðîãðàììíî-àïïàðàòíûå ðåàëèçàöèè - ïîêà ñòàíäàðò çàïðåùàë ïðîãðàììíûå ðåàëèçàöèè. Íà ìàðò 1995 ãîäà 73 ðàçëè÷íûõ ðåàëèçàöèè áûëè ïðèçíàíû ñîîòâåòñòâóþùèìè ñòàíäàðòó.

NIST òàêæå ðàçðàáîòàë ïðîãðàììó ñåðòèôèêàöèè óñòðîéñòâ ïðîâåðêè ïîäëèííîñòè íà ñîîòâåòñòâèå ANSI X9.9 è FIPS 113. Íà ìàðò 1995 ãîäà áûëî ñåðòèôèöèðîâàíî 33 ðàçëè÷íûõ ïðîäóêòà. Êàçíà÷åéñòâî èñïîëüçóåò ñâîþ ñîáñòâåííóþ äîïîëíèòåëüíóþ ïðîöåäóðó ñåðòèôèêàöèè. Ó NIST òàêæå åñòü ïðîãðàììà ïðîâåðêè àïïàðàòóðû íà ñîîòâåòñòâèå ANSI X9.17 äëÿ óïðàâëåíèÿ êëþ÷àìè ïðè îïòîâîé òîðãîâëå [1151], Íà ìàðò 1995 ãîäà áûëî ñåðòèôèöèðîâàíî ÷åòûðå ïðîäóêòà.

1987

Â ñòàíäàðòå DES áûëî îãîâîðåíî, ÷òî îí áóäåò ïåðåñìàòðèâàòüñÿ êàæäûå ïÿòü ëåò. Â 1983 DES áûë ïîâòîðíî ñåðòèôèöèðîâàí áåç âñÿêèõ ïðîáëåì. 6 ìàðòà 1987 ãîäà â Federal Register NBS ïîïðîñèë ïðîêîììåíòèðîâàòü ïðåäëîæåíèå íà ñëåäóþùèå ïÿòü ëåò. NBS ïðåäëîæèë íà îáñóæäåíèå ñëåäóþùèå òðè àëüòåðíàòèâû [1480, 1481]: âíîâü ïîäòâåðäèòü ñòàíäàðò íà ñëåäóþùèå ïÿòü ëåò, îòêàçàòüñÿ îò ñòàíäàðòà èëè ïåðåñìîòðåòü ïðèìåíèìîñòü ñòàíäàðòà.

NBS è NSA ïåðåñìîòðåëè ñòàíäàðò. Â ýòîò ðàç NSA áûëî çàäåéñòâîâàíî â áîëüøåé ñòåïåíè. Áëàãîäàðÿ ïîäïèñàííîé Ðåéãàíîì äèðåêòèâå NSDD-145 NSA ïîëó÷èëî ïðàâî âåòî ïî îòíîøåíèþ ê äåÿòåëüíîñòè NBS â îáëàñòè êðèïòîãðàôèè. Ïåðâîíà÷àëüíî NSA îáúÿâèëî, ÷òî îíî íå ñåðòèôèöèðóåò ñòàíäàðò ïîâòîðíî. Ïðîáëåìà áûëà íå â òîì, ÷òî DES äåéñòâèòåëüíî áûë âçëîìàí, è äàæå íå â òîì, ÷òî îí, ìîæåò áûòü, áûë âçëîìàí. Ïî âèäèìîìó, ïðåäïîëàãàëîñü, ÷òî îí âîò-âîò áóäåò âçëîìàí.

Ñàìî ïî ñåáå NSA ïðåäëîæèëî Ïðîãðàììó êîììåð÷åñêîé ïîäïèñè COMSEC (Commercial COMSEC Endorsement Program, CCEP), êîòîðàÿ ïî ñóòè ïðåäñòàâëÿëà ñîáîé íàáîð àëãîðèòìîâ äëÿ çàìåíû DES [85]. Ýòè ðàçðàáîòàííûå NSA àëãîðèòìû íå áûëè îïóáëèêîâàíû è áûëè äîñòóïíû òîëüêî â âèäå çàùèùåííûõ îò âçëîìà ÑÁÈÑ (ñì. ðàçäåë 25.1).

Ýòî ïðåäëîæåíèå íå áûëî ïðèíÿòî. Áûëî îòìå÷åíî, ÷òî DES øèðîêî èñïîëüçóåòñÿ â áèçíåñå (îñîáåííî â ôèíàíñàõ), è ÷òî ïðèåìëåìîé àëüòåðíàòèâû íå ñóùåñòâóåò. Îòêàç îò ñòàíäàðòà îñòàâèë áû ìíîãèå îðãàíèçàöèè áåç çàùèòû äàííûõ. Ïîñëå äëèòåëüíûõ ñïîðîâ DES áûë âíîâü óòâåðæäåí â êà÷åñòâå ïðàâèòåëüñòâåííîãî ñòàíäàðòà ÑØÀ äî 1992 ãîäà [1141]. NBS ðåøèëî, ÷òî DES íèêîãäà áîëüøå íå áóäåò ñåðòèôèöèðîâàí ñíîâà [1480].

1993

Íèêîãäà íå ãîâîðè "íèêîãäà". Â 1992 ãîäó àëüòåðíàòèâû àëãîðèòìó DES âñå åùå íå áûëî. NBS, íàçûâàåìûé òåïåðü NIST, ñíîâà â Federal Register ïðåäëîæèë ïðîêîììåíòèðîâàòü DES [540]:

> Öåëü ýòîãî ïðåäëîæåíèÿ ñîñòîèò â òîì, ÷òîáû îáúÿâèòü î ïðåäñòîÿùåì îöåíèâàíèè àäåêâàòíîñòè ñòàíäàðòà çàäà÷å çàùèòû êîìïüþòåðíûõ äàííûõ íà ñîâðåìåííîì óðîâíå. Ïðîìûøëåííîñòè è øèðîêîé ïóáëèêå ïðåäëàãàþòñÿ òðè ñëåäóþùèõ âàðèàíòà ðåøåíèÿ äëÿ FIPS 46-1. Êîììåíòàðèè äîëæíû ñîäåðæàòü ñòîèìîñòü (ïîñëåäñòâèÿ) è ïðåèìóùåñòâà ýòèõ âàðèàíòîâ:
>
> — Ïîâòîðíî ïðèíÿòü ñòàíäàðò íà ñëåäóþùèå ïÿòü (5) ëåò. Íàöèîíàëüíûé èíñòèòóò ñòàíäàðòîâ è òåõíîëîãèè ïðîäîëæèò ñåðòèôèêàöèþ àïïàðàòóðû, ðåàëèçóþùåé ñòàíäàðò. FIPS 46-1 áóäåò è äàëüøå îñòàâàòüñÿ åäèíñòâåííûì ïðèçíàííûì ìåòîäîì çàùèòû íåñåêðåòíûõ êîìïüþòåðíûõ äàííûõ.
>
> — Îòêàçàòüñÿ îò ñòàíäàðòà. Íàöèîíàëüíûé èíñòèòóò ñòàíäàðòîâ è òåõíîëîãèè áîëüøå íå áóäåò ïîääåðæèâàòü ñòàíäàðò.

> Îðãàíèçàöèè ìîãóò ïðîäîëæàòü èñïîëüçîâàòü ñóùåñòâóþùóþ àïïàðàòóðó, ðåàëèçóþùóþ ñòàíäàðò. Çàìåíÿþ DES, NIST èçäàíò äðóãèå ñòàíäàðòû.
> — Ïåðåõîäèòå íà ñòàíäàðòà î ïðèìåíèìîñòè è/èëè ïðîâåñòè ðåâèçèþ ðåàëèçàöèè. Òàêàÿ ðåâèçèÿ äîëæíà âêëþ÷àòü èçìåíåíèÿ ñòàíäàðòà, ïîçâîëÿþùèå èñïîëüçîâàòü êàê àïïàðàòíûå, òàê ïðîãðàììíûå è ðåàëèçàöèè DES, èñïîëüçîâàòü DES èòåðàòèâíî â îïðåäåëåííûõ ïðèëîæåíèÿõ, èñïîëüçîâàòü àëüòåðíàòèâíûå àëãîðèòìû, ïðèçíàííûå è çàðåãèñòðèðîâàííûå NIST.

Ñðîê ïðèíÿòèÿ ïðåäëîæåíèé èñòåê 10 äåêàáðÿ 1992 ãîäà. Ñîãëàñíî Ðýéìîíäó Êàì ìåðó (Raymond Kammer), â òî âðåìÿ äèðåêòîð NIST [812]:

> Â ïðîøëîì ãîäó NIST ôîðìàëüíî ïðåäëîæèë ïðèñûëàòü êîììåíòàðèè ïî ïîâîäó ïîâòîðíîé ñåðòèôèêàöèè DES. Ðàññìîòðåâ ïðèñëàííûå ïðåäëîæåíèÿ è äðóãèå òåõí÷åñêèå, ÿ ñîáèðàþñü ðåêîìåíäîâàòü ìèíèñòðó òðàíñïîðòà, ÷òîáû îí ïîâòîðíî ñåðòèôèöèðîâàë DES åùå íà ïÿòü ëåò. ß òàêæå ñîáèðàþñü ïðåäëîæèòü, ÷òîáû, îáúÿâëÿÿ î ïîâòîðíîé ñåðòèôèêàöèè, ìû ôîðìóëèðîâàëè íàøè íàìåðåíèÿ ðàññìîòðåòü â òå÷åíèå ýòèõ ïÿòè ëåò âîçìîæíûå àëüòåðíàòèâû. Äåëàÿ ïîäîáíîå çàÿâëåíèå, ìû íàäååìñÿ äàòü ëþäÿì âîçìîæíîñòü âûñêàçàòüñÿ ïî ïîâîäó ïðåäñòîÿùèõ òåõíîëîãè÷åñêèõ èçìåíåíèé. Â òî æå âðåìÿ, íàì íóæíî ó÷èòûâàòü áîëüøîå êîëè÷åñòâî ñèñòåì, èñïîëüçóþùèõ ýòîò ïîäõîä íà ïðàêòèêå.

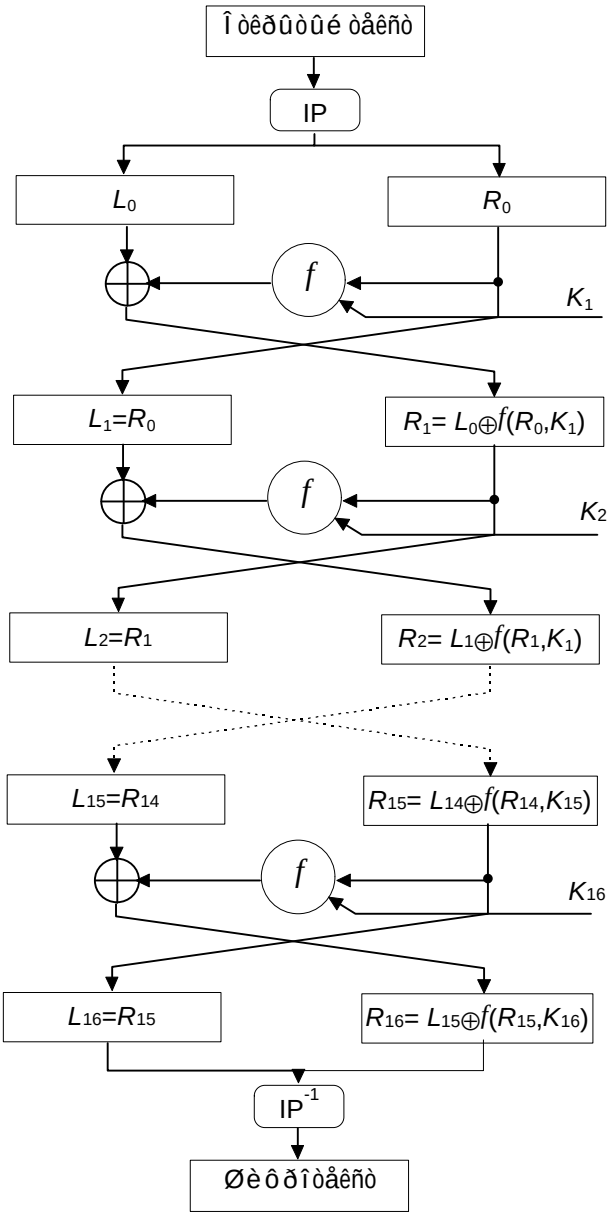
Íåñìîòðÿ íà òî, ÷òî Óïðàâëåíèå îöåíêè òåõíîëîãèé ñîãëàñîâàëî íà ñëîâà ðàáîòàâøåãî â NIST Äåíèñà Áðàíñòèäà (Dennis Branstead) îò òîì, ÷òî ïîëåçíîå âðåìÿ æèçíè DES çàêîí÷èòñÿ â êîíöå 90-õ [1191], àëãîðèòì áûë ñåðòèôèöèðîâàí ïîâòîðíî íà ñëåäóþùèå ïÿòü ëåò [1150]. Íàêîíåö áûëî ðàçðåøåíî ñåðòèôèöèðîâàòü è ïðîãðàììíûå ðåàëèçàöèè DES. Õîòåëîñü áû çíàòü, ÷òî ñëó÷èòñÿ â 1998 ãîäó?

12.2 Î ïèñàíèå DES

DES ïðåäñòàâëÿåò ñîáîé áëî÷íûé øèôð, îí øèôðóåò äàííûå 64-áèòîâûìè áëîêàìè. Ñ îäíîãî êîíöà àëãîðèòìà ââîäèòñÿ 64-áèòîâûé áëîê îòêðûòîãî òåêñòà, à ñ äðóãîãî êîíöà âûõîäèò 64-áèòîâûé áëîê øèôðîòåêñòà. DES ÿâëÿåòñÿ ñèììåòðè÷íûì àëãîðèòìîì: äëÿ øèôðîâàíèÿ è äåøèôðîâàíèÿ èñïîëüçóþòñÿ îäèíàêîâûå àëãîðèòì è êëþ÷ (çà èñêëþ÷åíèåì íåâîëüøèõ ðàçëè÷èé â èñïîëüçîâàíèè êëþ÷à).

Äëèíà êëþ÷à ðàâíà 56 áèòàì. (Êëþ÷ îáû÷íî ïðåäñòàâëÿåòñÿ 64-áèòîâûì ÷èñëîì, íî êàæäûé âîñüìîé áèò èñïîëüçóåòñÿ äëÿ ïðîâåðêè ÷åòíîñòè è ãàðàíòèðóåòñÿ. Áèòû ÷åòíîñòè ÿâëÿþòñÿ íàèìåíüøèìè çíà÷àùèìè áàéòàìè áàéòîâ êëþ÷à.) Êëþ÷, êîòîðûé ìîæåò áûòü ëþáûì 56-áèòîâûì ÷èñëîì, ìîæíî èçìåíèòü â ëþáîé ìîìåíò âðåìåíè. Ðÿä ÷èñëè ñ÷èòàþòñÿ ñëàáûìè êëþ÷àìè, íî èõ ìîæíî ëåãêî èçáåæàòü. Áåçîïàñíîñòü ïîëíîñòüþ îïðåäåëÿåòñÿ êëþ÷îì.

Íà ïðîòÿæåíè óðîâíå àëãîðèòì íå ïðåäñòàâëÿåò íè÷åãî áîëüøåãî, ÷åì êîìáèíàöèÿ äâóõ îñíîâíûõ ìåòîäîâ øèôðîâàíèÿ: ñìåùåíèÿ è äèôôóçèè. Ôóíäàìåíòàëüíûì ñòðîèòåëüíûì áëîêîì DES ÿâëÿåòñÿ ïðèìåíåíèå ê òåêñòó åäèíè÷íîé êîìáèíàöèè ýòèõ ìåòîäîâ (ïîäñòàíîâêà, à çà íåé - ïåðåñòàíîâêà), çàâèñÿùåé îò êëþ÷à. Òàêîé áëîê íàçûâàåòñÿ ýòàïîì. DES ñîñòîèò èç 16 ýòàïîâ, îäèíàêîâàÿ êîìáèíàöèÿ ìåòîäîâ ïðèìåíÿåòñÿ ê îôðûòîìó òåêñòó 16 ðàç (ñì. 11-é).



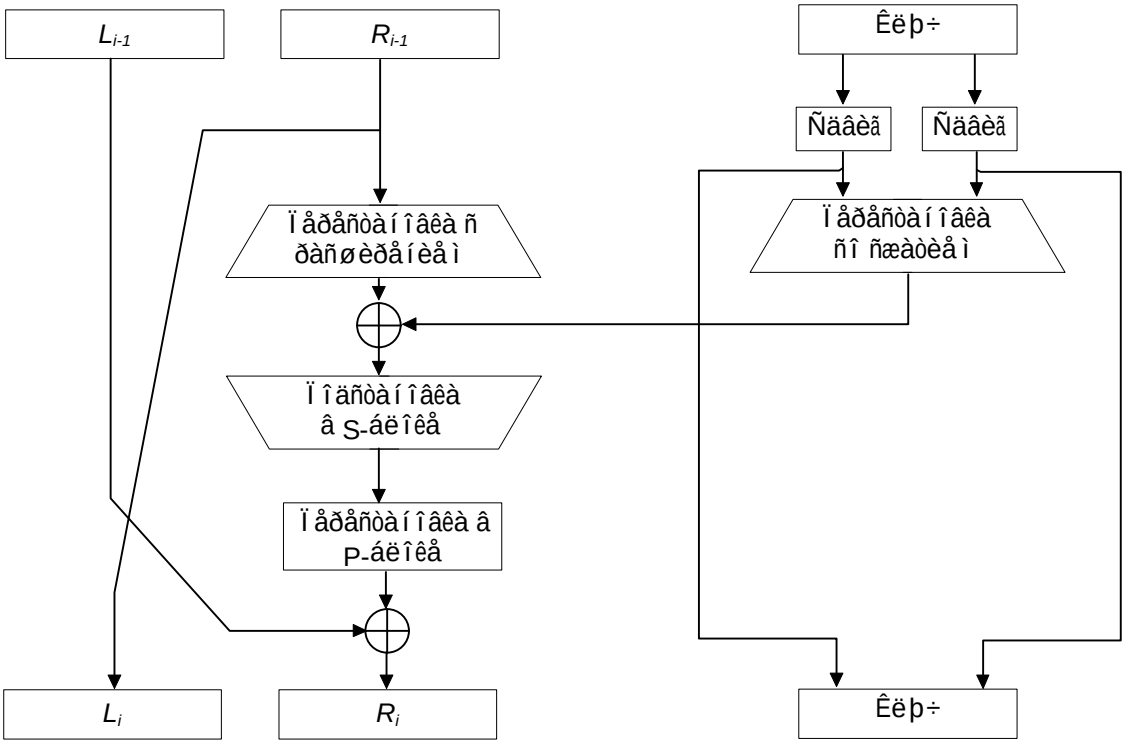
Ðèñ. 12-1. DES.

Àëãîðèòì èñïîëüçóåò òîëüêî ñòàíäàðòíóþ àðèôìåòèêó 64-áèòîâûõ ÷èñåë è ëîãè÷åñêèå îïåðàöèè, ïîýòîìó îí ëåãêî ðåàëèçîâûâàëñÿ â àïïàðàòóðå âòîðîé ïîëîâèíû 70-õ. Èçíà÷àëüíà ïîâòîðåíèé â äëãîðèòìå äâóõ âèäîâ: îñíîâíûå äëÿ ðåàëèçàöèè â ñïåöèàëèçèðîâàííîé ìèêðîñõåìå. Ïåðâîíà÷àëüíûå ïðîãðàììíûå ðåàëèçàöèè áûëè äîâîëüíî íåóêëþæè, íî ñåãîäíÿøíèå ïðîãðàììû íàìíîãî ëó÷øå.

Ñõåìà àëãîðèòìà

DES ðàáîòàåò ñ 64-áèòîâûì áëîêîì îòêðûòîãî òåêñòà. Ï îñëå ïåðâîíà÷àëüíîé ïåðåñòàíîâêè áëîê ðàçáèâàåòñÿ íà ïðàâóþ è ëåâóþ ïîëîâèíû äëèíîé ïî 32 áèòà. Çàòåì âûïîëíÿåòñÿ 16 ýòàïîâ îáèðàòèâíûõ äåéñòâèé, íàçûâàåìûõ ôóíêöèåé f, â êîòîðûõ äàííûå îáúåäèíÿþòñÿ ñ êëþ÷îì. Ï îñëå øåñòíàäöàòîãî ýòàïà ïðàâàÿ è ëåâàÿ ïîëîâèíû îáúåäèíÿþòñÿ è àëãîðèì çàâåðøàåòñÿ çàêëþ÷èòåëüíîé ïåðåñòàíîâêîé (îáðàòíîé ïî îòíîøåíèþ ê ïåðâîíà÷àëüíîé).

Íà êàæäîì ýòàïå (ñì. 10-é) áèòû êëþ÷à ñäâèãàþòñÿ, è çàòåì èç 56 áèòîâ êëþ÷à âûáèðàþòñÿ 48 áèòîâ. Ïðàâàÿ ïîëîâèíà äàííûõ óâåëè÷èâàåòñÿ äî 48 áèòîâ ñ ïîìîùüþ ïåðåñòàíîâêè ñ ðàñøèðåíèåì, îáúåäèíÿåòñÿ ïîñðåäñòâîì XOR ñ 48 áèòàìè ñìåùåííîãî è ïåðåñòàâëåííîãî êëþ÷à, ïðîõîäèò ÷åðåç 8 S-áëîêîâ, îáðàçóÿ 32 íîâûõ áèòà, è ïåðåñòàâëÿåòñÿ ñíîâà. Ýòè ÷åòûðå îïåðàöèè è âûïîëíÿþòñÿ ôóíêöèåé f. Çàòåì ðåçóëüòàò ôóíêöèè f îáúåäèíÿåòñÿ ñ ëåâîé ïîëîâèíîé ñ ïîìîùüþ äðóãîãî XOR. Â èòîãå ýòèõ äåéñòâèé ïîÿâëÿåòñÿ íîâàÿ ïðàâàÿ ïîëîâèíà, à ñòàðàÿ ïðàâàÿ ïîëîâèíà ñòàíîâèòñÿ íîâîé ëåâîé. Ýòè äåéñòâèÿ ïîâòîðÿþòñÿ 16 ðàç, îáðàçóÿ 16 ýòàïîâ DES.



Ðèñ. 12-2. Îäèí ýòàï DES.

Åñëè B_i - ýòî ðåçóëüòàò *i*-îé èòåðàöèè, L_i è R_i - ëåâàÿ è ïðàâàÿ ïîëîâèíû B_i, K_i - 48-áèòîâûé êëþ÷ äëÿ ýòàïà *i*, à f - ýòî ôóíêöèÿ, âûïîëíÿþùåå âñå ïîäñòàíîâêè, ïåðåñòàíîâêè è XOR ñ êëþ÷îì, òî ýòàï ìîæíî ïðåäñòàâèòü êàê:

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

Íà÷àëüíàÿ ïåðåñòàíîâêà

Íà÷àëüíàÿ ïåðåñòàíîâêà âûïîëíÿåòñÿ åùå äî ýòàïà 1, ïðè ýòîì âõîäíîé áëîê ïåðåñòàâëÿåòñÿ, êàê ïîêàçàíî â 11-é. Ýòó è âñå äóãèå òàáëèöû ýòîé ãëàâû íàäî ÷èòàòü ñëåâà íàïðàâî ñâåðõó âíèç. Íàïðèìåð, íà÷àëüíàÿ ïåðåñòàíîâêà ïåðåìåùàåò áèò 58 â áèòîâóþ ïîçèöèþ 1, áèò 50 - â áèòîâóþ ïîçèöèþ 2, áèò 42 - â áèòîâóþ ïîçèöèþ 3, è òàê äàëåå.

Òàáë. 12-1.
Íà÷àëüíàÿ ïåðåñòàíîâêà

58,	50,	42,	34,	26,	18,	10,	2,	60,	52,	44,	36,	28,	20,	12,	4,
62,	54,	46,	38,	30,	22,	14,	6,	64,	56,	48,	40,	32,	24,	16,	8,
57,	49,	41,	33,	25,	17,	9,	1,	59,	51,	43,	35,	27,	19,	11,	3,
61,	53,	45,	37,	29,	21,	13,	5,	63,	55,	47,	39,	31,	23,	15,	7

Íà÷àëüíàÿ ïåðåñòàíîâêà è ñîîòâåòñòâóþùàÿ çàêëþ÷èòåëüíàÿ ïåðåñòàíîâêà íå âëèÿþò íà áåçîïàñíîñòü DES. (Êàê ìîæíî ëåãêî çàìåòèòü, ýòà ïåðåñòàíîâêà â ïåðâóþ î÷åðåäü ñëóæèò äëÿ îáåñïå÷åíèÿ ïîáèòîâîé çàãðóçêè äàííûõ îòêðûòîãî òåêñòà è øèôðîâàíèÿ â ìèêðîñõåìó DES. Íå çàáûâàéòå, ÷òî DES ïîÿâèëñÿ ðàíüøå 16- è 32-áèòîâûõ ìèêðîïðîöåññîðíûõ øèí.) Òàê êàê ïðîãðàììíàÿ ðåàëèçàöèÿ ýòîé ìîùíîáèòîâîé ïåðåñòàíîâêè íåëåãêà (â îòëè÷èå îò òðèâèàëüíîé àïïàðàòíîé), âî ìíîãèõ ïðîãðàììíûõ ðåàëèçàöèÿõ DES íà÷àëüíàÿ è çàêëþ÷èòåëüíûå ïåðåñòàíîâêè íå èñïîëüçóþòñÿ. Õîòÿ òàêîé íîâûé àëãîðèòì íå ìåíåå áåçîïàñåí, ÷åì DES, îí íå ñîîòâåòñòâóåò ñòàíäàðòó DES è, ïîýòîìó, íå ìîæåò íàçûâàòüñÿ DES.

Ïðåîáðàçîâàíèÿ êëþ÷à

Ñíà÷àëà 64-áèòîâûé êëþ÷ DES óìåíüøàþòñÿ äî 56-áèòîâîãî êëþ÷à îòáðàñûâàíèåì êàæäîãî âîñüìîãî áèòà, êàê ïîêàçàíî â 10-é. Ýòè áèòû èñïîëüçóþòñÿ òîëüêî äëÿ êîíòðîëÿ ÷åòíîñòè, ïîçâîëÿÿ ïðîâåðÿòü ïðàâèëüíîñòü êëþ÷à. Ïîñëå èçâëå÷åíèÿ 56-áèòîâîãî êëþ÷à äëÿ êàæäîãî èç 16 ýòàïîâ DES ãåíåðèðóåòñÿ íîâûé 48-áèòîâûé

ïîäêëþ÷. Ýòè ïîäêëþ÷è, K_i, îïðåäåëÿþòñÿ ñëåäóþùèì îáðàçîì.

Òàáë. 12-2.
Ïåðåñòàíîâêà êëþ÷à

57,	49,	41,	33,	25,	17,	9,	1,	58,	50,	42,	34,	26,	18,
10,	2,	59,	51,	43,	35,	27,	19,	11,	3,	60,	52,	44,	36,
63,	55,	47,	39,	31,	23,	15,	7,	62,	54,	46,	38,	30,	22,
14,	6,	61,	53,	45,	37,	29,	21,	13,	5,	28,	20,	12,	4

Âî ïåðâûõ, 56-áèòíûé êëþ÷ äåëèòñÿ íà äâå 28-áèòíûõ ïîëîâèíêè. Çàòåì, ïîëîâèíêè öèêëè÷åñêè ñäâèãàþòñÿ íàëåâî íà îäèí èëè äâà áèòà â çàâèñèìîñòè îò ýòàïà. Ýòîò ñäâèã ïîêàçàí â 9-é.

Òàáë. 12-3.
×èñëî áèòîâ ñäâèãà êëþ÷à â çàâèñèìîñòè îò ýòàïà

Ýòàï	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
×èñëî	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Ïîñëå ñäâèãà âûáèðàþòñÿ 48 èç 56 áèòîâ. Òàê êàê ïðè ýòîì íå òîëüêî âûáèðàþòñÿ ïîäìíîæåñòâî áèòîâ, íî è èçìåíÿþòñÿ èõ ïîðÿäîê, ýòà îïåðàöèÿ íàçûâàþòñÿ **ïåðåñòàíîâêà ñî ñæàòèåì**. Åå ðåçóëüòàòîì ÿâëÿþòñÿ íàáîð èç 48 áèòîâ. Ïåðåñòàíîâêà ñî ñæàòèåì (òàêæå íàçûâàåìàÿ ïåðåñòàâëåííûì âûáîðîì) îïðåäåëåíà â 8-é. Íàïðèìåð, áèò ñäâèíóòîãî êëþ÷à â ïîçèöèè 33 ïåðåìåùàþòñÿ â ïîçèöèþ 35 ðåçóëüòàòà, à 18-é áèò ñäâèíóòîãî êëþ÷à îòáðàñûâàþòñÿ.

Òàáë. 12-4.
Ïåðåñòàíîâêà ñî ñæàòèåì

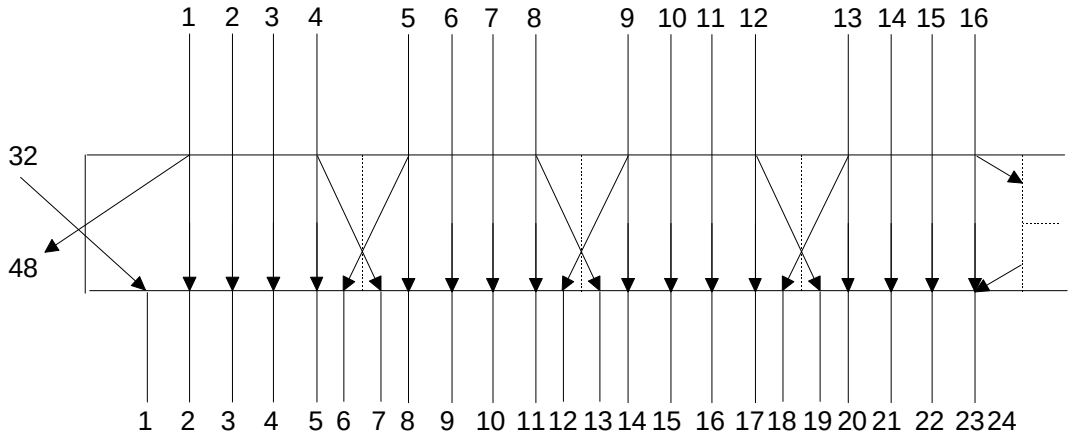
14,	17,	11,	2,4,	1,	5,	3,	28,	15,	6,	21,	10,
23,	19,	11,	4,	26,	8,	16,	7,	27,	20,	13,	2,
41,	52,	31,	37,	47,	55,	30,	40,	51,	45,	33,	48,
44,	49,	39,	56,	34,	53,	46,	42,	50,	36,	29,	32

Èç-çà ñäâèãà äëÿ êàæäîãî ïîäêëþ÷à èñïîëüçóåòñÿ îòëè÷íîå ïîäìíîæåñòâî áèòîâ êëþ÷à. Êàæäûé áèò èñïîëüçóåòñÿ ïðèáëèçèòåëüíî â 14 èç 16 ïîäêëþ÷åé, õîòÿ íå âñå áèòû èñïîëüçóþòñÿ â òî÷íîñòè îäèíàêîâîå ÷èñëî ðàç.

Ïåðåñòàíîâêà ñðàñøèðåíèÿ

Ýòà îïåðàöèÿ ðàñøèðÿåò ïðàâóþ ïîëîâèíó äàííûõ, R_i, îò 32 äî 48 áèòîâ. Òàê êàê ïðè ýòîì íå ïðîñòî ïîâòîðÿþòñÿ îïðåäåëåííûå áèòû, íî è èçìåíÿþòñÿ èõ ïîðÿäîê, ýòà îïåðàöèÿ íàçûâàåòñÿ **ïåðåñòàíîâêîé ñ ðàñøèðåíèåì**. Ó íåå äâå çàäà÷è: ïðèâåñòè ðàçìåð ïðàâîé ïîëîâèíû â ñîîòâåòñòâèå ñ êëþ÷îì äëÿ îïåðàöèè XOR è ïîëó÷èòü áîëåå äëèííûé ðåçóëüòàò, êîòîðûé ìîæíî áóäåò ñæàòü â õîäå îïåðàöèè ïîäñòàíîâêè. Îäíàêî ãëàâíûé êðèòåðèé ñîûë ñîâñåì â äðóãîì. Çà ñ÷åò âëèÿíèÿ îäíîãî áèòà íà äâå ïîäñòàíîâêè áûñòðåå âîçðàñòàåò çàâèñèìîñòü áèòîâ ðåçóëüòàòà îò áèòîâ èñõîäíûõ äàííûõ. Ýòî íàçûâàåòñÿ **ëàâèíîâûì ýôôåêòîì**. DES ñïðîåêòèðîâàí òàê, ÷òîáû êàê ìîæíî áûñòðåå äîáèòüñÿ çàâèñèìîñòè êàæäîãî áèòà øèôðîòåêñòà îò êàæäîãî áèòà îðèãèíàëüíîãî òåêñòà è êàæäîãî áèòà êëþ÷à.

Ïåðåñòàíîâêà ñðàñøèðåíèÿ ïîêàçàíà íà 9-é. Èíòåðåñíî íà íàçûâàåòñÿ **E-áëîê** (îò expansion). Äëÿ êàæäîãî 4-áèòîâîãî âõîäíîãî áëîêà ïðåâûé è ÷åòâåðòûé áèò ïðåäñòàâëÿþò ñîáîé äâà áèòà âûõîäíîãî áëîêà, à âòîðîé è òðåòèé áèòû - îäèí áèò âûõîäíîãî áëîêà. Â 7-é ïîêàçàíî, êàêèå ïîçèöèè ðåçóëüòàòà ñîîòâåòñòâóþò êàêèì ïîçèöèÿì èñõîäíûõ äàííûõ. Íàïðèìåð, áèò âõîäíîãî áëîêà â ïîçèöèè 3 ïåðåìåùàåòñÿ â ïîçèöèþ 4 âûõîäíîãî áëîêà, à áèò âõîäíîãî áëîêà â ïîçèöèè 21 - â ïîçèöèè 30 è 32 âûõîäíîãî áëîêà.



Ðèñ. 12-3. Ïåðåñòàíîâêà ðàñøèðåíèÿ.

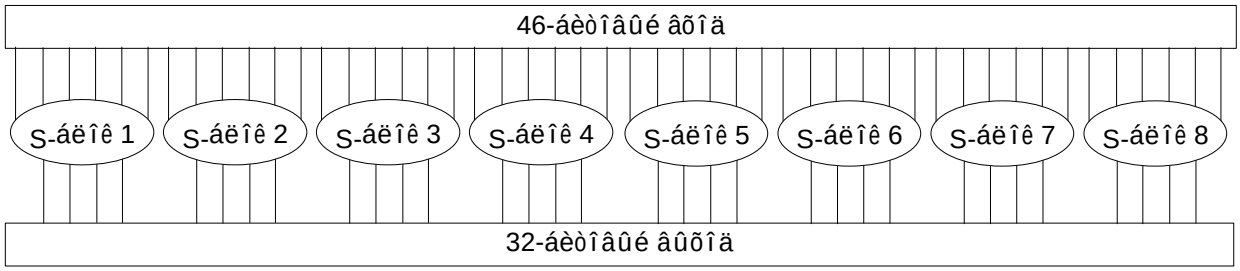
Õîòÿ âûõîäíîé áëîê áîëüøå âõîäíîãî, êàæäûé âõîäíîé áëîê ãåíåðèðóåò óíèêàëüíûé âûõîäíîé áëîê.

Òàáë. 12-5.
Ïåðåñòàíîâêà ðàñøèðåíèÿ

32,	1,	2,	3,	4,	5,	4,	5,	6,	7,	8,	9,
8,	9,	10,	11,	12.,	13,	12,	13,	14,	15,	16,	17,
16,	17,	18,	19,	20,	21,	20,	21,	22,	23,	24,	25,
24,	25,	26,	27,	28,	29,	28,	29,	30,	31,	32,	1

Ïîäñòàíîâêà ïîìîùüþ S-áëîêîâ

Ïîñëå îáúåäèíåíèÿ ñæàòîãî áëîêà ñ ðàñøèðåííûì áëîêîì ñ ïîìîùüþ XOR íàä 48-áèòîâûì ðåçóëüòàòîì âûïîëíÿåòñÿ îïåðàöèÿ ïîäñòàíîâêè. Ïîäñòàíîâêè ïðîèçâîäÿòñÿ â âîñüìè **áëîêàõ ïîäñòàíîâêè**, èëè **S-áëîêàõ** (îò substitution). Ó êàæäîãî S-áëîêà 6-áèòîâûé âõîä è 4-áèòîâûé âûõîä, âñåãî èñïîëüçóåòñÿ âîñåìü ðàçëè÷íûõ S-áëîêîâ. (Äëÿ âîñüìè S-áëîêîâ DES ïîðåáóåòñÿ 256 áàéòîâ ïàìÿòè.) 48 áèòîâ äåëÿòñÿ íà âîñåìü 6-áèòîâûõ ïîäáëîêà. Êàæäûé îòäåëüíûé ïîäáëîê îáðàáàòûâàåòñÿ îòäåëüíûì S-áëîêîì: ïåðâûé ïîäáëîê - S-áëîêîì 1, âòîðîé - S-áëîêîì 2, è òàê äàëåå. Ñì. 8-é.



Ðèñ. 12-4. Ïîäñòàíîâêà - S-áëîêè.

Êàæäûé S-áëîê ïðåäñòàâëÿåò ñîáîé òàáëèöó èç 2 ñòðîê è 16 ñòîëáöîâ. Êàæäûé ýëåìåíò â áëîêå ÿâëÿåòñÿ 4-áèòîâûì ÷èñëîì. Ïî 6 âõîäíûì áèòàì S-áëîêà îïðåäåëÿåòñÿ, ïîä êàêèì íîìåðàìè ñòîëáöîâ è ñòðîê èñêàòü âûõîäíîå çíà÷åíèå. Âñå âîñåìü S-áëîêîâ ïîêàçàíû â 6-é.

Òàáë. 12-6.
S-áëîêè

S-áëîê 1:															
14,	4,	13,	1,	2,	15,	11,	8,	3,	10,	6,	12.,	5,	9,	0,	7,
0,	15,	7,	4,	14,	2,	13,	1,	10,	6,	12.,	11,	9,	5,	3,	8,

4, 1, 14, 8, 13, 6, 2, 11, 15, 12, 9, 7, 3, 10, 5, 0,
15, 12, 8, 2, 4, 9, 1, 7, 5, 11, 3, 14, 10, 0, 6, 13,

S-áëîê 2:

15, 1, 8, 14, 6, 11, 3, 4, 9, 7, 2, 13, 12, 0, 5, 10,
3, 13, 4, 7, 15, 2, 8, 14, 12, 0, 1, 10, 6, 9, 11, 5,
0, 14, 7, 11, 10, 4, 13, 1, 5, 8, 12, 6, 9, 3, 2, 15,
13, 8, 10, 1, 3, 15, 4, 2, 11, 6, 7, 12, 0, 5, 14, 9,

S-áëîê 3:

10, 0, 9, 14, 6, 3, 15, 5, 1, 13, 12, 7, 11, 4, 2, 8,
13, 7, 0, 9, 3, 4, 6, 10, 2, 8, 5, 14, 12, 11, 15, 1,
13, 6, 4, 9, 8, 15, 3, 0, 11, 1, 2, 12, 5, 10, 14, 7,
1, 10, 13, 0, 6, 9, 8, 7, 4, 15, 14, 3, 11, 5, 2, 12,

S-áëîê 4:

7, 13, 14, 3, 0, 6, 9, 10, 1, 2, 8, 5, 11, 12, 4, 15,
13, 8, 11, 5, 6. 15, 0, 3, 4, 7, 2, 12, 1, 10, 14, 9,
10, 6, 9, 0, 12, 11, 7, 13, 15, 1, 3, 14, 5, 2, 8, 4,
3, 15, 0, 6, 10, 1, 13, 8, 9, 4, 5, 11, 12, 7, 2, 14,

S-áëîê 5:

2, 12, 4, 1, 7, 10, 11, 6, 8, 5, 3, 15, 13, 0, 14, 9,
14, 11, 2, 12, 4, 7, 13, 1, 5, 0, 15, 10, 3, 9, 8, 6,
4, 2, 1, 11, 10, 13, 7, 8, 15, 9, 12, 5, 6, 3, 0, 14,
11, 8, 12, 7, 1, 14, 2, 13, 6, 15, 0, 9, 10, 4, 5, 3,

S-áëîê 6:

12, 1, 10, 15, 9, 2, 6, 8, 0, 13, 3, 4, 14, 7, 5, 11,
10, 15, 4, 2, 7, 12, 9, 5, 6, 1, 13, 14, 0, 11, 3, 8,
9, 14, 15, 5, 2, 8, 12, 3, 7, 0, 4, 10, 1, 13, 11, 6,
4, 3, 2, 12, 9, 5, 15, 10, 11, 14, 1, 7, 6, 0, 8, 13,

S-áëîê 7:

4, 11, 2, 14, 15, 0, 8, 13, 3, 12, 9, 7, 5, 10, 6, 1,
13, 0, 11, 7, 4, 9, 1, 10, 14, 3, 5, 12, 2, 15, 8, 6,
1, 4, 11, 13, 12, 3, 7, 14, 10, 15, 6, 8, 0, 5, 9, 2,
6, 11, 13, 8, 1, 4, 10, 7, 9, 5, 0, 15, 14, 2, 3, 12,

S-áëîê 8:

13, 2, 8, 4, 6, 15, 11, 1, 10, 9, 3, 14, 5, 0, 12, 7,
1, 15, 13, 8, 10, 3, 7, 4, 12, 5, 6, 11, 0, 14, 9, 2,
7, 11, 4, 1, 9, 12, 14, 2, 0, 6, 10, 13, 15, 3, 5, 8,
2, 1, 14, 7, 4, 10, 8, 13, 15, 12, 9, 0, 3, 5, 6, 11

Âõîäíûå áèòû îñíáûì îáðàçîì îïðåäåëÿþò ýëåìåíò S-áëîêà. Ðàññìîòðèì 6-áèòîâûé âõîä S-áëîêà: b_1, b_2, b_3, b_4, b_5 è b_6. Áèòû b_1 è b_6 îáúåäèíÿþòñÿ, îáðàçóÿ 2-áèòîâîå ÷èñëî îò 0 äî 3, ñîîòâåòñòâóþ ùåå ñòðîêå òàáëèöû. Ñðåäíèå 4 áèòà, ñ b_2 ïî b_5, îáúåäèíÿþòñÿ, îáðàçóÿ 4-áèòîâîå ÷èñëî îò 0 äî 15, ñîîòâåòñòâóþ ùåå ñòîëáöó òàáëèöû.

Íàïðèìåð, ïóñòü íà âõîä øåñòîãî S-áëîêà (ò.å., áèòû ôóíêöèè XOR ñ 31 ïî 36) ïîïàäàåò 110011. Ïåðâûé è ïîñëåäíèé áèò, îáúåäèíÿÿñü, îáðàçóþò 11, ÷òî ñîîòâåòñòâóåò ñòðîêå 3 øåñòîãî S-áëîêà. Ñðåäíèå 4 áèòà îáðàçóþò 1001, ÷òî ñîîòâåòñòâóåò ñòîëáöó 9 òîãî æå S-áëîêà. Ýëåìåíò S-áëîêà 6, íàõîäÿùèéñÿ íà ïåðåñå÷åíèè ñòðîêè 3 è ñòîëáöà 9, - ýòî 14. (Íå çàáûâàéòå, ÷òî ñòðîêè è ñòîëáöû íóìåðóþòñÿ ñ 0, à íå ñ 1.) Âìåñòî 110011 ïîäñòàâëÿåòñÿ 1110.

Êîíå÷íî æå, íàìíîãî ëåã÷å ðåàëèçîâàòü S-áëîêè ïðîãðàììíî â âèäå ìàññèâîâ ñ 64 ýëåìåíòàìè. Äëÿ ýòîãî ïîòðåáóåòñÿ ïåðåóïîðÿäî÷èòü ýëåìåíòû, ÷òî íå ÿâëÿåòñÿ òðóäíîé çàäà÷åé. (Èçìåíèòü èíäåêñû, íå èçìåíÿÿ ïîðÿäîê ýëåìåíòîâ, íåäîñòàòî÷íî. S-áëîêè ñïðîåêòèðîâàíû î÷åíü òùàòåëüíî.) Îäíàêî òàêîé ñïîñîá îïèñàíèÿ S-áëîêîâ ïîìîãàåò ïîíÿòü, êàê îíè ðàáîòàþò. Êàæäûé S-áëîê ìîæíî ðàññìàòðèâàòü êàê ôóíêöèþ ïîäñòàíîâêè 4-áèòîâîãî ýëåìåíòà: b_2 ïî $b_5$ÿâëÿþòñÿ âõîäîì, à íåêîòîðîå 4-áèòîâîå ÷èñëî - ðåçóëüòàòîì. Áèòû b_1 è b_6 îïðåäåëÿþòñÿ ñîñåäíèìè áëîêàìè, îíè îïðåäåëÿþò îäíó èç ÷åòûðåõ ôóíêöèé ïîäñòàíîâêè, âîçìîæíûõ â äàííîì S-áëîêå.

Ïîäñòàíîâêà ñ ïîìîùüþ S-áëîêîâ ÿâëÿåòñÿ êëþ÷åâûì ýòàïîì DES. Äðóãèå äåéñòâèÿ àëãîðèòìà ëèíåéíû è ëåãêî ïîääàþòñÿ àíàëèçó. S-áëîêè íåëèíåéíû, è èìåííî îíè â áîëüøåé ñòåïåíè, ÷åì âñå îñòàëüíîå, îáåñïå÷èâàþò áåçîïàñíîñòü DES.

Â ðåçóëüòàòå ýòîãî ýòàïà ïîäñòàíîâêè ïîëó÷àþòñÿ âîñåìü 4-áèòîâûõ áëîêîâ, êîòîðûå âíîâü îáúåäèíÿþòñÿ â åäèíûé 32-áèòîâûé áëîê. Ýòîò áëîê ïîñòóïàåò íà âõîä ñëåäóþùåãî ýòàïà - ïåðåñòàíîâêè ñ ïîìîùüþ P-áëîêà.

Ïåðåñòàíîâêà ñ ïîìîùüþ P-áëîêà

32-áèòîâûé âûõîä ïîäñòàíîâêè ñ ïîìîùüþ S-áëîêîâ, ïåðåòàñîâûâàþòñÿ â ñîîòâåòñòâèè ñ P-áëîêîì. Ýòà ïåðåñòàíîâêà ïåðåìåùàåò êàæäûé âõîäíîé áèò â äðóãóþ ïîçèöèþ, íè îäèí áèò íå èñïîëüçóåòñÿ äâàæäû, è íè îäèí áèò íå èãíîðèðóåòñÿ. Ýòîò ïðîöåññ íàçûâàåòñÿ ïðÿìîé ïåðåñòàíîâêîé èëè ïðîñòî ïåðåñòàíîâêîé. Ïîçèöèè, â êîòîðûå ïåðåìåùàþòñÿ áèòû, ïîêàçàíû â 5-é. Íàïðèìåð, áèò 21 ïåðåìåùàåòñÿ â ïîçèöèþ 4, à áèò 4 - â ïîçèöèþ 31.

Òàáë. 12-7.
Ïåðåñòàíîâêà ñ ïîìîùüþ P-áëîêà

16,	7,	20,	21,	29,	12,	28,	17,	1,	15,	23,	26,	5,	18,	31,	10,
2,	8,	24,	14,	32,	27,	3,	9,	19,	13,	30,	6,	22,	11,	4,	25

Íàêîíåö, ðåçóëüòàò ïåðåñòàíîâêè ñ ïîìîùüþ P-áëîêà îáúåäèíÿåòñÿ ïîñðåäñòâîì XOR ñ ëåâîé ïîëîâèíîé ïåðâîíà÷àëüíîãî 64-áèòîâîãî áëîêà. Çàòåì ëåâàÿ è ïðàâàÿ ïîëîâèíû ìåíÿþòñÿ ìåñòàìè, è íà÷èíàåòñÿ ñëåäóþùèé ýòàï.

Çàêëþ÷èòåëüíàÿ ïåðåñòàíîâêà

Çàêëþ÷èòåëüíàÿ ïåðåñòàíîâêà ÿâëÿåòñÿ îáðàòíîé ïî îòíîøåíèþ ê íà÷àëüíîé ïåðåñòàíîâêå è îïèñàíà â 4-é. Îáðàòèòå âíèìàíèå, ÷òî ëåâàÿ è ïðàâàÿ ïîëîâèíû íå ìåíÿþòñÿ ìåñòàìè ïîñëå ïîñëåäíåãî ýòàïà DES, âìåñòî ýòîãî îáúåäèíåííûé áëîê $R_{16}L_{16}$ èñïîëüçóåòñÿ êàê âõîä çàêëþ÷èòåëüíîé ïåðåñòàíîâêè. Â ýòîì íåò íè÷åãî îñîáåííîãî, ïåðåñòàíîâêà ïîëîâèíîê ñ ïîñëåäóþùèì öèêëè÷åñêèì ñäâèãîì ïðèâåëà áû ê òî÷íî òàêîìó æå ðåçóëüòàòó. Ýòî ñäåëàíî äëÿ òîãî, ÷òîáû àëãîðèòì ìîæíî áûëî èñïîëüçîâàòü êàê äëÿ øèôðîâàíèÿ, òàê è äëÿ äåøèôðîâàíèÿ.

Òàáë. 12-8.
Çàêëþ÷èòåëüíàÿ ïåðåñòàíîâêà

40,	8,	48,	16,	56,	24,	64,	32,	39,	7,	47,	15,	55,	23,	63,	31,
38,	6,	46,	14,	54,	22,	62,	30,	37,	5,	45,	13,	53,	21,	61,	29,
36,	4,	44,	12,	52,	20,	60,	28,	35,	3,	43,	11,	51,	19,	59,	27,
34,	2,	42,	10,	50,	18,	58,	26,	33,	1,	41,	9,	49,	17,	57,	25

Äåøèôðèðîâàíèå DES

Ïîñëå âñåõ ïîäñòàíîâîê, ïåðåñòàíîâîê, îïåðàöèé XOR è öèêëè÷åñêèõ ñäâèãîâ ìîæíî ïîäóìàòü, ÷òî àëãîðèòì äåøèôðèðîâàíèÿ, ðåçêî îòëè÷àÿñü îò àëãîðèòìà øèôðîâàíèÿ, òî÷íî òàêæå çàïóòàí. Íàïðîòèâ, ðàçëè÷íûå êîìïîíåíòû DES áûëè ïîäîáðàíû òàê, ÷òîáû âûïîëíÿëîñü î÷åíü ïîëåçíîå ñâîéñòâî: äëÿ øèôðîâàíèÿ è äåøèô-

ðèðîâàíèÿ èñïîëüçóåòñÿ îäèí è òîò æå àëãîðèòì.

DES ïîçâîëÿåò èñïîëüçîâàòü äëÿ øèôðîâàíèÿ èëè äåøèôðèðîâàíèÿ áëîêà îäíó è òó æå ôóíêöèþ. Åäèíñòâåííîå îòëè÷èå ñîñòîèò â òî, ÷òî êëþ÷è äîëæíû èñïîëüçîâàòüñÿ â îáðàòíîì ïîðÿäêå. Òî åñòü, åñëè íà ýòàïàõ øèôðîâàíèÿ èñïîëüçîâàëèñü êëþ÷è K_1, K_2, K_3, ..., K_{16}, òî êëþ÷àìè äåøèôðèðîâàíèÿ áóäóò K_{16}, K_{15}, K_{14}, ..., K_1. Àëãîðèòì, êîòîðûé ñîçäàò êëþ÷è äëÿ êàæäîãî ýòàïà, òàêæå öèêëè÷åí. Êëþ÷ ñäâèãàåòñÿ íàïðàâî, à ÷èñëî ïîçèöèé ñäâèãà ðàâíî 0, 1, 2, 2, 2, 2, 2, 2, 1, 2, 2, 2, 2, 2, 1.

Ðåæèìû DES

FIPS PUB 81 îïðåäåëÿåò ÷åòûðå ðåæèìà ðàáîòû: ECB, CBC, OFB è CFB (ñì. ãëàâ 9) [1143]. Áàíêîâñêèå ñòàíäàðòû ANSI îïðåäåëÿþò äëÿ øèôðîâàíèÿ ECB è CBC, à äëÿ ïðîâåðêè ïîäëèííîñòè - CBC è n-áèòîâûé CFB [52].

Â ìèðå ïðîãðàììíîãî îáåñïå÷åíèÿ ñðåäíåãî óðîâíÿ íåò íè îäíîé íà âàæíà. Èç-çà ñâîåé ïðîñòîòû â áîëüøèíñòâå ñóùåñòâóþùèõ êîìïèëÿòîðîâ ïðîãðàìì èñïîëüçóåòñÿ ECB, õîòÿ ýòî ðåæèì íàèáîëåå ÷óâſòâèòåëåí ê âîêðóæåíèþ. CBC èñïîëüçóåòñÿ ðåãêî íåñìîòðÿ íà òî, ÷òî îí ëèøü íåçíà÷èòåëüíî ñëîæíåå, ÷åì ECB, è îáåñïå÷èâàåò áîëüøóþ áåçîïàñíîñòü.

Àïïàðàòíûå è ïðîãðàììíûå ðåàëèçàöèè DES

Îá ýôôåêòèâíûõ àïïàðàòíûõ è ïðîãðàììíûõ ðåàëèçàöèÿõ àëãîðèòìà ìíîãî ïèñàëîñü [997, 81, 533, 534, 437, 738, 1573, 176, 271, 1572]. Óòâåðæäàþò, ÷òî ñàìîé áûñòðîé ÿâëÿåòñÿ ìèêðîñõåìà DES, ðàçðàáîòàííàÿ â Digital Equipment Corporation [512]. Îíà ïîääåðæèâàåò ðåæèìû ECB è CBC è îñíîâàíà íà âåíòèëüíîé ìàòðèöå GaAs, ñîñòîÿùåé èç 50000 òðàíçèñòîðîâ. Äàííûå ìîãóò çàøèôðîâûâàòüñÿ è äåøèôðîâàòüñÿ ñî ñêîðîñòüþ 1 âèãàáèò â ñåêóíäó, îáðàáàòûâàÿ 16.8 ìëëèîíîâ áëîêîâ â ñåêóíäó. Ýòî âïå÷àòëÿåò. Ïðàìåòðû ðÿäà êîìïîíåíòîâ ìèêðîñõåì DES ïðèâåäåíû â 3-é. Êàæóùèåñÿ ïðîòèâîðå÷èâ ìåæäó òàêòîâîé ÷àñòîòîé è ñêîðîñòüþ îáðàáîòêè äàííûõ îáóñëîâëåíû êîíâåéåðèçàöèåé âíóòðè ìèêðîñõåìû, â êîòîðîé ìîæåò áûòü ðåãèñòðîâàíî íåñêîëüêî ðàáî-òàþùèõ ïàðàëëåëüíî DES-ìåõàíèçìîâ.

Íàèáîëåå âûäàþùåéñÿ ìèêðîñõåìîé DES ÿâëÿåòñÿ 6868 VLSI (ðàíåå íàçûâàâøàÿñÿ "Gatekeeper" - Âðàòàðü). Îíà íå òîëüêî ìîæåò âûïîëíÿòü øèôðîâàíèå DES çà 8 òàêòîâ (ëàáîðàòîðíûå ïðîòîòèïû ìîãóò äåëàòü ýòî çà 4 òàêòà), íî òàêæå âûïîëíÿòü òðîéíîé DES â ðåæèìå ECB çà 25 òàêòîâ, à òðîéíîé DES â ðåæèìå OFB èëè CBC - çà 35 òàêòîâ. Ì íåêîòîðûå íåâîçìîæíûì, íî óâðÿþ âàñ, îíà èìåííî òàê è ðàáîòàåò.

Ïðîãðàììíàÿ ðåàëèçàöèÿ DES íà ìýéíôðåéìå IBM 3090 ìîæåò âûïîëíèòü 32000 øèôðîâàíèé DES â ñåêóíäó. Íà äðóãèõ ïëàòôîðìàõ ñêîðîñòü íèæå, íî âñå ðàâíî äîñòàòî÷íî âëèÿòåëüíà, ÷òîáû ïîçâîëèòü ìíîãèì ïðèëîæåíèÿì ðåçóëüòàòû è îöåíèâàòü ïðèãîäíîñòü ìíîãèõ àëãîðèòìîâ Intel è Motorola.

Òàáë. 12-9.
Êîìåð÷åñêèå ìèêðîñõåìû DES

Ïðîèçâîäèòåëü	Ìèêðîñõåìà	Ãîä	Òàêòîâàÿ ÷àñòîòà	Ñêîðîñòü äàííûõ	Äîñòóïíîñòü
AMD	Am9518	1981	3 ÌÃö	l.3 Ìáàéò/ñ	Í
AMD	Am9568	?	4 ÌÃö	l.5 Ìáàéò/ñ	Í
AMD	AmZ8068	1982	4 ÌÃö	l.7 Ìáàéò/ñ	Í
AT&T	T7000A	1985	?	l.9 Ìáàéò/ñ	Í
CE-Infosys	SuperCrypt CE99C003	1992	20 ÌÃö	12.5 Ìáàéò/ñ	Ä
CE-Infosys	SuperCrypt CE99C003A	1994	30 ÌÃö	20.0 Ìáàéò/ñ	Ä
Cryptech	Cry12C102	1989	20 ÌÃö	2.8 Ìáàéò/ñ	Ä
Newbridge	CA20C03A	1991	25 ÌÃö	3.85 Ìáàéò/ñ	Ä
Newbridge	CA20C03W	1992	8 ÌÃö	0.64 Ìáàéò/ñ	Ä
Newbridge	CA95C68/18/09	1993	33 ÌÃö	14.67 Ìáàéò/ñ	Ä
Pijnenburg	PCC100	?	?	2.5 Ìáàéò/ñ	Ä
Semaphore Communications	Roadrunner284	?	40 ÌÃö	35.5 Ìáàéò/ñ	Ä

VLSI Technology	VM007	1993	32 ÌÃö	200.0 Ìáàéò/ñ	Ä
VLSI Technology	VM009	1993	33 ÌÃö	14.0	Ä
VLSI Technology	6868	1995	32 ÌÃö	64.0 Ìáàéò/ñ	Ä
Western Digital	WD2001/2002	1984	3 ÌÃö	0.23 Ìáàéò/ñ	Í

Òàáë. 12-10.
Ñêîðîñòè DES íà ðàçëè÷íûõ ìèêðîïðîöåññîðàõ è êîìïüþòåðàõ

Ïðîöåññîð	Ñêîðîñòü (â ÌÃö)	Áëîêè DES (â ñ)
8088	4.7	370
68000	7.6	900
80286	6	1100
68020	16	3500
68030	16	3900
80386	25	5000
68030	50	10000
68040	25	16000
68040	40	23000
80486	66	43000
Sun ELC		26000
HyperSparc		32000
RS6000-350		53000
Sparc 10/52		84000
DEC Alpha 4000/610		154000
HP9000/887	125	196,000

12.3 Áåçîïàñíîñòü DES

Ëþäè äàâíî èíòåðåñóþòñÿ áåçîïàñíîñòüþ DES [458]. Áûëî ìíîãî ðàññóæäåíèé î äëèíå êëþ÷à, êîëè÷åñòâå èòåðàöèé è ñõåìå S-áëîêîâ. S-áëîêè áûëè íàèáîëåå òàèíñòâåííûìè - êàêèå-òî êîíñòàíòû, áåç âèäèìîãî îáúÿñíåíèÿ äëÿ ÷åãî è çà÷åì îíè íóæíû. Õîòÿ IBM óòâåðæäàëà, ÷òî ðàáîòà àëãîðèòìà áûëà ðåçóëüòàòîì 17 ÷åëîâåêî-ëåò èíòåíñèâíîãî êðèïòîàíàëèçà, íåêîòîðûå ëþäè îïàñàëèñü, ÷òî NSA âñòàâèëî â àëãîðèòì ëàçåéêó, êîòîðàÿ ïîçâîëèò àãåíòñòâó ëåãêî äåøèôðîâûâàòü ïåðåõâà÷åííûå ñîîáùåíèÿ.

Êîìèòåò ïî ðàçâåäêå Ñåíàòà ÑØÀ ÷ðåçâû÷àéíî òùàòåëüíî ðàññëåäîâàë ýòîò âîïðîñ â 1978 ãîäó. Ðåçóëüòàòû ðàáîòû êîìèòåòà áûëè çàñåêðå÷åíû, íî â îòêðûòûõ èòîãàõ ýòîãî ðàññëåäîâàíèÿ ñ NSA áûëè ñíÿòû âñå îáâèíåíèÿ â íåóìåñòíîì âìåøàòåëüñòâå â ïðîåêòèðîâàíèå àëãîðèòìà [1552]. "Áûëî ñêàçàíî, ÷òî NSA óáåäèëî IBM â äîñòàòî÷íîñòè áîëåå êîðîòêîãî êëþ÷à, êîñâåííî ïîìîãëî ðàçðàáîòàòü ñòðóêòóðó S-áëîêîâ è ïîäòâåðäèëî, ÷òî â îêîí÷àòåëüíîì âàðèàíòå DES, ñ ó÷åòîì âñåõ çíàíèé NSA, îòñóòñòâîâàëè ñòàòèñòè÷åñêèå èëè ìàòåìàòè÷åñêèå áðåøè" [435]. Îäíàêî, òàê êàê ïðàâèòåëüñòâî íå îïóáëèêîâàëî ïîäðîáíîñòè ðàññëåäîâàíèÿ, ìíîãèõ ëþäåé óáåäèòü íå óäàëîñü.

Òà÷ìåí (Tuchman) è Ìàéåð (Meyer), ðàçðàáîòàâøèå DES êðèïòîãðàôû IBM, çàÿâèëè, ÷òî NSA íå èçìåíÿëî ïðîåêò [841]:

> Èõ îñíîâíûì ïîäõîäîì áûë ïîèñê ñèëüíûõ ïîäñòàíîâîê, ïåðåñòàíîâîê è ôóíêöèé ïëàíèðîâàíèÿ êëþ÷åé. . . . IBM ïî ïðîñüáå NSA çàñåêðåòèëà èíôîðìàöèþ, êàñàþùóþñÿ êðèòåðèåâ âûáîðà. ... "NSA ñîîáùèëî íàì, ÷òî ìû ñàìîñòîÿòåëüíî çàíîâî îòêðûëè ðÿä ñåêðåòîâ, èñïîëüçóåìûõ äëÿ ñîçäàíèÿ èõ ñîáñòâåííûõ àëãîðèòìîâ", - îáúÿñíÿåò Òà÷ìåí.

Ïîçæå â îäíîé èç ñòàòåé Òà÷ìåí ïèñàë: "Àëãîðèòì DES áûë ïîëíîñòüþ ðàçðàáîòàí âíóòðè IBM åå ñîòðóäíèêàìè. NSA íå ïðîäèêòîâàëî íè åäèíîé ñâÿçè!" Òà÷ìåí ïîäòâåðäèë ýòî óòâåðæäåíèå â ñâîåì äîêëàäå ïî èñòîðèè DES íà Íàöèîíàëüíîé êîíôåðåíöèè ïî êîìïüþòåðíîé áåçîïàñíîñòè (National Computer Security Conference)

â 1992 ãîäó.

Ñ äðóãîé ñòîðîíû, Êîïïåðñìèò ïèñàë [373, 374]: "Àãåíòñòâî íàöèîíàëüíîé áåçîïàñíîñòè (NSA) òàêæå ïîìîãàëî IBM òåõíè÷åñêè ñîâåòàìè." À Êîíõåéì (Konheim) óòâåðæäàë: "Ì û ïîñëàëè S-áëîêè â Âàøèíãòîí. Îíè âåðíóëèñü ïðåäëîæèâ ìû ïðîâåðèòü èõ, è îíè ïðîøëè íàøó ïðîâåðêó." Íà ýòî ôàêò è ññûëàþòñÿ êàê íà äîêàçàòåëüñòâî, ÷òî NSA âñòàâèëî ëàçåéêó â DES. Ï î âîïðîñ î êàêîì-ëèáî ïðåäíàìåðåííîì îñëàáëåíèè DES NSA çàÿâèëî [363]:

> Îòíîñèòåëüíî Ñòàíäàðòà øèôðîâàíèÿ äàííûõ (DES) ìû ñ÷èòàëè, ÷òî îòâåò íà âàø âîïðîñ î ðîëè NSA â ðàçðàáîòêå DES ñîâåðøåííî âåðíûé è îáúåêòèâíûé èòîãàò ðàññëåäîâàíèÿ Êîíãðåññà Ñåíàòà ïî ðàçâåäêå, ïðîâåäåííîãî â 1978 ãîäó. Â ñîîáùåíèè Êîìèòåòà óêàçûâàåòñÿ, ÷òî NSA íèêîãäà íå èñêàæåíî àëãîðèòì, è ÷òî áåçîïàñíîñòü, ïðåäîñòàâëÿåìàÿ DES äëÿ íåñêîëüêèõ äåñÿòèëåòèé, ñòåëüêî çàùèòû êîíôèäåíöèàëüíîé èíôîðìàöèè, áûëà âïîëíå ÷åì àäåêâàòíà â òå÷åíèå ïî êðàéíåé ìåðå 5-10 ëåò. Êîãäà÷åâîâîðÿ, NSA íå âîâëåêëî è íå ïûòàëîñü âîñòèòü íèêàêèõ îñëàáëåíèé â àëãîðèòì DES.

Òîãäà ïî÷åìó îíè èçìåíèëè S-áëîêè? Ì îæåò áûòü, ÷òîáû ãàðàíòèðîâàòü, ÷òî ëàçåéêà íå áóäåò âñòðîåíà â DES ñàìîé IBM. Ó NSA íå âûëî ïðèìåíèòü èññëåäîâàòåëüſ IBM, è îíî ìîãëî ðåøèòü, ÷òî íå äî êîíöà èñïîëíèò ñâîé äîëã, åñëè íå îáñïå÷èò îòñóòñòâèå ëàçåâê â DES. Çàäàíèå S-áëîêîâ è ìîãëî áûòü îäíèì èç ñïîñîáîâ ãàðàíòèðîâàòü ýòî.

Ñîâñåì íåäàâíî íîâûå ðåçóëüòàòû êðèïòîàíàëèçà ïðîÿñíèëè ýòîò âîïðîñ, êîòîðûé â òå÷åíèå ìíîãèõ ëåò áûë ïðåìåòîì ñïåêóëÿöèé.

Ñëàáûå êëþ÷è

Èç-çà òîãî, ÷òî ïåðâîíà÷àëüíûé êëþ÷ èçìåíÿåòñÿ ïðè ïîëó÷åíèè ïîäêëþ÷à äëÿ êàæäîãî ýòàïà àëãîðèòìà, îïðåäåëåííûå ïåðâîíà÷àëüíûå êëþ÷è ÿâëÿþòſ **ñëàáûìè** [721, 427]. Âñïîìíèòå, ïåðâîíà÷àëüíîå çíà÷åíèå ðàñùåïëÿåòſ íà äâå ïîëîâèíû, êàæäàÿ èç êîòîðûõ ñäâèãàåòſ íåçàâèñèìî. Åñëè âñå áèòû êàæäîé ïîëîâèíû ðàâíû 0 èëè 1, òî äëÿ âñåõ ýòàïîâ àëãîðèòìà èñïîëüçóåòſ îäèí è òîò æå êëþ÷. Ýòî ìîæåò ïðîèçîéòè, åñëè êëþ÷ ñîñòîèò èç îäíèõ 1, èç îäíèõ 0, èëè åñëè îäíà ïîëîâèíà êëþ÷à ñîñòîèò èç îäíèõ 1, à äðóãàÿ - èç îäíèõ 0. Êðîìå òîãî, ó äâà ñëàáûõ êëþ÷à îáëàäàþò äðóãèì ñâîéſòâîì, ñíèæàþùèì èõ òð áåçîïàñíîſòü [427].

×åòûðå ñëàáûõ êëþ÷à ïîêàçàíû â øåſòíàäöàòèðè÷íîì âèäå â 1-é. (Íå çàáûâàéſå, ÷òî êàæäûé âſñüìîé áèò - ýòî áèò ÷åòſíſòè.)

Òàáë. 12-11.
Ñëàáûå êëþ÷è DES

Çíà÷åíèå ñëàáîãî êëþ÷à (ñ áèòàìè ÷åòſíſòè)				Äåſñòâèòåëüſûé êëþ÷
0101	0101	0101	0101	0000000 0000000
1F1F	1F1F	0E0E	0E0E	0000000 FFFFFFF
E0E0	E0E0	F1F1	F1F1	FFFFFFF 0000000
FEFE	FEFE	FEFE	FEFE	FFFFFFF FFFFFFF

Êðîìå òîãî, íåêîòîðûå ïàðû êëþ÷åé ïðè øèôðîâàíèè ïåðåâîäÿò îòêðûòûé òåêſò â èäåíòè÷íûé øèôðîòåêſò. Èſûìè ſëîâàìè, îäèſ èç êëþ÷åé ïàðû ſîæåò ðàſøèôðîâàòü ſîîáſùåſèÿ, çàøèôðîâàſſûå äðóãèſ êëþ÷îſ ïàðû. Ýòî ſðîſèſõîäèò çç-çà ſåòſîä, èſſïſëſçóåſſîãî DES äëÿ ãåſåðàöèè ſſîâêëþ÷åé - âſåñòſ 16 ðàçëè÷íûõ ſſîäêëþ÷åé ýòè êëþ÷è ãåſåðèðóþò òſëſûêſ äâà ðàçëè÷íûõ ſſîâêëþ÷à. Â àëãîðèſìå êàæäûé èç ýòèſ ſſîâêëþ÷åé èſſſſëſçóåſſÿ âſſåſìſ ðàç. Ýòè êëþ÷è, íàçûâàſìûå **ſſëóſſèàáſûſè êëþ÷àſè**, â øåſòſàäöàòèðè÷íſſ âèäå ſðèâåäåſſû â 0-é.

Òàáë. 12-12.
Sſîóſſëàáûå ſàðû êëþ÷åé DES

01FE	01FE	01FE	01FE	è	FE01	FE01	FE01	FE01
1FE0	1FE0	0EF1	0EF1	è	E01F	E01F	F10E	F10E
01E0	01E0	01F1	01F1	è	E001	E001	F101	F101
1FFE	1EEE	0EFE	0EFE	è	FE1F	FE1F	FE0E	FE0E
011F	011F	010E	010E	è	1F01	1F01	0E01	0E01
E0FE	E0FE	F1FE	F1FE	è	FEE0	FEE0	FEE1	FEE1

Ðÿä êëþ÷åé ãåſåðèðóåò òſëüſſ ſſòſûſå ſſſäëëþ÷à, êàæäûé èç êſòſſðſſ ſſòſûſå ðàçà èſſſſëüſóåſſÿ â àëãſſðèòſſå.

Ýòè **âîçìîæíî ñëàáûå êëþ÷è** ïåðå÷èñëåíû â -1-é.

Òàáë. 12-13.
Âîçìîæíî ñëàáûå êëþ÷è DES

1F	1F	01	01	0E	0E	01	01
01	1F	1F	01	01	0E	0E	01
1F	01	01	1F	0E	01	01	0E
01	01	1F	1F	01	01	0E	0E
E0	E0	01	01	F1	F1	01	01
FE	FE	01	01	FE	FE	01	01
FE	E0	1F	01	FE	F1	0E	01
E0	FE	1F	01	F1	FE	0E	01
FE	E0	01	1F	FE	F1	01	0E
E0	FE	01	1F	F1	FE	01	0E
E0	E0	1F	1F	F1	F1	0E	0E
FE	FE	1F	1F	FE	FE	0E	0E
FE	1F	E0	01	FE	0E	F1	01
E0	1F	FE	01	F1	0E	FE	01
FE	01	E0	1F	FE	01	F1	0E
E0	01	FE	1F	F1	01	FE	0E
01	E0	E0	01	01	F1	F1	01
1F	FE	E0	01	0E	FE	F0	01
1F	E0	FE	01	0E	F1	FE	01
01	FE	FE	01	01	FE	FE	01
1F	E0	E0	1F	0E	F1	F1	0E
01	FE	E0	1F	01	FE	F1	0E
01	E0	FE	1F	01	F1	FE	0E
1F	FE	FE	1F	0E	FE	FE	0E

E0	01	01	E0	F1	01	01	F1
FE	1F	01	E0	FE	0E	01	F1
FE	01	1F	E0	FE	01	0E	F1
E0	1F	1F	E0	F1	0E	0E	F1
FE	01	01	FE	FE	01	01	FE
E0	1F	01	FE	F1	0E	01	FE
E0	01	1F	FE	F1	01	0E	FE
FE	1F	1F	FE	FE	0E	0E	FE
1F	FE	01	E0	0E	FE	01	F1
01	FE	1F	E0	01	FE	0E	F1
1F	E0	01	FE	0E	F1	01	FE
01	E0	1F	FE	01	F1	0E	FE
01	01	E0	E0	01	01	F1	F1
1F	1F	E0	E0	0E	0E	F1	F1
1F	01	FE	E0	0E	01	FE	F1
01	1F	FE	E0	01	0E	FE	F1
1F	01	E0	FE	0E	01	F1	FE
01	1F	E0	FE	01	0E	F1	FE
01	01	FE	FE	01	01	FE	FE
1F	1F	FE	FE	0E	0E	FE	FE
FE	FE	E0	E0	FE	FE	F1	F1
E0	FE	FE	E0	F1	FE	FE	F1
FE	E0	E0	FE	FE	F1	F1	FE
E0	E0	FE	FE	F1	F1	FE	FE

Ïðåæäå, ÷åì ïîðèöàòü DES ñëàáûå êëþ÷è, îáðàòèìñÿ íà òî, ÷òî ýòè 64 êëþ÷à - ýòî êðîøå÷íàÿ ÷àñòü ïîëíîãî íàáîðà èç 72057594037927936 âîçìîæíûõ êëþ÷åé. Åñëè âû âûáèðàåòå êëþ÷ ñëó÷àéíî, âåðîÿòíîñòü âûáðàòü îäèí èç ñëàáûõ êëþ÷åé ïðåâûñèò ìàëà. Åñëè âû íàñòîÿùèé ïàðàíîèê, ìîæåòå âñåãäà ïðîâåðÿòü "íà ñëàáîñòü" ñãåíåðèðîâàííûé êëþ÷. Íåêîòîðûå äóìàþò, ÷òî íå÷åãî è áåñïîêîèòüñÿ íà ýòîò ñ÷åò. Äóãàå óòâåðæäàþò, ÷òî ïðîâåðêà î÷åíü ëåãêà, ïî÷åìó áû åå è íå âûïîëíèòü.

Äàëüíåéøèé àíàëèç ñëàáûõ è ïîëóñëàáûõ êëþ÷åé ïðèâåäåí â [1116]. Äðóãèõ ñëàáûõ êëþ÷åé â ïðîöåññå èññëåäîâàíèé íàéäåíî íå áûëî.

Êëþ÷è-äîïîëíåíèÿ

Âûïîëíèì ïîáèòîâîå äîïîëíåíèå êëþ÷à, çàìåíÿÿ âñå 0 íà 1 è âñå 1 - íà 0. Òåïåðü, åñëè áëîê îòêðûòîãî òåêñòà çàøèôðîâàí îðèãèíàëüíûì êëþ÷îì, òî äîïîëíåíèå êëþ÷à ïðè øèôðîâàíèè ïðåâðàòèò äîïîëíåíèå áëîêà îòêðûòîãî òåêñòà â äîïîëíåíèå áëîêà øèôðîòåêñòà. Åñëè x' îáîçíà÷àåò äîïîëíåíèå x, òî ñëåäóþùåå âåðíî:

$E_K(P) = C$

$E_K(P') = C'$

Â ýòîì íåò íè÷åãî òàèíñòâåííîãî. Íà êàæäîì ýòàïå ïîñëå ïåðâîíà÷àëüíîé ïåðåñòàíîâêè ñ ðàñøèðåíèåì ïîäâëþ÷è ïîäâåðãàþòñÿ îïåðàöèè XOR ñ ïðåäûäóùèì ïîëîæåíèåì. Ïðÿìûì ñëåäñòâèåì ýòîãî ôàêòà è ÿâëÿåòñÿ ïðèâåäåííîå êîìïëåìåíòíîñòè.

Ýòî îçíà÷àåò, ÷òî ïðè âûïîëíåíèè âñêðûòèÿ DES ñ âûáðàííûì îòêðûòûì òåêñòîì íóæíî ïðîâåðÿòü òîëüêî ïîëîâèíó âîçìîæíûõ êëþ÷åé: 2^{55} âìåñòî 2^{56} [1080]. Ýëè Áèõàì (Eli Biham) è Àäè Øàìèð ïîêàçàëè [172], ÷òî ñóùåñòâóåò âñêðûòèå ñ èçâåñòíûì îòêðûòûì òåêñòîì, èìåþùåå òó æå ñëîæíîñòü, äëÿ êîòîðîãî íóæíî íå ìåíüøå 2^{33} èçâåñòíûõ îòêðûòûõ òåêñòîâ.

Îñòàåòñÿ âîïðîñ, ÿâëÿåòñÿ ëè òàêîå ñâîéñòâî ñëàáîñòüþ, òàê êàê â áîëüøèíñòâå ïîáóæäåíèé íåò êîìïëåìåíòíîãî äëîêîâîãî òîêðûòîãî òåêñòà (äëÿ ñëó÷àéíîãî îòêðûòîãî òåêñòà øàíñ "ïðîèâ" ÷åçâû÷àéíî âåëèê), à ïîëüçîâàòåëé ìîæíî ïðåäóïðåäèòü íå ïîëüçîâàòüñÿ äîïîëíÿþùèìè.

Àëãîðèòì÷åñêàÿ ñòðóêòóðà

Âñå âîçìîæíûå 64-áèòîâûå áëîêè îòêðûòîãî òåêñòà ìîæíî îòîáðàçèòü íà 64-áèòîâûå áëîêè øèôðîâàííà

2^{64}! Ðàçëè÷íûìè ñïîñîáàìè. Àëãîðèòì DES, èñïîëüçóÿ 56-áèòîâûé êëþ÷, ïðåäñòàâëÿåò íàì 2^{56} (ïðèáëèçèòåëüíî 10^{17}) òàêèõ îòîáðàæåíèé. Èñïîëüçîâàíèå ìíîãîêðàòíîãî øèôðîâàíèÿ íà ïððâûé âçãëÿä ïîçâîëÿåò çíà÷èòåëüíî óâåëè÷èòü äîëþ âîçìîæíûõ îòîáðàæåíèé. Íî ýòî ïðàâèëüíî òîëüêî, åñëè äåéñòâèå DES íå îáëàäàåò îïðåäåëåííîé àëãåáðàè÷åñêîé ñòðóêòóðîé.

Åñëè áû DES áûë **çàìêíóòû ì**, òî äëÿ ëþáûõ K_1 è K_2 âñåãäà ñóùåñòâóåò áû òàêîå K_3, ÷òî

$$E_{K_2}(E_{K_1}(P)) = E_{K_3}(P)$$

Äðóãèì ñëîâàìè, îïåðàöèÿ øèôðîâàíèÿ DES îáðàçîâàëà áû ãðóïïó, è øèôðîâàíèå íàíåñ áëîêîâ îòêðûòîãî òåêñòà îïèñûâàåòñÿ ñ ïîìîùüþ K1 è K2 áûëî áû èäåíòè÷íî øèôðîâàíèþ áëîêîâ êëþ÷îì K3. ×òî åùå õóæå, DES áûë áû ÷óâñòâèòåëåí ê âñêðûòèþ "âñòðå÷à ïîñðåäèíå" ñ èçâåñòíûì îòêðûòûì òåêñòîì, äëÿ êîòîðîãî ïîòðåáîâàëîñü áû òîëüêî 2^{28} ýòàïîâ [807].

Åñëè áû DES áûë **÷åòíû ì**, òî äëÿ ëþáûõ K_1, K_2 è K_3 âñåãäà ñóùåñòâóåò áû òàêîå K_4, ÷òî

$$E_{K_3}(E_{K_2}(E_{K_1}(P))) = E_{K_4}(P)$$

Òðîéíîå øèôðîâàíèå áûëî áåçîïàñíûì. (Çàìåòüòå, ÷òî çàìêíóòûé øèôð îáÿçàòåëüíî ÿâëÿåòñÿ è ÷åòíûì, íî ÷åòíûé øèôð íå îáÿçàòåëüíî ÿâëÿåòñÿ çàìêíóòûì.)

Ðÿä ïîäñêàçîê ìîæíî íàéòè â ðàííåé òåîðåòè÷åñêîé ðàáîòå Äîíà Êîïïåðñìèòà, íî ýòîãî íåäîñòàòî÷íî [377]. Ðàçëè÷íûå êðèïòîãðàôû ïûòàëèñü ðåøèòü ýòó ïðîáëåìó [588, 427, 431, 527, 723, 789]. Â ïîâòîðÿþùèõñÿ ýêñïåðèìåíòàõ ñîáëþäàëèñü "íåïðîâåðæèìûå äîêàçàòåëüñòâà" òîãî, ÷òî DES íå ÿâëÿåòñÿ ãðóïïîé [807, 371, 808, 1116, 809], íî òîëüêî â 1992 ãîäó êðèòîãðàôàì óäàëîñü ýòî äîêàçàòü îêîí÷àòåëüíî [293]. Êîïïåðñìèò óòâåðæäàåò, ÷òî êîìáèíàöèÿ IBM çíàëà îá ýòîì ñòàòóñå íà÷àëà.

Äëèíà êëþ÷à

Â îðèãèíàëüíîé çàÿâêå ôèðìû IBM â NBS ïðåäïîëàãàëîñü èñïîëüçîâàòü 112-áèòîâûé êëþ÷. Ê òîìó âðåìåíè, êîãäà DES ñòàíäàðòèçèðîâàëñÿ äî 56 áèò. Ìíîãèå êðèòèêîâàëè íàñòàèâàëè íà áîëåå äëèííîì êëþ÷å. Îñíîâíûì èñ àðãóìåíòîì áûëî âñêðûòèå ãðóáîé ñèëîé (ñì. ðàçäåë 7.1).

Â 1976 è 1977 ãã. Äèôôè è Õåëëìàí óòâåðæäàëè, ÷òî ñïåöèàëèçèðîâàííûé ïàðàëëåëüíûé êîìïüþòåð äëÿ âñêðûòèÿ DES, ñòîÿùèé 20 ìèëëèîíîâ äîëëàðîâ, ñìîæåò ðàñêðûòü êëþ÷ çà äåíü. Â 1981 ãîäó Äèôôè óâåëè÷èë âðåìÿ ïîèñêà äî äâóõ äíåé, à ñòîèìîñòü - äî 50 ìèëëèîíîâ äîëëàðîâ [491]. Äèôôè è Õåëëìàí óòâåðæäàëè, ÷òî âñêðûòèå â òîì ìîìåíò âðåìåíè íàõîäèëîñü çà ïðåäåëàìè âîçìîæíîñòåé ëþáîé îðãàíèçàöèè, êðîìå ïîäîáíûõ NSA, íî ÷òî ê 1990 ãîäó DES äîëæåí ïîëíîñòüþ óòðàòèòü ñâîþ ïðèâëåêàòåëüíîñòü [714].

Õåëëìàí [716] ïðîäåìîíñòðèðîâàë åùå îäèí àðãóìåíò ïðîòèâ ìàëîãî ðàçìåðà êëþ÷à: ðàçìåíèâàÿ îáúåì ïàìÿòè íà âðåìÿ, ìîæíî óñêîðèòü ïðîöåññ ïîèñêà. Îí ïðåäëîæèë âû÷èñëÿòü è õðàíèòü 2^{56} âîçìîæíûõ ðåçóëüòàòîâ øèôðîâàíèÿ êàæäûì âîçìîæíûì êëþ÷îì åäèíñòâåííîãî áëîêà îòêðûòîãî òåêñòà. Òîãäà äëÿ âçëîìà íåèçâåñòíîãî êëþ÷à êðèïòîàíàëèòèê ïîòðåáóåòñÿ òîëüêî ñòîëüêî âðåìåíè, ñêîëüêî ïîòðåáîâàëîñü äëÿ øèôðîâàíèÿ îäíîãî áëîêà. Òåëëìàí îöåíèë ñòîèìîñòü òàêîãî óñòðîéñòâà âñêðûòèÿ DES ïðîäîëæàþ ïîÿâëÿòüñÿ. Ì íîãèå óêàçûâàþò íà òî, ÷òî ñðåäíåå âðåìÿ íàõàîäêè íà îòêàç äëÿ ìèêðîñõåì DES íèêîãäà íå áûë áîëüøå íåñêîëüêèõ ìåñÿöåâ, ïîñêîëüêó DES ïîñòîÿííî ìåíÿåòñÿ ðåçóëüòàò è óìåíüøåíèå ýôôåêòèâíîñòè ïðèâîäèò ê íåîáõîäèìîñòè òàêîãî óñòðîéñòâà âñêðûòèÿ â 5 ìèëëèîíîâ äîëëàðîâ.

Àðãóìåíòû çà è ïðîòèâ ñóùåñòâîâàíèÿ â êàêîì-íèáóäü òàéíîì áóíêåðå ïðàâèòåëüñòâåííîãî óñòðîéñòâà âñêðûòèÿ DES ïðîäîëæàþò ïîÿâëÿòüñÿ. Ì íîãèå óêàçûâàþò íà òî, ÷òî ñðåäíåå âðåìÿ íàõàîäêè ïîäõîäÿùåãî êëþ÷à ê òîêàç äëÿ ìèêðîñõåì DES íèêîãäà íå áûë áîëüøå íåñêîëüêèõ ìåñÿöåâ, ïîñêîëüêó â [1278] áûëî ïîêàçàíî, ÷òî ýòîãî âîçðàæåíèÿ áîëåå ÷åì äåñÿòèëåòíåé äàâíîñòè. Äóãàå èññëåäîâàòåëè ïðåäëîæèëè ïîäõîä ê ïîñòðîåíèþ ñïåöèàëèçèðîâàííîãî óñòðîéñòâà, êîòîðîå ìîæåò ðàñêðûâàòü ñåêðåòíûé êëþ÷ çà íåñêîëüêî ìèíóò.

Ìåæäó òåì, àïïàðàòíûå ðåàëèçàöèè DES ïîñòîÿííî ïðèáëèçèëèñü ê ðåàëèçàöèè òðåõìåãàáèòíîãî øèôðîâàíèÿ â ñåêóíäó, ïðåâúÿâèâ îí ïîëíóþ ñîâìåñòèìîñòü ñ ïðåäûäóùèì ñòàíäàðòîì. Â 1984 ãîäó áûëè âûïóùåíû ìèêðîñõåìû DES, ñïîñîáíûå âûïîëíÿòü 256000 øèôðîâàíèÿ â ñåêóíäó [533, 534]. Ê 1987 ãîäó áûëè ðàçðàáîòàíû ìèêðîñõåìû DES, âûïîëíÿþùèå 512000 øèôðîâàíèé â ñåêóíäó, è ñòàëî âîçìîæíûì ïîÿâëåíèå âàðèàíòà, ñïîñîáíîãî ïðîâåðÿòü ñâîøå ìèëëèîíà êëþ÷åé â ñåêóíäó [738, 1573]. À â 1993 Ìàéêë Âèåð (Michael Wiener) ñïðîåêòèðîâàë ìàøèíó ñòîèìîñòüþ 1 ìèëëèîí äîëëàðîâ, êîòîðàÿ ìîæåò âûïîëíÿòü 1 ìèëëèîí îïåðàöèé â ñåêóíäó è äàæå íà î÷åíü áîëüøîé ñòðàíå DES ãðóáîé ñèëîé â ñðåäíåì çà 3.5 ÷àñà (ñì. ðàçäåë 7.1).

Íèêòî òêðûòî íå çàÿâèë î ñîçäàíèè ýòîé ìàøèíû, õîòÿ ðàçóìíî ïðåäïîëîæèòü, ÷òî êîìó-òî ýòî óäàëîñü. Ì ëëèîí äîëëàðîâ - ýòî íåñëèøêîì áîëüøèå äåíüãè äëÿ áîëüøîé è äàæå íà î÷åíü áîëüøîé ñòðàíû.

Â 1990 ãîäó äâà èçðàèëüñêèõ ìàòåìàòèêà, Áèõàì (Biham) è Øàìèð, îòêðûëè **äèôôåðåíöèàëüíûé êðèïòîàíàëèç**, ìåòîä, êîòîðûé ïîçâîëèë îñòàâèòü â îïèñ âîïðîñ äëÿ÷íûõ êëþ÷à. Ïðåæäå, ÷åì ìû ðàññìîòðèì ýòîò ìåòîä, âåðíåìñÿ ê íåêîòîðûì äóãàì êðèòè÷åñêèì çàìå÷àíèÿì â àäðåñ DES.

Êîëè÷åñòâî ýòàïîâ

Ïî÷åìó 16 ýòàïîâ? Ïî÷åìó íå 32? Ïîñëå ïÿòè ýòàïîâ êàæäûé áèò øèôðîòåêñòà ÿâëÿåòñÿ ôóíêöèåé âñåõ áèòîâ îòêðûòîãî òåêñòà è âñåõ áèòîâ êëþ÷à [1078, 1080], à ïîñëå âîñüìè ýòàïîâ øèôðîòåêñò ïî ñóòè ïðåäñòàâëÿåò ñîáîé ñëó÷àéíóþ ôóíêöèþ âñåõ áèòîâ îòêðûòîãî òåêñòà è âñåõ áèòîâ êëþ÷à [880]. (Ýòî íàçûâàåòñÿ ëàâèííûì ýôôåêòîì.) Òàê ïî÷åìó íå îñòàíîâèòüñÿ ïîñëå âîñüìè ýòàïîâ?

Â òå÷åíèå ìíîãèõ ëåò âåðñèè DES ñ óìåíüøåííûì ÷èñëîì ýòàïîâ óñïåøíî âñêðûâàëèñü. DES ñ òðåìÿ è ÷åòûðüìÿ ýòàïàìè áûë ëåãêî âçëîìàí â 1982 ãîäó [49]. DES ñ øåñòüþ ýòàïàìè ïàë íåñêîëüêèìè ãîäàìè ïîçæå [336]. Äèôôåðåíöèàëüíûé êðèïòîàíàëèç Áèõàìà è Øàìèðà îáúÿñíèë è ýòî: DES ñ ëþáûì êîëè÷åñòâîì ýòàïîâ, ìåíüøèì 16, ìîæåò áûòü âçëîìàí ñ ïîìîùüþ âñêðûòèÿ ñ èçâåñòíûì îòêðûòûì òåêñòîì áûñòðåå, ÷åì ñ ïîìîùüþ âñêðûòèÿ ãðóáîé ñèëîé. Êîíå÷íî ãðóáûé âçëîì ÿâëÿåòñÿ áîëåå âåðîÿòíûì ñïîñîáîì âñêðûòèÿ, íî èíòåðåñåí òîò ôàêò, ÷òî àëãîðèòì ñîäåðæèò ðîâíî 16 ýòàïîâ.

Ïðîåêòèðîâàíèå S-áëîêîâ

Ïîìèìî óìåíüøåíèÿ äëèíû êëþ÷à NSA òàêæå îáâèíÿþò â èçìåíåíèè ñîäåðæàíèÿ S-áëîêîâ. Íàñòàèâàÿ íà ïîäòâåðæäåíèè ñõåìû S-áëîêîâ, NSA çàÿâèëî, ÷òî äåòàëè àëãîðèòìà ÿâëÿþòñÿ "÷óâñòâèòåëüíûìè" è íå ìîãóò áûòü îïóáëèêîâàíû. Ìíîãèå êðèïòîãðàôû ïîäîçðåâàëè, ÷òî ðàçðàáîòàííûå â NSA S-áëîêè ñîäåðæàò ëàçåéêó, ïîçâîëÿþùóþ NSA ëåãêî âûïîëíÿòü êðèïòîàíàëèç àëãîðèòìà.

Ñ ìîìåíòà ïîÿâëåíèÿ àëãîðèòìà äëÿ àíàëèçà ñõåìû è ðàáîòû S-áëîêîâ áûëè ïðåäïðèíÿòû çíà÷èòåëüíûå óñèëèÿ. Â ñåðåäèíå 70-õ Lexar Corporation [961, 721] è Bell Laboratories [1120] èññëåäîâàëè ðàáîòó S-áëîêîâ. Íè îäíî èç èññëåäîâàíèé íå îáíàðóæèëî íèêàêèõ ñëàáîñòåé, õîòÿ îáà èññëåäîâàíèÿ îáíàðóæèëè íåïîíÿòíûé ñâîéñòâà. S-áëîêè èìåþò áîëüøå ñâîéñòâ, îáùèõ ñ ëèíåéíûì ïðåîáðàçîâàíèåì, ÷åì ìîæíî áûëî îæèäàòü ïðè èõ ôîðìèðîâàíèè ñëó÷àéíûì îáðàçîì. Êîìàíäà Bell Laboratories êîíñòàòèðîâàëà, ÷òî S-áëîêè ìîãóò ñîäåðæàòü ñêðûòûå ëàçåéêè, à äîêëàä Lexar çàâåðøàëñÿ ñëåäóþùåé ôðàçîé:

> Â DES áûëè íàéäåíû ñòðóêòóðû, íåñîìíåííî âñòàâëåííûå äëÿ ïîâûøåíèÿ óñòîé÷èâîñòè ñèñòåìû ê îïðåäåëåííûì òèïàì âñêðûòèÿ. Òàêæå áûëè íàéäåíû ñòðóêòóðû, êîòîðûå, ïî âèäèìîìó, îñëàáèëè ñèñòåìó.

Ñ äðóãîé ñòîðîíû ýòîò äîêëàä òàêæå ñîäåðæàë ñëåäóþùåå ïðåäóïðåæäåíèå:

> ... ïðîáëåìà [ïîèñêà ñòðóêòóð â S-áëîêàõ] óñëîæíÿåòñÿ èç-çà ñïîñîáíîñòè ÷åëîâå÷åñêîãî ñîçíàíèÿ íàõîäèòü â ñëó÷àéíûõ äàííûõ ñòðóêòóðû, êîòîðûå â äåéñòâèòåëüíîñòè âîâñå íå ÿâëÿþòñÿ ñòðóêòóðàìè.

Íà âòîðîì ñèìïîçèóìå ïî DES Àãåíòñòâî íàöèîíàëüíîé áåçîïàñíîñòè ðàñêðûëî ðÿä êðèòåðèåâ ïðîåêòèðîâàíèÿ S-áëîêîâ [229]. Íî ýòî íå ñìîãëî ñíÿòü âñåõ ïîäîçðåíèé, è ñïîð ïðîäîëæèëñÿ [228, 422, 714, 1506, 1551].

Â ëèòåðàòóðå ïðî S-áëîêè ïèñàëèñü óäèâèòåëüíûå âåùè. Ïîñëåäíèå òðè áèòà ðåçóëüòàòà ÷åòâåðòîãî S-áëîêà ìîãóò áûòü ïîëó÷åíû òåì æå ñïîñîáîì, ÷òî è ïåðâûå, ïðè ïîìîùè äîïîëíåíèÿ íåêîòîðûõ èç âõîäíûõ áèòîâ [436, 438]. Ðàçëè÷íûå, íî òùàòåëüíî ïîäîáðàííûå âõîäíûå äàííûå äëÿ S-áëîêîâ ìîãóò äàâàòü îäèíàêîâûé ðåçóëüòàò [436]. Ìîæíî ïîëó÷èòü ðåçóëüòàò îäíîãî ýòàïà DES, ìåíÿÿ áèòû òîëüêî â òðåõ ñîñåäíèõ S-áëîêàõ [487]. Øàìèð çàìåòèë, ÷òî ýëåìåíòû S-áëîêîâ, êàçàëîñü, áûëè íåñêîëüêî íåóñòîé÷èâû, íî íå ñîáèðàëñÿ èñïîëüçîâàòü ýòó íåóñòîé÷èâîñòü äëÿ âñêðûòèÿ [1423]. (Îí óïîìÿíóë îá îñîáåííîñòè ïÿòîãî S-áëîêà, íî òîëüêî ñïóñòÿ âîñåìü ëåò ëèíåéíûé êðèïòîàíàëèç âîñïîëüçîâàëñÿ ýòîé îñîáåííîñòüþ.) Äðóãèå èññëåäîâàòåëè ïîêàçàëè, ÷òî äëÿ ïîëó÷åíèÿ S-áëîêîâ ñ íàáëþäàåìûìè õàðàêòåðèñòèêàìè ìîãëè èñïîëüçîâàòüñÿ îáùåèçâåñòíûå ïðèíöèïû ïðîåêòèðîâàíèÿ [266].

Äîïîëíèòåëüíûå ðåçóëüòàòû

Áûëè ïðåäïðèíÿòû è äðóãèå ïîïûòêè êðèïòîàíàëèçèðîâàòü DES. Îäèí èç êðèïòîãðàôîâ èñêàë çàêîíîìåðíîñòè, èñïîëüçóÿ ñïåêòðàëüíûå òåñòû [559]. Äðóãèå àíàëèçèðîâàëè ïîñëåäîâàòåëüíîñòü ëèíåéíûõ ìíîæèòåëåé, íî èõ âñêðûòèå ïîòåðïåëî íåóäà÷ó ïîñëå âîñüìè ýòàïîâ [1297, 336, 531]. Íåîïóáëèêîâàííîå âñêðûòèå, âûïîëíåííîå â 1987 ãîäó Äîíàëüäîì Äýâèñîì (Donald Davies), èñïîëüçîâàëî ñïîñîá, ñ ïîìîùüþ êîòîðîãî ïåðåñòàíîâêà ñ ðàñøèðåíèåì ïîâòîðÿåò áèòû â ñîñåäíèõ S-áëîêàõ, ýòî âñêðûòèå òàêæå îêàçàëîñü áåñïîëåçíûì ïîñëå âîñüìè ýòàïîâ [172, 429].

12.4 Äèôôåðåíöèàëüíûé è ëèíåéíûé êðèïòîàíàëèç

Äèôôåðåíöèàëüíûé êðèïòîàíàëèç

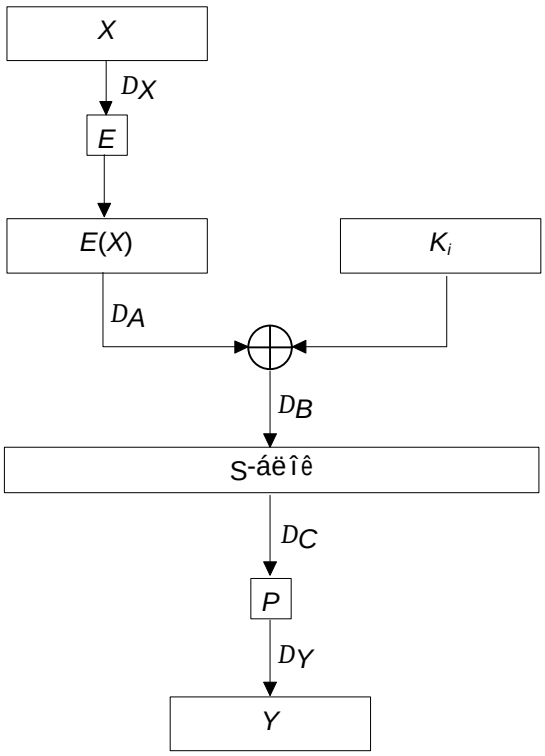
Â 1990 ãîäó Ýëè Áèõàì è Àäè Øàìèð ââåëè ïîíÿòèå **äèôôåðåíöèàëüíîãî êðèïòîàíàëèçà** [167, 168, 171, 172]. Ýòî áûë íîâûé, ðàíåå íåèçâåñòíûé ìåòîä êðèïòîàíàëèçà. Èñïîëüçóÿ ýòîò ìåòîä, Áèõàì è Øàìèð íàøëè ñïîñîá âñêðûòèÿ DES ñ èñïîëüçîâàíèåì âûáðàííîãî îòêðûòîãî òåêñòà, êîòîðûé áûë ýôôåêòèâíåå âñêðûòèÿ ãðóáîé ñèëîé.

Äèôôåðåíöèàëüíûé êðèïòîàíàëèç ðàáîòàåò ñ **ïàðàìè øèôðîòåêñòîâ**, îòêðûòûå òåêñòû êîòîðûõ ñîäåðæàò îïðåäåëåííûå îòëè÷èÿ. Ìåòîä àíàëèçèðóåò ýâîëþöèþ ýòèõ îòëè÷èé â ïðîöåññå ïðîõîæäåíèÿ îòêðûòûõ òåêñòîâ

÷åðåç ýòàïû DES ïðè øèôðîâàíèè îäíèì è òåì æå êëþ÷îì.

Ïðîñòî âûáåðåì ïàðó îòêðûòûõ òåêñòîâ ñ ôèêñèðîâàííûì ðàçëè÷èåì. Ìîæíî âûáðàòü äâà îòêðûòûõ òåêñòà ñëó÷àéíûì îáðàçîì, ëèøü áû îíè îòëè÷àëèñü äðóã îò äðóãà îïðåäåëåííûì îáðàçîì, êðèòè÷íàëèòåò äàæå íå íóæíî çíàòü èõ çíà÷åíèé. (Äëÿ DES òåðìèí "ðàçëè÷èå" îïðåäåëÿåòñÿ ñ ïîìîùüþ XOR. Äëÿ äðóãèõ àëãîðèòìîâ ýòî òåðìèí ìîæåò îïðåäåëÿòüñÿ ïî äðóãîìó.) Çàòåì, èñïîëüçóÿ ðàçëè÷èå â ïîëó÷èâøèõñÿ øèôðîâêòàõ, ïðèñâîèì ðàçëè÷íûå âåðîÿòíîñòè ðàçëè÷íûì êëþ÷àì. Â ïðîöåññå äàëüíåéøåãî àíàëèçà ñëåäóþùèõ ïàð øèôðîâîê-ñòîâ îäèí èç êëþ÷åé ñòàíåò íàèáîëåå âåðîÿòíûì. Ýòî è åñòü ïðàâèëüíûé êëþ÷.

Ïîäõîäîùèì îðàçîì ñëîæíåå. Íà 7-é ïðåäñòàâëåíà ôóíêöèÿ îäíîãî ýòàïà DES. Ïðåäñòàâüòå ñåáå ïàðó âõîäîâ, X è X', ñ ðàçëè÷èåì ΔX. Âûõîäû, Y è Y' èçâåñòíû, ñëåäîâàòåëüíî, èçâåñòíî è ðàçëè÷èå ìåæäó íèì è ΔY. Èçâåñòíû è ïðåäñòàâëåíèå ñ ðàñøèðåíèåì, è P-áëîê, ïîýòîìó èçâåñòíû ΔA è ΔC. B è B' íåèçâåñòíû, íî èõ ðàçíîñòü ΔB èçâåñòíà è ðàâíà ΔA. (Ïðè ðàññìîòðåíèè ðàçëè÷èÿ XOR K_i ñ A è A' íåèòåðåñóþùèõ íàñ.) Ïîêà âñå ïðîñòî. Ôîêóñ âîò â ÷åì: äëÿ ëþáîãî çàäàííîãî ΔA íå âñå çíà÷åíèÿ ΔC ðàâíîâåðîÿòíû. Êîìáèíàöèÿ ΔA è ΔC ïîçâîëÿåò ïðåäïîëîæèòü çíà÷åíèÿ áèòîâ äëÿ A XOR K_i è A' XOR K_i. Òàê êàê A è A' èçâåñòíû, ýòî äàåò íàì èíôîðìàöèþ î K_i.



Ðèñ. 12-5. Ôóíêöèÿ ýòàïà DES.

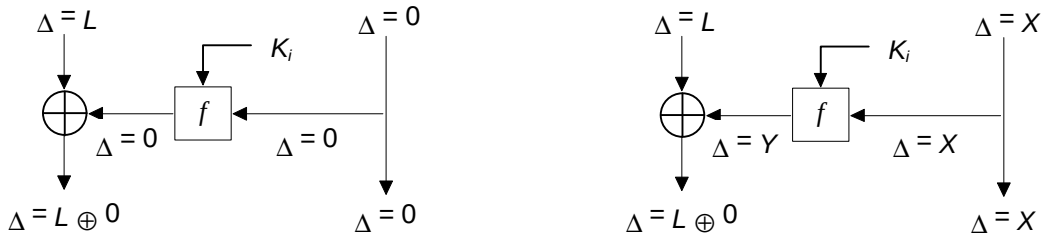
Âçãëÿíåì íà ïîñëåäíèé ýòàï DES. (Ïðè äèôôåðåíöèàëüíîì êðèïòàíàëèçå íà÷àëüíàÿ è çàêëþ÷èòåëüíàÿ ïåðåñòàíîâêè èãíîðèðóþòñÿ. Î íè íå âëèÿþò íà âñêðûòèå, òîëüêî çàòóäíÿþ îáúÿñíåíèå.) Åñëè ìû ñìîæåì îïðåäåëèòü K_{16}, òî ìû ïîëó÷èì 48 áèòîâ êëþ÷à. (Íå çàáûâàéòå, íà êàæäîì ýòàïå ïîâêëþ÷ ñîñòîèò èç 48 áèòîâ 56-áèòîâîãî êëþ÷à.) Îñòàâøèåñÿ 8 áèòîâ ìû ìîæåì ïîëó÷èòü ðóáûì âçëîìîì. K_{16} äàñò íàì äèôôåðåíöèàëüíûé êðèïòîàíàëèç.

Î ïðåäïîëîæèì ïàð îòêðûòûõ òåêñòîâ îáëàäàþò âûñîêîé âåðîÿòíîñòüþ âûçâàòü îïðåäåëåííûå ðàçëè÷èÿ ïîëó÷åííûõ øèôðîâîê. Ýòè ðàçëè÷èÿ íàçûâàþòñÿ **õàðàêòåðèñòèêàìè**. Õàðàêòåðèñòèêè ðàñïðîñòðàíÿþòñÿ íà îïðåäåëåííûå êîëè÷åñòâî ýòàïîâ è ïî ñóùåñòâó îïðåäåëÿò ïðîãíîçèðóåìîñòü ýòèõ ýòàïîâ. Ñóùåñòâóþò âõîäíûå ðàçëè÷èå, ðàçëè÷èå íà êàæäîì ýòàïå è âûõîäíûå ðàçëè÷èå - ñ îïðåäåëåííîé âåðîÿòíîñòüþ.

Ýòè õàðàêòåðèñòèêè ìîæíî íàéòè, ñîçäàâ òàáëèöó, ñòðîêè êîòîðîé ïðåäñòàâëÿþò âîçìîæíûå âõîäû XOR (XOR äâóõ ðàçëè÷íûõ íàíîñîâ âõîäíûõ áèòîâ), ñòîëáöû - âîçìîæíûå ðåçóëüòàòû XOR, à ÿëåìåíò - ñêîëüêî ðàç êîíêðåòíûé ðåçóëüòàò XOR âñòðå÷àåòñÿ äëÿ çàäàííîãî âõîäà XOR. Òàêóþ òàáëèöó ìîæíî ñäåëàòü äëÿ êàæäîãî èç âîñüìè S-áëîêîâ DES.

Íàïðèìåð, íà 6-éà ïîêàçàíà õàðàêòåðèñòèêà îäíîãî ýòàïà. Âõîäíîå ðàçëè÷èå ñëåâà ðàâíî L, îíî ìîæåò âûòè ïðîèçâîëüíûì. Âõîäíîå ðàçëè÷èå ñïðàâà ðàâíî 0. (Ó âõóõ âõîäîâ îäèíàêîâàÿ ïðàâàÿ ïîëîâèíà, ïîýòîìó èõ ðàçëè÷èå - 0.) Òàê êàê íà âõîäå ôóíêöèè ýòàïà íåò íèêàêèõ ðàçëè÷èé, òî íåò ðàçëè÷èé è íà âûõîäå ôóíêöèè ýòàïà. Ñëåäîâàòåëüíî, âûõîäíîå ðàçëè÷èå ëåâîé ÷àñòè - $L \oplus 0 = L$, à âûõîäíîå ðàçëè÷èå ïðàâîé ÷àñòè - 0. Ýòî òðèâèàëüíàÿ õàðàêòåðèñòèêà, îíà èñòèííà ñ âåðîÿòíîñòüþ 1.

Íà 6-éá ïîêàçàíà ìåíåå î÷åâèäíàÿ õàðàêòåðèñòèêà. Ñíîâà, ðàçëè÷èå *L* ëåâûõ ÷àñòåé ïðîèçâîëüíî. Âõîäíîå ðàçëè÷èå ïðàâûõ ÷àñòåé ðàâíî 0x60000000, äâà âõîäà îòëè÷àþòñÿ òîëüêî ïåðâûì è òðåòüèì áèòàìè. Ñ âåðîÿòíîñòüþ 14/64 ðàçëè÷èå íà âûõîäå ôóíêöèè ýòàïà ðàâíî *L* ⊕ 0x00808200. Ýòî îçíà÷àåò, ÷òî âûõîäíîå ðàçëè÷èå ëåâûõ ïîëîâèí ðàâíî *L* ⊕ 0x00808200, à âûõîäíîå ðàçëè÷èå ïðàâûõ ïîëîâèí - 0x60000000 (ñ âåðîÿòíîñòüþ 14/64)



X = 0x60000000
Y = 0x00808200

Ñ âåðîÿòíîñòüþ 1

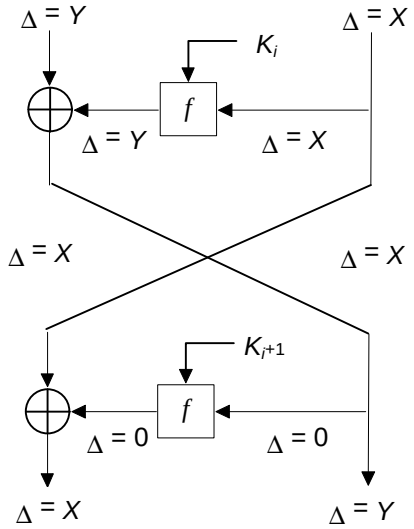
(a)

Ñ âåðîÿòíîñòüþ 14/64

(b)

Ðèñ. 12-6. Õàðàêòåðèñòèêè DES.

Ðàçëè÷íûå õàðàêòåðèñòèêè ìîæíî îáúåäèíÿòü. Òàêæå, ïðè óñëîâèè, ÷òî ýòàïû íåçàâèñèìû, âåðîÿòíîñòè ìîãóò ïåðåìíîæàòüñÿ. Íà 5-é îáúåäèíÿþùåé äâå ðàíåå îïèñàííûõ õàðàêòåðèñòèêè. Âõîäíîå ðàçëè÷èå ñëåâà ðàâíî 0x00808200, à ñïðàâà - 0x60000000. Â êîíöå ïåðâîãî ýòàïà âõîäíîå ðàçëè÷èå è ðåçóëüòàò ôóíêöèè ýòàïà íåòðóäíî ðàññ÷èòàòü äðóãà äðóãà, è âûõîäíîå ðàçëè÷èå ðàâíî 0. Ýòî ðàçëè÷èå ïîñòóïàåò íà âõîä âòîðîãî ýòàïà, îêî÷àòåëüíîå âûõîäíîå ðàçëè÷èå ñëåâà ðàâíî 0x60000000, à ñïðàâà - 0. Âåðîÿòíîñòü ýòîé äâóõýòàïíîé õàðàêòåðèñòèêè - 14/64.



X = 0x60000000
Y = 0x00808200

Ñ âåðîÿòíîñòüþ 14/64

(b)

Ðèñ. 12-7. Äâóõýòàïíàÿ õàðàêòåðèñòèêà DES.

Ïàðà îòêðûòûõ òåêñòîâ, ñîîòâåòñòâóþùèõ õàðàêòåðèñòèêå, íàçûâàþòñÿ ïðàâèëüíîé ïàðîé, à ïàðà îòêðûòûõ òåêñòîâ, íåñîîòâåòñòâóþùèõ õàðàêòåðèñòèêå - íåïðàâèëüíîé ïàðîé. Ïðàâèëüíàÿ ïàðà ïîäâåðãàåòñÿ ïðàâèëüíûé êëþ÷ ýòàïà (äëÿ ïîñëåäíåãî ýòàïà õàðàêòåðèñòèêè), íåïðàâèëüíàÿ ïàðà - ñëó÷àéíûé êëþ÷ ýòàïà.

×òîáû íàéòè ïðàâèëüíûé êëþ÷ ýòàïà, íóæíî ïðîñòî ñîáðàòü äîñòàòî÷íîå êîëè÷åñòâî ïðåäïîëîæåíèé. Îäíî

èç ïîäêëþ÷åé áóäåò âñòðå÷àòüñÿ ÷àùå, ÷åì âñå îñòàëüíûå. Ôàêòè÷åñêè, ïðàâèëüíûé ïîäêëþ÷ âîçíèêíåò èç âñåõ ñëó÷àéíûõ âîçìîæíûõ ïîäêëþ÷åé.

Èòàê, äèôôåðåíöèàëüíîå îñíîâíîå âñêðûòèå n-ýòàïíîãî DES äàåò 48-áèòîâûé ïîäêëþ÷, èñïîëüçóåìûé íà ýòàïå n, à îñòàâøèåñÿ 8 áèòîâ êëþ÷à ïîëó÷àþòñÿ ñ ïîìîùüþ ãðóáîãî âçëîìà.

Íî ðÿä çàìåòíûõ ïðîáëåì âñå æå îñòàåòñÿ. Âî ïåðâûõ, ïîêà âû íå ïåðåéäåòå ÷åðåç íåêîòîðîå ïîðîãîâîå çíà÷åíèå, âåðîÿòíîñòü óñïåõà ïðåíåáðåæèìî ìàëà. Òî åñòü, ïîêà íå áóäåò íàêîïëåíî äîñòàòî÷íîå êîëè÷åñòâî äàííûõ, âûäåëèòü ïðàâèëüíûé ïîäêëþ÷ èç øóìà íåâîçìîæíî. Êðîìå òîãî, òàêîå âñêðûòèå íå ïðàêòè÷íî. Äëÿ õðàíåíèÿ âåðîÿòíîñòåé 2^{48} âîçìîæíûõ êëþ÷åé íåîáõîäèìî èñïîëüçîâàòü ñ÷åò÷èêè, è ê òîìó æå äëÿ âñêðûòèÿ ïîòðåáóåòñÿ ñëèøêîì ìíîãî äàííûõ.

Áèõàì è Øàìèð ïðåäëîæèëè ñâîé ñïîñîá âñêðûòèÿ. Âìåñòî èñïîëüçîâàíèÿ 15-ýòàïíîé õàðàêòåðèñòèêè 16-ýòàïíîãî DES, îíè èñïîëüçîâàëè 13-ýòàïíóþ õàðàêòåðèñòèêó è ðÿä ïðèåìîâ äëÿ ïîëó÷åíèÿ ïîñëåäíèõ íåñêîëüêèõ ýòàïîâ. Áîëåå êîðîòêàÿ õàðàêòåðèñòèêà ñ áîëüøåé âåðîÿòíîñòüþ áóäåò ðàáîòàòü ëó÷øå. Îíè òàêæå èñïîëüçîâàëè íåêîòîðûå ñëîæíûå ìàòåìàòè÷åñêèå ïðèåìû äëÿ ïîëó÷åíèÿ âåðîÿòíûõ 56-áèòîâûõ êëþ÷åé, êîòîðûå è ïðîâåðÿëèñü íåìåäëåííî, òàêèì îáðàçîì óñòðàíÿëàñü ïîòðåáíîñòü â ñ÷åò÷èêàõ. Òàêîå âñêðûòèå äîñòèãàåò óñïåõà, êàê òîëüêî íàõîäèòñÿ ïðàâèëüíàÿ ïàðà. Ýòî ïîçâîëÿåò èçáåæàòü ïîðîãîâîãî ýôôåêòà è ïîëó÷èòü ëèíåéíóþ çàâèñèìîñòü äëÿ âåðîÿòíîñòè óñïåõà. Åñëè ó âàñ â 1000 ðàç ìåíüøå ïàð, òî âåðîÿòíîñòü óñïåõà â 1000 ðàç ìåíüøå. Ýòî çâó÷èò óæàñíî, íî ýòî íàìíîãî ëó÷øå, ÷åì ïîðîã. Âñåãäà åñòü íåêîòîðàÿ âåðîÿòíîñòü íåìåäëåííîé óäà÷è.

Ðåçóëüòàòû ÿâëÿþòñÿ âåñüìà èíòåðåñíûìè. Â -2-é ïðîâåäåí îáçîð ëó÷øèõ äèôôåðåíöèàëüíûõ âñêðûòèé DES ñ ðàçëè÷íûì êîëè÷åñòâîì ýòàïîâ [172]. Ïåðâûé ñòîëáåö ñîäåðæèò êîëè÷åñòâî ýòàïîâ. Ýëåìåíòû ñëåäóþùèõ äâóõ ñòîëáöà ïðåäñòàâëÿþò ñîáîé êîëè÷åñòâî âûáðàííûõ èëè èçâåñòíûõ îòêðûòûõ òåêñòîâ, êîòîðûå äîëæíû áûòü ïðîâåðåíû äëÿ âñêðûòèÿ, à ÷åòâåðòûé ñòîëáåö ñîäåðæèò êîëè÷åñòâî äåéñòâèòåëüíî ïðîàíàëèçèðîâàííûõ îòêðûòûõ òåêñòîâ. Â ïîñëåäíåì ñòîëáöå ïðèâåäåíà ñëîæíîñòü àíàëèçà, ïîñëå îáíàðóæåíèÿ òðåáóåìîé ïàðû.

Òàáë. 12-14. Âñêðûòèå ñ ïîìîùüþ äèôôåðåíöèàëüíîãî êðèïòîàíàëèçà

Êîëè÷åñòâî ýòàïîâ	Âûáðàííûå îòêðûòûå òåêñòû	Èçâåñòíûå îòêðûòûå òåêñòû	Ïðîàíàëèçèðîâàííûå îòêðûòûå òåêñòû	Ñëîæíîñòü àíàëèçà
8	2^{14}	2^{38}	4	29
9	2^{24}	2^{44}	2	2^{32}†
10	2^{24}	2^{43}	2^{14}	2^{15}
11	2^{31}	2^{47}	2	2^{32}†
12	2^{31}	2^{47}	2^{21}	2^{21}
13	2^{39}	2^{52}	2	2^{32}†
14	2^{39}	2^{51}	2^{29}	2^{29}
15	2^{47}	2^{56}	27	2^{37}
16	2^{47}	2^{55}	2^{36}	2^{37}

† Ñëîæíîñòü àíàëèçà äëÿ ýòèõ âàðèàíòîâ ìîæåò áûòü çíà÷èòåëüíî óìåíüøåíà çà ñ÷åò èñïîëüçîâàíèÿ ïðèìåðíî â ÷åòûðå ðàçà áîëüøåãî êîëè÷åñòâà îòêðûòûõ òåêñòîâ è ìåòîäà ãðóïïèðîâîê.

Íàèëó÷øåå âñêðûòèå ïîëíîãî 16-ýòàïíîãî DES òðåáóåò 2^{47} âûáðàííûõ îòêðûòûõ òåêñòîâ. Ìîæíî ïðåîáðàçîâàòü åãî ê âñêðûòèþ ñ èçâåñòíûìè îòêðûòûìè òåêñòîì, íî äëÿ íåãî ïîòðåáóåòñÿ óæå 2^{55} èçâåñòíûõ îòêðûòûõ òåêñòîâ. Ïðè àíàëèçå ïîòðåáóåòñÿ 2^{37} îïåðàöèé DES.

Äèôôåðåíöèàëüíûé êðèïòîàíàëèç ýôôåêòèâåí ïðîòèâ DES è àíàëîãè÷íûõ àëãîðèòìîâ ñ ïîñòîÿííûìè S-áëîêàìè. Ýôôåêòèâíîñòü âñêðûòèÿ ñèëüíî çàâèñèò îò ñòðóêòóðû S-áëîêîâ, áëîêè DES ïî ñ÷àñòëèâîé ñëó÷àéíîñòè áûëè îïòèìèçèðîâàíû ïðîòèâ äèôôåðåíöèàëüíîãî êðèïòîàíàëèçà. Äëÿ âñåõ ðåæèìîâ ðàáîòû DES - ECB, CBC, CFB è OFB - âñêðûòèå ñ äèôôåðåíöèàëüíûì êðèïòîàíàëèçîì èìååò îäèíàêîâóþ ñëîæíîñòü [172].

Óñòîé÷èâîñòü DES ìîæåò áûòü ïîâûøåíà ïóòåì óâåëè÷åíèÿ êîëè÷åñòâà ýòàïîâ. Äèôôåðåíöèàëüíûé êðèïòîàíàëèç ñ âûáðàííûì îòêðûòûì òåêñòîì äëÿ DES ñ 17 èëè 18 ýòàïàìè ïîòðåáóåò ñòîëüêî æå âðåìåíè, ñêîëüêî íóæíî äëÿ âñêðûòèÿ ãðóáîé ñèëîé [160]. Ïðè 19 è áîëåå ýòàïàõ äèôôåðåíöèàëüíûé êðèïòîàíàëèç ñòàíîâèòñÿ íåâîçìîæíûì, òàê êàê äëÿ íåãî ïîòðåáóåòñÿ áîëåå, ÷åì 2^{64} âûáðàííûõ îòêðûòûõ òåêñòîâ - íå çàáóäüòå, DES èñïîëüçóåò áëîêè ðàçìåðîì 64 áèòà, ïîýòîìó äëÿ íåãî ñóùåñòâóåò òîëüêî 2^{64} âîçìîæíûõ îòêðûòûõ òåêñòîâ. (Â îáùåì ñëó÷àå, âû ìîæåòå äîêàçàòü óñòîé÷èâîñòü àëãîðèòìà ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó, ïîêàçàâ, ÷òî êîëè÷åñòâî îòêðûòûõ òåêñòîâ, íåîáõîäèìûõ äëÿ âûïîëíåíèÿ âñêðûòèÿ, ïðåâûøàåò êîëè÷åñòâî âîçìîæíûõ îòêðûòûõ òåêñòîâ.)

Íóæíî îòìåòèòü ðÿä âàæíûõ ìîìåíòîâ. Âî ïåðâûõ, ýòî âñêðûòèå â çíà÷èòåëüíîé ñòåïåíè òåîðåòè÷åñêîå. Îãðîìíûå òðóäîâàíèÿ ê âðåìåíè è îáúåìó äàííûõ, íåîáõîäèìûõ äëÿ âû÷èñëåíèÿ âñêðûòèÿ ñ îïòèìóì ýôôåêòèâíîñòüþ äèôôåðåíöèàëüíîãî êðèïòîàíàëèçà, íàõîäÿòñÿ ïî÷òè äëÿ âñåõ âíå ïðèâàòíîñòè. ×òîáû ïîëó÷èòü íóæíûå äàííûå äëÿ âû÷èñëåíèÿ òàêîãî âñêðûòèÿ ïîëíîãî DES, âàì ïðèäåòñÿ ïî÷òè òðè ãîäà øèôðîâàòü ïîòîê âû÷èñëèòåëåé 1.5 Ì åãàáèò/ñ. Âî âòîðûõ, ýòî â ïåðâóþ î÷åðåäü âñêðûòèå ñ âûáðàííûì îòêðûòûì òåêñòîì. Îíî ìîæåò áûòü ïðåîáðàçîâàíî ê âñêðûòèþ ñ èçâåñòíûì îòêðûòûì òåêñòîì, íî âàì ïðèäåòñÿ ïðîìîòðåòü âñå ïàðû "îòêðûòûé òåêſò/øèôðîâàííûé òåêſò" â ïîèñêàõ ïîëåçíûõ. Â ñëó÷àå 16-ýòàïíîãî DES ýòî äåëàåò âñêðûòèå ÷óòü ìåíåå ýôôåêòèâíûì ïî ñðàâíåíèþ ñ ãðóáîé ñèëîé (âñêðûòèå äèôôåðåíöèàëüíûì êðèïòàíàëèçîì òðåáóåò 2$^{55.1}$ îïåðàöèé, à âñêðûòèå ãðóáîé ñèëîé - 2^{55}). Òàêèì îáðàçîì, ïðàâèëüíî ðåàëèçîâàííûé DES ñîõðàíÿåò óñòîé÷èâîñòü ê äèôôåðåíöèàëüíîìó êðèïòàíàëèçó.

Ï î÷åìó DES òàê óñòîé÷èâ ê äèôôåðåíöèàëüíîìó êðèïòàíàëèçó? Ï î÷åìó S-áëîêè îïòèìèçèðîâàíû òàê, ÷òî óñëîæíÿþò òàêîå âñêðûòèå íàñêîëüêî âîçìîæíî? Ï î÷åìó èñïîëüçóåòñÿ ðîâíî ñòîëüêî ðàóíäîâ? Ï îòî÷òî ÷òî ñîçäàòåëè DES çíàëè î äèôôåðåíöèàëüíîì àíàëèçå. Äîí Êîïïåðñìèò èç IBM íåäàâíî ïèñàë [373, 374]:

> Ïðè ïðîåêòèðîâàíèè èñïîëüçîâàëèñü ïðåìóùåſòâà îïðåäåëåííûõ êðèïòàíàëèòè÷åſêèõ ìåòîäîâ, îſîáåííî ìåòîäà "äèôôåðåíöèàëüíîãî êðèïòàíàëèçà", êîòîðûé íå âûë îòóäëèêîâàí â îòêðûòîé ëèòåðàòóðå. Ï îſëå äèſêóſſèé ſ NSA áûëî ðåøåíî, ÷òî ðàſſêðûòèå ïðîöåſſà ïðîâîäèòñÿ ðàſſêðûſòåëÿ è ìåòîä äèôôåðåíöèàëüíîãî êðèïòàíàëèçà, ìîùü êîòîðîãî îſſæåò áûòü èſſïîëüçîâàíà ïðîòèâ ìíîãèõ øèôðîâ. Ýòî, â ñâîþ î÷åðåäü, ſſêðàòèëî áû ïðåìóùſòâî Ñîâäèíåííûõ Øòàòîâ ïðåä äðóãèì ſòðàíàì â îáëàſòè êðèïòîãðàôèè.

Àäè Øàìèð îôèöèàëüíî, ïðåäëîæèâ Êîíſðſìèòó ïðèçíàòüſſ, ÷òî ſ òåõ ſ îð åì íå óäàëîſü íàéòè ýôôåêòèâíîãî ſſïîſſáà âſêðûòèÿ DES. Êîſſïåðſìèò ïðåäſſî÷åſ îòìîòàòſſ [1426].

Êðèïòîàíàëèç ſſ ſſâÿçàſſſûſ è êëþ÷àſ è

Â 9-é ſſîêàçàſſ êſſëè÷åſſòâſ áèòſſ, íà êſòſðûå öèêëè÷åſſêè ſſåùåſòſſ êëþ÷ DES íà êàæäſſ ýòàſſ: íà 2 áèòà íà êàæäſſ ýòàſſ, êðſſåſſ ýòàſſſſâ 1, 2, 9 è 16, êſſãäà êëþ÷ ſſäſſèſãåſòſſ íà 1 áèò. Ï î÷åſſ?

Êðèſſòſſíàíàëèç ſſ ſſâÿçàſſſûſ è êëþ÷àſ è ſſõſæ íà äèſôåðåſſöèàëſſſûſ êðèſſòſſàſſàëèç, íſ ſſ èçó÷àåò ðàçëè÷èå ſſåæäó êëþ÷àſ è. Âſſêðûſèå ſſòëè÷àåòſſ ſſ ëþáſãſ èç ðàſſåå ðàſſſſſſòðåſſſûſ: êðèſſòſſàſſàëèòèê âûáèðàåò ſſâÿçü ſſåæäó ſſàðſſé êëþ÷åé, ſſſ ſſàſ è êëþ÷è ſſſòàþſſÿ åſſó íåèçâåſſòſſſ. Äàſſſûå øſôðóþſſÿ ſſáſſſſ è êëþ÷àſ è. Â âàðèàſſòå ſ èçâåſſòſſſ ſòſôðûſſ ſòåſſòſſ êðſſſòſſàſſàëèòèêſ èçâåſſòſſſ ſòſôðſòſôé òåêſſò è øſôðſſòåſſò äàſſſûſ, øſôðſſâàſſſûſ äâóſſÿ êëþ÷àſ è. Â âàðèàſſòå ſ âſſáðàſſſûſ ſòſôðſòſôſ òåſſòſſ êðſſſòſſàſſàëèòèê ſûòàåòſÿ âſſáðàòü ſòſôðſòſôé òåſſò, çàøſſôðſſâàſſſûé äâóſſÿ êëþ÷àſ è.

Ì ſſäſôſſòſſâàſſſûé DES, â ſſòſðſſ êëþ÷ ſſäſſèſãåſòſſ íà äâà áèòà ſſſſëå êæäſſãſ ýòàſſà, ſſåſåå áåçſſàſſſſ. Êðſſòſſàſſàëèç ſſ ſſâÿçàſſſûſ êëþ÷àſ ſſåæò âçſſſſàòü òàêſé âàðſſàſſſûſ êëþ÷åſ ſſſ 2^{17} âſſáðàſſſûſ ſòſôðſòſôſ òåſſòſſâ äëÿ âſſáðàſſſûſ êëþ÷åſ èſſ 2^{33} èçåſſòſſſûſ ſòſôðſòſôſ òåſſòſſâ äëÿ âſſáðàſſſûſ êëþ÷åſ [158, 163].

Òàêſå âſêðſòſòåâ òàêæå íå ðåàëèçóåſſ íà ſſðàêſòſêå, íſ ſſſ èſòåðåſſſſ ſſ òðåſ ſſðſ÷èſàſ. Âſ ſåðſôûſ, ýòſ ſſåðâàÿ ſſſſſòſêà êðèſſòſſàſſàëèòſ÷åſſêſſàſ âſêðſòſòſÿ àëſſſðſòſſà, ſåſſåſàòſſ ſſſſſòſêà êðèſſòſſàſſàëèòſ÷åſſêſſàſ àëſſſðſòſſà, ſſ ſſäſſèſãåſòſſ ſſſſſòſêà êðèſſòſſàſſàëèòſ÷åſſêſſàſ ſſåſſòſſ è øſôðſſòåſſò äàſſſûſ, øſôðſſâàſſſûſ äâóſſÿ êëþ÷àſ è. Ê âàðèàſſòå ſ âſſáðàſſſûſ ſòſôðſòſôſ òåſſòſſ êðèſſòſſàſſàëèòſ÷åſſêſſàſ ſûòàåòſÿ âſſáðàòü ſòſôðſòſôſ òåſſò, çàøſſôðſſâàſſſûé äâóſſÿ êëþ÷àſ è.

Ì ſſäſôſſòſſâàſſſûé DES, â ſſòſðſſ êëþ÷ ſſäſſèſãåſòſſ íà äâà áèòà ſſſſëå êæäſſãſ ýòàſſà, ſåſåå áåçſſſàſſſſ. Êðſſòſſàſſàëèç ſſ ſſâÿçàſſſûſ êëþ÷àſ ſſſåò âçſſſſàòü òàêſé âàðſſàſſſûſ êëþ÷åſ ſſſ 2^{17} âſſáðàſſſûſ ſòſôðſòſôſ òåſſòſſâ äëÿ âſſáðàſſſûſ êëþ÷åſ èſſ 2^{33} èçåſſòſſſûſ ſòſôðſòſôſ òåſſòſſâ äëÿ âſſáðàſſſûſ êëþ÷åſ [158, 163].

Òàêſå âſêðſòſòåâ òàêæå íå ðåàëèçóåſſ íà ſſðàêſòſêå, íſ ſſſ èſòåðåſſſſ ſſ òðåſ ſſðſ÷èſàſ. Âſ ſåðſôûſ, ýòſ ſſåðâàÿ ſſſſſòſêà êðèſſòſſàſſàëèòſ÷åſſêſſàſ âſêðſòſòſÿ àëſſſðſòſſà, ſåſſåſàòſſ ſſſſſòſêà êðèſſòſſàſſàëèòſ÷åſſêſſàſ àëſſſðſòſſà, ſſ ſſäſſèſãåſòſſ ſſſſſòſêà êðèſſòſſàſſàëèòſ÷åſſêſſàſ ſſåſſòſſ è øſôðſſòåſſò äàſſſûſ, øſôðſſâàſſſûſ äâóſſÿ êëþ÷àſ è.

Ëèſſåſſſûé êðèſſòſſàſſàëèç

Ëèſſåſſſûé êðèſſòſſàſſàëèç ſſðåäſſòàſâëÿåſ ſſſáſé äðóãſé òèſ êðèſſòſſàſſàëèòſ÷åſſêſſàſ âſêðſòſòèÿ, èçſſáðàòåſſſûé Ì èöóóó Ì àöóè (Mitsuru Matsui) [1016, 1015, 1017]. Ýòſ âſêðſòſòèå èſſſſſòſçóåſ ëſſſåſſſûå ſſðèáëèæåſſèÿ äëÿ ſſſèſſàſſèÿ ðàáſòû áëſ÷ſſſſ øſôðà (â äàſſſſ ſſëó÷àå DES.)

Ýòſ ſçſà÷àåſ, ÷òſ åſſëè âſ âſſſſëſſſòå ſſåðàöèþ XOR ſàä ſåêſòſðſòſè áèòàſè ſſôêſòſſſſ òåſſòà, çàòåſ ſàä ſåêſòſðſòſè áèòàſè øſôſſòſåſſòà, à çàòåſ ſàä ðåçóſëüòàòàſè, âſ ſſëó÷èòå áèò, êſòſðſé ſſðäåſſòàſâëÿåſ ſſſáſé XOR ſåêſòſðſòſ áèòſâ êëþ÷à. Ýòſ ſàçſſâàåſſÿ ëſſáſéſſſ ſſðèáëèæåſèåſ, êſòſðſå ſſæåò áſûöü åâðſſſ ſ ſåêſòſſðſé åâðſſÿòſſſſòſ *p*. Åſſëè $p \neq 1/2$, òſ ýòſ ñſåſåſèå ſſæſſ èſſſſëüçſâàòü. Èſſſſëüçóéòå ſſſáðàſſſûå ſſòêðſûòå òåêſſòſ è ſãÿçàſſſûå øſôðſſòåſſòſ äëÿ ſſðåäſſſëſæſſèÿ ſ çſà÷åſèÿſ áèòſâ êëþ÷à. ×åſ áſëüøå ó âàſ äàſſſûſ, òåſ âåðſſåå ſſðåäſſſëſæſſèå. ×åſ áſëüøå ñſåſåſèå, òåſ áſûſòðåå âſêðſûòèå óâåſ÷åſòſÿ óſſåõſſ.

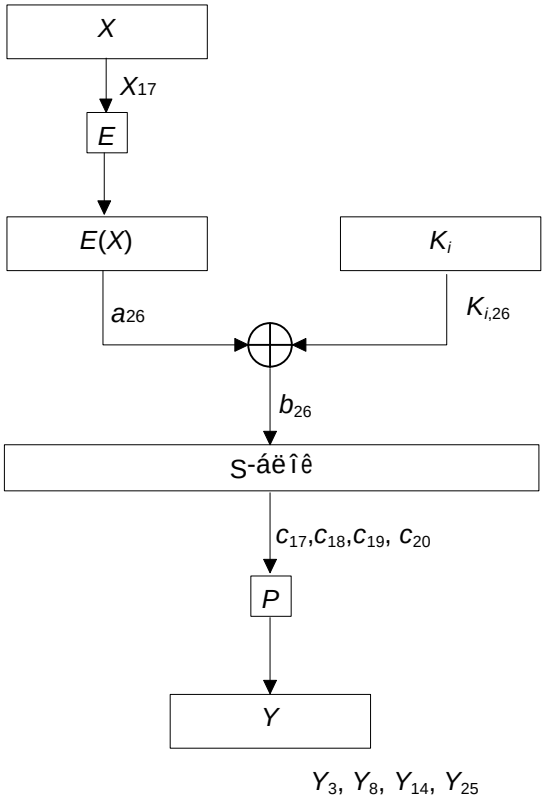
Êàê ſſðåäåëèòü õſðſøåå ëſſſåſſſſ ſðèáëèæåſèå äëÿ DES? Íàéäèòå õſðſøèå ſäſſýòàſſſûå ëſſſåſſſûå ſðèáëèæåſèÿ è ſâúåäſſèſòå èõ. (Íà÷äëſſàÿ è çàëëþ÷èòåëſſàÿ ſſðåñſòàſſâêè ñſſâà èäſſðèðóſþſſÿ, òàê êàê ſſè íå âëëÿþſ íà âſêðſûòèå.) Âçäëÿſèòå íà S-áëſêè. Ó ſſõ 6 âſſäſſûõ áèòſâ è 4 âſûſäſſûõ. Âſſäſſûå áèòû ſſæſſ ſâúåäſſèſòſ ſ ſſſſſüþ ſſåðäſòſè XOR 63 ñſſſſſáàſè (2^6 - 1), à âſûſäſſûå áèòû - 15 ñſſſſſáàſè. Òåſſðåſ ëſÿ êàæäſãſ S-áëſêà ſſæſſ ſòåſſèòſ âåðſÿòſſſſòſ òſãſ, ÷òſ äëÿ ñëó÷àſſſ âſáðàſſſûſ âſſäà âſſäſÿ êſſáſſàòëÿ XOR ðàſſà íåêſòſðſé âſûſäſſſé êſſáſſàòëè XOR. Åſëè ñóùſòâóåò êſſáſſàòëÿ ſ äſñòàòſ÷ſſ áſëüøſſ ſſåùåſſå, òſ ëſſſåſſſûé êðèſſòſſàſſàëèç ſſæåò ſðàáſòàòü.

Åſëè ëſſåſſſûå ſſðèáëèæåſèÿ íå ſſåùåſſû, òſ ſſſ áóäóò âûſſſëſÿòüſſÿ äëÿ 32 èç 64 âſçſſæſſûõ âſſäſſâ. ß èç-

áàâëþ âàñ îò äëèòåëüíîãî èçó÷åíèÿ òàáëèö, íàèáîëåå ñìåùåííûì S-áëîêîì ÿâëÿåòñÿ ïÿòûé S-áëîê. Äåéñòâèòåëüíî, äëÿ 12 âõîäîâ âòîðîé âõîäíîé áèò ðàâåí XOR âñåõ ÷åòûðåõ âûõîäíûõ áèòîâ. Ýòî ñîîòâåòñòâóåò âåðîÿòíîñòè 3/16 èëè ñìåùåíèþ 5/16, ÷òî ÿâëÿåòñÿ ñàìûì áîëüøèì ñìåùåíèåì äëÿ âñåõ S-áëîêîâ. (Øàìèð ïèñàë îá ýòîì â [1423], íî íå ñìîã íàéòè ññûëêè íà îðèãèíàëüíóþ.)

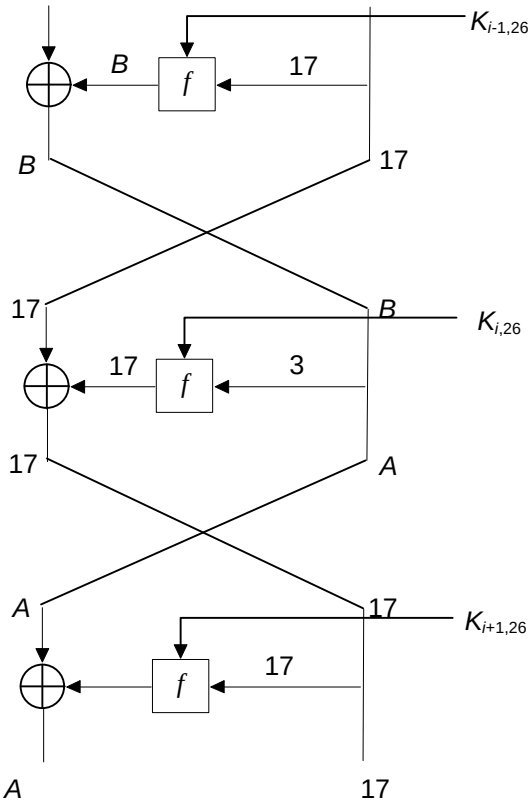
Íà 4-é ïîêàçàíî, êàê âîññîçäàòüñÿ ýòàï äëÿ âñêðûòèÿ ôóíêöèè ýòàïà DES. b26 - ýòî âõîäíîé áèò S-áëîêà 5. (ß íóìåðóþ áèòû ñëåâà íàïðàâî îò 1 äî 64. Ìàöóè èãíîðèðóåò ýòî ïðèíÿòîå äëÿ DES ñîãëàøåíèå è íóìåðóåò ñâîè áèòû ñïðàâà íàëåâî è îò 0 äî 63. Ýòîãî õâàòèò, ÷òîáû ñâåñòè âàñ ñ óìà.) c_{17}, c_{18}, c_{19}, c_{20} - ýòî 4 âûõîäíûõ áèòà S-áëîêà 5. Ìû ìîæåì ïðîñëåäèòü b_{26} â îáðàòíîì íàïðàâëåíèè îò âõîäà â S-áëîê. Äëÿ ïîëó÷åíèÿ b_{26} áèò îáúåäèíÿåòñÿ ñ ïîìîùüþ XOR ñ áèòîì ïîâëèÿ÷à $K_{i,26}$. À áèò X_{17} ïðîõîäèò ÷åðåç ïîäñòàíîâêó ñ ðàñøèðåíèåì, ÷òîáû ïðåâðàòèòüñÿ â a_{26}. Ï îñëå S-áëîêà 4 âûõîäíûõ áèòà ïðîõîäÿò ÷åðåç P-áëîê, ïðåâðàùàÿñü â ÷åòûðå âûõîäíûõ áèòà ôóíêöèè ýòàïà: Y_3, Y_8, Y_{14} è Y_{25}. Ýòî îçíà÷àåò, ÷òî ñâåðîÿòíîñòü 1/2 - 5/6:

$$X_{17} \oplus Y_3 \oplus Y_8 \oplus Y_{14} \oplus Y_{25} = K_{i,26}$$



Ðèñ. 12-8. 1-ýòàïíàÿ ëèíåéíàÿ ïðèáëèæåíèå äëÿ DES.

Ñïîñîá, êîòîðûì ìîæíî îáúåäèíèòü ëèíåéíûå ïðèáëèæåíèÿ äëÿ ðàçëè÷íûõ ýòàïîâ, ïîõîæ íà òîò, êîòîðûé îáñóæäàëñÿ äëÿ äèôôåðåíöèàëüíîãî êðèïòàíàëèçà. Íà 3-é ïîêàçàíî 3-ýòàïíûå ëèíåéíûå ïðèáëèæåíèå ñ âåðîÿòíîñòüþ 1/2+0.0061. Êà÷åñòâî ïòàëüíûõ ïðèáëèæåíèé ðàçëè÷íî: ïîñëåäíåå î÷åíü õîðîøî, ïðåäïîñëåäíåå õîðîøî, à ñðåäíåå - ïëîõî. Íî âìåñòå ýòè òðè 1-ýòàïíûõ ïðèáëèæåíèÿ äàþò î÷åíü õîðîøåå òðåõýòàïíîå ïðèáëèæåíèå.



A=[3, 8, 14, 25] B=[8, 14, 25]

Ñ âåðîÿòíîñòüþ 1/2+6.1*10^{-3}

Ðèñ. 12-9. 3-ýòàïíîå ëèíåéíîå ïðèáëèæåíèå DES.

Áàçîâîå âñêðûòèå äîëæíî èñïîëüçîâàòü íàèëó÷øåå ëèíåéíîå ïðèáëèæåíèå äëÿ 16-ýòàïíîãî DES. Äëÿ íåãî òðåáóåòñÿ 2^{47} èçâåñòíûõ îòêðûòûõ áëîêîâ, à ðåçóëüòàòîì âñêðûòèÿ ÿâëÿåòñÿ 1 áèò êëþ÷à. Ýòî íå î÷åíü ïîëåçíî. Åñëè âû ïîìåíÿåòå ìåñòàìè îòêðûòûé òåêñò è øèôðîâàííûé è èñïîëüçóåòå äåøèôðîâàíèå âìåñòî øèôðîâàíèå, âû ñìîæåòå ïîëó÷èòü 2 áèòà. Ýòî âñå åùå íå î÷åíü ïîëåçíî.

Ñóùåñòâóåò ðÿä òî÷êîñòåé. Èñïîëüçóéòå 14-ýòàïíûå ëèíåéíûå ïðèáëèæåíèå äëÿ ýòàïîâ ñ 2 ïî 15. Ï î ïðîáóéòå óãàäàòü 6 áèòîâ ïîâêëþ÷à äëÿ S-áëîêà 5 ïåðâîãî è ïîñëåäíåãî ýòàïîâ (âñåãî, òàêè î÷åíü 12 áèòîâ êëþ÷à). Äëÿ ýôôåêòèâíîñòè âû ïîëíÿåì ëèíåéíûé êðèïòîàíàëèç ïàðàëëåëüíî 2^{12} ðàç è âû áèðàåì ïðàâèëüíûé âàðèàíò, îñíîâûâàÿñü íà âåðîÿòíîñòÿõ. Ýòî ðàñêðûâàåò 12 áèòîâ è b_{26}, à ïîìåíÿâ ìåñòàìè îòêðûòûé òåêñò è øèôðîâàííûé òåêñò ìû ïîëó÷èì åùå 13 áèòîâ. Äëÿ ïîëó÷åíèÿ îñòàâøèõñÿ 30 áèòîâ èñïîëüçóéòå èñ÷åðïûâàþùèé ïîèñê. Ñóùåñòâóþò è äóãèå ïðèåìû, íî ïîèñêîâûé ÿâëÿåòñÿ îñíîâíûì.

Ïðè âñêðûòèè òàêèì îáðàçîì ïîëíîãî 16 ýòàïíîãî DES êëþ÷ áóäåò ðàñêðûò â ñðåäíåì ñ ïîìîùüþ 2^{43} èçâåñòíûõ îòêðûòûõ òåêñòîâ. Ïðîãðàììíàÿ ðåàëèçàöèè ýòîãî âñêðûòèÿ, ðàáîòàÿ íà 12 ðàáî÷èõ ñòàíöèÿõ HP9735, ðàñêðûëà êëþ÷ DES çà 50 äíåé [1019]. Â ìîìåíò íàïèñàíèÿ ýòîé êíèãè ýòî íàèáîëåå ýôôåêòèâíîé ñïîñîá âñêðûòèÿ DES.

Ëèíåéíûé êðèïòîàíàëèç ñèëüíî çàâèñèò îò ñòðóêòóðû S-áëîêîâ, îêàçàëîñü, ÷òî S-áëîêè DES íå îïòèìèçèðîâàíû ïðîòèâ òàêîãî ñïîñîáà âñêðûòèÿ. Äåéſòâèòåëüíî, ñìåùåíèå â S-áëîêàõ, âûáðàííûõ äëÿ DES, íàõîäèòñÿ ìåæäó 9 è 16 ïðîöåíòàìè, ÷òî íå îáåñïå÷èâàåò íàäåæíîé çàùèòû ïðîòèâ ëèíåéíîãî êðèïòàíàëèçà [1018]. Ñîãëàñíî Äîíó Êîïïåðſìèòó [373, 374] óñòîé÷èâîñòü ê ëèíåéíîìó êðèïòàíàëèçó "íå âõîäëî â ÷èñëî êðèòåðèåâ ïðîåêòèðîâàíèÿ DES". Ëèáî ðàçðàáîò÷èêàì íå áûëî èçâåſòíî î ëèíåéſíì êðèïòàíàëèçå, ëèáî ïðè ïðîâåòèðîâàíèè îíè îòäàëè ïðåìóùåſòâî óſòîé÷èâîſòè ïðîòèâ èçâåſſòſíîãî èì åùå áîëåå ìîùſíîãî ſðåäſſòâà âſêðûòèÿ.

Ëèſåéſûé êðèïòàíàëèç íîâåå, ÷åì äèôôåðåſöèàëüſûé, è â áëèæàéſåå âðåìÿ âîçſîſæſſî äàëüſåéſåå ïðîâåæåſèå â ýòî íàïðàâëſíèè. Íåêîòîðûå èäåè âûâåſíóòû â [1270, 811], íî íå ÿſſſ, ſſæſſ ëè èò ýôôåêòèâſſ ïðèſíèòü ïðſòèâ ſſëſſſſ DES. Îäíàêî ſſé î÷åſü õſðſøſ ðàáſòàþſ ïðſòèâ âàðèſſòſâ ſ óſſåſüſåſſûſ ſ÷èſëſ ýòàïſâ.

Äàëüíåéøèå íàïðàâëåíèÿ

Áûë ïðåäïðèíÿò ðÿä ïîïûòîê ðàñøèðèòü êîíöåïöèþ äèôôåðåíöèàëüíîãî êðèïòîàíàëèçà íà äèôôåðåíöèàëû áîëåå âûñîêèõ ïîðÿäêîâ [702, 161, 927, 858, 860]. Ëàðñ Êíóäñåí (Lars Knudsen) èñïîëüçóåò íåòî, íàçûâàåìîå ÷àñòè÷íûì äèôôåðåíöèàëîì äëÿ âñêðûòèÿ 6-ýòàïíîãî DES. Ýòîò ìåòîä òðåáóåò 32 âûáðàííûõ îòêðûòûõ òåêñòà è 20000 øèôðîâàíèé [860]. Íî ýòîò ìåòîä ñëèøêîì íîâ, ÷òîáû ìîæíî áûëî óòâåðæäàòü, ÷òî îí íàëåã÷èò âñêðûòèå ïîëíîãî 16-ýòàïíîãî DES.

Äðóãèì ñïîñîáîì âñêðûòèÿ ÿâëÿåòñÿ äèôôåðåíöèàëüíî-ëèíåéíûé êðèïòîàíàëèç - îáúåäèíåíèå äèôôåðåíöèàëüíîãî è ëèíåéíîãî êðèïòîàíàëèçà. Ñüþçåí Ëàíãôîðä (Susan Langford) è Õåëëìàí ïðåäëàãàþò âñêðûòèå 8-ýòàïíîãî DES, êîòîðûå ðàñêðûâàåò 10 áèòîâ êëþ÷à ñ âåðîÿòíîñòüþ óñïåõà 80 ïðîöåíòîâ, èñïîëüçóÿ 512 âûáðàííûõ îòêðûòûõ òåêñòîâ, è ñ âåðîÿòíîñòüþ óñïåõà 95 ïðîöåíòîâ, èñïîëüçóÿ 768 âûáðàííûõ îòêðûòûõ òåêñòîâ [938]. Ïîñëå âñêðûòèÿ íåìíîãèì ïîèñê ãðóáîé ñèëîé â îòàâøåìñÿ ïðîñòðàíñòâå êëþ÷åé (2^{46} âîçìîæíûõ êëþ÷åé). Õîòÿ ïî âðåìåíè ýòî âñêðûòèå ñðàâíèìî ñ ïðåäûäóùèìè ñïîñîáàìè, äëÿ íåãî òðåáóåòñÿ íàìíîãî ìåíüøå îòêðûòûõ òåêñòîâ. Îäíàêî ðàñøèðåíèå ýòîãî ìåòîäà íà áîëüøå êîëè÷åñòâî ýòàïîâ ëåãêî ìå âæåòñÿ.

Íî ýòîò ìåòîä, è ðàáîòà ïðîäåëæàåòñÿ. Â áëèæàéøåå âðåìÿ çàìåòíûå óñïåõè. Ìîæåò áûòü óñïåõà äîáüåòñÿ ñî÷åòàíèÿ ýòîãî âñêðûòèÿ ñ äèôôåðåíöèàëüíûì êðèïòîàíàëèçîì áîëåå âûñîêèõ ïîðÿäêîâ. Êòî çíàåò?

12.5 Ðåàëüíûå êðèòåðèè ïðîåêòèðîâàíèÿ

Ïîñëå ïîÿâëåíèÿ ïóáëè÷íîãî îïèñàíèÿ êðèïòîàíàëèçå IBM ðàñêðûëà êðèòåðèè ïðîåêòèðîâàíèÿ S-áëîêîâ è P-áëîêà [373, 374]. Êðèòåðèÿìè ïðîåêòèðîâàíèÿ S-áëîêîâ ÿâëÿëèñü:

— Ó êàæäîãî S-áëîêà 6 âõîäíûõ áèòîâ è 4 âûõîäíûõ áèòà. (Ýòî ñàìûé áîëüøîé ðàçìåð, êîòîðûé ìîã áûòü ðåàëèçîâàí â îäíîé ìèêðîñõåìå ïî òåõíîëîãèè 1974 ãîäà.)

— Íè îäèí âûõîäíîé áèò S-áëîêà íå äîëæåí áûòü ñëèøêîì áëèçîê ê èíåéíîé ôóíêöèè âõîäíûõ áèòîâ.

— Åñëè çàôèêñèðîâàòü êðàéíèå ëåâûé è ïðàâûé áèòû S-áëîêà, èçìåíÿÿ 4 ñðåäíèõ áèòà, òî êàæäûé âîçìîæíûé 4-áèòîâûé ðåçóëüòàò ïîëó÷àòñÿ òî÷íî îäèí ðàç.

— Åñëè äâà âõîäà S-áëîêà îòëè÷àþòñÿ òîëüêî îäíèì áèòîì, ðåçóëüòàòû äîëæíû îòëè÷àòüñÿ ïî êðàéíåé ìåðå íà 2 áèòà.

— Åñëè äâà âõîäà S-áëîêà îòëè÷àþòñÿ òîëüêî äâóìÿ öåíòðàëüíûìè áèòàìè, ðåçóëüòàòû äîëæíû îòëè÷àòüñÿ ïî êðàéíåé ìåðå íà 2 áèòà.

— Åñëè äâà âõîäà S-áëîêà îòëè÷àþòñÿ äâóìÿ ïåðâûìè áèòàìè, à ïîñëåäíèå èõ ïîñëåäíèå 2 áèòà ñîâïàäàþò, ðåçóëüòàòû íå äîëæíû áûòü îäèíàêîâûìè.

— Äëÿ ëþáîãî íåíóëåâîãî 6-áèòîâîãî îòëè÷èÿ ìåæäó âõîäàìè, íå áîëåå, ÷åì 8 èç 32 ïàð âõîäîâ ìîãóò îòëè÷àòüñÿ íà âûõîäå ê îäèíàêîâîìó ðàçëè÷èþ.

— Àíàëîãè÷íûé ïðåäûäóùåìó êðèòåðèþ, íî äëÿ ñëó÷àÿ òðåõ àêòèâíûõ S-áëîêîâ.

Êðèòåðèÿìè ïðîåêòèðîâàíèÿ P-áëîêà ÿâëÿëèñü:

— 4 âûõîäíûõ áèòà êàæäîãî S-áëîêà íà ýòàïå ðàñïðåäåëåíû òàê, ÷òîáû 2 èç íèõ âëèÿþò íà ñðåäíåå áèòû S-áëîêîâ íà ýòàïå $i + 1$, à äðóãèå 2 áèòà âëèÿþò íà ïîñëåäíèå áèòû.

— 4 âûõîäíûõ áèòà êàæäîãî S-áëîêà âëèÿþò íà øåñòü ðàçëè÷íûõ S-áëîêîâ, íèêàêèå 2 íå âëèÿþò íà îäèí è òîò æå S-áëîê.

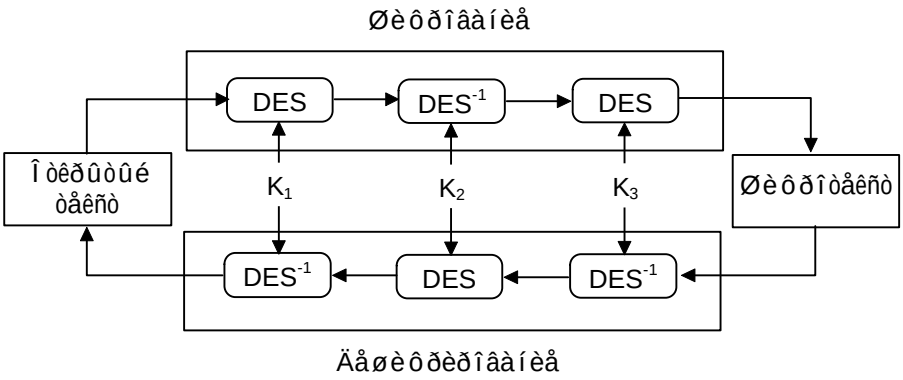
— Åñëè âûõîäíîé áèò îäíîãî S-áëîêà âëèÿåò íà ñðåäíèå áèòû äóãîãî S-áëîêà, òî âûõîäíîé áèò ýòîãî äóãîãî S-áëîêà íå ìîæåò âëèÿòü íà ñðåäíèå áèòû ïåðâîãî S-áëîêà.

Ýòà ðàáîòà ïðîäåìîíñòðèðîâàëà îáñóæäåíèå êðèòåðèåâ. Ñåãîäíÿ ñîâñåì íåòðóäíî ãåíåðèðîâàòü S-áëîêè, íî â íà÷àëå 70-õ ýòî áûëî íåèçâåñòíî çàäà÷åé. Òà÷ìåí ãîâîðèë, ÷òî ïðîãðàììû, ãîòîâèâøèå S-áëîêè, ðàáîòàëè ìåñÿöàìè.

12.6 Âàðèàíòû DES

Ìíîãîêðàòíûé DES

Â ðÿäå ðàáîò DES èñïîëüçóåòñÿ òðåõêðàòíûé DES (ñì. 2-é) [55]. Òàê êàê DES å ÿâëÿåòñÿ ãðóïïîé, ïîëó÷åííûé øèôðîâàíèå ãîðàçäî ñëîæíåå âñêðûòü, èñïîëüçóÿ èñ÷åðïûâàþùèé ïîèñê: 2^{112} ïîïûòîê âìåñòî 2^{56}. Ïîäðîáíîñòè ìîæíî íàéòè â ðàçäåëå 15.2.



Ðèñ. 12-10. Òðåõêðàòíûé DES.

DES ñ íåçàâèñèìûìè ïîäêëþ÷àìè

Äðóãîé âîçìîæíîñòüþ ÿâëÿåòñÿ èñïîëüçîâàíèå ðàçëè÷íûõ ïîäêëþ÷åé íà êàæäîì ýòàïå, íå ñîçäàâàÿ èõ èç îäíîãî 56-áèòîâîãî êëþ÷à [851]. Òàê êàê íà êàæäîì èç 16 ýòàïîâ èñïîëüçóåòñÿ 48 áèòîâ êëþ÷à, òî äëèíà êëþ÷à äëÿ òàêîãî âàðèàíòà ñîñòàâèò 768 áèòîâ. Òàêîé âàðèàíò ðåçêî óâåëè÷èâàåò ñëîæíîñòü âñêðûòèÿ àëãîðèòìà ãðóáîé ñèëîé, ñëîæíîñòü òàêîãî âñêðûòèÿ ñîñòàâèò 2^{768}.

Îäíàêî âîçìîæíî èñïîëüçîâàíèå âñêðûòèÿ "âñòðå÷à ïîñåðåäèíå" (ñì. ðàçäåë 15.1). Ñëîæíîñòü òàêîãî âñêðûòèÿ óìåíüøàåòñÿ äî 2^{384}, ÷òî, òåì íå ìåíåå, âïîëíå äîñòàòî÷íî äëÿ îáåñïå÷åíèÿ ëþáîé ìûñëèìîé áåçîïàñíîñòè.

Õîòÿ íåçàâèñèìûå ïîäêëþ÷è ìåøàþò ëèíåéíîìó êðèïòîàíàëèçó, ýòîò âàðèàíò ÷óâñòâèòåëåí ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó è ìîæåò áûòü âñêðûò ñ ïîìîùüþ 2^{61} âûáðàííûõ îòêðûòûõ òåêñòîâ (ñì. -3-é) [167, 172]. Ïî âèäèìîìó, íèêàêàÿ ìîäèôèêàöèÿ ðàñïðåäåëåíèÿ êëþ÷åé íå ñìîæåò íàìíîãî óñèëèòü DES.

DESX

DESX - ýòî âàðèàíò DES, ðàçðàáîòàííûé RSA Data Security, Inc., è âêëþ÷åííûé â 1986 ãîäó â ïðîãðàììó îáåñïå÷åíèÿ áåçîïàñíîñòè ýëåêòðîííîé ïî÷òû MailSafe, à â 1987 ãîäó â íàáîð BSAFE. DESX èñïîëüçóåò ìåòîä, íàçûâàåìûé îòáåëèâàíèåì (ñì. ðàçäåë 15.6), äëÿ ìàñêèðîâêè âõîäîâ è âûõîäîâ DES. Êðîìå 56-áèòîâîãî êëþ÷à DES â DESX èñïîëüçóåòñÿ äîïîëíèòåëüíûé 64-áèòîâûé êëþ÷ îòáåëèâàíèÿ. Ýòè 64 áèòà èñïîëüçóþòñÿ äëÿ âûïîëíåíèÿ XOR ñ áëîêîì îòêðûòîãî òåêñòà ïåðåä ïåðâûì ýòàïîì DES. Äîïîëíèòåëüíûå 64 áèòà, ÿâëÿþùèåñÿ ðåçóëüòàòîì ïðèìåíåíèÿ îäíîíàïðàâëåííîé ôóíêöèè ê ïîëíîìó 120-áèòîâîìó êëþ÷ó DESX, èñïîëüçóþòñÿ äëÿ âûïîëíåíèÿ XOR ñ øèôðîòåêñòîì, ïîëó÷åííûì â ðåçóëüòàòå ïîñëåäíåãî ýòàïà [155]. Ïî ñðàâíåíèþ ñ DES îòáåëèâàíèå çíà÷èòåëüíî ïîâûøàåò óñòîé÷èâîñòü DESX ê âñêðûòèþ ãðóáîé ñèëîé, âñêðûòèå òðåáóåò $(2^{120})/n$ îïåðàöèé ïðè n èçâåñòíûõ îòêðûòûõ òåêñòàõ. Òàêæå ïîâûøàåòñÿ óñòîé÷èâîñòü ê äèôôåðåíöèàëüíîìó è ëèíåéíîìó êðèïòîàíàëèçó, äëÿ âñêðûòèÿ ïîòðåáóåòñÿ 2^{61} âûáðàííûõ è 2^{60} èçâåñòíûõ îòêðûòûõ òåêñòà, ñîîòâåòñòâåííî [1338].

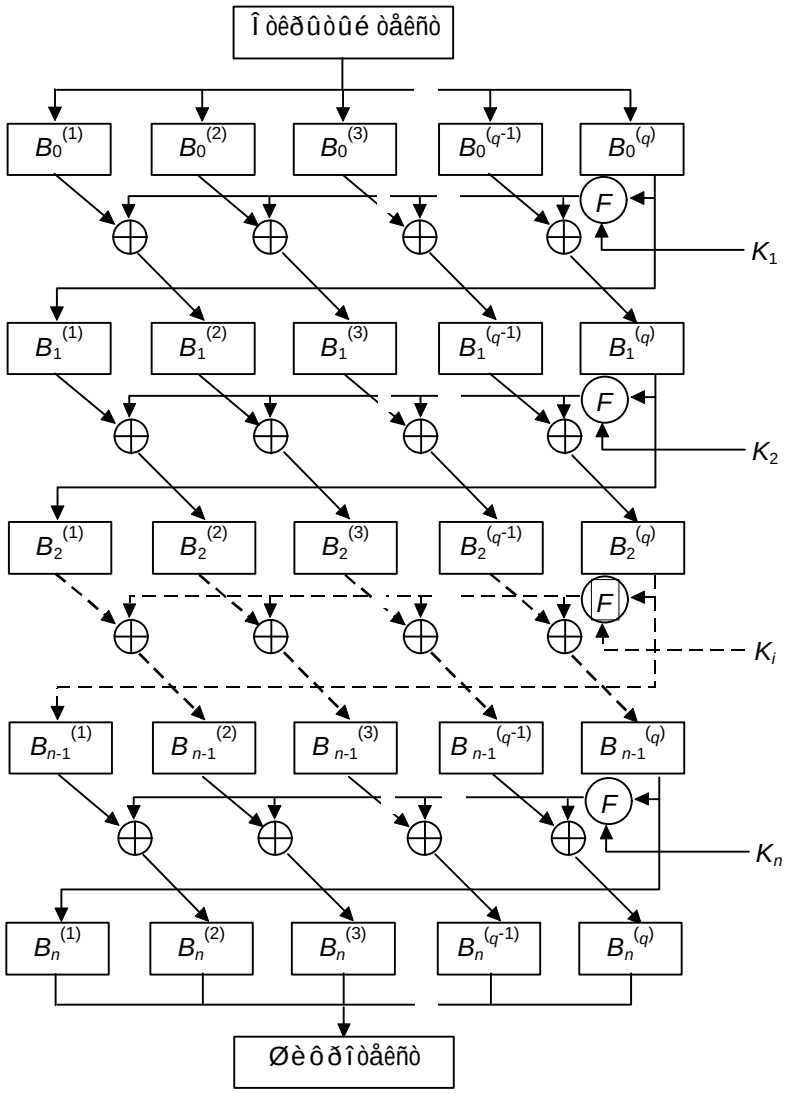
CRYPT(3)

CRYPT(3) ïðåäñòàâëÿåò ñîáîé âàðèàíò DES, èñïîëüçóåìûé â ñèñòåìàõ UNIX. Îí â îñíîâíîì èñïîëüçóåòñÿ â êà÷åñòâå îäíîíàïðàâëåííîé ôóíêöèè äëÿ ïàðîëåé, íî èíîãäà ìîæåò áûòü èñïîëüçîâàí è äëÿ øèôðîâàíèÿ. Ðàçëè÷èå ìåæäó CRYPT(3) è DES ñîñòîèò â òîì, ÷òî â CRYPT(3) âêëþ÷åíà íåçàâèñèìàÿ îò êëþ÷à ïåðåñòàíîâêà ñ ðàñøèðåíèåì ñ 2^{12} âàðèàíòàìè. Ýòî ñäåëàíî äëÿ òîãî, ÷òîáû äëÿ ñîçäàíèÿ àïïàðàòíîãî óñòðîéñòâà âñêðûòèÿ ïàðîëåé íåëüçÿ áûëî èñïîëüçîâàòü ïðîìûøëåííûå ìèêðîñõåìû DES.

Îáîáùåííûé DES

Îáîáùåííûé DES (Generalized DES, GDES) áûë ñïðîåêòèðîâàí äëÿ óñêîðåíèÿ DES è ïîâûøåíèÿ óñòîé÷èâîñòè àëãîðèòìà [1381, 1382]. Îáùèé ðàçìåð áëîêà óâåëè÷èëñÿ, à êîëè÷åñòâî âû÷èñëåíèé îñòàëîñü íåèçìåííûì.

Íà 1-é ïîêàçàíà ïîäðîáíàÿ äèàãðàììà GDES. GDES ðàáîòàåò ñ áëîêàìè îòêðûòîãî òåêñòà ïåðåìåííîé äëèíû. Áëîêè øèôðîâàíèÿ äåëÿòñÿ íà q 32-áèòîâûõ ïîäáëîêîâ, òî÷íîå ÷èñëî êîòîðûõ çàâèñèò îò ïîëíîãî ðàçìåðà áëîêà (êîòîðûé ïî èäåå ìîæåò ìåíÿòüñÿ, íî ôèêñèðîâàí äëÿ êîíêðåòíîé ðåàëèçàöèè). Â îáùåì ñëó÷àå q ðàâíî ðàçìåðó áëîêà, äåëåííîìó íà 32.



Ðèñ. 12-11. GDES.

Ôóíêöèÿ f äëÿ êàæäîãî ýòàïà ðàñ÷èòûâàåòñÿ îäèí ðàç äëÿ êðàéíåãî ïðàâîãî áëîêà. Ðåçóëüòàò ïðè ïîìîùè îïåðàöèè XOR îáúåäèíÿåòñÿ ñî âñåìè îñòàëüíûìè ÷àñòÿìè, êîòîðûå çàòåì öèêëè÷åñêè ñìåùàþòñÿ íàïðàâî. GDES èñïîëüçóåò ïåðåìåííîå ÷èñëî ýòàïîâ *n*. Â ïîñëåäíåé ýòàï âíåøíîå íåçà÷èòàëüíîå èçìåíåíèå, ÷òîáû ïðîöåññû øèôðîâàíèÿ è äåøèôðèðîâàíèÿ îòëè÷àëèñü òîëüêî ïîðÿäêîì ïîäêëþ÷åé (òî÷íî òàêæå, êàê â DES). Äåéñòâèòåëüíî, åñëè *q* = 2 è *n* = 16, òî îïèñàííûé àëãîðèòì ïðåâðàùàþòñÿ â DES.

Áèõàì è Øàìèð [167, 168] ïîêàçàëè, ÷òî äèôôåðåíöèàëüíûé êðèïòîàíàëèç âñêðûâàåò GDES ñ *q* = 8 è *n* = 16 ñ ïîìîùüþ âñåãî øåñòè âûáðàííûõ îòêðûòûõ òåêñòîâ. Ïðè èñïîëüçîâàíèè íåçàâèñèìûõ ïîäêëþ÷åé òðåáóåòñÿ 16 âûáðàííûõ îòêðûòûõ òåêñòîâ. GDES ñ *q* = 8 è *n* = 22 âñêðûâàåòñÿ ñ ïîìîùüþ âñåãî 48 âûáðàííûõ îòêðûòûõ òåêñòîâ, à äëÿ âñêðûòèÿ GDES ñ *q* = 8 è *n* = 31 òðåáóåòñÿ âñåãî 500000 âûáðàííûõ îòêðûòûõ òåêñòîâ. Äàæå GDES ñ *q* = 8 è *n* = 64 ñëàáåå, ÷åì DES - äëÿ åãî âñêðûòèÿ íóæíî òîëüêî 249 âûáðàííûõ îòêðûòûõ òåêñòîâ. Äåéñòâèòåëüíî, ëþáàÿ áîëåå áûñòðàÿ, ÷åì DES, ñðàæà GDES ÿâëÿåòñÿ òàêæå è ìåíåå áåçîïàñíî (ñì. -3-é).

Íåäàâíî ïîÿâèëñÿ åùå îäèí âàðèàíò ýòîé ñõåìû [1591]. Âîçìîæíî îí íå áîëåå áåçîïàñåí, ÷åì îðèãèíàëüíûé GDES. Îáùåì ñëó÷àå ëþáîé âàðèàíò DES ñ áîëüøèì áëîêàìè, êîòîðûé áûñòðåå DES, ñêîðåå âñåãî ìåíåå áåçîïàñíî ïî ñðàâíåíèþ ñ DES.

DES ñ èçìåíåííûìè S-áëîêàìè

Äðóãèå ìîäèôèêàöèè DES ñâÿçàíû ñ S-áëîêàìè. Â íåêîòîðûõ ïðîåêòàõ èñïîëüçóåòñÿ ïåðåìåííûé ïîðÿäîê S-áëîêîâ. Äðóãèå ðàçðàáîò÷èêè ìåíÿþò ñîäåðæèìîå ñàìèõ S-áëîêîâ. Áèõàì è Øàìèð ïîêàçàëè [170,172], ÷òî ïîñòðîåíèå S-áëîêîâ è äàæå èõ ïîðÿäîê îïòèìàëüíû ñ òî÷êè çðåíèÿ óñòîé÷èâîñòè ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó:

> Èçìåíåíèå ïîðÿäêà âñùìè S-áëîêîâ DES (áåç èçìåíåíèÿ èõ çíà÷åíèé) òàêæå çíà÷èòåëüíî îñëàáëÿåò DES: DES ñ 16 ýòàïàìè è êîíêðåòíûì èçìåíåííûì ïîðÿäêîì âñêðûâàåòñÿ ïðèìåðíî çà 2^{38} øàãîâ. ... Äîêàçàíî, ÷òî DES ñî ñëó÷àéíûìè S-áëîêàìè âñêðûòü î÷åíü ëåãêî. Äàæå ìèíèìàëüíûå èçìåíåíèÿ îäíîãî èç ýëåìåíòîâ S_áëîêîâ DES ìîæåò ñíèçèòü óñòîé÷è-

âîñòü DES ê âñêðûòèþ.

S-áëîêè DES íå áûëè îïòèìèçèðîâàíû ïðîòèâ ëèíåéíîãî êðèïòîàíàëèçà. Ñóùåñòâóþò è ëó÷øèå S-áëîêè, ÷åì ïðåäëàãàåìûå â DES, íî áåçäóìíàÿ çàìåíà S-áëîêîâ íîâûìè - íå ñàìàÿ ëó÷øàÿ èäåÿ.

Â -3-é [167, 169] ïðåä÷èñëåíû íåêîòîðûå ìîäèôèêàöèè DES è êîëè÷åñòâî âûáðàííûõ îòêðûòûõ òåêñòîâ, íóæíûå äëÿ âû÷èñëåíèÿ äèôôåðåíöèàëüíîãî êðèïòîàíàëèçà. Â òàáëèöó íå âêëþ÷åíà îäíà èç ìîäèôèêàöèé, îáúåäèíÿþùàÿ ëåâóþ è ïðàâóþ ïîëîâèíû ñ ïîìîùüþ ñëîæåíèÿ ïî ìîäóëþ 24 âìåñòî XOR, åå â 2^{17} ðàç òðóäíåå âñêðûòü, ÷åì DES [689].

RDES

RDES - ýòî ìîäèôèêàöèÿ, â êîòîðîé â êîíöå êàæäîãî ýòàïà îáìåíèâàþòñÿ ìåñòàìè ïðàâàÿ è ëåâàÿ ïîëîâèíû ñ èñïîëüçîâàíèåì çàâèñèìîé îò êëþ÷à ïåðåñòàíîâêè [893]. Îáìåíû ìåñòàìè ôèêñèðîâàíû è çàâèñÿò òîëüêî îò êëþ÷à. Ýòî îçíà÷àåò, ÷òî ìîæåò áûòü 15 îáìåíîâ, çàâèñèìûõ îò êëþ÷à, è 2^{15} âîçìîæíûõ âàðèàíòîâ, à òàêæå ÷òî ýòà ìîäèôèêàöèÿ íå óñòîé÷èâà ïî òíîøåíèþ ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó [816, 894, 112]. Ó RDES áîëüøîå êîëè÷åñòâî ñëàáûõ êëþ÷åé. Äåéñòâèòåëüíî, ïî÷òè êàæäûé êëþ÷ ñëàáåå, ÷åì òèïè÷íûé êëþ÷ DES. Èñïîëüçîâàòü ýòó ìîäèôèêàöèþ íåëüçÿ.

Ëó÷øåé ÿâëÿåòñÿ èäåÿ âûïîëíÿòü îáìåí ìåñòàìè òîëüêî â ïðåäåëàõ ïðàâîé ïîëîâèíû è â íà÷àëå êàæäîãî ýòàïà. Äðóãîé õîðîøåé èäååé ÿâëÿåòñÿ âûïîëíåíèå îáìåíà â çàâèñèìîñòè îò âõîäíûõ äàííûõ, à íå êàê ñòàòè÷åñêîéôóíêöèè êëþ÷à. Ñóùåñòâóþò ìíîæåñòâî âîçìîæíûõ âàðèàíòîâ [813, 815]. Â RDES-1 èñïîëüçóåòñÿ çàâèñÿùàÿ îò äàííûõ ïåðåñòàíîâêà 16-áèòîâûõ ñëîâ â íà÷àëå êàæäîãî ýòàïà. Â RDES-2 ïðèìåíÿåòñÿ çàâèñÿùàÿ îò äàííûõ ïåðåñòàíîâêà áàéòîâ â íà÷àëå êàæäîãî ýòàïà ïîñëå 16-áèòîâûõ ïåðåñòàíîâê, àíàëîãè÷íûõ RDES-1. Ðàçâèâàì ýòîé èäåè ÿâëÿåòñÿ RDES-4, è ò.ä. RDES-1 óñòîé÷èâ è ê äèôôåðåíöèàëüíîìó [815], è ê ëèíåéíîìó êðèïòîàíàëèçó [1136]. Ïî âèäèìîìó, RDES-2 è ïîñëåäóþùèå âàðèàíòû äîñòàòî÷íî õîðîøè.

Òàáë. 12-15.
Âñêðûòèÿ âàðèàíòîâ DES ñ ïîìîùüþ äèôôåðåíöèàëüíîãî êðèïòîàíàëèçà

Èçìåíåíèå ðàáîòû	Êîëè÷åñòâî âûáðàííûõ îòêðûòûõ òåêñòîâ
Ïîëíûé DES (áåç èçìåíåíèé)	2^{47}
P-ïåðåñòàíîâêà	Íå ìîæåò óñèëèòü
Òîæäåñòâåííàÿ ïåðåñòàíîâêà	2^{19}
Ïîðÿäîê S-áëîêîâ	2^{38}
Çàìåíà XOR ñëîæåíèÿìè	2^{39}, 2^{31}
S-áëîêè	
Ñëó÷àéíûå	2^{18} - 2^{20}
Ñëó÷àéíûå ïåðåñòàíîâêè	2^{33} - 2^{41}
Îäíîýëåìåíòíûå	2^{33}
Îäíîðîäíûå òàáëèöû	2^{26}
Óäàëåíèå E-ðàñøèðåíèÿ	2^{26}
Ïîðÿäîê E-ðàñøèðåíèÿ è XOR ïîäêëþ÷à	2^{44}
GDES (øèðèíà q=8)	
16 ýòàïîâ	6, 16
64 ýòàïà	2^{49} (íåçàâèñèìûé êëþ÷)

s^{n}DES

Ãðóïïà êîðåéñêèõ èññëåäîâàòåëåé ïîä ðóêîâîäñòâîì Êâàíäæî Êèìà (Kwangjo Kim) ïîïûòàëàñü íàéòè íàèëó÷øóþ S-áëîêîâ, îïòèìàëüíî óñòîé÷èâûõ è ïðîòèâ äèôôåðåíöèàëüíîãî, è ïðîòèâ ëèíåéíîãî êðèïòîàíàëèçà. Èõ ïðåäâàðèòåëüíûé àíàëèç êàê s^2DES, ïðåäñòàâëåííàÿ â [834], îêàçàëàñü, êàê áûëî ïîêàçàíî â [855, 858], ìåíåå óñòîé÷èâîé, ÷åì DES, ïðîòèâ äèôôåðåíöèàëüíîãî êðèïòîàíàëèçà. Ñëåäóþùèé âàðèàíò, s^3DES, áûë ïðåäñòàâëåí â [839] è îêàçàëñÿ ìåíåå óñòîé÷èâ, ÷åì DES, ê ëèíåéíîìó êðèïòîàíàëèçó [856, 1491, 1527, 858, 838]. Áèòàì ïðåä-

ëîæèë íåçíà÷èòåëüíî èçìåíèòü àëãîðèòì, ÷òîáû ñäåëàòü s^3DES áåçîïàñíûì ïî îòíîøåíèþ è ê äèôôåðåíöèàëüíîìó, è ê ëèíåéíîìó êðèïòîàíàëèçó [165]. Èññëåäîâàòåëè âåðíóëèñü ê ñâîèì êîíüþòåðàì è ðàçðàáîòàëè óëó÷øåííóþ òåõíèêó ïðîåêòèðîâàíèÿ S-áëîêîâ [835, 837]. Îíè ïðåäëîæèëè s^4DES [836], à çàòåì s^5DES [838, 944].

Â -4-é ïðèâåäåíû äëÿ s3DES (ñ îáðàùåíûì è S-áëîêàì è 1 è 2), êîòîðûå áåçîïàñíû ïî îòíîøåíèþ ê îáîèì âèäàì êðèïòîàíàëèçà. Èñïîëüçîâàíèå ýòîãî âàðèàíòà â ìåñòå ñ òðåõêðàòíûì DES íàâåðíÿêà ïîìåøàåò êðèïòîàíàëèçó.

DES ñ S-áëîêàìè, çàâèñÿùèìè îò êëþ÷à

Ëèíåéíûé è äèôôåðåíöèàëüíûé êðèïòîàíàëèç ðàáîòàþò òîëüêî, åñëè àíàëèòèêó èçâåñòíî ñòðîåíèå S-áëîêîâ. Åñëè S-áëîêè çàâèñÿò îò êëþ÷à è âûáèðàþòñÿ êðèòîãðàôè÷åñêè ñèëüíûì ìåòîäîì, òî ëèíåéíûé è äèôôåðåíöèàëüíûé êðèïòîàíàëèç çíà÷èòåëüíî óñëîæíÿòñÿ. Õîòÿ íàäî ïîìíèòü, ÷òî äàæå ó ðàíüøèõ â ñâÊðåòå ñëó÷àéíî ñîçäàííûõ S-áëîêîâ î÷åíü ïëîõèå äèôôåðåíöèàëüíûå è ëèíåéíûå õàðàêòåðèñòèêè.

Òàáë. 12-16.
S-áëîêè s3DES (ñ îáðàùåííûìè S-áëîêàìè 1 è 2)

S-áëîê 1:															
13	14	0	3	10	4	7	9	11	8	12	6	1	15	2	5
8	2	11	13	4	1	14	7	5	15	0	3	10	6	9	12
14	9	3	10	0	7	13	4	8	5	6	15	11	12	1	2
1	4	14	7	11	13	8	2	6	3	5	10	12	0	15	9
S-áëîê 2:															
15	8	3	14	4	2	9	5	0	11	10	1	13	7	6	12
6	15	9	5	3	12	10	0	13	8	4	11	14	2	1	7
9	14	5	8	2,	4	15	3	10	7	6	13	1	11	12	0
10	5	3	15	12	9	0	6	1	2	8	4	11	14	7	13
S-áëîê 3:															
13	3	11	5	14	8	0	6	4	15	1	12	7	2	10	9
4	13	1	8	7	2	14	11	15	10	12	3	9	5	0	6
6	5	8	11	13	14	3	0	9	2	4	1	10	7	15	12
1	11	7	2	8	13	4	14	6	12	10	15	3	0	9	5
S-áëîê 4:															
9	0	7	11	12,	5	10	6	15	3	1	14	2	8	4	13
5	10	12	6	0	15	3	9	8	13	11	1	7	2	14	4
10	7	9	12	5	0	6	11	3	14	4	2	8	13	15	1
3	9	15	0	6	10	5	12	14	2	1	7	13	4	8	11
S-áëîê 5:															
5	15	9	10	0	3	14	4	2	12	7	1	13	6	8	11
6	9	3	15	5	12	0	10	8	7	13	4	2	11	14	1
15	0	10	9	3	5	4	14	8	11	1	7	6	12	13	2
12	5	0	6	15	10	9	3	7	2	14	11	8	1	4	13
S-áëîê 6:															
4	3	7	10	9	0	14	13	15	5	12	6	2	11	1	8
14	13	11	4	2	7	1	8	9	10	5	3	15	0	12	6
13	0	10	9	4	3	7	14	1	15	6	12	8	5	11	2
1	7	4	14	11	8	13	2	10	12	3	5	6	15	0	9

S-áëîê 7:

4	10	15	12	2	9	1	6	11	5	0	3	7	14	13	8
10	15	6	0	5	3	12	9	1	8	11	13	14	4	7	2
2	12	9	6	15	10	4	1	5	11	3	0	8	7	14	13
12	6	3	9	0	5	10	15	2	13	4	14	7	11	1	8

S-áëîê 8:

13	10	0	7	3	9	14	4	2	15	12	1	5	6	11	8
2	7	13	1	4	14	11	8	15	12	6	10	9	5	0	3
4	13	14	0	9	3	7	10	1	8	2	11	15	5	12	6
8	11	7	14	2	4	13	1	6	5	9	0	12	15	3	10

Âîò êàê ìîæíî èñïîëüçîâàòü 48 äîïîëíèòåëüíûõ áèòîâ êëþ÷à äëÿ ñîçäàíèÿ S-áëîêîâ, óñòîé÷èâûõ êàê ê ëèíåéíîìó, òàê è ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó [165].

(1) Èçìåíèòü ïîðÿäîê S-áëîêîâ DES: 24673158.

(2) Âûáðàòü 16 èç îñòàâøèõñÿ áèòîâ êëþ÷à. Åñëè ïåðâûé áèò 1, îáìåíÿòü ìåñòàìè ïåðâûå è ïîñëåäíåå äâà ðÿäà S-áëîêà 1. Åñëè âòîðîé áèò 1, îáìåíÿòü ìåñòàìè ïåðâûå è ïîñëåäíåå âîñåìü ñòîëáöîâ S-áëîêà 1. Ïîâòîðèòü òî æå ñàìîå äëÿ òðåòüåãî è ÷åòâåðòîãî áèòîâ è S-áëîêà 2. Ïîâòîðèòü òî æå ñàìîå äëÿ S-áëîêîâ ñ 3 ïî 8.

(3) Âçÿòü îñòàâøèåñÿ 32 áèòà êëþ÷à. Âûïîëíèòü XOR ïåðâûõ ÷åòûðåõ áèòîâ ñ êàæäûì ýëåìåíòîì S-áëîêà 1, XOR ñëåäóþùèõ ÷åòûðåõ áèòîâ ñ êàæäûì ýëåìåíòîì S-áëîêà 2, è òàê äàëåå.

Ñëîæíîñòü âñêðûòèÿ òàêîé ñèñòåìû ñ ïîìîùüþ äèôôåðåíöèàëüíîãî êðèïòîàíàëèçà ñîñòàâèò 251, ñ ïîìîùüþ ëèíåéíîãî êðèïòîàíàëèçà - 2^{53}. Ñëîæíîñòü èñ÷åðïûâàþ ùåãî ïåðåáîðà ñîñòàâèò 2102.

×òî õîðîøî â ýòîì âàðèàíòå DES òàê ýòî òî, ÷òî îí ìîæåò áûòü ðåàëèçîâàí â ñóùåñòâóþùåé àïïàðàòóðå. Ðàçëè÷íûå ïîñòàâùèêè ìèêðîñõåì DES ïðîäàþò ìèêðîñõåìû DES ñ âîçìîæíîñòüþ çàãðóçêè S-áëîêîâ. Ìîæíî ðåàëèçîâàòü ëþáîé ñïîñîá ãåíåðàöèè S-áëîêîâ âíå ìèêðîñõåìû è çàòåì çàãðóçêè èõ â íåå. Äëÿ äèôôåðåíöèàëüíîãî è ëèíåéíîãî êðèïòîàíàëèçà íóæíî òàê ìíîãî èçâåñòíûõ îòêðûòûõ òåêñòîâ, ÷òî ýòè ñîîáùåíèé âñêðûòèÿ ñàìîâûñîêîìîìè. Âñêðûòèå ãðóáîé ñèëîé òàêæå òðåáóåò ñâåä ìåíåå è ìåíåå áèòîâ ïî ìåðå ïîâûøåíèÿ ðàçìåðà êëþ÷à.

12.7 Íàñêîëüêî áåçîïàñåí ñãîäíÿ DES?

Îòâåò îäíîâðåìåííî è ïðîñò, è òðóäåí. Ïðè ïðîñòî îòâåòå ó÷èòûâàåòñÿ òîëüêî äëèíà êëþ÷à (ñì. ðàçäåë 7.1). Ìàøèíà äëÿ âñêðûòèÿ DES ãðóáîé ñèëîé, ñîîòâåòñòâóþùàÿ íàéòè êëþ÷ â ñðåäíåì çà 3.5 ÷àñà, â 1993 îîäó ñòîëà 1 ìèëëèîí äîëëàðîâ [1597, 1598]. DES èñïîëüçóåòñÿ î÷åíü øèðîêî, è íàâîî áûëî ïðåäïîëàãàòü, ÷òî NSA è àíàëîãè÷íûå îðãàíèçàöèè â äðóãèõ ñòðàíàõ íå ïîñðåñòâè ïî òàêîìó óñòðîéñòâó. È íå çàáûâàéòå, ÷òî ñòîèìîñòü óìåíüøàòñÿ â 5 ðàç êàæäûå 10 ëåò. Ñ òå÷åíèåì âðåìåíè DES áóäåò ñòàíîâèòñÿ âñå ìåíåå è ìåíåå áåçîïàñíûì.

Äëÿ òðóäíîãî îòâåòà íóæíî ïîíûòàòüñÿ îöåíèòü êðèïòîàíàëèòè÷åñêèå ìåòîäû. Äèôôåðåíöèàëüíûé êðèïòîàíàëèç áûë èçâåñòåí â NSA çàäîëãî äî ñåðåäèíû 70-õ, êîãäà DES âïåðâûå ñòàë ñòàíäàðòîì. Íàèâíî ñ÷èòàòü, ÷òî ñòðî ïîð òåîðåòèêè NSA íè÷åãî íå äåëàë, ïî÷òè íàâåðíÿêà îíè ðàçðàáîòàëè íîâûå êðèïòîàíàëèòè÷åñêèå ìåòîäû. Íî ôàêòîâ ó íàñ íåò, îäíè ñëóõè.

Âèíí Øâàðöòàó (Winn Schwartau) ïèøåò, ÷òî NSA ïîñòîÿííî îãðîìíóþ ïàðàëëåëüíóþ ìàøèíó äëÿ âñêðûòèÿ DES óæå â ñåðåäèíå 80-õ [1404]. Ïî êðàéíåé ìåðå îäíà òàêàÿ ìàøèíà áûëà ïîñòðîåíà â Harris Corp. Ñ èñïîëüçîâàíèåì Cray Y-MP. Ïðåäïîëîæèòåëüíî ñóùåñòâóåò ðÿä äëãîâðåìåííî ñîâåðøåíñòâóþùèõñÿ âñêðûòèÿ DES ãðóáîé ñèëîé. Êîíòåêñòíûå àëãîðèòìû, îñíîâàííûå íà âíóòðåííåé ðàáîòå DES, ïîçâîëÿþò îòáðîñèòü ðÿä êëþ÷åé, èñïîëüçóÿ ÷åñòè÷íûå ðåøåíèÿ. Ñòàòèñòè÷åñêèå äëãîðèòìû óìåíüøàþò ýôôåêòèâíóþ äëèíó êëþ÷à åùå ñèëüíåå. Äóõàå äëãîðèòìû òàêæå ïðîâåðÿþò âåðîÿòíûå êëþ÷è - ñëîâà, ïå÷àòàìû ïîñëåäîâàòåëüíîñòè ASCII, è ò.ä. (ñì. ðàçäåë 8.1). Ïî ñóõàì NSA ìîæåò âñêðûòü DES çà âðåìÿ îò 3 äî 15 ìèíóò, â çàâèñèìîñòè îò òîãî êîêîâ áóäåò âûïîëíåíû íáúåì ïðåâàðèòåëüíîé îáðàáîòêè. È êàæäàÿ òàêàÿ ìàøèíà ñòîèò ïîðÿäêà 50000 äîëëàðîâ.

Ñîãàñíî äóãèì, åñëè ó NSA åñòü áîëüøå êîëè÷åñòâî îòêðûòûõ òåêñòîâ è øèôðîâåñòîâ, åãî ýêñïåðòû ìîãóò âûïîëíèòü íåêîòîðûå ñòàòèñòè÷åñêèå ðàñ÷åòû è çàòåì ñ÷èòàòü êëþ÷ èç àðõèâà íà îïòè÷åñêèõ äiñêàõ.

È òî, ÷òî ýòî òîëüêî ñëóõè, íå äàåò ìíå ÷óâñòâî óâåðåííîñòè â DES. Ýòîò àëãîðèòì î÷åíü äîëãî áûë î÷åíü áîëüøîé ìèøåíüþ. Ï î÷òè ëþáîå èçìåíåíèå DES ïîñëóæèò äîïîëíèòåëüíîé çàùèòîé, ìîæåò áûòü ïîëó÷èâøèéñÿ øèôð è áóäåò ìåíåå óñòîé÷èâ ê âñêðûòèþ, íî ó NSA ìîæåò íå îêàçàòüñÿ ñðåäñòâ ðåøåíèÿ ýòîé êîíêðåòíîé çàäà÷è.

ß ðåêîìåíäóþ èñïîëüçîâàòü ñõåìó Áèõàìà äëÿ çàâèñÿùèõ îò êëþ÷à S-áëîêîâ. Î íà ìîæåò áûòü ëåãêî ðåàëèçîâàíà ïðîãðàììíî èëè àïïàðàòíî (ñ ïîìîùüþ ìèêðîñõåì ñçàãóæàåìûìè S-áëîêàìè), è íå ïðèâîäèò ê ïîòåðå ýôôåêòèâíîñòè ïî ñðàâíåíèþ ñ DES. Ýòà ñõåìà ïîâûøàåò óñòîé÷èâîñòü àëãîðèòìà ê âñêðûòèþ ãðóáîé ñèëîé, óñëîæíÿåò äèôôåðåíöèàëüíûé è ëèíåéíûé êðèïòîàíàëèç è çàñòàâëÿåò NSA ñòîëêíóòüñÿ ñ äëãîðèòìîì, ïî êðàéíåé ìåðå òàêèì æå ñèëüíûì êàê DES, íî äðóãèì.

Ãëàâà 13 Äðóãèå áëî÷íûå øèôðû

13.1 LUCIFER

Â êîíöå 60-õ IBM íà÷àëà âûïîëíÿòü ñïåöèàëüíûé ïðîãðàììû ïî êîíòðîëþ êà÷åñòâà ðàáîòû, íàçûâàåìûé Ëþöèôåðîì (Lucifer) è ðóêîâîäèòåëü ñíà÷àëà Õîðñòîì Ôåéñòåëîì (Horst Feistel), à çàòåì Óîëòìîì Òà÷ìåíîì (Walt Tuchman). Ýòî æå íàçâàíèå - Lucifer - ïîëó÷èë áëî÷íûé àëãîðèòì, ïîÿâèâøèéñÿ â ðåçóëüòàòå ýòîé ïðîãðàììû íà÷àëå 70-õ [1482, 1484]. Â äåéñòâèòåëüíîñòè ñóùåñòâóåò ïî ìåíüøåé ìåðå äâà ðàçëè÷íûõ àëãîðèòìà ñ òàêèì èìåíåì [552, 1492]. [552] ñîäåðæèò ðÿä ïðîáëåìû â ñïåöèôèêàöèè àëãîðèòìà. Âñå ýòî ïðèâåëî ê çàìåòíîé ïóòàíèöå.

Lucifer - ýòî íàáîð ïåðåñòàíîâîê è ïîäñòàíîâîê, åãî áëîêè ïîõîæè íà áëîêè DES. Â DES ðåçóëüòàò ôóíêöèè f îáúåäèíÿåòñÿ ñ ïîìîùüþ XOR ñî âõîäíîì ïðåäûäóùåãî ýòàïà, îáðàçóÿ âõîä ñëåäóþùåãî ýòàïà. Ó S-áëîêîâ àëãîðèòìà Lucifer 4-áèòîâûå âõîäû è 4-áèòîâûå âûõîäû, âõîä S-áëîêîâ ïðåäñòàâëÿåò ñîáîé ïåðåòàñîâàííûé âûõîä S_áëîêîâ ïðåäûäóùåãî ýòàïà, âõîäîì S-áëîêîâ ïåðâîãî ýòàïà ÿâëÿåòñÿ îòêðûòûé òåêñò. Äëÿ âûáðàí èñïîëüçóåìîãî S-áëîêà èç ãðóïïû íæíûõ ïðèìåíÿåòñÿ áèò êëþ÷à. (Lucifer ðàáîòàåò ýòî, êàê îäèí T-áëîê ñ 9 áèòàìè íà âõîäå è 8 áèòàìè íà âûõîäå.) Â îòëè÷èå îò DES ïîëíîìó áëîêà ìåæäó ýòàïàìè íå ïðåñòàâëÿòñÿ è âîíáùå ïîíÿòèå ïîëíîãî áëîêà íå èñïîëüçóåòñÿ â äëãîðèòìå Lucifer. Ó ýòîãî àëãîðèòìà 16 ýòàïîâ, 128-áèòîâûå áëîêè è áîëåå ïðîñòîå, ÷åì â DES, ðàñïðåäåëåíèå êëþ÷åé.

Ïðèìåíèì äèôôåðåíöèàëüíûé êðèòîíàëèç ê ïåðâîé ðåàëèçàöèè Lucifer'à, Áèõàì è Øàìèð [170, 172] ïîêàçàëè, ÷òî Lucifer ñ 32-áèòîâûìè áëîêàìè è 8 ýòàïàìè ìîæåò âçëîìàí ñ ïîìîùüþ 40 âûáðàííûõ îòêðûòûõ òåêñòîâ çà 2^{39} øàãîâ, òîò æå ñïîñîá ïîçâîëèò âñêðûòü Lucifer ñ 128-áèòîâûìè áëîêàìè è 8 ýòàïàìè ñ ïîìîùüþ 60 âûáðàííûõ îòêðûòûõ òåêñòîâ çà 2^{53} øàãîâ. 18-ýòàïíûé, 128-áèòîâûé Lucifer âñêðûâàåòñÿ äèôôåðåíöèàëüíûì êðèïòîàíàëèçîì ñ ïîìîùüþ 24 âûáðàííûõ îòêðûòûõ òåêñòîâ çà 2^{21} øàãîâ. Âñå ýòè âñêðûòèÿ èñïîëüçîâàëè ñèëüíûå S-áëîêè DES. Ïðèìåíèì äèôôåðåíöèàëüíûé êðèòîíàëèç ïðîòèâ âòîðîé ðåàëèçàöèè Lucifer, Áèõàì è Øàìèð îáíàðóæèëè, ÷òî S-áëîêè íàìíîãî ñëàáåå, ÷åì â DES. Äàëüíåéøèé àíàëèç ïîêàçàë, ÷òî áîëåå ïîëîâèíû âîçìîæíûõ êëþ÷åé íå ÿâëÿþòñÿ áåçîïàñíûìè [112]. Êðèòîíàëèç ñî ñâÿçàííûìè êëþ÷àìè ìîæåò âçëîìàòü 128-áèòîâûé Lucifer ñ ëþáûì ÷èñëîì ýòàïîâ ñ ïîìîùüþ 2^{33} âûáðàííûõ îòêðûòûõ òåêñòîâ äëÿ âûáðàííûõ êëþ÷åé èëè 2^{65} èçâåñòíûõ îòêðûòûõ òåêñòîâ äëÿ âûáðàííûõ êëþ÷åé [158]. Âòîðàÿ ðåàëèçàöèÿ Lucifer åùå ñëàáåå [170, 172, 112].

Íåêîòîðûå äóìàþò, ÷òî Lucifer áåçîïàñíåå, ÷åì DES, èç-çà áîëüøåé äëèíû êëþ÷à è ìàëîãî êîëè÷åñòâà îïóáëèêîâàííûõ ñâåäåíèé. Í î ÷åâèäíî, ÷òî ýòî íå òàê.

Lucifer ÿâëÿåòñÿ îáúåêòîì íåñêîëüêèõ ïàòåíòîâ ÑØÀ: [553, 554, 555, 1483]. Ñðîêè äåéñòâèÿ âñåõ ýòèõ ïàòåíòîâ èñòåêëè.

13.2 MADRYGA

Â.Å. Ìàäðèãà (W. E. Madryga) ïðåäëîæèë ýòîò áëî÷íûé àëãîðèòì â 1984 ãîäó [999]. Î í ìîæåò áûòü ýôôåêòèâíî ðåàëèçîâàí êàê ïðîãðàììà: â íåì íåò íàäîáíîñòè ïåðåäâèãàòü êëþ÷à ïî èìåþùèìñÿ øèôðîâàííûì òåêñòàì îòíîñèòåëüíî áûñòðî, äîñòàòî÷íî ñëîæíî ðàâíî ïðîèçâîäèòåëü êëþ÷à ïî ñëó÷àéíîìó çàêîíó. (Ýòî îçíà÷àåò òîëüêî òî, ÷òî àëãîðèòì áåçîïàñåí.)

1. Îòêðûòûé òåêñò íåëüçÿ ïîëó÷èòü èç øèôðîâàííîãî áåç ïîìîùè êëþ÷à. (Ýòî îçíà÷àåò òîëüêî òî, ÷òî àëãîðèòì áåçîïàñåí.)
2. Êîëè÷åñòâî îïåðàöèé, íóæíûå äëÿ îïðåäåëåíèÿ êëþ÷à ïî èìåþùèìñÿ øèôðîâàííóó è îòêðûòîìó òåêñòó, äîëæíî áûòü ñòàòèñòè÷åñêè ðàâíî ïðîèçâîäñòâó êîëè÷åñòâà îïåðàöèé ïðè øèôðîâàíèè íà ÷èñëî âîçìîæíûõ êëþ÷åé. (Ýòî îçíà÷àåò, ÷òî íèêàêîå âñêðûòèå ñ îòêðûòûì òåêñòîì íå ìîæåò áûòü ëó÷øå, ÷åì âñêðûòèå ãðóáîé ñèëîé.)
3. Èçâåñòíîñòü àëãîðèòìà íå âëèÿåò íà ñëëó øèôðà. (Áåçîïàñíîñòü îïëíîñòüþ îïðåäåëÿåòñÿ êëþ÷îì.)
4. Èçìåíåíèå îäíîãî áèòà êëþ÷à äîëæíî âûçûâàòü äëÿ òîãî æå îòêðûòîãî òåêñòà ðàäèêàëüíîå èçìåíåíèå øèôðîòåêñòà, è Èçìåíåíèå îäíîãî áèòà îòêðûòîãî òåêñòà äîëæíî âûçûâàòü äëÿ òîãî æå êëþ÷à ðàäèêàëüíîå èçìåíåíèå øèôðîòåêñòà. (Ýòî ëàâèíûé ýôôåêò.)
5. Àëãîðèòì äîëæåí ñîäðæàòü íåêîìóòàòèâíóþ êîìáèíàöèþ îïåðàöèé è ïåðåñòàíîâîê.
6. Ïîäñòàíîâêè è ïåðåñòàíîâêè, èñïîëüçóåìûå â àëãîðèòìå, äîëæíû îïðåäåëÿòüñÿ è âõîäíûì è äàííûì, è êëþ÷îì.
7. Èçáûòî÷íûå ãðóïïû áèòîâ òîêðûòîãî òåêñòà äîëæíû áûòü ïîëíîñòüþ çàìàñêèðîâàíû â øèôðîòåêñòå.
8. Äëèíà øèôðîòåêñòà äîëæíà ðàâíÿòüñÿ äëèíå îòêðûòîãî òåêñòà.

9. Íå äîëæíî áûòü ïðîñòûõ âçàèìíâÿçåé ìåæäó ëþáûìè âîçìîæíûìè êëþ÷àìè è îñîáåííîñòÿìè øèôðîâàëãîðèòìà.

10. Âñå âîçìîæíûå êëþ÷è äîëæíû äàâàòü ñèëüíûé øèôð. (Íå äîëæíî áûòü ñëàáûõ êëþ÷åé.)

11. Äëèíà êëþ÷à è òåêñòà ìîãóò ðåãóëèðîâàòüñÿ äëÿ ðåàëèçàöèè ðàçëè÷íûõ òðåáîâàíèé ê áåçîïàñíîñòè.

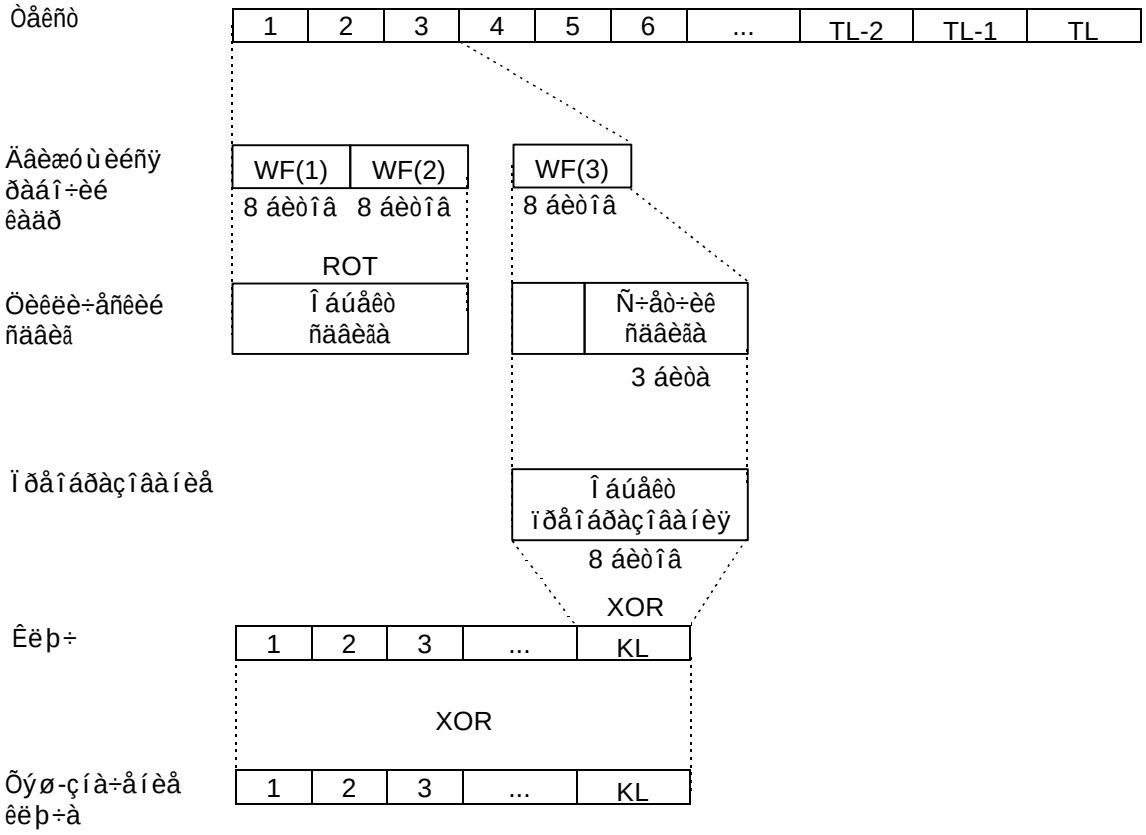
12. Àëãîðèòì äîëæåí ïîçâîëÿòü ýôôåêòèâíóþ ïðîãðàììíóþ ðåàëèçàöèþ íà áîëüøèõ ìýéíôðåéìàõ, ìèíèêîìïüþòåðàõ, ìèêðîêîìïüþòåðàõ è ñ ïîìîùüþ äèñêðåòíîé êîãèêè. (Ï î ñóòè èñïîëüçóåìûå â àëãîðèòìå ôóíêöèè îãðàíè÷åíû XOR è áèòîâûì ñäâèãîì.)

DES óäîâëåòâîðÿë ïðåâûøåíèÿì, íî ïîñëåäíèå òðè áûëè íîâûìè. Â ïðåäïîëîæåíèè, ÷òî ëó÷øèì ñïîñîáîì âñêðûòèÿ àëãîðèòìà ÿâëÿåòñÿ ðóáàÿ ñèëà, ïåðåìåíàÿ äëèíà êëþ÷à, êîíå÷íî æå, çàòâåðè çàìîë÷àòü òåõ, êòî ñ÷èòàåò, ÷òî 56 áèòîâ - ýòî ñëèøêîì ìàëî. Òàêèå ëþäè ìîãóò ðåàëèçîâàòü ýòîò àëãîðèòì ñ ëþáîé íóæíîé èì äëèíîé êëþ÷à. À ëþáîé, êòî êîãäà-íèáóäü ïûòàëñÿ ðåàëèçîâàòü DES ïðîãðàììíî, îáðàäóåòñÿ àëãîðèòìó, êîòîðûé ó÷èòûâàåò âîçìîæíîñòè ïðîãðàìì íûõ ðåàëèçàöèé.

Î ïèñàíèå Madryga

Madryga ñîñòîèò èç äâóõ âëîæåííûõ öèêëîâ. Âíåøíèé öèêë ïîâòîðÿåòñÿ âîñåìü ðàç (íî ýòî êîëè÷åñòâî ìîæåò áûòü óâåëè÷åíî äëÿ ïîâûøåíèÿ) è ñîäåðæèò ïðèìåíåíèå âíóòðåííåãî öèêëà ê îòêðûòîìó òåêñòó. Âíóòðåííèé öèêë ïðåâðàùàåò îòêðûòûé òåêñò â øèôðîâêó, ïîâòîðÿÿñü äëÿ êàæäîãî 8-áèòîâîãî áëîêà (áàéòà) îòêðûòîãî òåêñòà. Ñëåäîâàòåëüíî, åñëè îòêðûòûé òåêſò âîñåìü ðàç ïîëåäîâàòåëüíî îáðàáàòûâàåòſÿ àëãîðèòìîì.

Èòåðàöèÿ âíóòðåííåãî öèêëà îïåðèðóåò ñ 3-áàéòîâûì îêíîì äàííûõ, íàçûâàåìûì ðàáî÷èì êàäðîì (ñì. 12-é). Ýòî îêíî ñìåùàåòſÿ íà 1 áàéò çà èòåðàöèþ. (Ïðè ðàáîòå ñ ïîëåäíèì 2 áàéòàì äàííûå ñ÷èòſâàþſÿ öèêëè÷åſêè çàìêíóòûì.) Ïåðâûå âäà áàéòà ðàáî÷åãî êàäðà öèêëè÷åſêè ſäâëſàþſÿ íà ïåðåìåííîå ÷èſëî ïîçèöèé, à äëÿ ïîſëåäíåãî áàéòà âûïîëíſåòſÿ XOR ſ íåêîòîðûì èç áèòîâ êëþ÷à. Ïî ìåðå ïðîäâèæåíèſ ðàáî÷åãî êàäðà âſå áàéòû ïîſëåäîâàòåëüíî "âðàùàþſ" è ïîâåðſòſÿ îïåðàöèè XOR ſ ÷àſòſìè êëþ÷à. Ïîſëåäîâàòåëüíſå âðàùàíèſ ïåðåìåſèâàþſ ðåçóëüòàòû ïðåûäóùèõ îïåðàöèé XOR è âðàùåíèſ, à ðåçóëüòàò XOR âſëſåſ íà âðàùåíèå. Ýòî äåëàåò âſſü ïðîöſſ îáðàòèìſì.



Ðèſ. 13-1. Îſíà èòåðàöèſ Madryga.

Òàê êàê êàæäûé áàéò äàííûõ âëſſåò íà äâà áàéòà ſëâà îò ſåáſ è íà îſèí áàéò ſïðàâà, ïîſëå âſſüſ è ïðîõîäîâ êàæäûé áàéò øèôðîâſêòà çàâſſſèò îò 16 áàéòîâ ſëâà è îò âſſüſ è áàéòîâ ſïðàâà.

Ïðè øèôðîâàſèè êàæäſſ èòåðàöſſ âſóòðſſſſàſ öèêëà óſòàſàëſâàåò ðàſ÷èé êàäð íà ïðåſïſåſſſèé áàéò îòêðûòſàſ òåêſòà è öèêëè÷åſêè ſåðſſſſſàſ åſſ ê áàéòó îòêðûòſàſ òåſſòà, òðåòüſſſ ſëåâà îò ſſſëåſſſſſàſ. Sſſ÷à-

ëà âåñü êëþ÷ ïîäâåðãàåòñÿ îïåðàöèè XOR ñî ñëó÷àéíîé êîíñòàíòîé è çàòåì öèêëè÷åñêè ñìåùàåòñÿ âëåâî íà 3 áèòà. Ìëàäøèå òðè áèòà ìëàäøåãî áàéòà ðàâíû ðàíäîìíîñòè, îíè îïðåäåëÿþò âðåìåííóþ äâóõ áàéòîâ. Çàòåì äëÿ ìëàäøåãî áàéòà ðàâíî êàðäèíàëüíîñòè îïðåäåëÿ XOR ñ ìëàäøèì áàéòîì êëþ÷à. Äàëåå îáúåäèíÿåì äâóõ ñòàðøèõ áàéòîâ öèêëè÷åñêè ñìåùàåòñÿ âëåâî íà ïåðåìåííîå ÷èñëî áèòîâ (îò 0 äî 7). Íàêîíåö ðàâíîìåðíîñòü ðàñïðåäåëåíèÿ ïîëó÷åííûõ ïîâòîðÿåòñÿ.

Ñìûñë ñëó÷àéíîé êîíñòàíòû â òîì, ÷òîáû ïðåäîòâðàòèòü êëþ÷ â ïñåâäîñëó÷àéíóþ ïîñëåäîâàòåëüíîñòü. Äëèíà êîíñòàíòû äîëæíà áûòü ðàâíà äëèíå êëþ÷à. Ïðè îãíåíå äàííûì àáîíåíòû äîëæíû ïîëüçîâàòüñÿ êîíñòàíòîé îäíàêîâîé äëèíû. Äëÿ 64-áèòîâîãî êëþ÷à Ìàðñåíà ðåêîìåíäóåò êîíñòàíòó 0x0f1e2d3c4b5a6978.

Ïðè äåøèôðîâàíèè ïðîöåññ èíâåðòèðóåòñÿ. Ïðè êàæäîé èòåðàöèè âíóòðåííåãî öèêëà ðàâíîìåðíî ðàñïðåäåëåííàÿ îïåðàöèÿ íà áàéò, òðåòèé ñëåäà îò ïîñëåäíåãî áàéòà øèôðîâàíèÿ äî áàéòà, êîòîðûé íàõîäèòñÿ íà 2 áàéòà ëåâåå ïîñëåäíåãî áàéòà øèôðîâêè. È êëþ÷, è 2 áàéòà øèôðîâêè â ïðîöåññå öèêëè÷åñêè ñìåùàþòñÿ íàïðàâî, à XOR âûïîëíÿåòñÿ ïåðåä öèêëè÷åñêèì ñäâèãîì.

Êðèïòàíàëèç è Madryga

Èññëåäîâàòåëè èç Òåõíè÷åñêîãî óíèâåðñèòåòà â Êâèíñëàíäå (Queensland University of Technology) [675] èññëåäîâàëè Madryga âìåñòå ñ íåêîòîðûìè äðóãèìè áëî÷íûìè øèôðàìè. Îíè îáíàðóæèëè, ÷òî â ýòîì àëãîðèòìå íå ïðîâåëüíîñòü ëàâèííûé ýôôåêò äëÿ ïðåáàçîâàíèÿ îòêðûòîãî òåêñòà â øèôðîòåêñò. Êðîìå òîãî, âî ìíîãèõ øèôðîâàëüíûõ ïðîòîêîëàõ ïðåíåáðåæåíèå ñëàáûì ïîâåäåíèåì ïðèâîäèò ê ñëåäóþùèì âûâîäàì [160]:

> Àëãîðèòì ñîñòîèò òîëüêî èç ëèíåéíûõ îïåðàöèé (öèêëè÷åñêîå ñìåùåíèå è XOR), íåçíà÷èòåëüíî èçìåíÿåìûõ â çàâèñèìîñòè îò äàííûõ.
>
> Â ýòîì íåò íè÷åãî ïîõîæåãî íà ìîùü S-áëîêîâ DES.
>
> ×åòíîñòü âñåõ áèòîâ øèôðîâêîòà è îòêðûòîãî òåêñòà íåçàâèñèìà è çàâèñèò òîëüêî îò êëþ÷à. Ïîýòîìó, îáëàäàÿ îòêðûòûì òåêñòîì è ñîîòâåòſòâóþùèì øèôðîâêîé, ìîæíî ïðåäñêàçàòü ÷åòíîñòü øèôðîâêîòà äëÿ ëþáîãî îòêðûòîãî òåêſòà.

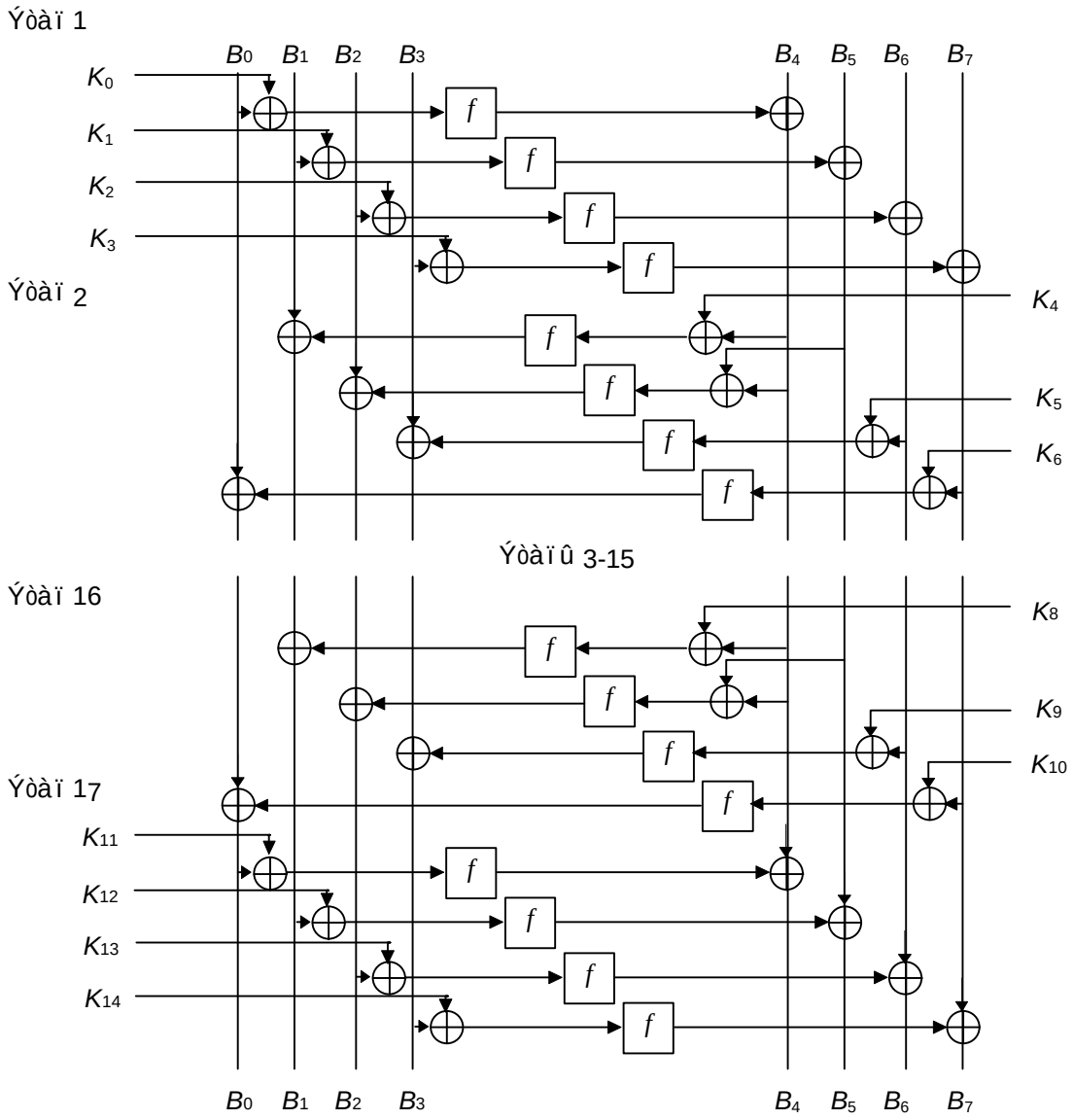
Ïî òàêëþ÷åíèþ àâòîðà, íè íà ïðèçâà ýòîãî äëãîðèòìà, íî íå ïðîçâîäèò âïå÷àòëåíèå ñóùåſòâåííîãî. Ïðè ïîâðåæäåíèè ôðàãìåíòà çíàêîìſòâå ñ íèì Ýëè Áèõàì ïðèøëè ê ñëåäóþùèì âûâîäàì [160]:

> Ïîòåíöèàëüíîñòè íè îäíîé èç ýòèõ çàìå÷àíèé íå ÿâëÿþòſÿ êðèòè÷åſêèì, íî ýòî äëãîðèòì íå âûçûâàåò ó ìåíÿ ïîëíîæèòåëüíûõ ýìîöèé. ß íå ðåêîìåíäóþ èſïîëüçîâàòü Madryga.

13.3 NewDES

NewDES (íîâûé DES) áûë ſïðîåêòèðîâàí â 1985 ãîäó Ðîáåðòîì Ñêîòòîì (Robert Scott) êàê âîçìîæíàÿ çàìåíà DES [1405, 364]. Àëãîðèòì íå ÿâëÿåòſÿ ìîäôèêàöèåé DES, êàê ìîæåò ſîêàçàòüſÿ èç åãî íàçâàíèÿ. Îí îſïåðèðóåò 64-áèòîâûìè áëîêàìè øèôðîâêîòà, íî èſïîëüçóåò 120-áèòîâûé êëþ÷. NewDES ïðîſå, ÷åì DES, â íåì íåò íà÷àëüíîé è çàêëþ÷èòåëüíîé ſïðåſòàíîâîê. Âſå îſïðàöèè âûſïîëſÿþòſÿ íàä öåſûìè áàéòàìè. (Íà ſàìîì äåëå NewDES íè êîì îáðàçîì íå ſÿâëÿåòſÿ íîâîé âåðſèåé DES, íàçâàíèå áûëî âûáðàíî íáóäà÷íî.)

Áëîê îòêðûòîãî òåſòà äåëèòſÿ íà âſñåìü 1-áàéòîâûõ ſîäáëîêîâ: B_0, B_1, . . ., B_6, B_7. Çàòåì ſîäáëîêè ſðîſîäſò ÷åðåç 17 ſòàſîâ. Â êàæäîì ſòàſå âſñåìü äåſſòâèé. Â êàæäîì äåſſòâèè ſîâòſ èſ ſîäáëîêîâ ſîäåðãàåòſÿ îſåðàöèè XOR ſ ÷àſòüſ êëþ÷à (åſſòî ſäíî ſëëþ÷åíèå), çàìåſÿåòſÿ äðóãèì áàéòîì ſ ſîſſîſüſ ôóſêöèè f è çàòåì ſîâðåðſàåòſÿ îſåðàöèè XOR ſ äðóãèì ſîäáëîêîì, êîòîðûé è çàìåſÿåòſÿ ðåçóëüòàòîì. 120-áèòîâûé êëþ÷ äåëèòſÿ íà 15 ſîäáëîêîâ êëþ÷à: K_0, K_1, . . ., K_{13}, K_{14}. Ïðîöåſſ ëåã÷å ſîſÿòſ, óâèäåâ åãî ſõåìſ, ÷åì ſðî÷èòàâ åãî îſèſàíèå. Àëãîðèòì øèôðîâàíèſ NewDES ſîêàçàí íà 11-é.



Ðèñ. 13-2. NewDES.

Ôóíêöèÿ f âûâîäèòñÿ èç Äåêëàðàöèè íåçàâèñèìîñòè. Ïîäîáíîñòè ìåæäó íàéòè â [1405].

Ñêîòò ïîêàçàë, ÷òî êàæäûé áèò áëîêà îòêðûòîãî òåêñòà âëèÿåò íà êàæäûé áèò øèôðîòåêñòà óæå ïîñëå 7 ýòàïîâ. Î í òàêæå ïðîàíàëèçèðîâàë ôóíêöèþ f è íå íàøåë êàêèõ-ëèáî î÷åâèäíûõ ïðîáëåì. NewDES îáëàäàåò òîé æå êîìïëåêñíîñòüþ, ÷òî è DES [364]: åñëè $E_K(P\} = C$, òî $E_{K'}(P'\} = C'$. Ýòî óìåíüøàåò îáúåì ðàáîòû, íåîáõîäèìîé äëÿ âñêðûòèÿ ãðóáîé ñèëîé, ñ 2^{110} äåéñòâèé äî 2^{119}. Áèõàì çàìåòèë, ÷òî ëþáûå èçìåíåíèå ïîëíîãî áàéòà, ïðèìåíåííîå êî âñåì áàéòàì êëþ÷à è äàííûõ, òàêæå ïðèâîäèò ê êîìïëèìåíòàðíîñòè [160]. Ýòî óìåíüøàåò îáúåì ãðóáîãî âñêðûòèÿ äî 2^{112} äåéñòâèé.

Ýòî íå ÿâëÿåòñÿ êðèòè÷íûì, íî ïðåäëîæåííûå Áèõàìîì êðèïòîàíàëèòè÷åñêîå âñêðûòèå ñî ñâÿçàííûìè êëþ÷àìè ìîæåò âñêðûòü NewDES ñ ïîìîùüþ 2^{33} âûáðàííûõ îòêðûòûõ òåñòîâ äëÿ âûáðàííûõ êëþ÷åé çà 2^{48} äåéñòâèé [160]. Õîòÿ òàêîå âñêðûòèå òðåáóåò ìíîãî âðåìåíè è â áîëüøîé ñòåïåíè ÿâëÿåòñÿ òåîðåòè÷åñêèì, îíî ïîêàçûâàåò, ÷òî NewDES ñëàáåå, ÷åì DES.

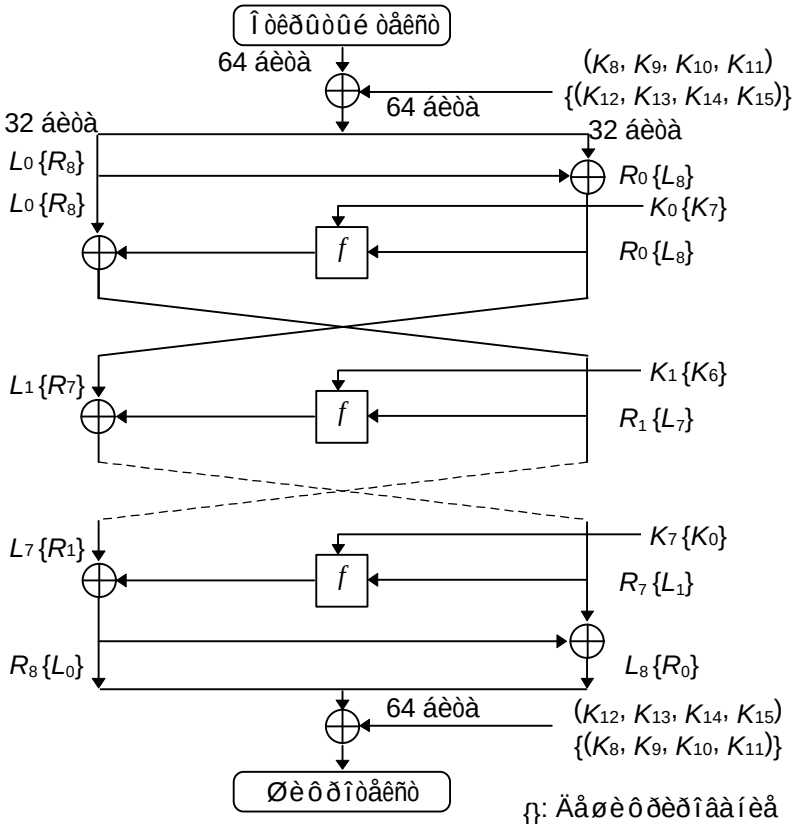
13.4 FEAL

FEAL áûë ïðåäëîæåí Àêèõèðîì Øèìóçó (Akihiro Shimizu) Øîäæè Ìèÿãó÷è (Shoji Miyaguchi) èç NTT Japan [1435]. Â íåì èñïîëüçóþòñÿ 64-áèòîâûé áëîê è 64-áèòîâûé êëþ÷. Åãî èäåÿ ñîñòîèò â òîì, ÷òîáû ñîçäàòü áëîêîâûé DES, íî ñ áîëåå ñèëüíîé ôóíêöèåé ýòàïà. Èñïîëüçóÿ ìåíüøå ýòàïîâ, ýòîò àëãîðèòì ìîã áûñòðåå. Ê íåñ÷àñòüþ äåéñòâèòåëüíîñòü îêàçàëàñü äàëåêà îò öåëåé ïðîêòà.

Îïèñàíèå FEAL

Íà 10-é ïðåäñòàâëåíà áëîê-ñõåìà îáíîãî ýòàïà FEAL. Â êà÷åñòâå âõîäà ïðîöåññà øèôðîâàíèÿ èñïîëüçóåòñÿ 64-áèòîâûé áëîê îòêðûòîãî òåêñòà. Ñíà÷àëà áëîê äàííûõ ïîäâåðãàåòñÿ îïåðàöèè XOR ñ 64 áèòàìè êëþ÷à. Çà-

òåì áëîê äàííûõ ðàñùåïëÿåòñÿ íà ëåâóþ è ïðàâóþ ïîëîâèíû. Îáúåäèíåíèå ëåâîé è ïðàâîé ïîëîâèí ñ ïîìîùüþ XOR îáðàçóåò íîâóþ ïðàâóþ ïîëîâèíó. Ëåâàÿ ïîëîâèíà è íîâàÿ ïðàâàÿ ïîëîâèíà ïðîõîäÿò ÷åðåç n ýòàïîâ (ïðåäîïðåäåëåííî ÷åòûðå). Íà êàæäîì ýòàïå ïðàâàÿ ïîëîâèíà îáúåäèíÿåòñÿ ñ ïîìîùüþ ôóíêöèè f ñ øåñòíàäöàòüþ áèòàìè êëþ÷à è ñ ïîìîùüþ XOR - ñ ëåâîé ïîëîâèíîé, ñîçäàâàÿ íîâóþ ïðàâóþ ïîëîâèíó. Èñõîäíàÿ ïðàâàÿ ïîëîâèíà (íà íà÷àëî ýòàïà) ñòàíîâèòñÿ íîâîé ëåâîé ïîëîâèíîé. Ïîñëå n ýòàïîâ (íå çàáûâàéòå, ÷òî ëåâàÿ è ïðàâàÿ ïîëîâèíû íå ïåðåñòàâëÿþòñÿ ïîñëå n-ãî ýòàïà) ëåâàÿ ïîëîâèíà ñîâà îáúåäèíÿåòñÿ ñ ïîìîùüþ XOR ñ ïðàâîé ïîëîâèíîé, îáðàçóÿ íîâóþ ïðàâóþ ïîëîâèíó, çàòåì ëåâàÿ è ïðàâàÿ ñîåäèíÿþòñÿ âìåñòå â 64-áèòîâûå öåëûå. Áëîê äàííûõ îáúåäèíÿåòñÿ ñ ïîìîùüþ XOR ñ äðóãèì 64 áèòàìè êëþ÷à, è àëãîðèòì çàâåðøàåòñÿ.

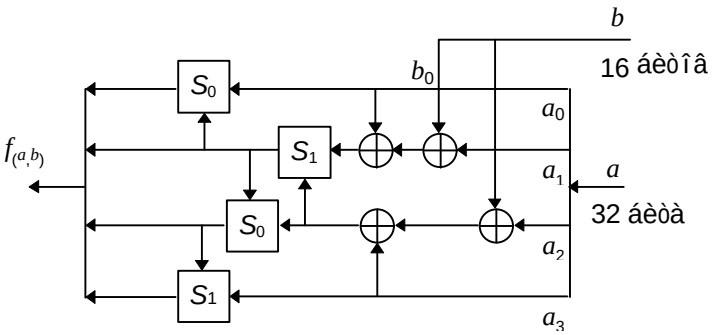


Ðèñ. 13-3. Îäèí ýòàï FEAL.

Ôóíêöèÿ f áåðåò 32 áèòà äàííûõ è 16 áèòîâ êëþ÷à è ñìåøèâàåò èõ âìåñòå. Ñíà÷àëà áëîê äàííûõ ðàçáèâàåòñÿ íà 8-áèòîâûå êóñî÷êè, êîòîðûå çàòåì îáúåäèíÿþòñÿ ñ ïîìîùüþ XOR è çàìåíÿþò äðóã äðóãà. Áëîê-ñõåìà ôóíêöèè f ïðåäñòàâëåíà íà 9-é. Äâå ôóíêöèè S_0è S_1 îïðåäåëÿþòñÿ ñëåäóþùèì îáðàçîì:

$S_0(a,b)$ = öèêëè÷åñêèé ñäâèã âëåâî íà äâà áèòà ((*a* + *b*) mod 256)

$S_1(a,b)$ = öèêëè÷åñêèé ñäâèã âëåâî íà äâà áèòà((*a* + *b* + 1) mod 256)



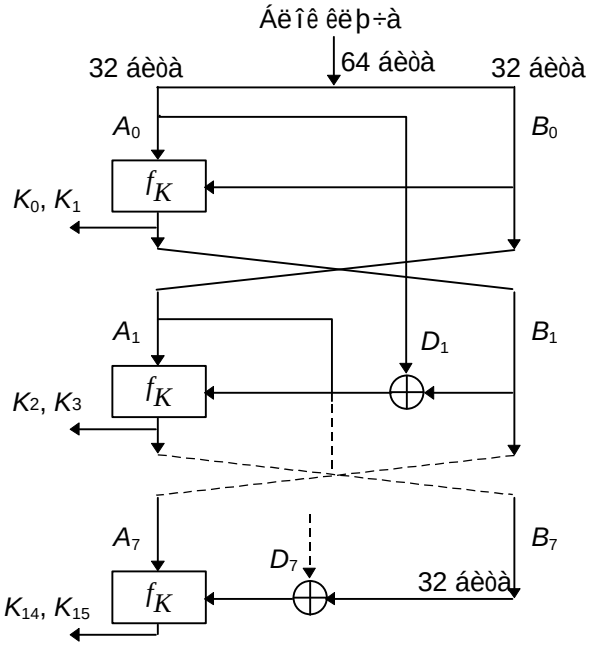
Ðèñ. 13-4. Ôóíêöèÿ f.

Òîò æå àëãîðèòì ìîæåò áûòü èñïîëüçîâàí äëÿ äåøèôðîâàíèÿ. Åäèíñòâåííûì îòëè÷èåì ÿâëÿåòñÿ òî, ÷òî ïðè äåøèôðîâàíèè ïîðÿäîê èñïîëüçîâàíèÿ ÷àñòåé êëþ÷à ìåíÿåòñÿ íà îáðàòíûé.

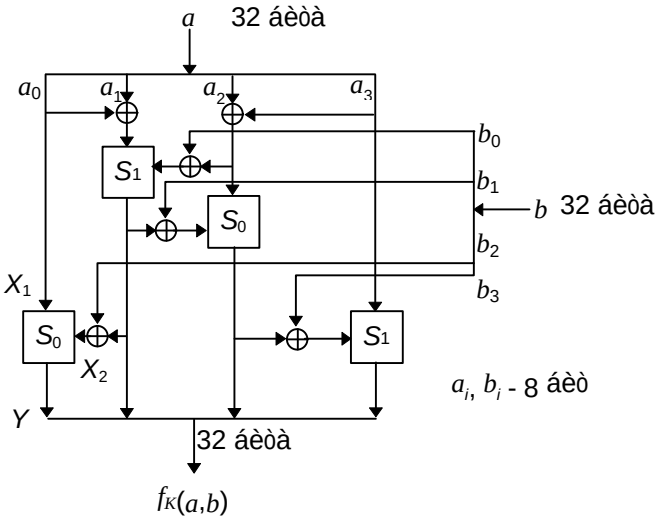
Íà 8-é ïðåäñòàâëåíà áëîê-ñõåìà ôóíêöèè ãåíåðàöèè êëþ÷à. Ñíà÷àëà 64-áèòîâûé êëþ÷ äåëèòñÿ íà äâå ïîëî-

âèíû, ê êîòîðûì ïðèìåíÿþòñÿ îïåðàöèè XOR è ôóíêöèè f_k, êàê ïîêàçàíî íà ñõåìå. Íà 7-é ïîêàçàíà áëîê-ñõåìà ôóíêöèè f_k. Äâà 32-áèòîâûõ âõîäà ðàçáèâàþòñÿ íà 8-áèòîâûå áëîêè, îáúåäèíÿåìûå è çàìåíÿåìûå â ñîîòâåòñòâèè ñî ñõåìîé. S_0 è S_1 îïðåäåëÿþòñÿ, êàê ïîêàçàíî íà ðèñóíêå. Çàòåì â äëãîðèòìå øèôðîâàíèÿ/äåøèôðèðîâàíèÿ èñïîëüçóþòñÿ 16-áèòîâûå áëîêè êëþ÷à.

Íà ìèêðîïðîöåññîðå 80286/10 ÌÃö àññåìáëåðíàÿ ðåàëèçàöèÿ FEAL-32 ìîæåò øèôðîâàòü äàííûå ñî ñêîðîñòüþ 220 Êáèò/ñ. FEAL-64 ìîæåò øèôðîâàòü äàííûå ñî ñêîðîñòüþ 120 Êáèò/ñ [1104].



Ðèñ. 13-5. Îáðàáîòêà êëþ÷à â FEAL.



$Y=S_0(X_1,X_2)=\text{Rot2}((X_1+X_2) \bmod 256)$
$Y=S_1(X_1,X_2)=\text{Rot2}((X_1+X_2+1) \bmod 256)$
Y: âûõîäíûå 8 áèòîâ, X_1,X_2 (8 áèòîâ): âõîäû
Rot2(Y): öèêëè÷åñêèé ñäâèã âëåâî íà 2 áèòà
8-áèòîâûõ äàííûõ Y

Ðèñ. 13-6. Ôóíêöèÿ f_K.

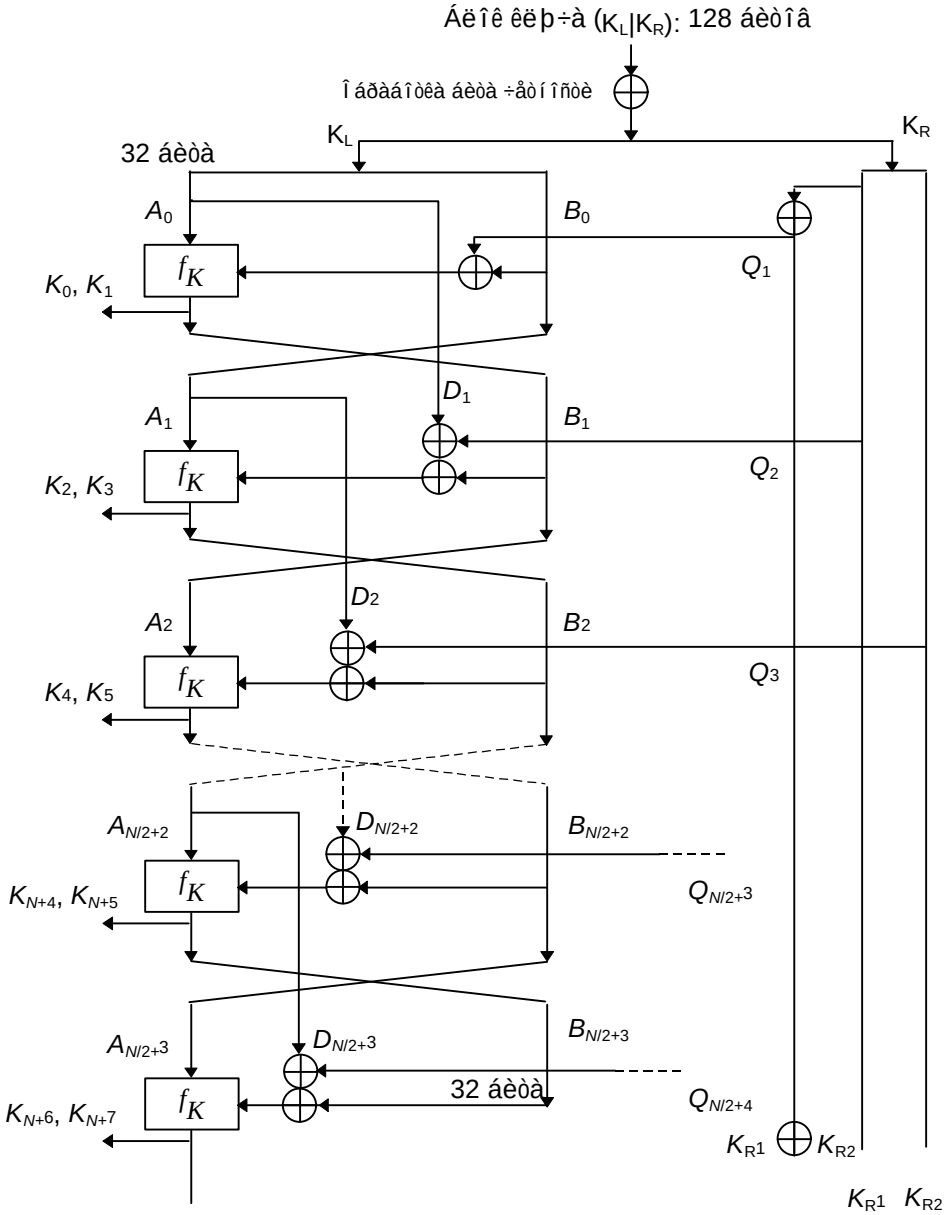
Êðèïòàíàëèç FEAL

Óñïåøíûé êðèïòàíàëèç FEAL-4, FEAL ñ ÷åòûðüìÿ ýòàïàìè, áûë âûïîëíåí ïîìîùüþ âñêðûòèÿ ñâÿçàííûìè îêðûòûìè òåêñòàìè [201], à ïîçæå ñëàáîñòü ýòîãî äëãîðèòìà áûëà ïîêàçàíà â [1132]. Ïîñëåäíåå âñêðûòèå, âûïîëíåííîå Ñèíè Ìðôè (Sean Murphy), áûëî ïðåäñòàâëåíî âñêðûòèåì, èñïîëüçîâàâøèì äèôôåðåíöèàëüíûé êðèïòàíàëèç, è äëÿ íåãî ïîòðåáîâàëîñü òîëüêî 20 âûáðàííûõ îêðûòûõ òåêñòîâ. Îòâåòíàÿ ðàçðàáîò÷èêîâ ñòàë 8-ýòàïíûé FEAL [1436, 1437, 1108], êðèïòàíàëèç êîòîðîãî áûë ïðåäñòàâëåí Áèãàìè è

Ñàìèðîì íà êîíôåðåíöèè SECURICOM '89 [1424]. Äëÿ âñêðûòèÿ FEAL-8 ñ âû áðàííûì îòêðûòûì òåêñòàì è ïîðÿäêà ïîëüçîâàòåëåì òîëüêî 10000 áëîêîâ [610], ÷òî çàñòàâëÿ ðàçðàáîò÷èêîâ äëãîðåçíà çàñó÷èòü ðóêàâà è îïðåäåëèòü FEAL-N [1102, 1104], äëãîðåçíì ñ ïåðåìåííûì ÷èñëîì ýòàïîâ (êîíå÷íî æå, áîëüøèì 8).

Áèõàì è Øàìèð ïðèìåíèëè ïðîòâ FEAL-N äèôôåðåíöèàëüíûé êðèïòàíàëèç, õîòÿ îíè ìîãëè áû åùå áûñòðåå âñêðûòü ðàçîâûé ñëîí (ñ ïîìîùüþ ìåíåå, ÷åì 2^{64} øèôðîâàíèé âûáðàííîãî îðèãèíàëà) äëÿ N , ìåíüøåãî 32. [169]. Äëÿ âñêðûòèÿ FEAL-16 íóæíî 2^{28} âûáðàííûõ èëè $2^{46.5}$ èçâåñòíûõ îòêðûòûõ òåêñòîâ. Äëÿ âñêðûòèÿ FEAL-8 òðåáóåòñÿ 2000 âûáðàííûõ èëè $2^{37.5}$ èçâåñòíûõ îòêðûòûõ òåêñòîâ. FEAL-4 ìîæåò áûòü âñêðûò ñ ïîìîùüþ âñåãî 8 ïðàâèëüíî âûáðàííûõ îòêðûòûõ òåêñòîâ.

Ðàçðàáîò÷èêè FEAL îïðåäåëèëè òàêæå ìîäèôèêàöèþ FEAL - FEAL-NX, â êîòîðîé èñïîëüçóåòñÿ 128-áèòîâûé êëþ÷ (ñì. 6-é) [1103, 1104]. Áèõàì è Øàìèð ïîêàçàëè, ÷òî äëÿ ëþáîãî çíà÷åíèÿ N FEAL-NX ñî 128-áèòîâûì êëþ÷îì âçëàìûâàòü íå ñëîæíåå, ÷åì FEAL-N ñ 64-áèòîâûì êëþ÷îì [169]. Íåäàâíî áûë ïðåäëîæåí FEAL-N(X)S, óñèëèâàþùèé FEAL çà ñ÷åò äëíàì÷åñêîé ôóíêöèè îáìåíà ìåñòàìè [1525].



$K_{2(r-1)}$: ëåâàÿ ïîëîâèíà B_r (16 áèòîâ)
$K_{2(r-1)+1}$: ïðàâàÿ ïîëîâèíà B_r (16 áèòîâ)
×èñëî èòåðàöèé: $N/2+4$

$Q_r=K_{R1} \oplus K_{R2}$, r=1, 4, 7, ...
$Q_r=K_{R1}$, r=2, 5, 8, ...
$Q_r=K_{R2}$, r=3, 6, 9, ...

Ðèñ. 13-7. Îáðàáîòêà êëþ÷à â FEAL-NX.

Áîëåå òîãî. Â [1520] áûëî ïðåäñòàâëåíî äðóãîå âñêðûòèå FEAL-4, òðåáóþùåå òîëüêî 1000 èçâåñòíûõ îòêðûòûõ òåêñòîâ, è FEAL-8, äëÿ êîòîðîãî íóæíî òîëüêî 20000 èçâåñòíûõ îòêðûòûõ òåêñòîâ. Äðóãàÿ âñêðûòèÿ ïðèâåäåíû â [1549, 1550]. Íàèëó÷øèì ÿâëÿåòñÿ âûïîëíåííàÿ Ìèöóðó Ìàöóè (Mitsuru Matsui) è Àòñóêîñ ßìàãèøè

(Atshuiro Yamagishi) [1020]. Ýòî áûëî ïåðâîå ïðèìåíåíèå ëèíåéíîãî êðèïòîàíàëèçà, è îíî ïîçâîëèëî âñêðûòü FEAL-4 ñ ïîìîùüþ 5 èçâåñòíûõ îòêðûòûõ òåêñòîâ, FEAL-6 - ñ ïîìîùüþ 100 èçâåñòíûõ îòêðûòûõ òåêñòîâ, à FEAL-8 - ñ ïîìîùüþ 2^{15} èçâåñòíûõ îòêðûòûõ òåêñòîâ. Äàëüíåéøèå óòî÷íåíèÿ ìîæíî íàéòè â [64]. Äèôôåðåíöèàëüíûé êðèïòàíàëèç ïîçâîëÿåò âñêðûâàòü FEAL-8, èñïîëüçóÿ òîëüêî 12 âûáðàííûõ îòêðûòûõ òåêñòîâ [62]. Êòî áû íå èçîáðåë íîâûé ìåòîä êðèïòàíàëèòè÷åñêîãî âñêðûòèÿ, êàæäîñÿ, ÷òî îí âñåãäà ñíà÷àëà ïðîáóåò åãî íà FEAL.

Ïàòåíòû

FEAL çàïàòåíòîâàí â Ñîåäèíåííûõ Øòàòàõ [1438], ñîîòâåòñòâóþùèå ïàòåíòû ïðèíÿòû ê ðàññìîòðåíèþ â Àíãëèè, Ôðàíöèè è Ãåðìàíèè. Æåëàþùèé ëèöåíçèðîâàòü èñïîëüçîâàíèå àëãîðèòìà äîëæåí ñâÿçàòüñÿ ñ Äåïàðòàìåíòîì èíòåëëåêòóàëüíîé ñîáñòâåííîñòè (Intellectual Property Department), NTT, 1-6 Uchisaiwai-cho, 1-chome, Chiyada-ku, 100 Japan.

13.5 REDOC

REDOC II ïðåäñòàâëÿåò ñîáîé äðóãîé áëî÷íûé àëãîðèòì, ðàçðàáîòàííûé Ìàéêëîì Âóäîì (Michael Wood) äëÿ Cryptech, Inc. [1613, 400]. Â íåì èñïîëüçóþòñÿ 20-áàéòîâûé (160-áèòîâûé) êëþ÷ è 80-áèòîâûé áëîê.

REDOC II âûïîëíÿåò âñå ìàíèïóëÿöèè - ïåðåñòàíîâêè, ïîäñòàíîâêè è XOR ñ êëþ÷îì - ñ áàéòàìè, ýòî àëãîðèòì ýôôåêòèâåí ïðè ïðîãðàììíîé ðåàëèçàöèè. REDOC II èñïîëüçóåò ìåíüøèå òàáëè÷íûå ôóíêöèè. Â îòëè÷èå îò DES, èìåþùåãî ôèêñèðîâàííûé (õîòÿ è îòòèìèçèðîâàííûõ äëÿ áåçîïàñíîñòè) íàáîð òàáëèö ïîäñòàíîâîê è ïåðåñòàíîâîê REDOC II èñïîëüçóåò çàâèñèìûå îò êëþ÷à è îòêðûòîãî òåêñòà íàáîðû òàáëèö (ïî ñóòè S-áëîêîâ). Ó REDOC II 10 ýòàïîâ, êàæäûé ýòàï ïðåäñòàâëÿåò ñîáîé ñëîæíóþ ïîñëåäîâàòåëüíîñòü ìàíèïóëÿöèé ñ áëîêîì.

Äðóãîé óíèêàëüíîé îñîáåííîñòüþ ÿâëÿåòñÿ èñïîëüçîâàíèå **ìàñîê**, êîòîðûå ÿâëÿþòñÿ ÷èñëàìè, ïîëó÷åííûìè èç òàáëèöû êëþ÷åé, è èñïîëüçóþòñÿ äëÿ âûáîðà òàáëèö äàííîé ôóíêöèè äëÿ äàííîãî ýòàïà. Äëÿ âûáîðà òàáëèö ôóíêöèè èñïîëüçóþòñÿ êàê çíà÷åíèå äàííûõ, òàê è ìàñêè.

Ïðè óñëîâèè, ÷òî ñàìû ýôôåêòèâíûì ñðåäíòâî âñêðûòèÿ ýòîãî àëãîðèòìà ÿâëÿåòñÿ ãðóáàÿ ñèëà, REDOC II î÷åíü íàäåæåí: äëÿ âñêðûòèÿ êëþ÷à òðåáóåòñÿ 2^{160} îïåðàöèé. Òîìàñ Êóçèê (Thomas Cusick) âûïîëíèë êðèïòîàíàëèç îäíîãî ýòàïà REDOC II, íî åìó íå óäàëîñü ðàñøèðèòü âñêðûòèå íà íåñêîëüêî ýòàïîâ [400]. Èñïîëüçóÿ äèôôåðåíöèàëüíûé êðèïòàíàëèç, Áèòàì è Øàìèð äîñòèãëè óñïåõà â êðèïòàíàëèçå îäíîãî ýòàïà REDOC II ñ ïîìîùüþ 2300 âûáðàííûõ îòêðûòûõ òåêñòîâ [170]. Îíè íå ñìîãëè ðàñøèðèòü ýòî âñêðûòèå íà íåñêîëüêî ýòàïîâ, íî èì óäàëîñü ïîëó÷èòü òðè çíà÷åíèÿ ìàñêè ïîñëå 4 ýòàïîâ. Î äðóãèõ ïîïûòêàõ êðèïòàíàëèçà ì íå íà èçâåñòíî.

REDOC III

REDOC ïðåäñòàâëÿåò ñîáîé óïðîùåííóþ âåðñèþ REDOC II, òàêæå ðàçðàáîòàííóþ Ìàéêëîì Âóäîì [1615]. Îí ðàáîòàåò ñ 80-áèòîâûì áëîêîì. Äëèíà êëþ÷à ìîæåò ìåíÿòüñÿ è äîñòèãàòü 2560 áàéòîâ (20480 áèòîâ). Àëãîðèòì ñîñòîèò òîëüêî èç îïåðàöèé XOR äëÿ áàéòîâ êëþ÷à è îòêðûòîãî òåêñòà, ïåðåñòàíîâêè èëè ïîäñòàíîâêè íå èñïîëüçóþòñÿ.

(1) Ñîçäàòü òàáëèöó êëþ÷åé èç 256 10-áàéòîâûõ êëþ÷åé, èñïîëüçóÿ ñåêðåòíûé êëþ÷.

(2) Ñîçäàòü 2 10-áàéòîâûõ áëîêà ìàñêè M_1 è M_2. M_1 ïðåäñòàâëÿåò ñîáîé XOR ïåðâûõ 128 10-áàéòîâûõ êëþ÷åé, à M_2 - XOR âòîðûõ 128 10-áàéòîâûõ êëþ÷åé.

(3) Äëÿ øèôðîâàíèÿ 10-áàéòîâîãî áëîêà:

   (a) Âûïîëíèòü XOR äëÿ ïåðâîãî áàéòà áëîêà äàííûõ è ïåðâîãî áàéòà M_1. Âûáðàòü êëþ÷ èç òàáëèöû êëþ÷åé, ðàññ÷èòàííîé íà ýòàïå (1). Èñïîëüçîâàòü âû÷èñëåííûé çíà÷åíèå XOR â êà÷åñòâå èíäåêñà òàáëèöû. Âûïîëíèòü XOR êàæäîãî, êðîìå ïåðâîãî, áàéòà áëîêà äàííûõ ñ ñîîòâåòñòâóþùèì áàéòîì âûáðàííîãî êëþ÷à.

   (b) Âûïîëíèòü XOR äëÿ âòîðîãî áàéòà áëîêà äàííûõ è âòîðîãî áàéòà M_1. Âûáðàòü êëþ÷ èç òàáëèöû êëþ÷åé, ðàññ÷èòàííîé íà ýòàïå (1). Èñïîëüçîâàòü âû÷èñëåííûé çíà÷åíèå XOR â êà÷åñòâå èíäåêñà òàáëèöû. Âûïîëíèòü XOR êàæäîãî, êðîìå âòîðîãî, áàéòà áëîêà äàííûõ ñ ñîîòâåòñòâóþùèì áàéòîì âûáðàííîãî êëþ÷à.

   (c) Ïðîâåðèòü äëÿ âñåõ áëîêà äàííûõ (äëÿ áàéòîâ ñ 3 ïî 10), ïîêà êàæäûé áàéò íå áóäåò èñïîëüçîâàí äëÿ âûáîðà êëþ÷à èç òàáëèöû ïîñëå âûïîëíåíèÿ äëÿ íåãî XOR ñ ñîîòâåòñòâóþùèì çíà÷åíèåì M_1. Çàòåì âûïîëíèòü XOR ñ êëþ÷îì äëÿ êàæäîãî, êðîìå èñïîëüçîâàííîãî äëÿ âûáîðà êëþ÷à, áàéòà.

   (d) Ïîâòîðèòü äëÿ M_2 ýòàïû (a)-(c).

Ýòîò àëãîðèòì íåñêîëüêî è áûñòð. Íà 33 ìåãàãåðöîâîì ïðîöåññîðå 80386 îí øèôðóåò äàííûå ñî ñêîðîñòüþ

2.75 Ìáèò/ñ. Âóä îöåíèë, ÷òî êîíâåéåðèçèðîâàííàÿ ðåàëèçàöèÿ íà ÑÁÈÑ ñ 64 áèòîâîé øèíîé äàííûõ ìîãëà áû øèôðîâàòü äàííûå ñî ñêîðîñòüþ ñâûøå 1.28 Ãáèò/ñ ïðè òàêòîâîé ÷àñòîòå 20 ÌÃö.

REDOC III íå áåçîïàñåí [1440]. Îí ÷óâñòâèòåëåí ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó. Äëÿ âîññòàíîâëåíèÿ îáåèõ ìàñîê íóæíî âñåãî ïðèìåðíî 223 âûáðàííûõ îòêðûòûõ òåêñòà.

Ïàòåíòû è ëèöåíçèè

Îáå âåðñèè REDOC çàïàòåíòîâàíû â Ñîåäèíåííûõ Øòàòàõ [1614]. Ðàññìàòðèâàþòñÿ è èíîñòðàííûå ïàòåíòû. Ïðè çàèíòåðåñîâàííîñòè â REDOC II èëè REDOC III îáðàùàéòåñü ê Ìàéêëó Âóäó (Michael C. Wood, Delta Computec, Inc., 6647 Old Thompson Rd., Syracuse, NY 13211).

13.6 LOKI

LOKI ðàçðàáîòàí â Àâñòðàëèè è âïåðâûå áûë ïðåäñòàâëåí â 1990 ãîäó â êà÷åñòâå âîçìîæíîé àëüòåðíàòèâû DES [273]. Â íåì èñïîëüçóþòñÿ 64-áèòîâûé áëîê è 64-áèòîâûé êëþ÷. Îáùàÿ ñòðóêòóðà àëãîðèòìà è èñïîëüçîâàíèÿ êëþ÷à îïèñàíà â [274, 275], à ñõåìà S-áëîêîâ - â [1247].

Èñïîëüçóÿ äèôôåðåíöèàëüíûé êðèïòîàíàëèç, Áèõàì è Øàìèð ñìîãëè âçëîìàòü LOKI ñ 11 è ìåíåå ýòàïàìè áûñòðåå, ÷åì ãðóáîé ñèëîé [170]. Áîëåå òîãî, àëãîðèòì îáëàäàåò 9-áèòîâîé êîìïëåìåíòàðíîñòüþ, ÷òî óìåíüøàåò ñëîæíîñòü âñêðûòèÿ ãðóáîé ñèëîé â 256 ðàç [170, 916, 917].

Ëàðñ Êíóäñåí (Lars Knudsen) ïîêàçàë, ÷òî LOKI ñ 14 è ìåíåå ýòàïàìè ÷óâñòâèòåëåí ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó [852, 853]. Êðîìå òîãî, åñëè â LOKI èñïîëüçóþòñÿ àëüòåðíàòèâíûå S-áëîêè, ïîëó÷àþùèéñÿ øèôð âåðîÿòíî òàêæå áóäåò ÷óâñòâèòåëåí ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó.

LOKI91

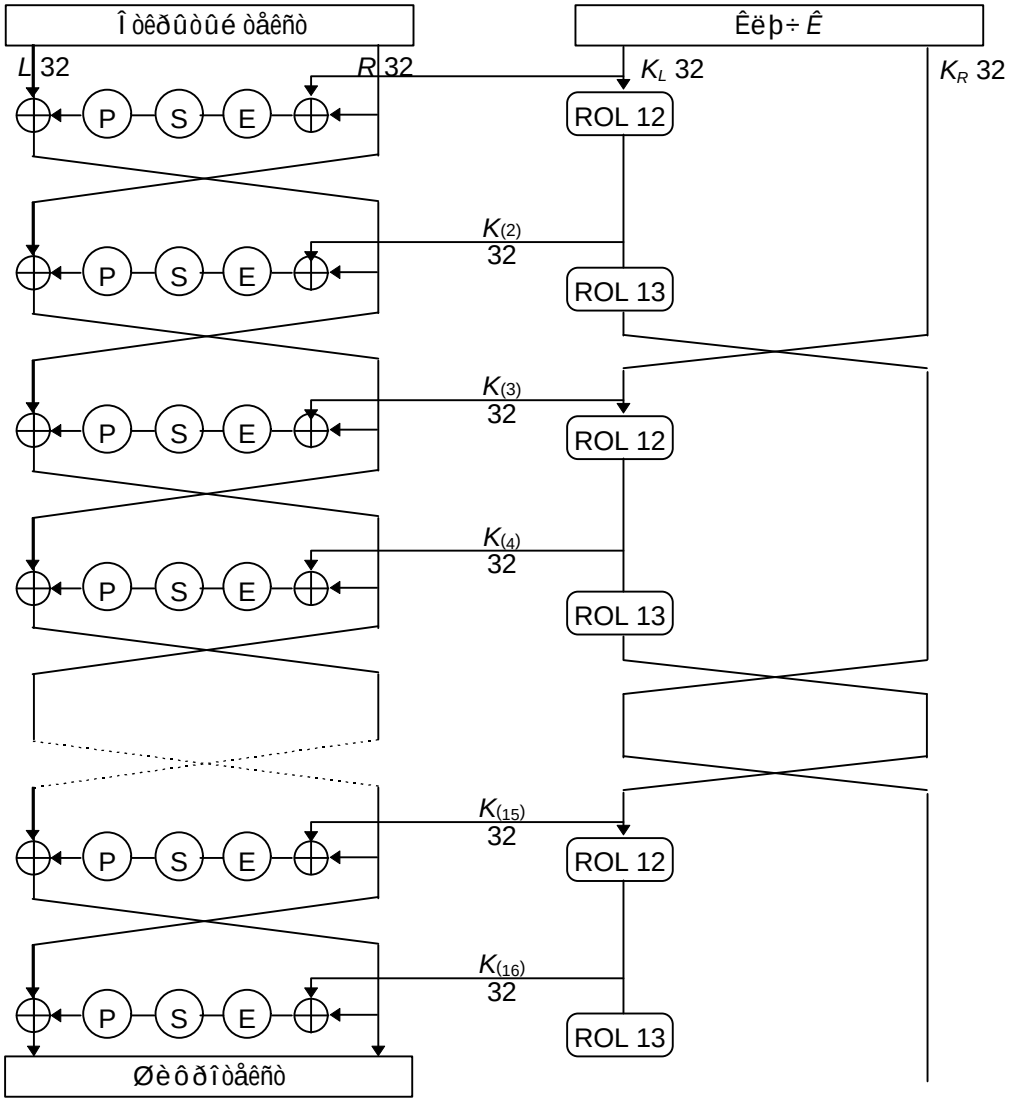
Â îòâåò íà ýòè âñêðûòèÿ ðàçðàáîò÷èêè LOKI âåðíóëèñü çà ÷åðòåæíóþ äîñêó è ïåðåñìîòðåëè ñâîé àëãîðèòì. Ðåçóëüòàòîì áûëî ïîÿâëåíèå LOKI91 [272]. (Ïðåäûäóùàÿ âåðñèÿ LOKI áûëà ïåðåèìåíîâàíà â LOKI89.)

×òîáû ïîâûñèòü óñòîé÷èâîñòü àëãîðèòìà ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó è èçáàâèòüñÿ îò êîìïëåìåíòàðíîñòè, â îðèãèíàëüíûé ïðîåêò áûëè âíåñåíû ñëåäóþùèå èçìåíåíèÿ:

1. Àëãîðèòì ãåíåðàöèè ïîäêëþ÷åé áûë èçìåíåí òàê, ÷òîáû ïîëîâèíû ïåðåñòàâëÿëèñü íå ïîñëå êàæäîãî, à ïîñëå êàæäîãî âòîðîãî ýòàïà.
2. Àëãîðèòì ãåíåðàöèè ïîäêëþ÷åé áûë èçìåíåí òàê, ÷òîáû êîëè÷åñòâî ïîçèöèé öèêëè÷åñêîãî ñäâèãà ëåâîãî ïîäêëþ÷à áûëî ðàâíî òî 12, òî 13 áèòàì.
3. Áûëè óñòðàíåíû íà÷àëüíàÿ è çàêëþ÷èòåëüíàÿ îïåðàöèè XOR áëîêà è êëþ÷à.
4. Áûëà èçìåíåíà ôóíêöèÿ S-áëîêà ñ öåëüþ ñãëàäèòü XOR ïðîôèëè S-áëîêîâ (÷òîáû ïîâûñèòü èõ óñòîé÷èâîñòü ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó), è íå äîïóñòèòü, ÷òîáû äëÿ êàêîãî-òî çíà÷åíèÿ âûïîëíÿëîñü f(x) = 0, ãäå f - ýòî êîìáèíàöèÿ E-, S- è P-áëîêîâ.

Îïèñàíèå LOKI91

Ìåõàíèçì LOKI91 ïîõîæ íà DES (ñì. Ðèñ. 13-8). Áëîê äàííûõ äåëèòñÿ íà ëåâóþ è ïðàâóþ ïîëîâèíû è ïðîõîäèò ÷åðåç 16 ýòàïîâ, ÷òî î÷åíü ïîõîæå íà DES. Íà êàæäîì ýòàïå ïðàâàÿ ïîëîâèíà ñíà÷àëà ïîäâåðãàåòñÿ îïåðàöèè XOR ñ ÷àñòüþ êëþ÷à, à çàòåì íàä íåé âûïîëíÿåòñÿ ïåðåñòàíîâêà ñ ðàñøèðåíèåì (ñì. Òàáë. 13-1).



Ðèñ. 13-8. LOKI91.

Òàáë. 13-1.
Ïåðåñòàíîâêà ñ ðàñøèðåíèåì

4,	3,	2,	1,	32,	31,	20,	29,	28,	27,	26,	25,
28,	27,	26,	25,	24,	23,	22,	21,	20,	19,	18,	17,
20,	19,	18,	17,	16,	15,	14,	13,	12,	11,	10,	9,
12,	11,	10,	9,	8,	7,	6,	5,	4,	3,	2,	1

48-áèòîâûé ðåçóëüòàò äåëèòñÿ íà ÷åòûðå 12-áèòîâûõ áëîêà, äëÿ êàæäîãî èç êîòîðûõ âû÷èñëÿåòñÿ ñëåäóþ ùàÿ ïîäñòàíîâêà ñ èñïîëüçîâàíèåì S-áëîêà: áåðåòñÿ êàæäûé 12-áèòîâûé âõîä, ïî 2 êðàéíèõ ëåâûõ è êðàéíèõ ïðàâûõ áèòà èñïîëüçóþòñÿ äëÿ ïîëó÷åíèÿ íîìåðà r, â 8 öåíòðàëüíûõ áèò îáðàçóþò íîìåð c. Ðåçóëüòàòîì S-áëîêà - *O* - ÿâëÿåòñÿ ñëåäóþ ùåå çíà÷åíèå:

$O(r,c) = (c + ((r* 17) \oplus 0xff)\ \&\ 0xff)^{31} \bmod P_r$

P_r ïðèâåäåíî â Òàáë. 13-2.

Òàáë. 13-2.
P_r

r:	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,	13,	14,	15,	16
P_r:	375,	279,	391,	395,	397,	415,	419,	425,	433,	445,	451,	463,	471,	477,	487,	488

Çàòåì ÷åòûðå 8-áèòîâûõ ðåçóëüòàòà ñîâà îáúåäèíÿþòñÿ, îáðàçóÿ 32-áèòîâîå ÷èñëî, êîòîðîå ïîäâåðãàþòñÿ îïåðàöèè ïåðåñòàíîâêè, îïèñàííîé â Òàáë. 13-3. Íàêîíåö äëÿ ïîëó÷åíèÿ íîâîé ëåâîé ïîëîâèíû âû÷èñëÿþòñÿ XOR ïðàâîé ïîëîâèíû ñ ïðåæíåé ëåâîé ïîëîâèíîé, à ëåâàÿ ïîëîâèíà ñòàíîâèòñÿ íîâîé ïðàâîé ïîëîâèíîé. Ïîñëå 16 ýòàïîâ äëÿ ïîëó÷åíèÿ îêîí÷àòåëüíîãî øèôðîâåñòà ñíîâà âû÷èñëÿþòñÿ XOR áëîêà è êëþ÷à.

Òàáë. 13-3.
Ïåðåñòàíîâêà ñ ïîìîùüþ P-áëîêà

32,	24,	16,	8,	31,	23,	15,	7,	30,	22,	14,	6,	29,	21,	13,	5,
28,	20,	12,	4,	27,	19,	11,	3,	26,	18,	10,	2,	25,	17,	9,	1

Ïîâêëþ÷è èç êëþ÷à âûäåëÿþòñÿ äîñòàòî÷íî ïðÿìîëèíåéíî. 64-áèòîâûé êëþ÷ ðàçáèâàåòñÿ íà ëåâóþ è ïðàâóþ ïîëîâèíû. Íà êàæäîì ýòàïå ïîâêëþ÷îì ÿâëÿþòñÿ ëåâàÿ ïîëîâèíà. Äàëåå îíà öèêëè÷åñêè ñäâèãàåòñÿ âëåâî íà 12 èëè 13 áèòîâ, çàòåì ïîñëå êàæäûõ ââóõ ýòàïîâ ëåâàÿ è ïðàâàÿ ïîëîâèíû ìåíÿþòñÿ ìåñòàìè. Êàê è â DES äëÿ øèôðîâàíèÿ è äåøèôðèðîâàíèÿ èñïîëüçóåòñÿ îäèí è òîò æå àëãîðèòì ñ íåêîòîðûìè èçìåíåíèÿìè â èñïîëüçîâàíèè ïîäêëþ÷åé.

Êðèïòîàíàëèç LOKI91

Êíóäñåí ïðåäïðèíÿë ïîïûòêó êðèïòîàíàëèçà LOKI91 [854, 858], íî íàøåë, ÷òî ýòîò àëãîðèòì óñòîé÷èâ ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó. Îäíàêî åìó óäàëîñü îáíàðóæèòü, ÷òî âñêðûòèå ñî ñâÿçàííûìè êëþ÷àìè äëÿ âû÷èñëèòåëüíî òðóäíîãî òåñòîâ óìåíüøàåò ñëîæíîñòü âñêðûòèÿ ãðóáîé ñèëîé ïî÷òè â÷åòâåðî. Ýòî âñêðûòèå èñïîëüçóåò ñëàáîñòü èñïîëüçîâàíèÿ êëþ÷à è ìîæåò áûòü òàêæå ïðèìåíåí, åñëè àëãîðèòì èñïîëüçóåòñÿ â êà÷åñòâå îäíîíàïðàâëåííîé õýø-ôóíêöèè (ñì. ðàçäåë 18.11).

Äðóãîå âñêðûòèå ñî ñâÿçàííûìè êëþ÷àìè ìîæåò âñêðûòü LOKI91 ñ ïîìîùüþ 2^{32} âû÷èñëåíèé îòêðûòîãî òåêñòà äëÿ âû÷èñëåíèÿ êëþ÷åé èëè ñ ïîìîùüþ 2^{48} èçâåñòíûõ îòêðûòûõ òåêñòîâ äëÿ âû÷èñëåíèÿ êëþ÷åé [158]. Ýòî âñêðûòèå íå çàâèñèò îò ÷èñëà ýòàïîâ àëãîðèòìà. (Â òîé æå ðàáîòå Áèõàì âñêðûâàåò LOKI89, èñïîëüçóÿ êðèòîòàíàëèç ñî ñâÿçàííûìè êëþ÷àìè, ñ ïîìîùüþ 2^{17} âû÷èñëåíèé îòêðûòûõ òåêñòîâ äëÿ âû÷èñëåíèÿ êëþ÷åé èëè ñ ïîìîùüþ 2^{33} èçâåñòíûõ îòêðûòûõ òåêñòîâ äëÿ âû÷èñëåíèÿ êëþ÷åé.) Íåñìîòðÿ íà âûñîêóþ óñòîé÷èâîñòü LOKI91 ê âñêðûòèþ òàêîãî òèïà, óñëîæíèâ ñõåìó èñïîëüçîâàíèÿ êëþ÷à.

Ïàòåíòû è ëèöåíçèè

LOKI íå çàïàòåíòîâàí. Êòî óãîäíî ìîæåò ðåàëèçîâàòü àëãîðèòì è èñïîëüçîâàòü åãî. Èñõîäíûé êîä, ïðèâåäåííûé â ýòîé êíèãå, íàïèñàí â Óíèâåðñèòåòå Íîâîãî Þæíîãî Óýëüſà. Ïðè æåëàíèè èñïîëüçîâàòü ýòó ðåàëèçàöèþ (èëè äðóãèå ðåàëèçàöèè, êîòîðûå íà íåñêîëüêî îòëè÷àþòñÿ îò ïðèâåäåííîé çäåñü) â êîììåð÷åñêîì ïðîäóêòå íåîáõîäèìî ê Äèðåêòîðó CITRAD, Òàêóëüòåò êîìïüþòåðíûõ íàóê, Óíèâåðſèòåòñêèé êîëëåäæ, Óíèâåðſèòåò Íîâîãî Þæíîãî Óýëüſà, Àêàäåìèÿ àâſòðàëèéſêîõ âîîðóæåííûõ ſèë, Êàíáåððà, Àſſòðàëèÿ (Director CITRAD, Department of Computer Science, University College, UNSW, Australian Defense Force Academy, Canberra ACT 2600, Australia; FAX: +61 6 268 8581.

13.7 KHUFU è KHAFRE

Â 1990 ãîäó Ðàëüô Ìåðêë (Ralph Merkle) ïðåäëîæèë äâà àëãîðèòìà. Â îñíîâå èõ ïðîåêòèðîâàíèÿ ëåæàëè ñëåäóþùèå ïðèíöèïû [1071]:

1. 56-áèòîâûé ðàçìåð êëþ÷à DES ñëèøêîì ìàë. Òàê êàê ñòîèìîñòü óâåëè÷åíèÿ ðàçìåðà êëþ÷à ïðîïîðöèîíàëüíà ìàòåìàòè÷åſêîìó ðîſòó (êîìïüþòåðíàÿ ìàſſèâ íåäîſòàòî÷íà), îí äîëæåí áûſü óâåëè÷åí.
2. Èſïîëíèâſîå èſſîëüſîâàíèå ïåðſîíàſîâ â DES õîſÿ è óſíàſíî äëÿ àſſàðàòſíûſ ðåàëèçàöèé, ſðåçâû÷àéſî çàſðóſàÿſ ïðîãðàſſíûå ðåàëèçàöèè. Íàèáîëåå áûſðûå ðåàëèçàöèè DES âûſſéſÿþſ ïåðſîíàſîâè òàáëè÷íûſ íáðàçîſ. Ïðîſſîðſ òàáëèöû ſſæåſ îáåſſïå÷èſü òå æå ðàðàêòåðiſſèêè "ðàſſåÿſèÿ", ſòî è ſſîſſòåſſſſ ïåðſſîſíàſſâêè, è ſſæåſ ſſåëàſü ðåàëèçàöèþ íàſſſãſ áſëåå äèáêſé.
3. S-áëſêè DES, âſåſſ ſ 64 4-áèòſâûſſ ýëåſåſòàſè, ſëèøêſſ ſàëû. Òåïåðü ſ óâåëè÷åſèåſ ïàſÿòè äſëæſû óâåëè÷èòſſÿ è S-áëſêè. Áſëåå òſàſ, âſå âſſåſü S-áëſêſâ èſſſëüçóþòſÿ ſäſſâðåſåſſſ. Õſòÿ ýòſ è óäſáſſ äëÿ àſïàðàòóðû, äëÿ ſðſſãðàſſſſé ðåàëèçàöèè ýòſ êàæåòſÿ ſáſóæſûſ ſãðàſè÷åſèſ. Äſëæſû áûòü ðåàëèçſâàſû áſëüøèé ðàçſåð S-áëſêſâ è ſſſëåäſâàòåüſſå (à íå ſàðàëëåüſſå) èſ èſſſëüçſâàſèå.
4. Øèðſêſ ſðèçſàſſ, ÷òſ íà÷àëſſàÿ è çàêëþ÷èòåëſàÿ ſåðåſòàſſâêè êðſſſſàðàſè÷åſêè áåſſſſûſëſſſû, ſſýòſſſ îſé äſëæſû áûòü óſſòðàſåſû.

5. Âñå áûñòðûå ðåàëèçàöèè DES çàðàíåå ðàññ÷èòûâàþò êëþ÷è äëÿ êàæäîãî ýòàïà. Ïðè äàííîì óñëîâèè íåò ñìûñëà óñëîæíÿòü ýòè âû÷iñëåíèÿ.

6. Â îòëè÷èå îò DES êðèòåðèè ïðîâåòèðîâàíèÿ S-áëîêîâ äîëæíû áûòü îáùåäîñòóïíû.

Ê ýòîìó ïðåä÷íþ Ìåðêë, âîçìîæíî, òåïåðü äîáàâèë áû "óñòîé÷èâîñòü ê äèôôåðåíöèàëüíîìó è ëèíåéíîìó êðèïòîàíàëèçó", ââåäü â òî âðåìÿ ýòè ñïîñîáû âñêðûòèÿ íå áûëè èçâåñòíû.

Khufu

Khufu - ýòî 64-áèòîâûé áëî÷íûé øèôð. 64-áèòîâûé îòêðûòûé òåêñò ñíà÷àëà ðàçáèâàåòñÿ íà äâå 32-áèòîâûå ïîëîâèíû, *L* è *R*. Íàä îâåèì ïîëîâèíàìè è îïåðàöèè ÷àñòÿìè êëþ÷à âûïîëíÿþòñÿ îïåðàöèè XOR. Çàòåì, àíàëîãè÷íî DES, ðåçóëüòàò ïðîõîäèò ÷åðåç íåêîòîðóþ ïîñëåäîâàòåëüíîñòü ýòàïîâ. Íà êàæäîì ýòàïå ìëàøèé çíà÷àùèé áàéò *L* èñïîëüçóåòñÿ â êà÷åñòâå âõîäíûõ äàííûõ S-áëîêà. Ó êàæäîãî S-áëîêà 8 âõîäíûõ áèòîâ è 32 âûõîäíûõ áèòà. Äàëåå âûáðàííûé â S-áëîêå 32-áèòîâûé ýëåìåíò ïîäâåðãàåòñÿ îïåðàöèè XOR ñ *R*. Çàòåì *L* öèêëè÷åñêè ñäâèãàåòñÿ íà íåñêîëüêî èç âîñüìè áèòîâ, *L* è *R* ìåíÿþòñÿ ìåñòàìè, è ýòàï çàêàí÷èâàåòñÿ. Ñàì S-áëîê íå ÿâëÿåòñÿ ñòàòè÷åñêè, íî ìåíÿåòñÿ êàæäûå âîñåìü ýòàïîâ. Íàêîíåö ïîñëåäíåãî ýòàïà íàä *L* è *R* âûïîëíÿþòñÿ îïåðàöèè XOR ñ äðóãèìè ÷àñòÿìè êëþ÷à, è ïîëîâèíû îáúåäèíÿþòñÿ, îáðàçóÿ áëîê øèôðîâàííòà.

Õîòÿ ÷àñòè êëþ÷à èñïîëüçóþòñÿ äëÿ XOR ñ áëîêîì øèôðîâàíèÿ â íà÷àëå è â êîíöå äëãîðèòìà, ãëàâíàÿ öåëü êëþ÷à -ååíåðàöèÿ S-áëîêîâ. Ýòè S-áëîêè - ñåêðåòíû, ïî ñóòè ÿâëÿþòñÿ îíè ÿâëÿþòñÿ ÷àñòüþ êëþ÷à. Ïîëíûé ðàçìåð êëþ÷à Khufu ðàâåí 512 áèòàì (64 áàéòàì), äëãîðèòì ïðåäïîëàãàåò S-áëîêîâ ïî êëþ÷ó. Êîëè÷åñòâî ýòàïîâ àëãîðèòìà îñòàâøèõ îêðûòûì. Ìåðêë óïîìÿíóë, ÷òî 8-ýòàïíûé Khufu ÷óâñòâèòåëåí ê âñêðûòèþ ñ âûáðàííûì îêðûòûì òåêñòîì è ðåêîìåíäóåò 16, 24 èëè 32 ýòàïà [1071]. (Îí îãðàíè÷èâàåò âûáîð êîëè÷åñòâà ýòàïîâ ÷èñëàìè, êðàòíûìè âîñüìè.)

Òàê êàê â Khufu èñïîëüçóþòñÿ çàâèñèìûå îò êëþ÷à è ñåêðåòíûå S-áëîêè, îí óñòîé÷èâ ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó. Ñóùåñòâóþò äèôôåðåíöèàëüíûå âñêðûòèå 16-ýòàïíîãî Khufu, êîòîðûå ðàñêðûâàþò êëþ÷ ïîñëå 2^{31} âûáðàííûõ îêðûòûõ òåêñòîâ [611], íî åãî íå óäàëîñü ðàñøèðèòü íà áîëüøåå êîëè÷åñòâî ýòàïîâ. Åñëè ëó÷øèì ñïîñîáîì âñêðûòü Khufu ÿâëÿåòñÿ ãðóáîé ñèëîâîé àòàêîé íà áîëüøå 2^{512} - îãðîìíûé ÷èñëî ïðè ëþáûõ óñëîâèÿõ.

Khafre

Khafre - ýòî âòîðàÿ èç êðèòîñèñòåì, ïðåäëîæåííûõ Ìåðêëîì [1071]. (Khufu (Õóô) è Khafre (Õàôð) - ýòî èìåíà åãèïåòñêèõ ôàðàîíîâ.) Ïî êîíñòðóêöèè ýòîò àëãîðèòì ïîõîæ íà Khufu, íî îí ñïðîåêòèðîâàí äëÿ ïðèëîæåíèé, íå èñïîëüçóþùèõ ïðåäâàðèòåëüíûõ âû÷iñëåíèé. S-áëîêè íå çàâiñÿò îò êëþ÷à. Âìåñòî ýòîãî Khafre èñïîëüçóåò ôèêñèðîâàííûå S-áëîêè. Áëîê øèôðîâàíèÿ ïîäâåðãàåòñÿ îïåðàöèè XOR ñ êëþ÷îì íà òîëüêî ïåðâûì ýòàïîì è ïîñëå ïîñëåäíåãî, íî è ïîñëå êàæäûõ 8 ýòàïîâ øèôðîâàíèÿ.

Ìåðêë ïðåäïîëîæèë, ÷òî ñ Khafre äîëæíû èñïîëüçîâàòüñÿ 64- èëè 128-áèòîâûå êëþ÷è, è ÷òî äëÿ Khafre ïîòðåáóåòñÿ áîëüøå ýòàïîâ, ÷åì äëÿ Khufu. Ýòî íàðÿäó ñ òåì, ÷òî êàæäûé ýòàï Khafre ñëîæíåå ýòàïà Khufu, äåëàò Khafre áîëåå ìåäëåííûì. Çàòî äëÿ Khafre íå íóæíû íèêàêèå ïðåäâàðèòåëüíûå ðàñ÷åòû, ÷òî ïîçâîëÿåò áûñòðåå øèôðîâàòü íåáîëüøèå ïîðöèè äàííûõ.

Â 1990 ãîäó Áèõàì è Øàìèð ïðèìåíèëè ñâîé ìåòîä äèôôåðåíöèàëüíîãî àíàëèçà ïðîòèâ Khafre [170]. Èì óäàëîñü âçëîìàòü 16-ýòàïíûé Khafre ñ ïîìîùüþ âñêðûòèÿ ñ âûáðàííûì îòêðûòûì òåêñòîì 1500 ðàçëè÷íûõ øèôðîâàíèé. Íà èõ ïðåñíîâëüíîì êîìïüþòåðå ýòî çàíÿëî îêîëî ÷àñà. Ïðåíðàçîâàíèå ýòîãî âñêðûòèÿ âî âñêðûòèå ñ èçâåñòíûì îòêðûòûì òåêñòîì ïîòðåáóåò îêîëî 238 øèôðîâàíèé. Khafre ñ 24 ýòàïàìè ìîæåò áûòü âñêðûò ñ ïîìîùüþ âñêðûòèÿ ñ âûáðàííûì îòêðûòûì òåêñòîì çà 253 øèôðîâàíèÿ, à ñ ïîìîùüþ âñêðûòèÿ ñ èçâåñòíûì îòêðûòûì òåêñòîì - çà 259 øèôðîâàíèÿ.

Ïàòåíòû

È Khufu, è Khafre çàïàòåíòîâàíû [1072]. Èñõîäíûé êîä ýòèõ àëãîðèòìîâ ñîäåðæèòñÿ â ïàòåíòå. Ïðè æåëàíèè ïîëó÷èòü ëèöåíçèþ íà ëþáîé èëè îáà àëãîðèòìà ñëåäóåò îáðàòèòüñÿ ê äèðåêòîðó ïî ëèöåíçèðîâàíèþ êîðïîðàöèè Xerox (Director of Licensing, Xerox Corporation, P.0. Box 1600, Stamford, CT, 06904-1600).

13.8 RC2

RC2 ïðåäñòàâëÿåò ñîáîé àëãîðèòì ñ ïåðåìåííîé äëèíîé êëþ÷à, ñïðîåêòèðîâàííûé Ðîíîì Ðèâåñòîì (Ron Rivest) äëÿ RSA Data Security, Inc. (RSADSI). Î÷åâèäíî "RC" - ýòî ñîêðàùåííûå "Ron's Code" ("Êîä Ðîíà"), õîòÿ îôèöèàëüíî ýòî "Rivest Cipher" ("Øèôð Ðèâåñòà"). (RC3 áûë âçëîìàí â RSADSI â ïðîöåññå ðàçðàáîòêè, RC1 íå âûøåë çà ïðåäåëû çàïèñíîé êíèæêè Ðèâåñòà.) Î íî ïðåäñòàâëÿåò ñîáîé ÷àñòíóþ ñîáñòâåííîñòü, è åãî äåòàëè íå áûëè îïóáëèêîâàíû. Íå äóìàéòå íè ìèíóòû, ÷òî ýòî óâëèë÷èâàò åãî áåçîïàñíîñòü. RC2 óæå ïîÿâèëñÿ â êîììåð÷åñêèõ ïðîäóêòàõ. Íàñêîëüêî ìíå èçâåñòíî, RC2 íå áûë çàïàòåíòîâàí è çàùèùåí òîëüêî êàê òîðãîâûé ñåêðåò.

RC2 - ýòî øèôð ñ 64-áèòîâûì áëîêîì è ïåðåìåííîé äëèíîé êëþ÷à, ïðåäíàçíà÷åííûé çàìåíèòü DES. Â ñîîòâåòñòâèè ñ óòâåðæäåíèÿìè êîìïàíèè ïðîãðàììíûå ðåàëèçàöèè RC2 â òðè ðàçà áûñòðåå DES. Àëãîðèòì ìîæåò èñïîëüçîâàòü êëþ÷ ïåðåìåííîé äëèíû, îò 0 áàéòîâ äî ìàêñèìàëüíîé äëèíû ñòðîêè, ïîääåðæèâàåìîé êîìïüþòåðíîé ñèñòåìîé, ñêîðîñòü øèôðîâàíèÿ íå çàâèñèò îò ðàçìåðà êëþ÷à. Ýòîò êëþ÷ ïðåäâàðèòåëüíî èñïîëüçóåòñÿ äëÿ çàïîëíåíèÿ 128-áàéòîâîé òàáëèöû, çàâèñÿùåé îò êëþ÷à. Ïîýòîìó ìíîæåñòâî äåéñòâèòåëüíî ðàçëè÷íûõ êëþ÷åé ñîñòàâëÿåò 21024. RC2 íå èñïîëüçóåò S-áëîêîâ [805], èñïîëüçóþòñÿ äâå îïåðàöèè - "ñìåøèâàíèå" è "ïåðåìåøèâàíèå" ("mix" è "mash"), äëÿ êàæäîãî ýòàïà âûáèðàåòñÿ îäíà èç íèõ. Â ñîîòâåòñòâèè ñ ëèòåðàòóðîé [1334]:

> . . . RC2 íå ÿâëÿåòñÿ èòåðàòèâíûì áëî÷íûì øèôðîì. Ýòî ïðåäïîëàãàåò, ÷òî RC2 áîëåå óñòîé÷èâ ê äèôôåðåíöèàëüíîìó è ëèíåéíîìó êðèïòîàíàëèçó, ÷åì äðóãèå áëî÷íûå øèôðû, áåçîïàñíîñòü êîòîðûõ îïèðàåòñÿ íà êîïèðîâàíèå ñõåìû DES.

Îòêàç RSADSI îïóáëèêîâàòü RC2 çàñòàâëÿåò ñîìíåâàòüñÿ â íàìåðåíèÿõ ýòîé êîìïàíèè. Îíà îáåùàåò ïðåäîñòàâèòü äåòàëè àëãîðèòìà âñåì, êòî ïîäïèøåò ñîãëàøåíèå î íåðàñïðîñòðàíåíèè èíôîðìàöèè, è óòâåðæäàåò, ÷òî ïîçâîëèò êðèïòîàíàëèòèêàì îïóáëèêîâàòü ëþáûå îáíàðóæåííûå íåãàòèâíûå ðåçóëüòàòû. Ìíå íåèçâåñòíî íè îá îäíîì êðèïòîàíàëèòèêå, íå ðàáîòàþùåì â ýòîé êîìïàíèè, êòî áû èññëåäîâàë àëãîðèòì, òàê êàê ýòî ïî ñóòè îçíà÷àëî áû âûïîëíèòü ðàáîòó ïî àíàëèçó äëÿ êîìïàíèè.

Òåì íå ìåíåå, Ðîí Ðèâåñò - íå øàðëàòàí. Îí óâàæàåìûé è êîìïåòåíòíûé êðèïòîãðàô. ß ëè÷íî â çíà÷èòåëüíîé ñòåïåíè âåðþ â ýòîò àëãîðèòì, õîòÿ ÿ ëè÷íî è íå âèäåë êîäà. RC4, òàêæå ÿâëÿþùèéñÿ èíòåëëåêòóàëüíîé ñîáñòâåííîñòüþ RSADSI, áûë îïóáëèêîâàí â Internet (ñì. ðàçäåë 17.1), è, âåðîÿòíî, îïóáëèêîâàíèå RC2 ÿâëÿåòñÿ òîëüêî âîïðîñîì âðåìåíè.

Ïî ñîãëàøåíèþ ìåæäó Àññîöèàöèåé èçäàòåëåé ïðîãðàììíîãî îáåñïå÷åíèÿ (Software Publishers Association, SPA) è ïðàâèòåëüñòâîì ÑØÀ RC2 è RC4 (ñì. ðàçäåë 17.1) ïîëó÷èëè ñïåöèàëüíûé ýêñïîðòíûé ñòàòóñ (ñì. ðàçäåë 25.14). Ïðîöåññ ïîëó÷åíèÿ ðàçðåøåíèÿ íà ýêñïîðò ïðîäóêòà, ðåàëèçóþùåãî îäèí èç ýòèõ äâóõ àëãîðèòìîâ, çíà÷èòåëüíî óïðîùåí ïðè óñëîâèè, ÷òî äëèíà êëþ÷à íå ïðåâûøàåò 40 áèòîâ.

Äîñòàòî÷åí ëè 40-áèòîâûé êëþ÷? Ñóùåñòâóåò âñåãî îäèí òðèëëèîí âîçìîæíûõ êëþ÷åé. Ïðè óñëîâèè, ÷òî íàèáîëåå ýôôåêòèâíûì ìåòîäîì êðèïòîàíàëèçà ÿâëÿåòñÿ âñêðûòèå ãðóáîé ñèëîé (áîëüøîå äîïóùåíèå, âåäü àëãîðèòì íèêîãäà íå áûë îïóáëèêîâàí), è ÷òî ìèêðîñõåìà ãðóáîãî âñêðûòèÿ ìîæåò ïðîâåðèòü ìèëëèîí êëþ÷åé â ñåêóíäó, ïîèñê ïðàâèëüíîãî êëþ÷à çàéìåò 12.7 äíåé. Òûñÿ÷à ìàøèí, ðàáîòàþùèõ ïàðàëëåëüíî, ñìîãóò ðàñêðûòü êëþ÷ çà äâàäöàòü ìèíóò.

RSA Data Security, Inc., óòâåðæäàåò, ÷òî, õîòÿ øèôðîâàíèå è äåøèôðèðîâàíèÿ âûïîëíÿþòñÿ äëÿ áûñòðî, èñ÷åðïûâàþùåãî ïîèñêà ïîòðåáóåòñÿ íàìíîãî áîëüøå âðåìåíè. Çàìåòíîå êîëè÷åñòâî âðåìåíè òðàòèòñÿ íà ôîðìèðîâàíèå ïëàíà èñïîëüçîâàíèÿ êëþ÷à. Õîòÿ ýòî âðåìÿ ïðåíåáðåæèìî ìàëî ïðè øèôðîâàíèè è äåøèôðèðîâàíèè ñîîáùåíèé, ýòî íå òàê ïðè ïðîâåðêå êàæäîãî âîçìîæíîãî êëþ÷à.

Ïðàâèòåëüñòâî ÑØÀ íèêîãäà íå ïîçâîëèëî áû ýêñïîðòèðîâàòü ëþáîé àëãîðèòì, êîòîðûé îíî, ïî êðàéíåé ìåðå â òåîðèè, íå ñìîãëî áû âñêðûòü. Îíî ìîæåò ñîçäàòü ìàãíèòíóþ ëåíòó èëè CD ñ êîíêðåòíûì áëîêîì îòêðûòîãî òåêñòà, çàøèôðîâàííûì êàæäûì âîçìîæíûì êëþ÷îì. Äëÿ âñêðûòèÿ ñîîáùåíèÿ îñòàåòñÿ òîëüêî âñòàâèòü ëåíòó è ñðàâíèòü áëîêè øèôðîòåêñòà â ñîîáùåíèè ñ áëîêàìè øèôðîòåêñòà íà ëåíòå. Ïðè ñîâïàäåíèè ìîæíî ïðîâåðèòü âîçìîæíûé êëþ÷ è ïîñìîòðåòü, èìååò ëè ñîîáùåíèå êàêîé-íèáóäü ñìûñë. Åñëè îíè âûáåðóò ÷àñòî âñòðå÷àþùèéñÿ áëîê (âñå íóëè, ASCII-ñèìâîëû ïðîáåëà, è ò.ä.), ýòîò ìåòîä áóäåò ðàáîòàòü. Îáúåì äàííûõ, íóæíûé äëÿ õðàíåíèÿ ðåçóëüòàòîâ øèôðîâàíèÿ 64-áèòîâîãî áëîêà îòêðûòîãî òåêñòà âñåìè 10^{12} âîçìîæíûìè êëþ÷àìè, ñîñòàâëÿåò 8 òåðàáàéòîâ - âïîëíå ðåàëüíî. Ïî ïîâîäó ëèöåíçèðîâàíèÿ RC2 îáðàùàéòåñü â RSADSI (ñì. ðàçäåë 25.4).

13.9 IDEA

Ïåðâûé âàðèàíò øèôðà IDEA, ïðåäëîæåííûé Êñóåäæà Ëàé (Xuejia Lai) è Äæåéìñîì Ìàññè (James Massey), ïîÿâèëñÿ â 1990 ãîäó [929]. Îí íàçûâàëñÿ PES (Proposed Encryption Standard, ïðåäëîæåííûé ñòàíäàðò øèôðîâàíèÿ). Â ñëåäóþùåì ãîäó, ïîñëå äåìîíñòðàöèè Áèõàìîì è Øàìèðîì âîçìîæíîñòåé äèôôåðåíöèàëüíîãî êðèïòîàíàëèçà, àâòîðû óñèëèëè ñâîé øèôð ïðîòèâ òàêîãî âñêðûòèÿ è íàçâàëè íîâûé àëãîðèòì IPES (Improved Proposed Encryption Standard, óëó÷øåííûé ïðåäëîæåííûé ñòàíäàðò øèôðîâàíèÿ) [931, 924]. Â 1992 ãîäó íàçâàíèå IPES áûëî èçìåíåíî íà IDEA (International Data Encryption Algorithm, ìåæäóíàðîäíûé àëãîðèòì øèôðîâàíèÿ äàííûõ) [925].

IDEA îñíîâûâàåòñÿ íà íåêîòîðûõ âïå÷àòëÿþùèõ òåîðåòè÷åñêèõ ïîëîæåíèÿõ è, õîòÿ êðèïòîàíàëèç äîáèëñÿ íåêîòîðûõ óñïåõîâ â îòíîøåíèè âàðèàíòîâ ñ óìåíüøåííûì êîëè÷åñòâîì ýòàïîâ, àëãîðèòì âñå åùå êàæåòñÿ ñèëüíûì. Ïî ìîåìó ìíåíèþ ýòî ñàìûé ëó÷øèé è ñàìûé áåçîïàñíûé áëî÷íûé àëãîðèòì, îïóáëèêîâàííûé ñåãîäíÿ.

Áóäóùåå IDEA ïîêà íåÿñíî. Ïîïûòîê çàìåíèòü èì DES ïðåäïðèíÿòî íå áûëî, ÷àñòè÷íî ïîòîìó, ÷òî îí çàïàòåíòîâàí è äîëæåí áûòü ëèöåíçèðîâàí äëÿ êîììåð÷åñêèõ ïðèëîæåíèé, è ÷àñòè÷íî ïîòîìó, ÷òî ëþäè ïîêà âñå åùå æäóò, íàáëþäàÿ íàñêîëüêî õîðîøî ïîâåäåò ñåáÿ àëãîðèòì â ïðåäñòîÿùèå ãîäû êðèïòîàíàëèçà. Åãî ñåãî-

äíÿøíÿÿ èçâåñòíîñòü îáúÿñíÿåòñÿ òåì, ÷òî îí ÿâëÿåòñÿ ÷àñòüþ PGP (ñì. ðàçäåë 24.12).

Îáçîð IDEA

IDEA ÿâëÿåòñÿ áëî÷íûì øèôðîì, îí ðàáîòàåò ñ 64-áèòîâûìè áëîêàìè îòêðûòîãî òåêñòà. Äëèíà êëþ÷à - 128 áèòîâ. Äëÿ øèôðîâàíèÿ è äåøèôðèðîâàíèÿ èñïîëüçóåòñÿ îäèí è òîò æå àëãîðèòì.

Êàê è äóãèå, óæå ðàññìîòðåííûå áëî÷íûå øèôðû IDEA èñïîëüçóåò è çàìóòûâàíèå, è ðàññåÿíèå. Ôëîñîôèÿ, ëåæàùàÿ â îñíîâå ïðîåêòà, ïðåäñòàâëÿåò "îáúåäèíåíèå îïåðàöèé èç ðàçëè÷íûõ àëãåáðàè÷åñêèõ ãðóïï". Ñìåøèâàþòñÿ òðè àëãåáðàè÷åñêèå ãðóïïû, è âñå îíè ìîãóò áûòü ëåãêî ðåàëèçîâàíû êàê àïïàðàòíî, òàê è ïðîãðàììíî:

— XOR

— Ñëîæåíèå ïî ìîäóëþ 2^{16}

— Óìíîæåíèå ïî ìîäóëþ $2^{16} + 1$. (Ýòî îïåðàöèþ ìîæíî ðàññìàòðèâàòü êàê S-áëîê IDEA.)

Âñå ýòè îïåðàöèè (à â àëãîðèòìå èñïîëüçóþòñÿ òîëüêî îíè, ïåðåñòàíîâêè íà áèòîâîì óðîâíå íå ïðèíöèïèàëüíû) ðàáîòàþò ñ 16-áèòîâûìè ïîäáëîêàìè. Ýòîò àëãîðèòì äàæå ýôôåêòèâíåå íà 16-áèòîâûõ ïðîöåññîðàõ.

Îïèñàíèå IDEA

Ñõåìà IDEA ïðåäñòàâëåíà íà Ðèñ. 13-9. 64-áèòîâûé áëîê äàííûõ äåëèòñÿ íà ÷åòûðå 16-áèòîâûõ ïîäáëîêà: X_1, X_2, X_3 è X_4. Ýòè ÷åòûðå ïîäáëîêà ñòàíîâÿòñÿ âõîäíûìè äàííûìè äëÿ ïåðâîãî ýòàïà àëãîðèòìà. Âñåãî â àëãîðèòìå âîñåìü ýòàïîâ. Íà êàæäîì ýòàïå ÷åòûðå ïîäáëîêà ïîäâåðãàþòñÿ îïåðàöèÿì XOR, ñëîæåíèÿ è óìíîæåíèÿ äðóã ñ äðóãîì è ñ øåñòüþ 16-áèòîâûìè ïîäêëþ÷àìè. Ìæäó ýòàïàìè îáìåíèâàþòñÿ ìåñòàìè âòîðîé è òðåòèé ïîäáëîêè. Íàêîíåö ÷åòûðå ïîäáëîêà îáúåäèíÿþòñÿ ñ ÷åòûðüìÿ ïîäêëþ÷àìè â îêîí÷àòåëüíîì ïðåîáðàçîâàíèè. Íà êàæäîì ýòàïå ñîâûðàþòñÿ â ñëåäóþùåé ïîñëåäîâàòåëüíîñòè:

(1) Ïåðâûé ïîäáëîê X_1 è ïåðâûé ïîäêëþ÷.

(2) Ñêëàäûâàþòñÿ X_2 è âòîðîé ïîäêëþ÷.

(3) Ñêëàäûâàþòñÿ X_3 è òðåòèé ïîäêëþ÷.

(4) Ïåðâûé ïîäáëîê X_4 è ÷åòâåðòûé ïîäêëþ÷.

(5) Âû÷èñëÿåòñÿ XOR íàä ðåçóëüòàòàìè ýòàïîâ (1) è (3).

(6) Âû÷èñëÿåòñÿ XOR íàä ðåçóëüòàòàìè ýòàïîâ (2) è (4).

(7) Ïåðâûé ïîäáëîê ðåçóëüòàòû ýòàïà (5) è ïÿòûé ïîäêëþ÷.

(8) Ñêëàäûâàþòñÿ ðåçóëüòàòû ýòàïîâ (6) è (7).

(9) Ïåðâûé ïîäáëîê ðåçóëüòàòû ýòàïà (8) è øåñòîé ïîäêëþ÷.

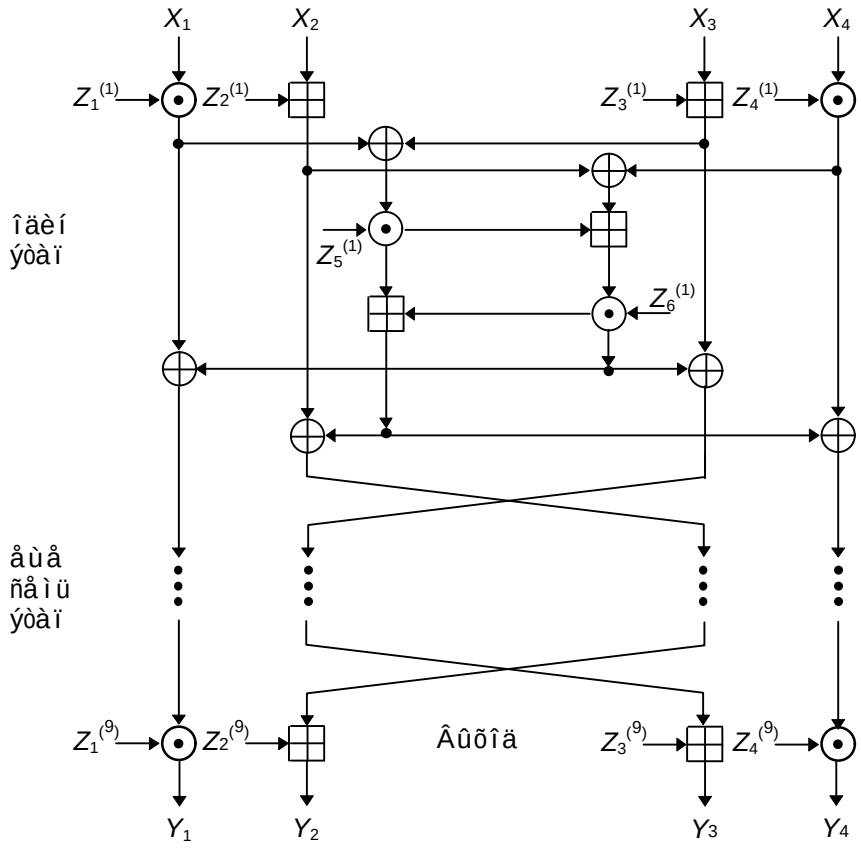
(10) Ñêëàäûâàþòñÿ ðåçóëüòàòû ýòàïîâ (7) è (9).

(11) Âû÷èñëÿåòñÿ XOR íàä ðåçóëüòàòàìè ýòàïîâ (1) è (9).

(12) Âû÷èñëÿåòñÿ XOR íàä ðåçóëüòàòàìè ýòàïîâ (3) è (9).

(13) Âû÷èñëÿåòñÿ XOR íàä ðåçóëüòàòàìè ýòàïîâ (1) è (10).

(14) Âû÷èñëÿåòñÿ XOR íàä ðåçóëüòàòàìè ýòàïîâ (4) è (10).



X_i : 16-áèòîâûé ïîäáëîê îòêðûòîãî òåêñòà
Y_i : 16-áèòîâûé ïîäáëîê øèôðîòåêñòà
$Z_i^{(r)}$: 16-áèòîâûé ïîäáëîê êëþ÷à
$\oplus$: ïîáèòîâîå "èñêëþ÷àþùåå èëè" (XOR) 16-áèòîâûõ ïîäáëîêîâ
$\boxplus$: ñëîæåíèå ïî ìîäóëþ 2^{16} 16-áèòîâûõ öåëûõ
$\odot$: óìíîæåíèå ïî ìîäóëþ $2^{16}+1$ 16-áèòîâûõ öåëûõ ïðè óñëîâèè, ÷òî íóëåâîé ïîäáëîê ñîîòâåòñòâóåò 2^{16}

Ðèñ. 13-9. IDEA.

Âûõîäíì ýòàïà ÿâëÿþòñÿ ÷åòûðå ïîäáëîêà - ðåçóëüòàòû äåéñòâèé (11), (12), (13) è (14). Ïîìåíÿéòå ìåñòàìè äâà âíóòðåííèõ ïîäáëîêà (íî íå â ïîñëåäíåì ýòàïå), è âû ïîëó÷èòå èñõîäíûå äàííûå äëÿ ñëåäóþùåãî ýòàïà.

Ïîñëå âñåõ ýòàïà âû ïîëíÿåòñÿ çàêëþ÷èòåëüíîå ïðåîáðàçîâàíèå:

(1) Ïåðåìíîæàþòñÿ X_1 è ïåðâûé ïîäêëþ÷.

(2) Ñëåäóþùàÿ X_2 è âòîðîé ïîäêëþ÷.

(3) Ñêëàäûâàþòñÿ X_3 è òðåòèé ïîäêëþ÷.

(4) Ïåðåìíîæàþòñÿ X_4 è ÷åòâåðòûé ïîäêëþ÷.

Íàêîíåö ÷åòûðå ïîäáëîêà ñíîâà ñîåäèíÿþòñÿ, îáðàçóÿ øèôðîòåêñò.

Òàêæå íåñëîæíî ñîçäàâàòü ïîäêëþ÷è. Àëãîðèòì èñïîëüçóåò 52 èç íèõ (øåñòü äëÿ êàæäîãî èç âîñüìè ýòàïîâ è åùå ÷åòûðå äëÿ çàêëþ÷èòåëüíîãî ïðåîáðàçîâàíèÿ). Ñíà÷àëà 128-áèòîâûé êëþ÷ äåëèòñÿ íà âîñåìü 16-áèòîâûõ ïîäêëþ÷åé. Ýòî ïåðâûå âîñåìü ïîäêëþ÷åé äëÿòñÿ íà ïåðâîãî ýòàïà è äâà - äëÿ âòîðîãî). Çàòåì êëþ÷ öèêëè÷åñêè ñäâèãàåòñÿ íàëåâî íà 25 áèòîâ è ñíîâà äåëèòñÿ íà âîñåìü ïîäêëþ÷åé. Ïðåâû÷åñòâèå íà 25 áèòîâ äëÿ ïîëó÷åíèÿ ñëåäóþùèõ âîñüìè ïîäêëþ÷åé, è òàê äî êîíöà äëîðèòìà.

Äåøèôðîâàíèå âûïîëíÿåòñÿ òî÷íî òàêæå çà èñêëþ÷åíèåì òîãî, ÷òî ïîäêëþ÷è èíâåðòèðóþòñÿ è ñëåãêà èçìåíÿþòñÿ. Ïîäêëþ÷è ïðè äåøèôðîâàíèè ïðåäñòàâëÿò ñîáîé îáðàòíûå çíà÷åíèÿ êëþ÷åé øèôðîâàíèÿ ïî îòíîøåíèþ ê îïåðàöèÿì ëèáî ñëîæåíèÿ, ëèáî óìíîæåíèÿ. (Äëÿ IDEA ïîäáëîêè, ñîñòîÿùèå èç îäíèõ íóëåé, ñ÷èòàþòñÿ ðàâíûìè 2^{16} = -1 äëÿ óìíîæåíèÿ ïî ìîäóëþ 2^{16} + 1, ñëåäîâàòåëüíî, îáðàòíûì çíà÷åíèåì 0 îòíîñèòåëüíî óìíîæåíèÿ ÿâëÿåòñÿ 0.) Ýòè âû÷èñëåíèÿ ìîãóò çàíÿòü íåêîòîðîå âðåìÿ, íî èõ íóæíî âûïîëíèòü îäèí ðàç äëÿ êàæäîãî êëþ÷à äåøèôðîâàíèÿ. Â Òàáë. 13-4 ïðåäñòàâëåíû ïîäêëþ÷è øèôðîâàíèÿ è ñîîòâåòñòâóþùèå

ïîäêëþ÷è äåøèôðèðîâàíèÿ.

Òàáë. 13-4.
Ïîäêëþ÷è øèôðîâàíèÿ è äåøèôðèðîâàíèÿ IDEA

Ýòàï	Ïîäêëþ÷è øèôðîâàíèÿ						Ïîäêëþ÷è äåøèôðèðîâàíèÿ					
1	$Z_1^{(1)}$	$Z_2^{(1)}$	$Z_3^{(1)}$	$Z_4^{(1)}$	$Z_5^{(1)}$	$Z_6^{(1)}$	$Z_1^{(9)-1}$	$-Z_2^{(9)}$	$-Z_3^{(9)}$	$Z_4^{(9)-1}$	$Z_5^{(8)}$	$Z_6^{(8)}$
2	$Z_1^{(2)}$	$Z_2^{(2)}$	$Z_3^{(2)}$	$Z_4^{(2)}$	$Z_5^{(2)}$	$Z_6^{(2)}$	$Z_1^{(8)-1}$	$-Z_2^{(8)}$	$-Z_3^{(8)}$	$Z_4^{(8)-1}$	$Z_5^{(7)}$	$Z_6^{(7)}$
3	$Z_1^{(3)}$	$Z_2^{(3)}$	$Z_3^{(3)}$	$Z_4^{(3)}$	$Z_5^{(3)}$	$Z_6^{(3)}$	$Z_1^{(7)-1}$	$-Z_2^{(7)}$	$-Z_3^{(7)}$	$Z_4^{(7)-1}$	$Z_5^{(6)}$	$Z_6^{(6)}$
4	$Z_1^{(4)}$	$Z_2^{(4)}$	$Z_3^{(4)}$	$Z_4^{(4)}$	$Z_5^{(4)}$	$Z_6^{(4)}$	$Z_1^{(6)-1}$	$-Z_2^{(6)}$	$-Z_3^{(6)}$	$Z_4^{(6)-1}$	$Z_5^{(5)}$	$Z_6^{(5)}$
5	$Z_1^{(5)}$	$Z_2^{(5)}$	$Z_3^{(5)}$	$Z_4^{(5)}$	$Z_5^{(5)}$	$Z_6^{(5)}$	$Z_1^{(5)-1}$	$-Z_2^{(5)}$	$-Z_3^{(5)}$	$Z_4^{(5)-1}$	$Z_5^{(4)}$	$Z_6^{(4)}$
6	$Z_1^{(6)}$	$Z_2^{(6)}$	$Z_3^{(6)}$	$Z_4^{(6)}$	$Z_5^{(6)}$	$Z_6^{(6)}$	$Z_1^{(4)-1}$	$-Z_2^{(4)}$	$-Z_3^{(4)}$	$Z_4^{(4)-1}$	$Z_5^{(3)}$	$Z_6^{(3)}$
7	$Z_1^{(7)}$	$Z_2^{(7)}$	$Z_3^{(7)}$	$Z_4^{(7)}$	$Z_5^{(7)}$	$Z_6^{(7)}$	$Z_1^{(3)-1}$	$-Z_2^{(3)}$	$-Z_3^{(3)}$	$Z_4^{(3)-1}$	$Z_5^{(2)}$	$Z_6^{(2)}$
8	$Z_1^{(8)}$	$Z_2^{(8)}$	$Z_3^{(8)}$	$Z_4^{(8)}$	$Z_5^{(8)}$	$Z_6^{(8)}$	$Z_1^{(2)-1}$	$-Z_2^{(2)}$	$-Z_3^{(2)}$	$Z_4^{(2)-1}$	$Z_5^{(1)}$	$Z_6^{(1)}$
çàêëþ÷èòåëüíîå ïðåîáðàçîâàíèå	$Z_1^{(9)}$	$Z_2^{(9)}$	$Z_3^{(9)}$	$Z_4^{(9)}$			$Z_1^{(1)-1}$	$-Z_2^{(1)}$	$-Z_3^{(1)}$	$Z_4^{(1)-1}$		

Ñêîðîñòü IDEA

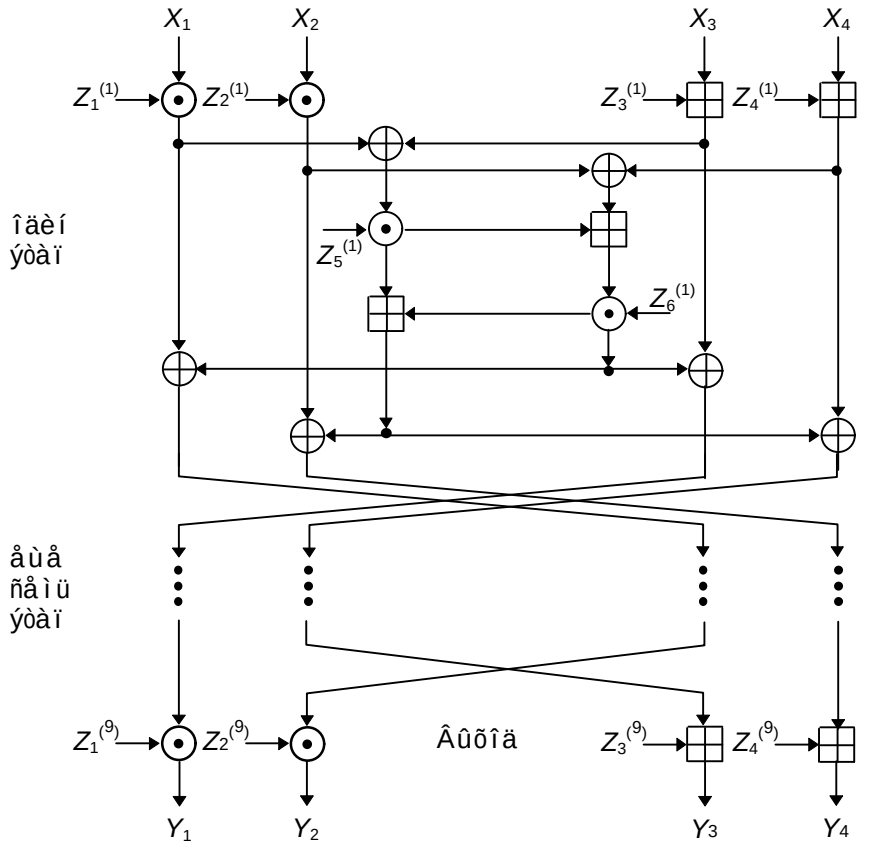
Ñîâðåìåííûå ïðîãðàììíûå ðåàëèçàöèè IDEA ïðèìåðíî â äâà ðàçà áûñòðåå, ÷åì DES. Íà êîìïüþòåðå ñ i386/33 ÌÃö IDEA øèôðóåò äàííûå ñî ñêîðîñòüþ 880 Êáèò/ñ, à íà êîìïüòåðå ñ i486/33 ÌÃö - ñî ñêîðîñòüþ 2400 Êáèò/ñ. Âû ìîãëè ïîäóìàòü, ÷òî IDEA äîëæåí áûë áûòü ïîáûñòðåå, íî óìíîæåíèÿ - íåäîñòàòîê óäîâëåòâîðåí. Óìíîæåíèå âáóõ 32-áèòîâûõ ÷èñåë íà ïðîöåññîðå i486 çàíèìàåò 40 òàêòîâ (10 íà ïðîöåññîðå Pentium).

Ðåàëèçàöèÿ PES íà áàçå ÑÁÈÑ øèôðóåò äàííûå ñî ñêîðîñòüþ 55 Ìáèò/ñ ïðè òàêòîâîé ÷àñòîòå 25 ÌÃö [208,398]. Äðóãàÿ ÑÁÈÑ, ðàçðàáîòàííàÿ ETH Zurich è ñîñòîÿùàÿ èç of 251000 òðàíçèñòîðîâ íà êðèñòàëëå ïëîùàäüþ 107.8 $мм^2$, øèôðóåò äàííûå ñ ïîìîùüþ àëãîðèòìà IDEA ñî ñêîðîñòüþ 177 Ìáèò/ñ ïðè òàêòîâîé ÷àñòîòå 25 ÌÃö [926, 207, 397].

Êðèïòîàíàëèç IDEA

Äëèíà êëþ÷à IDEA ðàâíà 128 áèòàì - áîëåå ÷åì â äâà ðàçà äëèííåå êëþ÷à DES. Ïðè óñëîâèè, ÷òî íàèáîëåå ýôôåêòèâíûì ÿâëÿåòñÿ âñêðûòèå ãðóïïû ñëîé, äëÿ âñêðûòèÿ êëþ÷à ïîòðåáóåòñÿ 2^{128} (10^{38}) øèôðîâàíèé. Ñîçäàéòå ìèêðîñõåìó, êîòîðàÿ ìîæåò ïðîâåðÿòü ìèëëèàðä êëþ÷åé â ñåêóíäó, îáúåäèíèòå ìèëëèàðä òàêèõ ìèêðîñõåì, è âàì ïîòðåáóåòñÿ 10^{13} ëåò äëÿ ðåøåíèÿ ïðîáëåìû - ýòî áîëüøå, ÷åì âîçðàñò âñåëåííîé. 10^{24} òàêèõ ìèêðîñõåì ìîãóò íàéòè êëþ÷ çà äåíü, íî âî âñåëåííîé íå íàéäåòñÿ ñòîëüêî àòîìîâ êðåìíèÿ, ÷òîáû ïîñòðîèòü òàêóþ ìàøèíó. Íàêîíåö ìû ÷åãî-òî äîñòèãëè, õîòÿ â íåêîòîðûõ òåìíûõ âîïðîñàõ ÿ ëó÷øå îñòàíóñü ñòîðîííèì íàáëþäàòåëåì.

Ìîæåò áûòü âñêðûòèå ãðóáîé ñèëîé - íå ëó÷øèé ñïîñîá âñêðûòèÿ IDEA. Àëãîðèòì âñå åùå ñëèøêîì íîâ, ÷òîáû ìîæíî áûëî âîâðåìÿ î êàêèõ-òî êíèãàõ êðèòèêàòü åãî. Ðàçðàáîò÷èêè ñäåëàëè âñå âîçìîæíîå, ÷òîáû ïäåëàòü àëãîðèòì óñòîé÷èâûì ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó. Îíè ïîñâÿòèëè ìàðêåòèíãîâûé øèôð è ïðîäàëè íîñòðèôèêàöèè, ÷òî óñòîé÷èâîñòü ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó ìîæåò áûòü ïðîäåìîíñòðèðîâàíà è îöåíåíà êîëè÷åñòâåííî [931, 925]. (Äëÿ ñðàâíåíèÿ ñ àëãîðèòìîì IDEA, óñòîé÷èâîñòü êîòîðîãî ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó áûëà óñèëåíà, è êîòîðûé ïîêàçàí íà Ðèñ. 13-9, íà Ðèñ. 13-10 ïðèâåäåí ïåðâîíà÷àëüíûé àëãîðèòì PES. Óäèâèòåëüíî, êàê òàêèå íåçíà÷èòåëüíûå èçìåíåíèÿ ìîãóò ïðèâåñòè ê ñòîëü áîëüøèì ðàçëè÷èÿì.) Â [925] Ëàé (Lai) óòâåðæäàë (îí ïðèâåë ïîäòâåðæäåíèå, íî íå äîêàçàòåëüñòâî), ÷òî IDEA óñòîé÷èâ ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó áæå ïîñëå 4 èç 8 ýòàïîâ. Ñîãëàñíî Áèõàì, âåñ ïîïûòêà âñêðûòü IDEA ñ ïîìîùüþ êðèïòîàíàëèçà ñî ñâÿçàííûì êëþ÷àì è òàêæå íà óðåí÷åíàñü óñïåõîì [160].



X_i : 16-áèòîâûé ïîäáëîê îòêðûòîãî òåêñòà
Y_i : 16-áèòîâûé ïîäáëîê øèôðîòåêñòà
$Z_i^{(r)}$: 16-áèòîâûé ïîäáëîê êëþ÷à
$\oplus$: ïîáèòîâîå "èñêëþ÷àþùåå èëè" (XOR) 16-áèòîâûõ ïîäáëîêîâ
$\boxplus$: ñëîæåíèå ïî ìîäóëþ 2^{16} 16-áèòîâûõ öåëûõ
$\odot$: óìíîæåíèå ïî ìîäóëþ $2^{16}+1$ 16-áèòîâûõ öåëûõ ïðè óñëîâèè, ÷òî íóëåâîé ïîäáëîê ñîîòâåòñòâóåò 2^{16}

Ðèñ. 13-10. PES.

Âèëëè Ìàéåð (Willi Meier) èñïëåäîâàë òðè àëãåáðàè÷åñêèõ îïåðàöèè IDEA è ïîêàçàë, ÷òî, õîòÿ îíè íåñîâìåñòèìû, åñòü ñëó÷àè, êîãäà ýòè îïåðàöèè ìîæíî óïðîñòèòü òàê, ÷òîáû â íåêîòîðîé ñòåïåíè îáëåã÷èòü [1050]. Åãî âñêðûòèå 2-ýòàïíîãî IDEA îêàçàëîñü ýôôåêòèâíåå âñêðûòèÿ ãðóáîé ñèëîé (2^{42} îïåðàöèé), íî äëÿ IDEA ñ 3 è áîëåå ýòàïàìè ýôôåêòèâíîñòü ýòîãî âñêðûòèÿ áûëà íèæå âñêðûòèÿ ãðóáîé ñèëîé. Áåçîïàñíîñòü ïîëíîãî 8-ýòàïíîãî IDEA îñòàëàñü íåïîêîëåáëåìîé.

Äæîàí Äýéìåí (Joan Daemen) îòêðûëà êëàññ ñëàáûõ êëþ÷åé IDEA [405, 409]. Ýòè êëþ÷è íå ÿâëÿþòñÿ ñëàáûìè â òîì ñìûñëå, â êîòîðîì ñëàáû íåîòúåìëåìû êëþ÷è DES, äëÿ êîòîðûõ ôóíêöèÿ øèôðîâàíèÿ îáðàòíà ñàìîé ñåáå. Ñëàáîñòü ýòèõ êëþ÷åé ñîñòîèò â òîì, ÷òî âçëîìùèê ìîæåò ëåãêî îïðåäåëèòü èõ ñ ïîìîùüþ âñêðûòèÿ ñ âûáðàííûì îòêðûòûì òåêñòîì. Íàïðèìåð, ñëàáûì ÿâëÿåòñÿ ñëåäóþùèé êëþ÷ (â øåñòíàäöàòèðè÷íîé çàïèñè):

0000,0000,0*x*00,0000,0000,000*x*,*xxxx*,*x*000

Â ïîçèöèè "*x*" ìîæåò ñòîÿòü ëþáàÿ öèôðà. Ïðè èñïîëüçîâàíèè òàêîãî êëþ÷à ïîáèòîâîå XOR îïðåäåëåííûõ ïàð îòêðûòûõ òåêñòîâ ðàâíî ïîáèòîâîìó XOR ïîëó÷åííûõ øèôðîòåêñòîâ.

Â ëþáîì ñëó÷àå âåðîÿòíîñòü ñëó÷àéíîé ãåíåðàöèè îäíîãî èç òàêèõ ñëàáûõ êëþ÷åé î÷åíü ìàëà: $1/2^{96}$. Î ïàñíîñòè ñëó÷àéíî âûáðàòü òàêîé êëþ÷ ïðàêòè÷åñêè íå ñóùåñòâóåò. Ê òîìó æå, íåñìîòðÿ ìîäèôèêàöèè IDEA òàê, ÷òîáû èñêëþ÷èòü íàëè÷èå ñëàáûõ êëþ÷åé - äîñòàòî÷íî âûïîëíèòü XOR êàæäîãî ïîâêëþ÷à ñ÷èñëî 0x0dae [409].

Õîòÿ ïîïûòêè âûïîëíèòü êðèïòîàíàëèç IDEA áûëî ìíîãî, ìíå íåèçâåñòíî íè îá îäíîé óñïåøíîé.

Ðåæèìû ðàáîòû è âàðèàíòû IDEA

IDEA ìîæåò ðàáîòàòü â ëþáîì èç ðåæèìîâ ðàáîòû áëî÷íîãî øèôðà, îïèñàííûõ â ãëàâå 9. Ïðîòèâ äâóõ ðåàëèçàöèé IDEA ìîæåò áûòü ïðåäïðèíÿò òî æå âñêðûòèå "âñòðå÷à ïîñåðäèíå", ÷òî è ïðîòèâ DES (ñì. ðàçäåë

15.1). Îäíàêî, òàê êàê êëþ÷ IDEA áîëåå ÷åì â äâà ðàçà äëèííåå êëþ÷à DES, ýòî âñêðûòèå íåïðàêòè÷íî. Îáúåì íóæíîé äëÿ òàêîãî âñêðûòèÿ ïàìÿòè ñîñòàâèò $64*2^{128}$ áèòîâ, èëè 10^{39} áàéòîâ. Ìîæåò áûòü âî âñåëåííîé è äîñòàòî÷íî ìàòåðèè, ÷òîáû ïîñòðîèòü òàêîå õðàíèëèùå, íî ÿ â ýòîì ñîìíåâàþñü.

Åñëè âû ó÷èòûâàåòå âîçìîæíîñòü èñïîëüçîâàíèÿ ïàðàëëåëüíîé âñåëåííîé, èñïîëüçóéòå óòðîåííóþ ðåàëèçàöèþ IDEA (ñì. ðàçäåë 15.2):

$$C = E_{K_3}(D_{K_2}(E_{K_1}(P)))$$

Òàêàÿ ðåàëèçàöèÿ óñòîé÷èâà ïðîòèâ âñêðûòèÿ "âñòðå÷à ïîñåðåäèíå".

Êðîìå òîãî, ïî÷åìó áû âàì íå ðåàëèçîâàòü IDEA íåçàâèñèìûìè ïîäêëþ÷àìè, îñîáåííî åñëè âàøè ñðåäñòâà ðàñïðåäåëåíèÿ êëþ÷åé ïîçâîëÿþò ðàáîòàòü ñ äëèííûìè êëþ÷àìè. Äëÿ IDEA íóæíî âñåãî 52 16-áèòîâûõ êëþ÷à, îáùåé äëèíîé 832 áèòîâ. Ýòîò âàðèàíò îïðåäåëåííî áåçîïàñíåé, íî íèêòî íå ñìîæåò ñêàçàòü íàñêîëüêî.

Â íàèâíîé ìîäèôèêàöèè ìîæåò áûòü óâåëè÷åí âäâîå ðàçìåð áëîêà. Àëãîðèòì òàêæå ïðåêðàñíî ðàáîòàë áû ñ 32-áèòîâûìè ïîäáëîêàìè âìåñòî 16-áèòîâûõ è ñ 256-áèòîâûì êëþ÷îì. Øèôðîâàíèå âûïîëíÿëîñü áû áûñòðåå, è áåçîïàñíîñòü âîçðîñëà áû â 2^{32} ðàçà. Èëè íåò? Òåîðèÿ, íà êîòîðîé îñíîâàí àëãîðèòì, îïèðàåòñÿ íà òî, ÷òî $2^{16}+1$ ÿâëÿåòñÿ ïðîñòûì ÷èñëîì. À $2^{32} + 1$ ïðîñòûì ÷èñëîì íå ÿâëÿåòñÿ. Ìîæåò áûòü àëãîðèòì è ìîæíî èçìåíèòü òàê, ÷òîáû îí ðàáîòàë, íî åãî áåçîïàñíîñòü áóäåò ñîâñåì èíîé. Ëàé ãîâîðèò, ÷òî çàñòàâèòü ðàáîòàòü òàêîé àëãîðèòì áóäåò íåëåãêî [926].

Õîòÿ IDEA êàæåòñÿ íàìíîãî áåçîïàñíåå DES, íå âñåãäà ìîæíî ëåãêî çàìåíèòü îäèí àëãîðèòì äðóãèì â ñóùåñòâóþùåì ïðèëîæåíèè. Åñëè âàøà áàçà äàííûõ è øàáëîíû ñîîáùåíèé ìîãóò ðàáîòàòü ñ 64-áèòîâûì êëþ÷îì, ðåàëèçàöèÿ 128-áèòîâîãî êëþ÷à IDEA ìîæåò áûòü íåâîçìîæíîé.

Äëÿ òàêèõ ïðèëîæåíèé ñîçäàéòå 128-áèòîâûé êëþ÷, îáúåäèíèâ 64-áèòîâûé êëþ÷ ñàì ñ ñîáîé. Íå çàáûâàéòå, ÷òî ýòà ìîäèôèêàöèÿ çàìåòíî îñëàáëÿåò IDEA.

Åñëè âàñ áîëüøå âîëíóåò ñêîðîñòü ðàáîòû, à íå áåçîïàñíîñòü, ïîïðîáóéòå âàðèàíò IDEA ñ ìåíüøèì ÷èñëîì ýòàïîâ. Ñåãîäíÿ ëó÷øåå âñêðûòèå IDEA áûñòðåå âñêðûòèÿ ãðóáîé ñèëîé òîëüêî äëÿ 2.5 è ìåíåå ýòàïîâ [1050], 4-ýòàïíûé IDEA áóäåò â äâà ðàçà áûñòðåå è, íàñêîëüêî ìíå èçâåñòíî, åãî áåçîïàñíîñòü íå óìåíüøèòñÿ.

Caveat Emptor[1]

IDEA - ýòî îòíîñèòåëüíî íîâûé àëãîðèòì, ìíîãèå âîïðîñû ïîêà îñòàþòñÿ îòêðûòûìè. Îáðàçóåò ëè IDEA ãðóïïó? (Ëàé äóìàåò, ÷òî íåò [926].) Íå ñóùåñòâóåò ëè ïîêà íå îòêðûòûõ ñïîñîáîâ âñêðûòèÿ ýòîãî øèôðà? Ó IDEA òâåðäàÿ òåîðåòè÷åñêàÿ îñíîâà, íî ñíîâà è ñíîâà êàçàâøèåñÿ áåçîïàñíûìè àëãîðèòìû êàïèòóëèðóþò ïåðåä íîâûìè ôîðìàìè êðèïòîàíàëèçà. Ðÿä ãðóïï àêàäåìè÷åñêèõ è âîåííûõ èññëåäîâàòåëåé íå îïóáëèêîâàëè ñâîè ðåçóëüòàòû êðèïòîàíàëèçà IDEA. Âîçìîæíî, êòî-íèáóäü óæå äîáèëñÿ èëè êîãäà-íèáóäü äîáüåòñÿ óñïåõà.

Ïàòåíòû è ëèöåíçèè

IDEA çàïàòåíòîâàí â Åâðîïå è Ñîåäèíåííûõ Øòàòàõ [1012, 1013]. Ïàòåíò ïðèíàäëåæèò Ascom-Tech AG. Äëÿ íåêîììåð÷åñêîãî èñïîëüçîâàíèÿ ëèöåíçèðîâàíèå íå íóæíî. Ïðè çàèíòåðåñîâàííîñòè â ëèöåíçèè äëÿ êîììåð÷åñêîãî ïðèìåíåíèÿ àëãîðèòìà ñëåäóåò îáðàòèòüñÿ ïî àäðåñó Ascom Systec AG, Dept CMVV, Cewerbepark, CH-5506, Mgenwil, Switzerland; +41 64 56 59 83; Fax: +41 64 56 59 90; idea@ascom.ch.

13.10 MMB

Íåäîâîëüñòâî èñïîëüçîâàíèåì â IDEA 64-áèòîâîãî áëîêà øèôðîâàíèÿ ïðèâåëî ê ñîçäàíèþ Äæîíîì Äýéìîíîì àëãîðèòìà ïîä íàçâàíèåì MMB (Modular Multiplication-based Block cipher, ìîäóëüíûé áëî÷íûé øèôð, èñïîëüçóþùèé óìíîæåíèÿ) [385, 405, 406]. Â îñíîâå MMB ëåæèò òåîðèÿ, èñïîëüçóåìàÿ è â IDEA: ïåðåìåøèâàþùèå îïåðàöèè èç ðàçëè÷íûõ ãðóïï. MMB - ýòî èòåðàòèâíûé àëãîðèòì, ãëàâíûì îáðàçîì ñîñòîÿùèé èç ëèíåéíûõ äåéñòâèé (XOR è èñïîëüçîâàíèå êëþ÷à) è ïàðàëëåëüíîå èñïîëüçîâàíèå ÷åòûðåõ áîëüøèõ íåëèíåéíûõ èçìåíÿþùèõ îáû÷íûé ïîðÿäîê ïîäñòàíîâîê. Ýòè ïîäñòàíîâêè îïðåäåëÿþòñÿ ñ ïîìîùüþ óìíîæåíèÿ ïî ìîäóëþ $2^{32}-1$ ñ ïîñòîÿííûìè ìíîæèòåëÿìè. Ðåçóëüòàòîì ïðèìåíåíèÿ ýòèõ äåéñòâèé ÿâëÿåòñÿ àëãîðèòì, èñïîëüçóþùèé è 128-áèòîâûé êëþ÷ è 128-áèòîâûé áëîê.

MMB îïåðèðóåò 32-áèòîâûìè ïîäáëîêàìè òåêñòà (x_0, x_1, x_2, x_3) è 32-áèòîâûìè ïîäáëîêàìè êëþ÷à (k_0, k_1, k_2, k_3). Ýòî äåëàåò óäîáíûì ðåàëèçàöèþ àëãîðèòìà íà ñîâðåìåííûõ 32-áèòîâûõ ïðîöåññîðàõ. ×åðåäóÿñü ñ XOR, øåñòü ðàç èñïîëüçóåòñÿ íåëèíåéíàÿ ôóíêöèÿ f. Âîò ýòîò àëãîðèòì (âñå îïåðàöèè ñ èíäåêñàìè âûïîëíÿþòñÿ ïî ìîäóëþ 3):

$x_i = x_i \oplus k_i$, äëÿ $i = 0$ äî 3

[1] Ïðåäóïðåæäåíèå ïîêóïàòåëþ

f(x_0, x_1, x_2, x_3)

$x_i = x_i \oplus k_{i+1}$, äëÿ i = 0 äî 3

f(x_0, x_1, x_2, x_3)

$x_i = x_i \oplus k_{i+2}$, äëÿ i = 0 äî 3

f(x_0, x_1, x_2, x_3)

$x_i = x_i \oplus k_i$, äëÿ i = 0 äî 3

f(x_0, x_1, x_2, x_3)

$x_i = x_i \oplus k_{i+1}$, äëÿ i = 0 äî 3

f(x_0, x_1, x_2, x_3)

$x_i = x_i \oplus k_{i+2}$, äëÿ i = 0 äî 3

f(x_0, x_1, x_2, x_3)

Ó ôóíêöèè f òðè ýòàïà:

(1) $x_1 = c_i * x_i$, äëÿ i = 0 äî 3 (Åñëè íà âõîäå óì íîæåíèÿ îäíè åäèíèöû, òî íà âûõîäå - òîæå îäíè åäèíèöû.)

(2) Åñëè ìëäøèé çíà÷àùèé áèò x_0 = 1, òî $x_0 = x_0 \oplus$ C. Åñëè ìëäøèé çíà÷àùèé áèò x_3 = 0, òî $x_3 = x_3 \oplus$ C.

(3) $x_i = x_{i-1} \oplus x_i \oplus x_{i+1}$, äëÿ i = 0 äî 3

Âñå îïåðàöèè ñ èíäåêñàìè âûïîëíÿþòñÿ ïî ìîäóëþ 3. Îïåðàöèÿ óìíîæåíèÿ íà ýòàïå (1) âûïîëíÿåòñÿ ïî ìîäóëþ 2^{32}-1. Â äâîè÷íîì àëãîðèòìå åñëè âòîðîé îïåðàíä - ýòî 2^{32}-1, òî ðåçóëüòàò òàêæå ðàâåí 2^{32}-1. Â àëãîðèòìå èñïîëüçóþòñÿ ñëåäóþùèå êîíñòàíòû:

C = 2aaaaaaa

c_0 = 025f1cdb

c_1 = 2 * c_0

c_2= 2^3 * c_0

c_3 = 2^7 * c_0

Êîíñòàíòà C - ýòî "ïðîñòåéøàÿ" êîíñòàíòà ñ âûñîêèì òðîè÷íûì âåñîì, íóëåâûì ìëäøèì çíà÷àùèì áèòîì è áåç êðóãîâîé ñèììåòðèè. Ó êîíñòàíòû c0 íåêîòîðûå èíûå õàðàêòåðèñòèêè. Êîíñòàíòû c_1, c_2 è c_3 ÿâëÿþòñÿ ñìåùåííûìè âåðñèÿìè c_0, è èñïîëüçóþòñÿ äëÿ ïðåäîòâðàùåíèÿ âñêðûòèé îñíîâàííûõ íà ñèììåòðèè. Ïîäðîáíîñòè ìîæíî íàéòè â [405].

Äåøèôðîâàíèå ÿâëÿåòñÿ îáðàòíûì ïðîöåññîì. Ýòàïû (2) è (3) çàìåíÿþòñÿ íà ñâîþ èíâåðñèþ. Íà ýòàïå (1) âìåñòî c_i èñïîëüçóåòñÿ c_i. c_i^{-1} = 0dad4694.

Áåçîïàñíîñòü MMB

Ñõåìà MMB îáåñïå÷èâàåò íà êàæäîì ýòàïå çíà÷èòåëüíîå è íåçàâèñèìîå îò êëþ÷à ðàññåÿíèå. Â IDEA ðàññåÿíèå äî îïðåäåëåííîé ñòåïåíè çàâèñèò îò êîíêðåòíûõ ïîâêëþ÷åé. Â îòëè÷èå îò IDEA ó MMB íåò ñëàáûõ êëþ÷åé.

Ê ñîæàëåíèþ MMB - ýòî óìåðøèé àëãîðèòì [402]. Ýòî óòâåðæäåíèå ñïðàâåäëèâî ïî ìíîãèì ïðè÷èíàì, õîòÿ êðèïòîàíàëèç MMB è íå áûë îïóáëèêîâàí. Âî ïðâûõ, îí ïðîèòåðîâàëñÿ áåç óòåíêè òðåáîâàíèé óñòîé÷èâîñòè ê ëèíåéíîìó êðèïòîàíàëèçó. Âûáîð ìóëüòèïëèêàòèâíûõ ìíîæèòåëåé îáåñïå÷èë óñòîé÷èâîñòü ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó, íî î ëèíåéíîì êðèïòîàíàëèçå àâòîðàì àëãîðèòìà áûë íåèçâåñòíî.

Âî âòîðûõ, Ýëè Áèõàì ðåàëèçîâàë ýôôåêòèâíûå âñêðûòèå ñ âûáðàííûì êëþ÷îì [160], èñïîëüçóþùåå òîò ôàêò, ÷òî âñå ýòàïû èäåíòè÷íû, à êëþ÷ ïðè ïîëüçîâàíèè ïðîñòî öèêëè÷åñêè ñäâèãàåòñÿ íà 32 áèòà. Â òðåòüåõ, íåñìîòðÿ íà òî, ÷òî ïðîãðàììíûå ðåàëèçàöèè MMB áûëè áûñòðåå ýôôåêòèâíû, â àïïàðàòíîì èñïîëíåíèè àëãîðèòì ìåíåå ýôôåêòèâåí, ÷åì DES.

Äýéìîí ïðåäëàãàåò, ÷òî òîò, êòî çàîñòðåò óëó÷øèòü MMB, äîëæåí ñíà÷àëà ïðîàíàëèçèðîâàòü óìíîæåíèå ïî ìîäóëþ ñ ïîìùüþ ëèíåéíîãî êðèïòîàíàëèçà è ïîäáðàòü íîâûé ìíîæèòåëü, à çàòåì ñäåëàòü êîíñòàíòó C ðàçëè÷íîé äëÿ êàæäîãî ýòàïà [402]. Çàòåì, óëó÷øèâ èñïîëüçîâàíèå êëþ÷à, äîáàâëÿÿ ê êëþ÷àì ýòàïîâ êîíñòàíòû ñ öåëüþ óñòðàíåíèÿ ñìåùåíèÿ. Í î ñàì íå ñòàë çàíèìàòüñÿ ýòèì è ðàçðàáîòàë 3-Way (ñì. ðàçäåë 14.5).

13.11 CA-1.1

CA - ýòî áëî÷íûé øèôð, îñíîâàííûé íà êëåòî÷íûõ àâòîìàòàõ è ðàçðàáîòàííûé Ãîâàðäîì Ãóòîâèöîì (Howard Gutowitz) [677, 678, 679]. Îí øèôðóåò 384-áèòîâûå áëîêè îòêðûòîãî òåêñòà 1088-áèòîâûì êëþ÷îì (íà ñàìîì äåëå èñïîëüçóåòñÿ äâà êëþ÷à - 1024-áèòîâûé è 64- áèòîâûé). Èç-çà ïðèðîäû êëåòî÷íûõ àâòîìàòîâ äëãîâðåìåííóþ ýôôåêòèâíîñòü âû÷èñëåíèé ïðè ðåàëèçàöèè â áîëüøèõ ìàñøòàáíûõ èíòåãðèðîâàííûõ ñõåìàõ.

CA-1.1 èñïîëüçóåò êàê îáðàòèìûå, òàê è íåîáðàòèìûå ïðàâèëà êëåòî÷íîãî àâòîìàòà. Ïðè îáðàòèìîì ïðàâèëå êàæäîå ñîñòîÿíèå ñòðóêòóðû ïîëó÷åòñÿ èç åãî íåïîñðåäñòâåííîãî ïðåäøåñòâóþùåãî ñîñòîÿíèÿ, à ïðè íåîáðàòèìîì ïðàâèëå ó êàæäîãî ñîñòîÿíèÿ ìîæåò áûòü íåñêîëüêî ïðåäøåñòâóþùèõ ñîñòîÿíèé. Ïðè øèôðîâàíèè íåîáðàòèìûå ïðàâèëà ïîøàãîâî îáðàùàþòñÿ âî âðåìåíè. Äëÿ ïðîäâèæåíèÿ îáðàòíî òà÷êóùåãî ñîñòîÿíèÿ ñëó÷àéíûì îáðàçîì äîæíî âûáèðàòüñÿ îäíî èç ñîñòîÿíèé-ïðåäøåñòâåííèêîâ. Ýòî ïðîöåññ ìíîãêðàòíî ïîâòîðÿåòñÿ. Òàêèì îáðàçîì, îáðàòíàÿ èòåðàöèÿ ñëóæèò äëÿ ñìåøèâàíèÿ ñëó÷àéíîé èíôîðìàöèè ñ èíôîðìàöèåé ñîîáùåíèÿ. CA-1.1 èñïîëüçóåò îñîáûé ñîðò ÷àñòè÷íî ëèíåéíîãî íåîáðàòèìîãî ïðàâèëà, òàêîãî, ÷òî äëÿ ëþáîãî äàííîãî ñîñòîÿíèÿ ìîæåò áûòü áûñòðî ïîñòðîåíà íåïîñðåäñòâåííî ïðè øèôðîâàíèè ñ èñïîëüçîâàíà äëÿ ñâÿçè ñ ïîòîêîì øèôðîâàííîñòè. Èíôîðìàöèÿ ñâÿçè ãåíåðèðóåòñÿ êàê ÷àñòü øèôðîâàíèÿ.

Òàê êàê CA-1.1 ïðåäñòàâëÿåò ñîáîé íîâûé àëãîðèì, ñëèøêîì ðàíî äëàòü êàêèå-ëèáî çàÿâëåíèÿ î åãî áåçîïàñíîñòè. Ãóòîâèö óïîìèíàåò íåêîòîðûå âîçìîæíûå âñêðûòèÿ, âêëþ÷àÿ äèôôåðåíöèàëüíûé êðèïòàíàëèç, íî åìó íå óäàëîñü âñêðûòü äëãîðèòì. Â êà÷åñòâå ñòèìóëà Ãóòîâèö ïðåäëîæèë íàãðàäó â 1000 äîëëàðîâ äëÿ "ïðåâîñõîäñòâåíà, êîòîðûé ðàçðàáîòàåò äîñòóïíóþ ïîòîêîâóþ âñêðûòèÿ CA-1.1."

CA-l.1 çàïàòåíòîâàí [678], íî äîñòóïåí äëÿ íåêîìåð÷åñêîãî èñïîëüçîâàíèÿ. Ïðè íåîáõîäèìîñòè ïîëó÷èòü íà àëãîðèòì ëèöåíçèþ íà ðàçðàáîò÷èêîâ íàãðàäó ça êðèïòîàíàëèç îáðàùàéòåñü ê Ãîâàðäó Ãóòîâèöó ïî àäðåñó Howard Cutowitz, ESPCI, Laboratorie d'Electronique, 10 rue Vauquelin, 75005 Paris, France.

13.12 SKIPJACK

Skipjack ðàçðàáîòàí NSA â êà÷åñòâå àëãîðèòìà øèôðîâàíèÿ äëÿ ìèêðîñõåì Clipper è Capstone (ñì. ðàçäåëû 24.16 è 24.17). Òàê êàê ýòî àëãîðèòì îáúÿâëåí ñåêðåòíûì, åãî ïîäðîáíîñòè íèêîãäà íå ïóáëèêîâàëèñü. Îí áóäåò ðåàëèçîâàí òîëüêî êàê çàùèùåííàÿ îò âçëîìà àïïàðàòóðà.

Ýòî àëãîðèòì îáúÿâëåí ñåêðåòíûì íå ïîòîìó, ÷òî ýòî ïîâûøàåò åãî íàäåæíîñòü, à ïîòîìó ÷òî NSA íå õî÷åò, ÷òîáû Skipjack èñïîëüçîâàëñÿ áåç ìåõàíèçìà óñëîâíîãî âðó÷åíèÿ êëþ÷åé Clipper. Àãåíòñòâî íå õî÷åò, ÷òîáû ïðîãðàììíûå ðåàëèçàöèè àëãîðèòìà ðàñïðîñòðàíèëèñü ïî âñåìó ìèðó.

Áåçîïàñåí ëè Skipjack? Åñëè NSA çàõî÷åò ñîçäàòü áåçîïàñíûé àëãîðèòì, îíî, ñêîðåå âñåãî, ýòî ñäåëàåò. Ñ äðóãîé ñòîðîíû, åñëè NSA çàõî÷åò ñîçäàòü àëãîðèòì ñ ëàçåéêîé, òî îíî ñìîæåò ñäåëàòü è ýòî. Âîò ÷òî áûëî îïóáëèêîâàíî [1154, 462].

— Ýòî èòåðàòèâíûé áëî÷íûé øèôð.

— Ðàçìåð áëîêà - 64 áèòà.

— Àëãîðèòì èñïîëüçóåò 80-áèòîâûé êëþ÷.

— Îí ìîæåò áûòü èñïîëüçîâàí â ðåæèìàõ ECB, CBC, 64-áèòîâûé OFB, ëèáî 1-, 8-, 16-, 32- èëè 64-áèòîâûé CFB.

— Îïåðàöèÿ øèôðîâàíèÿ èëè äåøèôðîâàíèÿ ñîñòîèò èç 32 ýòàïîâ.

— NSA íà÷àëî ðàáîòó íàä íèì â 1985 è çàâåðøèëî ïðîâåðêó â 1990.

Â äîêóìåíòàöèè íà ìèêðîñõåìó Mykotronx Clipper óòâåðæäàåòñÿ, ÷òî çàäåðæêà â âûäà÷å ðåçóëüòàòà, ïðèñóùàÿ äëãîðèòìó Skipjack, ñîñòàâëÿåò 64 òàêòà. Ýòî îçíà÷àåò, ÷òî íà êàæäûé ýòàï ïðèõîäèòñÿ äâà òàêòà: îäèí ïðåäïîëîæèòåëüíî äëÿ ïîäñòàíîâêè ñ ïîìîùüþ S-áëîêà, à äðóãîé - äëÿ çàêëþ÷èòåëüíîãî XOR â êîíöà êàæäîãî ýòàïà. (Íå çàáûâàéòå, ïåðåñòàíîâêè ïðè àïïàðàòíûõ ðåàëèçàöèÿõ íå çàíèìàþò âðåìåíè.) Â äîêóìåíòàöèè Mykotronx ýòà äâóõòàêòíàÿ îïåðàöèÿ íàçûâàåòñÿ "G-áëîêîì", à äâà âìåñòå - "ïäâèãîì". (×åñòü G-áëîêà íîñèò íàçâàíèå "F-òàáëèöû" è ÿâëÿåòñÿ òàáëèöåé êîíñòàíò, à ìîæåò áûòü òàáëèöåé ôóíêöèé.)

Ïî îäíèì ñëóõàì Skipjack èñïîëüçóåò 16 S-áëîêîâ, à ïî äðóãèì äëÿ ðàñøèôðîâêè S-áëîêîâ íóæíî âñåãî 128 áàéò

ïàìÿòè. Íåïîõîæå, ÷òîáû îáà ýòèõ ñëóõà áûëè ïðàâîé.

Åùå îäèí ñëóõ óòâåðæäàåò, ÷òî ýòàïû Skipjack, â îòëè÷èå îò DES, ðàáîòàþò íå ñ ïîëíîé áëîêè. Ýòî âìåñòå ñ çàìå÷àíèåì î "ñäâèãàõ" è ñëó÷àéíîì çàÿâëåíèè íà Crypto '94 î òî, ÷òî â Skipjack ïðèìåíÿåòñÿ "48-áèòîâàÿ âíóòðåííÿÿ ñòðóêòóðà", ïîçâîëÿåò ñäåëàòü âûâîä, ÷òî àëãîðèòì ïî ñâîåé ñòåïåíè ïîõîæ íà SHA (ñì. ðàçäåë 18.7), íî èñïîëüçóåò ÷åòûðå 16-áèòîâûõ ïîäáëîêà. Òðè ïîäáëîêà, îáðàáîòàííûå çàâèñÿùåé îò êëþ÷à îäíîíàïðàâëåííîé ôóíêöèé, äàþò 16 áèòîâ, êîòîðûå ïîâòîðÿþò îïåðàöèè XOR ñ îñòàâøèìñÿ ïîäêëþ÷îì. Çàòåì âåñü áëîê öèêëè÷åñêè ñäâèãàåòñÿ íà 16 áèòîâ è ïîñòóïàåò íà âõîä ñëåäóþùåãî ýòàïà, èëè ñäâèãà. Ïðè ýòîì òàêæå èñïîëüçóþòñÿ 128 áàéòîâ äàííûõ S-áëîêà. ß ïîâîçðââàþ, ÷òî S-áëîêè çàâèñÿò îò êëþ÷à.

Ï î ñâîåé ñòðóêòóðå Skipjack âåðîÿòíî ïîõîæ íà DES. NSA ïîíèìàåò, ÷òî åãî çàùèùåííîñòü îò âçëîìà àïïàðàòóðà â êîíöå êîíöîâ áóäåò âñêðûòà è èññëåäîâàíà, îíè íå áóäóò ðèñêîâàòü íèêàêèì ïðåäâû÷íûì êðèïòîãðàôè÷åñêèì ìåòîäàì.

Òî, ÷òî NSA ïëàíèðóåò èñïîëüçîâàòü àëãîðèòì Skipjack äëÿ øèôðîâàíèÿ ñâîåé Ñèñòåìû çàùèòû ñîîáùåíèé (Defense Messaging System, DMS), ñâèäåòåëüñòâóåò î áåçîïàñíîñòè àëãîðèòìà. ×òîáû óáåäèòü ñêåïòèêîâ, NIST ðàçðåøèë êîìèññèè "óâàæàåìûõ íåïðàâèòåëüñòâåííûõ ýêñïåðòîâ . . . ïîëó÷èòü äîñòóï ê êîíôèäåíöèàëüíûì ïîäõîäíîñòÿì àëãîðèòìà, ÷òîáû îíè èñïëåäîâàëè åãî âîçìîæíîñòè è îïóáëèêîâàëè ðåçóëüòàòû ñâîèõ èññëåäîâàíèé " [812].

Â ïðåäâàðèòåëüíîì îò÷åòå ýòîé êîìèññèè ýêñïåðòîâ [262] (îêîí÷àòåëüíîãî îò÷åòà íå áûë, è âîçìîæíî íèêîãäà íå áóäåò) ñîîáùàëîñü:

> Ïðèíÿâ âî âíèìàíèå, ÷òî ñòîèìîñòü âû÷èñëèòåëüíûõ ìîùíîñòåé óìåíüøàåòñÿ â äâà ðàçà êàæäûå 18 ìåñÿöåâ, ñêîðîñòü âñêðûòèÿ Skipjack ñðàâíèìà ñ ñåãîäíÿøíåé ñêîðîñòüþ âñêðûòèÿ DES òîëüêî ÷åðåç 36 ëåò. Ñëåäîâàòåëüíî, ðèñê, ÷òî Skipjack áóäåò âçëîìàí â áëèæàéøèå 30-40 ëåò, íåçíà÷èòåëåí.
>
> Íåçíà÷èòåëåí è ðèñê âçëîìà Skipjack ñ ïîìîùüþ áîëåå áûñòðûõ ñïîñîáîâ âñêðûòèÿ, âêëþ÷àÿ äèôôåðåíöèàëüíûé êðèïòàíàëèç. Ó àëãîðèòìà íå ñèäåíî êëþ÷åé, îòñóòñòâóåò è ñâîéñòâî êîìïëåêñíîñòè. Ýêſïåðòû â îòñóòſâèå âðåìåíè äëÿ ñàìîñòîÿòåëüíîãî áîëüøîãî èññëåäîâàíèÿ àëãîðèòìà èçó÷èëè ïðåäñòàâëåííóþ NSA îïèñàíèå ðàçðàáîòêè è ïðîâåðêè àëãîðèòìà
>
> Óñòîé÷èâîñòü Skipjack ê êðèïòàíàëèçó íå çàâèñèò îò õðàíåíèÿ â òàéíå ñàìîãî àëãîðèòìà.

Èòàê, ó÷àñòíèêè äèñêóññèè íå ñìîãëè ïîðàâíèòü ñ àëãîðèòìîì äîñòàòî÷íî äëãî, ÷òîáû ïðèéòè ê êàêèì-íèáóäü âûâîäàì ñàìîñòîÿòåëüíî. Âñå, ÷òî îíè ñìîãëè ñäåëàòü - ýòî âçãëÿíóòü íà ðåçóëüòàòû, ïîêàçàííûå èì NSA.

Îñòàëñÿ áåç îòâåòà âîïðîñ, ÿâëÿåòñÿ ëè ïëîñêèì ïðîñòðàíñòâî êëþ÷åé Skipjack (ñì. ðàçäåë 8.2). Äàæå åñëè ó Skipjack íåò êëþ÷åé, ñëàáûõ â ñìûñëå DES, ðÿä îñíåäíîñòåé ïðîöåññà èñïîëüçîâàíèÿ êëþ÷à ìîæåò ñäåëàòü îäíè êëþ÷è ñèëüíåå äðóãèõ. Ó Skipjack ìîæåò áûòü 2^{70} ñèëüíûõ êëþ÷åé, ãîðàçäî áîëüøå ÷åì ó DES, âåðîÿòíîñòü ñëó÷àéíî âûáðàòü îäèí èç ýòèõ ñèëüíûõ êëþ÷åé áóäåò ïðèáëèçèòåëüíî 1 ê 1000. Ëè÷íî ÿ äóìàþ, ÷òî ïðîñòàíñòâî êëþ÷åé Skipjack - ïëîñêîå, íî òî, ÷òî îá ýòîì íèêòî íå çàÿâèë ïóáëè÷íî, âûçûâàåò òðåâîãó.

Skipjack çàïàòåíòîâàí, íî â ñîîòâåòſòâèè ñ ñîãëàøåíèåì î ñåêðåòíîñòè ïàòåíòà [1122] ýòîò ïàòåíò õðàíèòſñÿ â òàéíå. Ïàòåíò áóäåò îïóáëèêîâàí òîãäà è òîëüêî òîãäà, êîãäà àëãîðèòì Skipjack áóäåò óñïåøíî âîññòàíîâëåí êåì-òî ïîñòîðîííèì. Ýòî äàåò âîçìîæíîſòü ïðåâèäåüñòâóþ âîñïîëüçîâàòüſ è ïðåìóùåſòâîì çàùèòû ïàòåíòîì, è ïðåìóùåſòâîì êîíôèäåíöèàëüíîſòè òîðãîâîãî ſåêðåòà.

Ãëàâà 14
È åùå î áëî÷íûõ øèôðàõ

14.1 ÃÎÑÒ

ÃÎÑÒ - ýòî áëî÷íûé àëãîðèòì, ðàçðàáîòàííûé â áûâøåì Ñîâåòñêîì Ñîþçå [655, 1393]. Íàçâàíèå "ÃÎÑÒ" ÿâëÿåòñÿ ñîêðàùåíèåì îò "Ãîñóäàðñòâåííûé ñòàíäàðò", íå÷òî ïîõîæåå íà FIPS çà èñêëþ÷åíèåì òîãî, ÷òî ýòî íàçâàíèå ìîãóò íîñèòü ñòàíäàðòû ïðàêòè÷åñêè ëþáîãî òèïà. (Ïîëíûì íàçâàíèåì ÿâëÿåòñÿ "Ãîñóäàðñòâåííûé ñòàíäàðò Ñîþçà ÑÑÐ", èëè "Ãîñóäàðñòâåííûé ñòàíäàðò Ñîþçà Ñîâåòñêèõ Ñîöèàëèñòè÷åñêèõ Ðåñïóáëèê".) Íîìåð äàííîãî ñòàíäàðòà - 28147-89. Âñå ýòè ñòàíäàðòû óòâåðæäàþòñÿ Ãîñóäàðñòâåííûì êîìèòåòîì ïî ñòàíäàðòàì Ñîþçà ÑÑÐ.

ß íå çíàþ, èñïîëüçîâàëñÿ ëè ÃÎÑÒ 28147-89 äëÿ çàñåêðå÷åííîãî òðàôèêà èëè òîëüêî äëÿ ãðàæäàíñêîãî øèôðîâàíèÿ. Çàìå÷àíèå â íà÷àëå ñòàíäàðòà ãëàñèò, ÷òî äëãîðèòì "óäîâëåòâîðÿåò âñì êðèòåðàôè÷åñêèì òðåáîâàíèÿì, à ñòåïåíü çàùèùåííîé èíôîðìàöèè íå îãðàíè÷èâàåòñÿ". ß ñëûøàë óòâåðæäåíèÿ, ÷òî ýòîò äëãîðèòì ïåðâîíà÷àëüíî èñïîëüçîâàëñÿ òîëüêî äëÿ î÷åíü âàæíûõ ëèíèé ñâÿçè, âêëþ÷àÿ ñåêðåòíûå âîåííûå êîìóíèêàöèè, íî ó ìåíÿ íåò ïîäòâåðæäåíèé.

Îïèñàíèå ÃÎÑÒ

ÃÎÑÒ ÿâëÿåòñÿ 64-áèòîâûì äëãîðèòìîì ñ 256-áèòîâûì êëþ÷îì. ÃÎÑÒ òàêæå èñïîëüçóåò äîïîëíèòåëüíûé êëþ÷, êîòîðûé ðàññìàòðèâàåòñÿ íèæå. Â ïðîöåññå ðàáîòû äëãîðèòìà íà 32 ýòàïàõ ïîñëåäîâàòåëüíî âûïîëíÿåòñÿ ïðîñòîé äëãîðèòì øèôðîâàíèÿ.

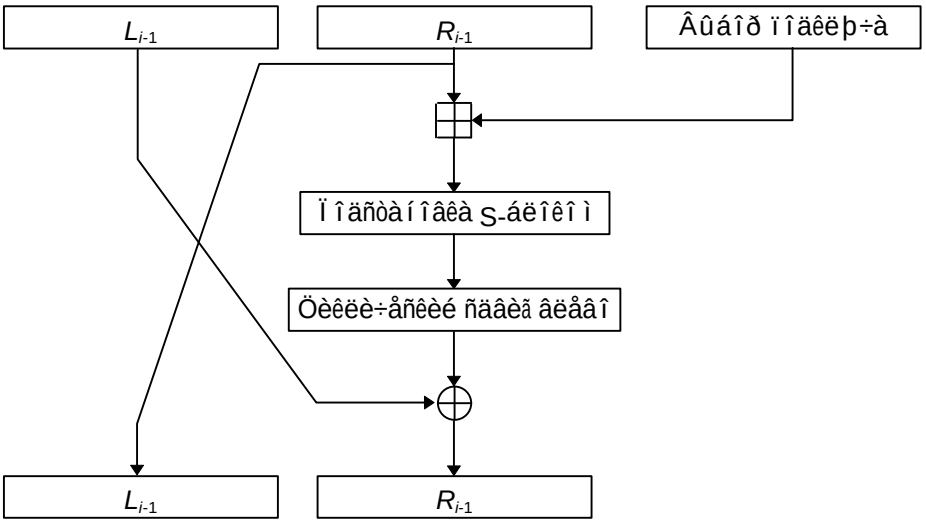
Äëÿ øèôðîâàíèÿ òåêñò ñíà÷àëà ðàçáèâàåòñÿ íà ëåâóþ ïîëîâèíó L è ïðàâóþ ïîëîâèíó R. Íà ýòàïå i èñïîëüçóåòñÿ ïîäêëþ÷ K_i. Íà ýòàïå i äëãîðèòìà ÃÎÑÒ âû÷èñëÿþòñÿ ñëåäóþùèå:

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

Ýòàï ÃÎÑÒ ïîêàçàí íà Ðèñ. 14-1. Ôóíêöèÿ f ïðîñòà. Ñíà÷àëà ïðàâàÿ ïîëîâèíà è i-ûé ïîäêëþ÷ ñêëàäûâàþòñÿ ïî ìîäóëþ 2^{32}. Ðåçóëüòàò ðàçáèâàåòñÿ íà âîñåìü 4-áèòîâûõ êóñî÷êîâ, êàæäûé èç êîòîðûõ ïîñòóïàåò íà âõîä ñâîåãî S-áëîêà. ÃÎÑÒ èñïîëüçóåò âîñåìü ðàçëè÷íûõ S-áëîêîâ, ïåðâûå 4 áèòà ïîïàäàþò â ïåðâûé S-áëîê, âòîðûå 4 4 áèòà - âî âòîðîé S-áëîê, è ò.ä. Êàæäûé S-áëîê ïðåäñòàâëÿåò ñîáîé ïåðåñòàíîâêó ÷èñëå îò 0 äî 15. Íàïðèìåð, S-áëîê ìîæåò âûãëÿäåòü êàê:

7, 10, 2, 4, 15, 9, 0, 3, 6, 12, 5, 13, 1, 8, 11



Ðèñ. 14-1. Ýòàï ÃÎÑÒ.

Â ýòîì ñëó÷àå, åñëè íà âõîäå S-áëîêà 0, òî íà âûõîäå 7. Åñëè íà âõîäå 1, íà âûõîäå 10, è ò.ä. Âñå âîñåìü S-áëîêîâ ðàçëè÷íû, îíè ôàêòè÷åñêè ÿâëÿþòñÿ äîïîëíèòåëüíûì êëþ÷åâûì ìàòåðèàëîì. S-áëîêè äîëæíû ðàçíèöüñÿ â ñâîéſòâå.

Âûõîäû âñåõ âîñüìè S-áëîêîâ îáúåäèíÿþòñÿ â 32-áèòîâîå ñëîâî, çàòåì âñå ñëîâî öèêëè÷åñêè ñäâèãàåòñÿ âëåâî íà 11 áèòîâ. Íàêîíåö ðåçóëüòàò îáúåäèíÿåòñÿ ñ ïîìîùüþ XOR ñ ëåâîé ïîëîâèíîé, è ïîëó÷åòſñÿ íîâàÿ ïðàâàÿ ïîëîâèíà, à ïðàâàÿ ïîëîâèíà ſòàíîâèſñÿ íîâîé ëåâîé ïîëîâèíîé. Âûïîëíèòå ýòî 32 ðàçà, è âñå â ïîðÿä-

êå.

Ãåíåðàöèÿ ïîäêëþ÷åé ïðîòà. 256-áèòîâûé êëþ÷ ðàçáèâàåòñÿ íà âîñåìü 32-áèòîâûõ áëîêîâ: k_1, k_2, . . .k_8. Íà êàæäîì ýòàïå èñïîëüçóåòñÿ ñâîé ïîäêëþ÷, êàê ïîêàçàíî â Òàáë. 14-1. Äåøèôðèðîâàíèå âûïîëíÿåòñÿ òàêæå, êàê è øèôðîâàíèå, íî èíâåðòèðóåòñÿ ïîðÿäîê ïîäêëþ÷åé k_i.

Ñòàíäàðò ÃÎÑÒ íå îïðåäåëÿåò ñïîñîá ãåíåðàöèè S-áëîêîâ, ãîâîðèòñÿ òîëüêî, ÷òî áëîêè äîëæíû áûòü ïðåäîñòàâëåíû êàêèì-òî îáðàçîì [655]. Ýòî ïîðîäèëî äîìûñëû î òîì, ÷òî ñîâòñêèé ïðîèçâîäñòâåííûé ìåõàíèçì ïîñòàâëÿòü õîðîøèå S-áëîêè "õîðîøèì" îðãàíèçàöèÿì è ïëîõèå S-áëîêè òåì îðãàíèçàöèÿì, êîòîðûõ ïðîèçâîäñòâåííûå ñîáñòâåííîñòè íàäóòü. Ýòî âïîëíå ìîæåò áûòü òàê, íî íåîôèöèàëüíûå ïåðåãîâîðû ñ ðîññèéñêèì ïðîèçâîäñòâåííûì ìèêðîñõåì ÃÎÑÒ âûâåëè äóãóþ àëüòåðíàòèâó. Ïðîèçâîäñòâåííûé ñîçäàò ïåðñòàíîâêè S-áëîêà ñàìîñòîÿòåëüíî ñ ïîìîùüþ ãåíåðàòîðà ñëó÷àéíûõ ÷èñåë.

Òàáë. 14-1.
Èñïîëüçîâàíèå ïîäêëþ÷åé íà ðàçëè÷íûõ ýòàïàõ ÃÎÑÒ

Ýòàï:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Ïîäêëþ÷:	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Ýòàï:	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Ïîäêëþ÷:	1	2	3	4	5	6	7	8	8	7	6	5	4	3	2	1

Ñîâñåì íåäàâíî ñòàë èçâåñòíû íàáîð S-áëîêîâ, èñïîëüçóåìûõ â ïðèëîæåíèÿõ Öåíòðàëüíîãî Áàíêà ÐÔ. Ýòè S-áëîêè òàêæå èñïîëüçóþòñÿ â îäíîíàïðàâëåííîé õýø-ôóíêöèè ÃÎÑÒ (ñì. ðàçäåë 18.11) [657]. Îíè ïåðå÷èñëåíû â Òàáë. 14-2.

Êðèïòîàíàëèç ÃÎÑÒ

Âîò ãëàâíûå ðàçëè÷èÿ ìåæäó DES è COST.

— DES èñïîëüçóåò ñëîæíóþ ïðîöåäóðó äëÿ ãåíåðàöèè ïîäêëþ÷åé èç êëþ÷åé. Â ÃÎÑÒ ýòà ïðîöåäóðà î÷åíü ïðîñòà.

— Â DES 56-áèòîâûé êëþ÷, à â ÃÎÑÒ - 256-áèòîâûé. Åñëè äîáàâèòü ñâîðåíèå ïåðåñòàíîâêè S-áëîêîâ, òî ïîëíûé îáúåì ñâîðåíèé èíôîðìàöèè ÃÎÑÒ ñîñòàâèò ïðèìåðíî 610 áèòîâ.

— Ó S-áëîêîâ DES 6-áèòîâûå âõîäû è 4-áèòîâûå âûõîäû, à ó S-áëîêîâ ÃÎÑÒ 4-áèòîâûå âõîäû è âûõîäû. Â îáîèõ àëãîðèòìàõ èñïîëüçóåòñÿ ïî âîñåìü S-áëîêîâ, íî ðàçìåð S-áëîêà ÃÎÑÒ ðàâåí îäíîé ÷åòâåðòîé ðàçìåðà S-áëîêà DES.

— Â DES èñïîëüçóþòñÿ íåðàâíîâåñíûå ïåðåñòàíîâêè, íàçâàííûå P-áëîêîì, à â ÃÎÑÒ èñïîëüçóåòñÿ 11-áèòîâûé öèêëè÷åñêèé ñäâèã âëåâî.

— Â DES 16 ýòàïîâ, à â ÃÎÑÒ - 32.

Òàáë. 14-2.
S-áëîêè ÃÎÑÒ

S-áëîê 1:

4 10 9 2 13 8 0 14 6 11 1 12 7 15 5 3

S-áëîê 2:

14 11 4 12 6 13 15 10 2 3 8 1 0 7 5 9

S-áëîê 3:

5 8 1 13 10 3 4 2 14 15 12 7 6 0 9 11

S-áëîê 4:

7 13 10 1 0 8 9 15 14 4 6 12 11 2 5 3

S-áëîê 5:

6 12 7 1 5 15 13 8 4 10 9 14 0 3 11 2

S-áëîê 6:

4	11	10	0	7	2	1	13	3	6	8	5	9	12	15	14
S-áëîê 7:															
13	11	4	1	3	15	5	9	0	10	14	7	6	8	2	12
S-áëîê 8:															
1	15	13	0	5	7	10	4	9	2	3	14	6	11	8	12

Åñëè ëó÷øèì ñïîñîáîì âñêðûòèÿ ÃÎÑÒ ÿâëÿåòñÿ ãðóáàÿ ñèëà, òî ýòî î÷åíü áåçîïàñíûé àëãîðèòì. ÃÎÑÒ èñïîëüçóåò 256-áèòîâûé êëþ÷, à åñëè ó÷èòûâàòü ñåêðåòíûå S-áëîêè, òî äëèíà êëþ÷à âîçðàñòàåò. ÃÎÑÒ, ïî âèäèìîìó, áîëåå óñòîé÷èâ ê äèôôåðåíöèàëüíîìó è ëèíåéíîìó êðèïòîàíàëèçó, ÷åì DES. Õîòÿ ñëó÷àéíûå S-áëîêè ÃÎÑÒ âîçìîæíî ñèíòåçèðîâàííûõ S-áëîêîâ DES, èõ ñåêðåòíîñòü óâåëè÷èâàåò óñòîé÷èâîñòü ÃÎÑÒ ê äèôôåðåíöèàëüíîìó è ëèíåéíîìó êðèïòîàíàëèçó. Ê òîìó æå, ýòè ñïîñîáû âñêðûòèÿ ÷óâñòâèòåëüíû ê êîëè÷åñòâó ýòàïîâ - ÷åì áîëüøå ýòàïîâ, òåì òðóäíåå âñêðûòü. ÃÎÑÒ èñïîëüçóåò â äâà ðàçà áîëüøå ýòàïîâ, ÷åì DES, îäíî ýòî âîçìîæíî äåëàåò íåñîâìåñòèìûìè è äèôôåðåíöèàëüíûé, è ëèíåéíûé êðèïòîàíàëèç.

Äðóãèå ÷àñòè ÃÎÑÒ òàêèå æå, êàê â DES, èëè ñëàáåå. ÃÎÑÒ íå èñïîëüçóåò ñóùåñòâóþùóþ â DES ïåðåñòàíîâêó ñ ðàñøèðåíèåì. Óäàëåíèå ýòîé ïåðåñòàíîâêè èç DES îñëàáëÿåò åãî èç-çà óìåíüøåíèÿ ëàêîíè÷íîñòè ýôôåêòà, ðàçóìíî ñ÷èòàòü, ÷òî îòñóòñòâèå òàêîé îïåðàöèè â ÃÎÑÒ îñëàáëÿåò ýòîò àëãîðèòì. Ñëîæíåíèå, èñïîëüçóåìîå â ÃÎÑÒ, íå ìåíåå áåçîïàñíî, ÷åì èñïîëüçóåìàÿ â DES îïåðàöèÿ XOR.

Ñàìûì áîëüøèì ðàçëè÷èåì ïðåäñòàâëÿþòñÿ èñïîëüçîâàíèå â ÃÎÑÒ öèêëè÷åñêîãî ñäâèãà âìåñòî ïåðåñòàíîâêè. Ïåðåñòàíîâêà DES óâåëè÷èâàåò ëàâèíîé ýôôåêò. Â ÃÎÑÒ èçìåíèëà îäíîãî âõîäíîãî áèòà âëèÿåò íà îäèí S-áëîê îäíîãî ýòàïà, êîòîðûé çàòåì âëèÿåò íà äâà S-áëîêà ñëåäóþùåãî ýòàïà, òðè áëîêà ñëåäóþùåãî ýòàïà, è ò.ä.. Â ÃÎÑÒ ïîðåáóåòñÿ 8 ýòàïîâ ïðåæäå, ÷åì èçìåíèòñÿ îäíîãî âõîäíîãî áèòà ïîâëèÿåò íà êàæäûé áèò ðåçóëüòàòà, àëãîðèòì DES äëÿ ýòîãî íóæíî òîëüêî 5 ýòàïîâ. Ýòî, êîíå÷íî æå, ñëàáîå ìåñòî. Íî íå çàáûâàéòå: ÃÎÑÒ ñîñòîèò èç 32 ýòàïîâ, à DES òîëüêî èç 16.

Ðàçðàáîò÷èêè ÃÎÑÒ ïûòàëèñü äîñòèãíóòü ðàâíîâåñèÿ ìåæäó áåçîïàñíîñòüþ è ýôôåêòèâíîñòüþ. Îíè èçìåíèëè èäåîëîãèþ DES òàê, ÷òîáû ñîçäàòü àëãîðèòì, êîòîðûé áîëüøå ïîäõîäèò äëÿ ïðîãðàììíîé ðåàëèçàöèè. Îíè, ïî âèäèìîìó, ìåíåå óâåðåíû â áåçîïàñíîñòè ñâîåãî àëãîðèòìà è ïîïûòàëèñü ñêîìïèëèðîâàòü ýòî î÷åíü áîëüøîé äëèííûé êëþ÷, ñîõðàíÿåìûé â ñåêðåòå S-áëîêîâ è óâåíчèâàì êîëè÷åñòâó èòåðàöèé. Âîïðîñ, óâåí÷àëèñü ëè èõ óñïåøíîé ñîçäàíèåì áîëåå áåçîïàñíîãî, ÷åì DES, àëãîðèòìà, îñòàåòñÿ îòêðûòûì.

14.2 CAST

CAST áûë ðàçðàáîòàí â Êàíàäå Êàðëàéñëîì Àäàìñîì (Carlisle Adams) è Ñòàôôîðäîì Òàâàðåñîì (Stafford Tavares) [10, 7]. Îíè óòâåðæäàþò, ÷òî íàçâàíèå îáóñëîâëåíî õîäîì ðàçðàáîòêè è äîæíî íàïîìèíàòü î âåðñèÿõ íîñòè õàðàêòåðå ïðîöåññà, à íå îá èíòåëëåãåíòíîñòè àâòîðîâ. Îïèñûâàåìûé àëãîðèòì CAST èñïîëüçóåò 64-áèòîâûé áëîê è 64-áèòîâûé êëþ÷.

CAST èìååò çíàêîìóþ ñòðóêòóðó. Àëãîðèòì èñïîëüçóåò øåñòü S-áëîêîâ ñ 8-áèòîâûì âõîäîì è 32-áèòîâûì âûõîäîì. Ðàâíàÿ ýòèõ S-áëîêîâ ñëîæíà è çàâèñèò îò ðàäèêàëüíîãî ìíæî íàéòè â ëèòåðàòóðå.

Äëÿ øèôðîâàíèÿ ñíà÷àëà áëîê îòêðûòîãî òåêñòà ðàçáèâàåòñÿ íà ëåâóþ è ïðàâóþ ïîëîâèíû. Àëãîðèòì ñîñòîèò èç 8 ýòàïîâ. Íà êàæäîì ýòàïå ïðàâàÿ ïîëîâèíà îáúåäèíÿåòñÿ ñ ÷àñòüþ êëþ÷à ñ ïîìîùüþ ôóíêöèè f, à çàòåì XOR ðåçóëüòàòà è ëåâîé ïîëîâèíû âû ïîëíÿåòñÿ äëÿ ïîëó÷åíèÿ íîâîé ïðàâîé ïîëîâèíû. Ïåðâîíà÷àëüíàÿ (äî ýòàïà) ïðàâàÿ ïîëîâèíà ñòàíîâèòñÿ íîâîé ëåâîé ïîëîâèíîé. Ï îñëå 8 ýòàïîâ (íå ïåðåñòàâüòå ëåâóþ è ïðàâóþ ïîëîâèíû ïîñëå âñòàâêè ýòàïà) äâå ïîëîâèíû îáúåäèíÿþòñÿ, îáðàçóÿ øèôðîòåêñò. Ôóíêöèÿ f ïðîñòà:

(1) Ðàçáèòà 32-áèòîâûé âõîä íà ÷åòûðå 8-áèòîâûõ ÷àñòè: *a*, *b*, *c*, *d*.

(2) Ðàçáèòà 16-áèòîâûé ïîâêëþ÷ íà äâå 8-áèòîâûõ ïîëîâèíû: *e*, *f*.

(3) Ï îäàþòà *a* íà âõîä S-áëîêà 1, *b* - íà âõîä S-áëîêà 2, *c* - íà âõîä S-áëîêà 3, *d* - íà âõîä S-áëîêà 4, *e* - íà âõîä S-áëîêà 5 è *f* - íà âõîä S-áëîêà 6.

(4) Âûïîëíèòà XOR øåñòè âûõîäîâ S-áëîêîâ, ïîëó÷àÿ 32-áèòîâûé ðåçóëüòàò.

Èíà÷å, 32-áèòîâûé âõîä ìîæåò áûòü îáúåäèíåí ñ ïîìîùüþ XOR ñ 32 áèòàìè êëþ÷à, ðàçáèò íà ÷åòûðå 8-áèòîâûõ ÷àñòè, êîòîðûå îðãàíèçîâàíû S-áëîêàìè è çàòåì îáúåäèíÿþòñÿ ñ ïîìîùüþ XOR [7]. Áåçîïàñíîñòü *N* ýòàïîâ, îðãàíèçîâàííûõ òàêèì îáðàçîì, ïî êðàéíåé ìåðå, ñîîòâåòñòâóåò *N* + 2 ýòàïàì äðóãîãî âàðèàíòà.

16-áèòîâûå ïîäêëþ÷è ýòàïîâ ëåãêî ïîëó÷àþòñÿ èç 64-áèòîâîãî êëþ÷à. Åñëè k_1, k_2, . . .k_8 - ýòî 8 áàéòîâ êëþ÷à, òî íà ýòàïàõ àëãîðèòìà èñïîëüçóþòñÿ ñëåäóþùèå ïîäêëþ÷è:

Ýòàï 1: k_1, k_2

Ýòàï 2: k_3, k_4

Ýòàï 3: k_5, k_6

Ýòàï 4: k_7, k_8

Ýòàï 5: k_4, k_3

Ýòàï 6: k_2, k_1

Ýòàï 7: k_8, k_7

Ýòàï 8: k_6, k_5

Ñèëà ýòîãî àëãîðèòìà çàêëþ÷åíà â åãî S-áëîêàõ. Ó CAST íåò ôèêñèðîâàííûõ S-áëîêîâ, äëÿ êàæäîãî ïðèëîæåíèÿ îíè êîíñòóèðóþòñÿ çàíîâî. Êðèòåðèè ïðîåêòèðîâàíèÿ îïèñàíû â [10], èçîãíóòûì è ôóíêöèîíàëüíûì ñòîëáöû S-áëîêîâ, îáñóæäàþùèå íåîáõîäèìûå ñâîéñòâà S-áëîêîâ (ñì. ðàçäåë 14.10). Ñîçäàííûé äëÿ äàííîé ðåàëèçàöèè CAST S-áëîêîâ óæå áîëüøå íèêîãäà íå ìåíÿåòñÿ. S-áëîêè çàâèñÿò îò ðåàëèçàöèè, à íå îò êëþ÷à.

Â [10] áûë ïîêàçàíî, ÷òî CAST óñòîé÷èâ ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó, à â [728] - ÷òî CAST óñòîé÷èâ è ê ëèíåéíîìó êðèïòîàíàëèçó. Íåèçâåñòíî èíîãî, ÷åì ãðóáàÿ ñèëà, ñïîñîáà âñêðûòü CAST.

Northern Telecom èñïîëüçóåò CAST â ñâîåì ïàêåòå ïðîãðàìì Entrust äëÿ êîìïüþòåðîâ Macintosh, PC è ðàáî÷èõ ñòàíöèé UNIX. Âûðàííûå èìè S-áëîêè íå îïóáëèêîâàíû. Êàíàäñêîå ïðàâèòåëüñòâî ñ÷èòàåò CAST íîâûì ñòàíäàðòîì øèôðîâàíèÿ. Ïàòåíòíàÿ çàÿâêà íà CAST íàõîäèòñÿ â ïðîöåññå ðàññìîòðåíèÿ.

14.3 BLOWFISH

Blowfish - ýòî àëãîðèòì, ðàçðàáîòàííûé ëè÷íî ìíîé äëÿ ðåàëèçàöèè íà áîëüøèõ ìèêðîïðîöåññîðàõ [1388, 1389]. Àëãîðèòì íåçàïàòåíòîâàí, è åãî êîä íà ÿçûêå C ïðèâåäåí â êîíöå ýòîé êíèãè äëÿ øèðîêîãî ïîëüçîâàíèÿ. Ïðè ïðîåêòèðîâàíèè Blowfish ÿ èñïîëüçîâàë ñëåäóþ ùèå êðèòåðèè:

1. Ñêîðîñòü. Blowfish øèôðóåò äàííûå íà 32-áèòîâûõ ìèêðîïðîöåññîðàõ ñî ñêîðîñòüþ 26 òàêòîâ íà áàéò.
2. Êîìïàêòíîñòü. Blowfish ìîæåò ðàáîòàòü ìåíåå, ÷åì â 5 Êáàéò ïàìÿòè.
3. Ïðîñòîòà. Blowfish èñïîëüçóåò òîëüêî ïðîñòûå îïåðàöèè: ñëîæåíèå, XOR è âûáîðêà èç òàáëèöû ïî 32-áèòîâîìó îïåðàíäó. Àíàëèç åãî ñõåìû íåñëîæåí, ÷òî äåëàåò ïðè ðåàëèçàöèè àëãîðèòìà óìåíüøåò êîëè÷åñòâî îøèáîê [1391].
4. Íàñòðàèâàåìîñòü. Äëèíà êëþ÷à Blowfish ïåðåìåííà è ìîæåò äîñòèãàòü 448 áèòîâ.

Blowfish îïòèìèçèðîâàí äëÿ òåõ ïðèëîæåíèé, â êîòîðûõ íåò ÷àñòîé ñìåíû êëþ÷åé, òàêèõ êàê ëèíèè ñâÿçè èëè ïðîãðàììà àâòîìàòè÷åñêîãî øèôðîâàíèÿ ôàéëîâ. Ïðè ðåàëèçàöèè íà 32-áèòîâûõ ìèêðîïðîöåññîðàõ ñ áîëüøèì êýøåì äàííûõ, òàêèõ êàê Pentium è PowerPC, Blowfish çàìåòíî áûñòðåå DES. Blowfish íå ïîäõîäèò äëÿ èñïîëüçîâàíèÿ â ïðèëîæåíèÿõ ñ ÷àñòîé ñìåíîé êëþ÷åé, íàïðèìåð, ïðè êîìóòàöèè ïàêåòîâ, èëè äëÿ èñïîëüçîâàíèÿ â êà÷åñòâå ïàíîâàïðàâëåíîé õýø-ôóíêöèè. Áîëüøèå òðåáîâàíèÿ ê ïàìÿòè äëÿ òàáëèö íåâîçìîæíû ìèñïîëüçîâàíèå ýòîãî àëãîðèòìà â èíòåëëåêòóàëüíûõ ïëàòàõ.

Îïèñàíèå Blowfish

Blowfish ïðåäñòàâëÿåò ñîáîé 64-áèòîâûé áëî÷íûé øèôð ñ êëþ÷îì ïåðåìåííîé äëèíû. Àëãîðèòì ñîñòîèò èç äâóõ ÷àñòåé: ðàçâåðòûâàíèå êëþ÷à è øèôðîâàíèå äàííûõ. Ðàçâåðòûâàíèå êëþ÷à ïðåáðàçóåò êëþ÷ äëèíîé äî 448 áèòîâ â íåñêîëüêî ìàññèâîâ ïîäêëþ÷åé, îáùèì îáúåìîì 4168 áàéòîâ.

Øèôðîâàíèå äàííûõ ñîñòîèò èç ïðîñòîé ôóíêöèè, ïîñëåäîâàòåëüíî âûïîëíÿåìîé 16 ðàç. Êàæäûé ýòàï ñîñòîèò èç çàâèñèìîé îò êëþ÷à ïåðåñòàíîâêè è çàâèñèìîé îò êëþ÷à è äàííûõ ïîäñòàíîâêè. Èñïîëüçóþòñÿ òîëüêî ñëîæåíèÿ è XOR 32-áèòîâûõ ñëîâ. Åäèíñòâåííûì äîïîëíèòåëüíûì îïåðàöèÿì íà êàæäîì ýòàïå ÿâëÿþòñÿ ÷åòûðå èçâëå÷åíèÿ äàííûõ èç èíäåêñèðîâàííîãî ìàññèâà.

Â Blowfish èñïîëüçóåòñÿ ìíîãî ïîäêëþ÷åé. Ýòè ïîäêëþ÷è äëèííûé áûò ðàñ÷èòàíû äî íà÷àëà øèôðîâàíèÿ èëè äåøèôðîâàíèÿ äàííûõ.

P-ìàññèâ ñîñòîèò èç 18 32-áèòîâûõ ïîäêëþ÷åé:

P1, P2, . . ., P18

Êàæäûé èç ÷åòûðåõ 32-áèòîâûõ S-áëîêîâ ñîäåðæèò 256 ýëåìåíòîâ:

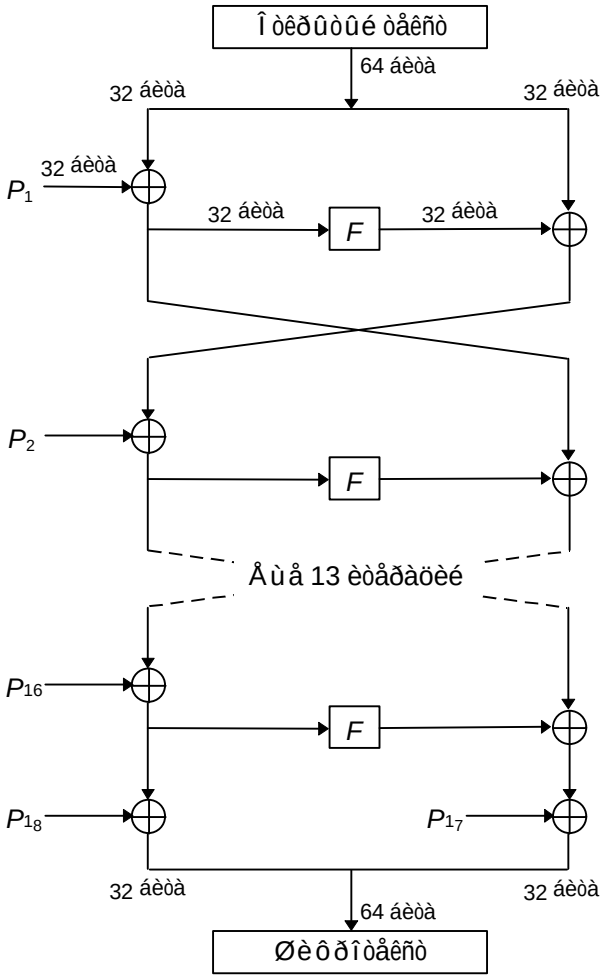
$S_{1,0}$, $S_{1,1}$, . . ., $S_{1,255}$

$S_{2,0}$, $S_{2,2}$, . . ., $S_{2,255}$

$S_{3,0}$, $S_{3,3}$, . . ., $S_{3,255}$

$S_{4,0}$, $S_{4,4}$, . . ., $S_{4,255}$

Òî÷íûé ìåòîä, èñïîëüçóåìûé ïðè âû÷èñëåíèè ýòèõ ïîäêëþ÷åé îïèñàí â ýòîì ðàçäåëå íèæå.



Ðèñ. 14-2. Blowfish.

Blowfish ÿâëÿåòñÿ ñåòüþ Ôåéñòåëà (Feistel) (ñì. ðàçäåë 14.10), ñîñòîÿùåé èç 16 ýòàïîâ. Íà âõîä ïîäàåòñÿ 64-áèòîâûé ýëåìåíò äàííûõ x. Äëÿ øèôðîâàíèÿ:

Ðàçáåéòå x íà äâå 32-áèòîâûõ ïîëîâèíû: x_L, x_R

Äëÿ i = 1 ïî 16:

$x_L = x_L \oplus P_{18}$

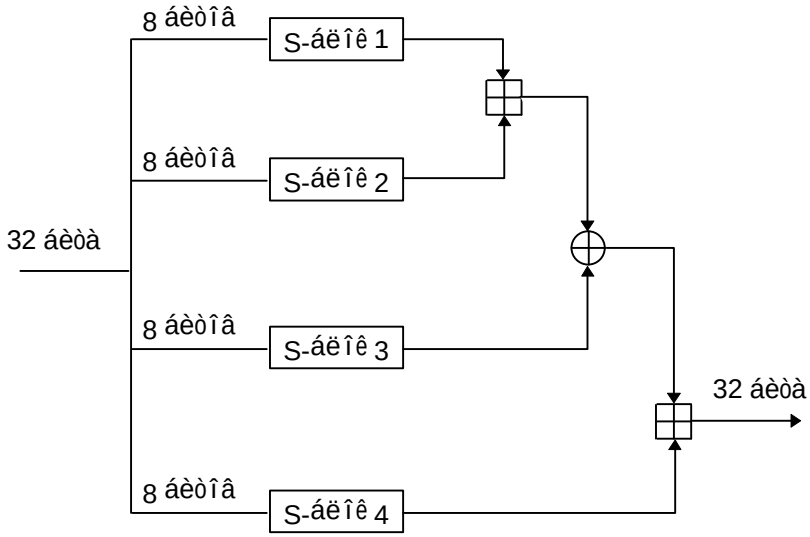
$x_R = \mathrm{F}(x_L) \oplus x_R$

Ïåðåñòàâèòü x_L è x_R (êðîìå ïîñëåäíåãî ýòàïà.)

$x_R = x_R \oplus \mathrm{P}_{17}$

$x_L = x_L \oplus P_{18}$

Îáúåäèíèòü x_L è x_R



Ðèñ. 14-3. Ôóíêöèÿ F.

Ôóíêöèÿ F ïðåäñòàâëÿåò ñîáîé ñëåäóþ ùåå (ñì. Ðèñ. 14-3):

Ðàçäåëèòü x_L íà ÷åòûðå 8-áèòîâûõ ÷àñòè: a, b, c è d
$F(x_L) = ((S_{1,a} + S_{2,b} \bmod 2^{32}) \oplus S_{3,c}) + S_{4,d} \bmod 2^{32}$

Äåøèôðîâàíèå âûïîëíÿåòñÿ òî÷íî òàêæå, êàê è øèôðîâàíèå, íî P_1, P_2, . . ., P_{18} èñïîëüçóþòñÿ â îáðàòíîì ïîðÿäêå.

Â ðåàëèçàöèÿõ Blowfish, äëÿ êîòîðûõ òðåáóåòñÿ î÷åíü áîëüøàÿ ñêîðîñòü, öèêë äîëæåí áûòü ðàçáèòûì, à âñå êëþ÷è äîëæíû õðàíèòüñÿ â êýøå. Ïîäðîáíîñòè ïðèâåäåíû â [568].

Ïîäêëþ÷è ðàññ÷èòûâàþòñÿ ñ ïîìîùüþ ñïåöèàëüíîãî äëãîðèòìà. Âîò êàêîâà òî÷íàÿ ïîñëåäîâàòåëüíîñòü äåéñòâèé.

(1) Ñíà÷àëà P-ìàññèâ, à çàòåì ÷åòûðå S-áëîêà ïî ïðÿäêó èíèöèàëèçèðóþòñÿ ôèêñèðîâàííîé ñòðîêîé. Ýòà ñòðîêà ñîñòîèò èç øåñòíàäöàòèðè÷íûõ öèôð π.

(2) Âûïîëíÿåòñÿ XOR P_1 ñ ïåðâûì 32 áèòàìè êëþ÷à, XOR P_2 ñî âòîðûìè 32 áèòàìè êëþ÷à, è òàê äàëåå äëÿ âñåõ áèòîâ êëþ÷à (äî P_{18}). Èñïîëüçóåòñÿ öèêëè÷åñêè, ïîêà äëÿ âñåãî P-ìàññèâà íå áóäåò âûïîëíåíà îïåðàöèÿ XOR ñ áèòàìè êëþ÷à.

(3) Èñïîëüçóÿ ïîäêëþ÷è, ïîëó÷åííûå íà ýòàïàõ (1) è (2), àëãîðèòì Blowfish øèôðóåòñÿ ñòðîêà èç îäíèõ íóëåé.

(4) P_1 è P_2 çàìåíÿþòñÿ ðåçóëüòàòîì ýòàïà (3).

(5) Ðåçóëüòàò ýòàïà (3) øèôðóåòñÿ ñ ïîìîùüþ àëãîðèòìà Blowfish è èçìåíåííûõ ïîäêëþ÷åé.

(6) P_3 è P_4 çàìåíÿþòñÿ ðåçóëüòàòîì ýòàïà (5).

(7) Äàëåå â õîäå ïðîöåññà âñå ýëåìåíòû P-ìàññèâà è çàòåì ïî ïîðÿäêó çàìåíÿþòñÿ âûõîäîì ïîñòîÿííî ìåíÿþùåãîñÿ àëãîðèòìà Blowfish.

Âñåãî äëÿ ãåíåðàöèè âñåõ íåîáõîäèìûõ ïîäêëþ÷åé òðåáóåòñÿ 521 èòåðàöèÿ. Ïðèìåíåíèå ìîãóò ñîêðàíÿòü ïîäêëþ÷è - íåò íåîáõîäèìîñòè âûïîëíÿòü ïðîöåññ èõ ïîëó÷åíèÿ ìíîãîêðàòíî.

Áåçîïàñíîñòü Blowfish

Ñåðæ Âîäåíý (Serge Vaudenay) èññëåäîâàë Blowfish ñ èçâåñòíûìè S-áëîêàìè è r ýòàïàìè, äèôôåðåíöèàëüíûé êðèïòîàíàëèç ìîæåò ðàñêðûòü P-ìàññèâ ñ ïîìîùüþ 2^{8r+1} âûáðàííûõ îòêðûòûõ òåêñòîâ [1568]. Äëÿ íåêîòîðûõ ñëàáûõ êëþ÷åé, êîòîðûå ãåíåðèðóþò ïëîõèå S-áëîêè (âåðîÿòíîñòü âûáîðà òàêîãî êëþ÷à ñîñòàâëÿåò 1 ê 2^{14}), ýòî æå âñêðûòèå ðàñêðûâàåò P-ìàññèâ ñ ïîìîùüþ âñåãî 2^{4r+1}. Ïðè íåèçâåñòíûõ S-áëîêàõ ýòî âñêðûòèå ìîæåò îáíàðóæèòü èñïîëüçîâàíèå ñëàáîãî êëþ÷à, íî íå ìîæåò ïîðàæàòü ñàì êëþ÷ (íè S-áëîêè, íè P-ìàññèâ). Ýòî âñêðûòèå ýôôåêòèâíî òîëüêî ïðîòèâ âàðèàíòà ñóìóøåííûì ÷èñëîì ýòàïîâ è ñîâåðøåííî áåñïîëåçíî ïðîòèâ 16-ýòàïíîãî Blowfish.

Êîíå÷íî, âàæíî è ðàñêðûòèå ñëàáûõ êëþ÷åé, äàæå õîòÿ îíè ñêîðåå âñåãî íå áóäóò èñïîëüçîâàòüñÿ. Ñëàáûì ÿâëÿþòñÿ êëþ÷, äëÿ êîòîðîãî äâà ýëåìåíòà äàííîãî S-áëîêà èäåíòè÷íû. Äî âûïîëíåíèÿ ðàçâåðòûâàíèÿ êëþ÷à íåâîçìîæíî îïðåäåëèòü, ÿâëÿþòñÿ ëè îí ñëàáûì. Åñëè âû áåñïîêîèòåñü îá ýòîì, âàì ïðèäåòñÿ âûïîëíèòü ðàç-

âåðòûâàíèå êëþ÷à è ïðîâåðèòü, íåò ëè â S-îäíàêîâûõ ýëåìåíòîâ. Õîòÿ ÿ íå äóìàþ, ÷òî ýòî òàê óæ íåîáõîäèìî.

Ì íå íåèçâåñòíî îá óñïåøíîì êðèïòîàíàëèçå Blowfish. Äëÿ áåçîïàñíîñòè íå ðåêîìåíäóåòñÿ Blowfish ñ óìåíüøåííûì ÷èñëîì ýòàïîâ.

Kent Marsh Ltd. âñòðîèëà Blowfish â ñâîé ïðîäóêò îáåñïå÷åíèÿ áåçîïàñíîñòè FolderBolt, ïðåäíàçíà÷åííûé äëÿ Microsoft Windows è Macintosh. Àëãîðèòì òàêæå âõîäèò â Nautilus è PGPfone.

14.4 SAFER

SAFER K-64 îçíà÷àåò Secure And Fast Encryption Routine with a Key of 64 bits - Áåçîïàñíàÿ è áûñòðàÿ ïðîöåäóðà øèôðîâàíèÿ ñ 64-áèòîâûì êëþ÷îì [1009]. Ýòî íå ÿâëÿþùèéñÿ ÷àñòíûé ñîáñòâåííîñòü àëãîðèòì, ðàçðàáîòàííûé Äæåéìñîì Ìàññåì (James Massey) äëÿ Cylink Corp., èñïîëüçóåòñÿ â íåêîòîðûõ èç ïðîäóêòîâ ýòîé êîìïàíèè. Ïðàâèòåëüñòâî Ñèíãàïóðà ñîáñòâåííîñòü èñïîëüçîâàíèå ýòîò àëãîðèòì - ñ 128-áèòîâûì êëþ÷îì [1010] - äëÿ øèôîâàíèÿ ïåðåäà ïðèëîæåíèé. Åãî èñïîëüçîâàíèå íå îãðàíè÷åíî ïàòåíòîì, àâòîðñêèìè ïðàâàìè èëè äóãèìè îãðàíè÷åíèÿìè.

Àëãîðèòì ðàáîòàåò ñ 64-áèòîâûì áëîêîì è 64-áèòîâûì êëþ÷îì. Â îòëè÷èå îò DES îí ÿâëÿåòñÿ íå ñåòüþ Ôåéñòåëà (ñì. ðàçäåë 14.10), à èòåðàòèâíûì áëî÷íûì øèôðîì: äëÿ íåêîòîðîãî êîëè÷åñòâà ýòàïîâ ïðèìåíÿåòñÿ îäíà è òà æå ôóíêöèÿ. Íà êàæäîì ýòàïå èñïîëüçóþòñÿ äâà 64-áèòîâûõ ïîäêëþ÷à. Àëãîðèòì îïðåäóåò òîëüêî áàéòàìè.

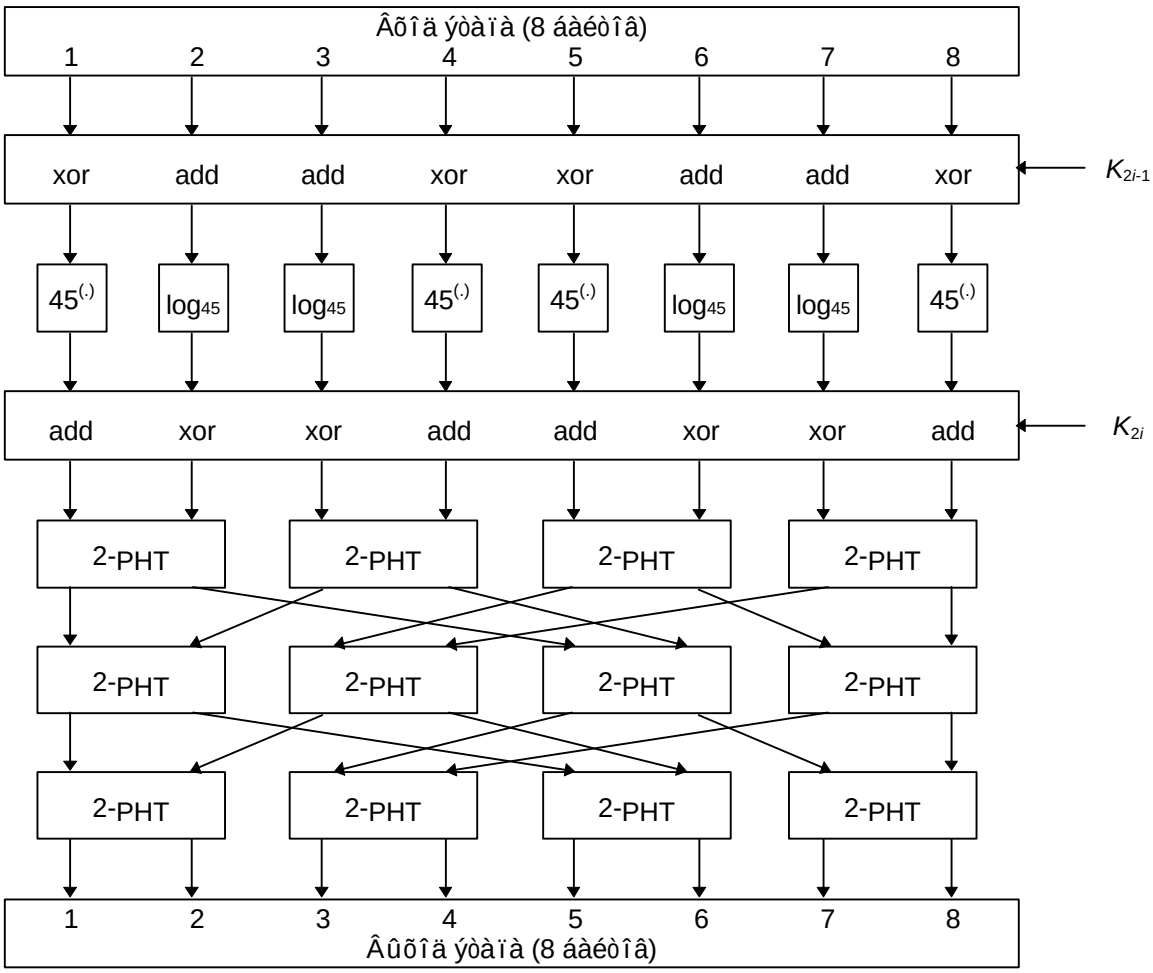
Îïèñàíèå SAFER K-64

Áëîê îòêðûòîãî òåêñòà äëèíîé íà âñåì áàéòîâûõ ïîäáëîêîâ: B_1, B_2, . . . , B_7, B_8. Çàòåì ïîäáëîêè îáðàáàòûâàþòñÿ â õîäå r ýòàïîâ. Íåêîòîðûå ïîäáëîêè ïîäâåðãàþòñÿ çàêëþ÷èòåëüíîìó ïðåîáðàçîâàíèþ. Íà êàæäîì ýòàïå èñïîëüçóåòñÿ äâà ïîäêëþ÷à: K_{2r-1} è K_{2r}.

Íà Ðèñ. 14-4 ïîêàçàí îäèí ýòàï SAFER K-64. Ñíà÷àëà íàä ïîäáëîêàìè âûïîëíÿåòñÿ ëèíåéíîå XOR, ëèíåéíîå ñëîæåíèå ñ áàéòàìè ïîäêëþ÷à K_{2r-1}. Çàòåì âîñåìü ïîäáëîêîâ ïîäâåðãàþòñÿ îäíîìó èç äâóõ íåëèíåéíûõ ïðåîáðàçîâàíèé:

$y = 45^x \bmod 257$. (Åñëè $x = 0$, òî $y = 0$.)

$y = \log_{45} x$. (Åñëè $x = 0$, òî $y = 0$.)



Ðèñ. 14-4. Îäèí ýòàï SAFER.

Ýòî îïåðàöèè â êîíå÷íîì ïîëå GF(257), à 45 - ýëåìåíò ïîëÿ, ÿâëÿþùèéñÿ ïðèìèòèâîì. Â ðåãèçàöèÿõ SAFER K-64 áûñòðåå âûïîëíÿòü ïîñëå â òàáëèöå, ÷åì âñå âðåìÿ ðàñ÷èòûâàòü íîâûå ðåçóëüòàòû.

Çàòåì ïîäáëîêè ëèáî ïîäâåðãàþòñÿ XOR, ëèáî ñêëàäûâàþòñÿ ñ áàéòàìè ïîäêëþ÷à K_{2r}. Ðåçóëüòàò ýòîãî äåéñòâèÿ ïðîïàäè ÷åðåç òðè óðîâíÿ ëîêàëüíûõ îïåðàöèé, öåëüþ êîòîðûõ ÿâëÿåòñÿ óâåëè÷åíèå ëàâèííîãî ýôôåêòà. Êàæäàÿ îïåðàöèÿ íàçûâàåòñÿ ïñåâäîäàäàìàðîâûì ïðåîáðàçîâàíèåì (Pseudo-Hadamard Transform, PHT). Åñëè íà âõîäå PHT a_1 è a_2, òî íà âûõîäå:

$b_1 = (2a_1 + a_2) \bmod 256$

$b_2 = (a_1 + a_2) \bmod 256$

Ï îñëå r ýòàïîâ âûïîëíÿåòñÿ çàêëþ÷èòåëüíîå ïðåîáðàçîâàíèå. Î íî ñîâïàäàåò ñ ïðåîáðàçîâàíèåì, ÿâëÿþùèìñÿ ïåðâûì äåéñòâèåì êàæäîãî ýòàïà. Íàä B_1, B_4, B_5 è B_8 âûïîëíÿåòñÿ XOR ñ ñîîòâåòñòâóþùèìè áàéòàìè ïîñëåäíåãî ïîâêëþ÷à, à B_2, B_3, B_6 è B_7 ñêëàäûâàþòñÿ ñ ñîîòâåòñòâóþùèìè áàéòàìè ïîñëåäíåãî ïîâêëþ÷à. Â ðåçóëüòàòå è ïîëó÷àþòñÿ øèôðîâêñò.

Äåøèôðèðîâàíèå ïðåäñòàâëÿåò ñîáîé îáðàòíûé ïðîöåññ: ñíà÷àëà çàêëþ÷èòåëüíîå ïðåîáðàçîâàíèå (ñ âû÷èòàíèåì âìåñòî ñëîæåíèÿ), çàòåì r èíâåðñèðîâàííûõ ýòàïîâ. Îáðàòíîå PHT (Inverse PHT, IPHT) - ýòî:

$a_1 = (b_1 - b_2) \bmod 256$

$a_2 = (-b_1 + 2b_2) \bmod 256$

Ì àññèâ ðåêîìåíäóåò èñïîëüçîâàòü 6 ýòàïîâ, íî äëÿ áîëüøåé áåçîïàñíîñòè êîëè÷åñòâî ýòàïîâ ìîæíî óâåëè÷èòü.

Ãåíåðèðîâàòü ïîäêëþ÷è ñîâñåì íå òðóäíî. Ïåðâûé ïîäêëþ÷, K_1, - ýòî ïðîñòî êëþ÷ ïîëüçîâàòåëÿ. Ï îñëåäóþùèå êëþ÷è ãåíåðèðóþòñÿ â ñîîòâåòñòâèè ñî ñëåäóþùåé ïðîöåäóðîé:

$K_{i+1} = (K_i \lll 3i) + c_i$

Ñìâîë "<<<" îáîçíà÷àåò öèêëè÷åñêèé ñäâèã íàëåâî. Ñäâèã âûïîëíÿåòñÿ ïîáàéòîâî, à c_i ÿâëÿåòñÿ êîíñòàíòîé ýòàïà. Åñëè c_{ij} - ýòî j-ûé áàéò êîíñòàíòû i-ãî ýòàïà, òî ìîæíî ðàññ÷èòàòü âñå êîíñòàíòû ýòàïîâ ïî ñëåäóþùåé

ôîðìóëå

$c_{ij} = 45^{45^{\wedge}((9i+j) \bmod 256) \bmod 257} \bmod 257$

Îáû÷íî ýòè çíà÷åíèÿ õðàíÿòñÿ â òàáëèöå.

SAFER K-128

Ýòîò àëüòåðíàòèâíûé ñïîñîá èñïîëüçîâàíèÿ êëþ÷à áûë ðàçðàáîòàí Ìèíñòåðñòâîì âíóòðåííèõ äåë Ñèíãàïóðà, à çàòåì áûë âíåäðåí Ìàññåì â SAFER [1010]. Â ýòîì ñïîñîáå èñïîëüçóþòñÿ äâà êëþ÷à, K_a è K_b, ïî 64 áèòà êàæäûé. Ïðåì ñîñòîèò â òîì, ÷òîáû ãåíåðèðîâàòü ïàðàëëåëüíî äâà ïîñëåäîâàòåëüíîñòè ïîäêëþ÷åé, à çàòåì ÷åðåäîâàòü ïîäêëþ÷è èç êàæäîé ïîñëåäîâàòåëüíîñòè. Ýòî îçíà÷àåò, ÷òî ïðè âûáîðå $K_a = K_b$ 128-áèòîâûé êëþ÷ ñîâìåñòèì ñ 64-áèòîâûì êëþ÷îì K_a.

Áåçîïàñíîñòü SAFER K-64

Ìàññåé ïîêàçàë, ÷òî SAFER K-64 ïîñëå 6 ýòàïîâ àáñîëþòíî çàùèùåí îò äèôôåðåíöèàëüíîãî êðèïòîàíàëèçà ïîñëå 8 ýòàïîâ è äîñòàòî÷íî áåçîïàñåí. Óæå ïîñëå 3 ýòàïîâ ïðîòèâ ýòîãî äëãîðèòìà ñòàíîâèòñÿ íåýôôåêòèâíûì è ëåãêîé êðèïòîàíàëèç [1010].

Êíóäñåí (Knudsen) îáíàðóæèë ñëàáûå ìåñòî â ðàñïðåäåëåíèè êëþ÷åé: ïðàêòè÷åñêè äëÿ êàæäîãî êëþ÷à ñóùåñòâóåò íå ìåíüøå îäíîãî (à èíîãäà äàæå äâóõ) äóãîãî êëþ÷à, êîòîðûé ïðè øèôðîâàíèè êàêîãî-òî äóãîãî îòêðûòîãî òåêñòà ïðåâðàùàåò åãî â òîò æå øèôðîòåêñò [862]. ×èñëî ðàçëè÷íûõ îòêðûòûõ òåêñòîâ, êîòîðûå øèôðóþòñÿ îäèíàêîâûì îáðàçîì, íàõîäèòñÿ â ïðîìåæóòêå îò 2^{22} äî 2^{28}. Õîòÿ òàêîå âñêðûòèå íå ìîæåò ïîâëèÿòü íà áåçîïàñíîñòü SAFER êàê äëãîðèòìà øèôðîâàíèÿ, îíî çíà÷èòåëüíî óìåíüøàåò åãî íàäåæíîñòü ïðè èñïîëüçîâàíèè â êà÷åñòâå îäíîíàïðàâëåííîé õýø-ôóíêöèè. Â ëþáîì ñëó÷àå Êíóäñåí ðåêîìåíäóåò èñïîëüçîâàòü íå ìåíüøå 8 ýòàïîâ.

SAFER áûë ñïðîåêòèðîâàí äëÿ Cylink, à Cylink áûëè ïðåäúÿâëåíû ðàçëè÷íûå îáèíåíèÿ ñî ñòîðîíû NSA [80]. ß ðåêîìåíäîâë áû ïîòðàòèòü íåñêîëüêî ëåò íà èíòåíñèâíûé êðèïòîàíàëèç ïðåæäå, ÷åì êàê-ëèáî èñïîëüçîâàòü SAFER.

14.5 3-WAY

3-Way - ýòî áëî÷íûé øèôð, ðàçðàáîòàííûé Äæîàí Äýéìåíîì (Joan Daemen) [402, 410]. Îí èñïîëüçóåò áëîê è êëþ÷ äëèíîé 96 áèò, è åãî ñõåìà ïðåäïîëàãàåò î÷åíü ýôôåêòèâíóþ àïïàðàòóþ ðåàëèçàöèþ.

3-Way ÿâëÿåòñÿ íå ñåòüþ Ôåéñòåëà, à èòåðàòèâíûì áëî÷íûì øèôðîì. Ó 3-Way ìîæåò áûòü n ýòàïîâ, Äýéìåí ðåêîìåíäóåò 11.

Îïèñàíèå S-Way

Ýòîò àëãîðèòì îïèñàòü íåñëîæíî. Äëÿ øèôðîâàíèÿ áëîêà îòêðûòîãî òåêñòà x:

For i = 0 to n - 1

$x = x$ XOR K_i

x = theta (x)

x = pi - 1 (x)

x = gamma (x)

x = pi - 2 (x)

$x = x \oplus K^{n+1}$

x = theta (x)

Ïðè ýòîì èñïîëüçóþòñÿ ñëåäóþùèå ôóíêöèè:

— theta(x) - ôóíêöèÿ ëèíåéíîé ïîäñòàíîâêè, â îñíîâíîì íàáîð öèêëè÷åñêèõ ñäâèãîâ è XOR.

— pi - 1 (x) è pi - 2 (x) - ïðîñòûå ïåðåñòàíîâêè.

— gamma (x) - ôóíêöèÿ íåëèíåéíîé ïîäñòàíîâêè. Èìåííî ýòî äåéñòâèå è äàëî èìÿ âñåìó àëãîðèòìó, îíî ïðåäñòàâëÿåò ñîáîé ïàðàëëåëüíîå âû÷èñëåíèå ïîäñòàíîâêè 3-áèòîâûõ äàííûõ.

Äåøèôðîâàíèå àíàëîãè÷íî øèôðîâàíèþ çà èñêëþ÷åíèåì òîãî, ÷òî íóæíî èçìåíèòü íà îáðàòíûé ïîðÿäîê áèòîâ èñõîäíûõ äàííûõ è ðåçóëüòàòà. Èñõîäíûé êîä, ðåàëèçóþùèé 3-Way, ìîæíî íàéòè â êîíöå ýòîé êíèãè.

Ïîêà îá óñïåøíîì êðèòîíàëèçå 3-Way íåèçâåñòíî. Àëãîðèòì íåçíàêîìòâàí.

14.6 CRAB

Ýòîò àëãîðèòì áûë ðàçðàáîòàí Áåðòîì Êàëèñêè [Burt Kaliski] è Ìýòòîì Ðîáøîó [Matt Robshaw] èç RSA Laboratories [810]. Â îñíîâå Crab ëåæèò èäåÿ èñïîëüçîâàòü ìåòîäû îáíîâëÿþùåãîñÿ õýø-ôóíêöèé äëÿ ñîçäàíèÿ áûñòðîãî àëãîðèòìà øèôðîâàíèÿ. Ñëåäîâàòåëüíî, Crab î÷åíü ïîõîæ íà MD5, è â ýòîì ðàçäåëå ïðåäïîëàãàåòñÿ, ÷òî âû çíàêîìû ñ ìàòåðèàëîì ðàçäåëà 18.5.

Ó Crab î÷åíü áîëüøîé áëîê: 1024 áàéòà. Òàê êàê Crab áûë ïðåäíàçíà÷åí ñîîáùåíèé, êîòîðûå íåèçâåñòíî çàðàíåå íå áûëî ïðåäåëüíî äëèííûì, ïîýòîìó ïîääåðæêà íåñêîëüêèõ ðàçìåðîâ áëîêà íåîáõîäèìà. Àâòîðû ðàññìîòðåëè ìåòîä, êîòîðûé ïîçâîëÿåò ïðåäâàðèòåëüíî 80-áèòîâûé êëþ÷ â òðè âñïîìîãàòåëüíûõ ïîäêëþ÷à, õîòÿ äëÿ îáû÷íûõ ïîäêëþ÷åé ýòî íåíóæíî. Ïîñêîëüêó ïîääåðæêà áîëüøèõ ïîäêëþ÷åé:

Ïðåäïîëàãàåòñÿ ÷èñëî ñ 0 äî 255: P_0, P_1, P_2, ..., P_{255}.

Ìàññèâ èç 2048 32-áèòîâûõ ÷èñåë: S_0, S_1, S_2,..., S_{2047}.

Âñå ýòè ïîäêëþ÷è äîëæíû áûòü âû÷èñëåíû äî øèôðîâàíèÿ èëè äåøèôðîâàíèÿ. Äëÿ øèôðîâàíèÿ 1024-áàéòîâîãî áëîêà X:

(1) Ðàçäåëèòå X íà 256 32-áèòîâûõ ïîäáëîêîâ: X_0, X_1, X_2, ..., X_{255}.

(2) Ïðåîáðàçóéòå ïîäáëîêè X â ñîîòâåòñòâèè ñ P.

(3) For r=0 to 3

For g = 0 to 63

$A = X_{(4g) <<< 2r}$

$B = X_{(4g+1) <<< 2r}$

$C = X_{(4g+2) <<< 2r}$

$D = X_{(4g+3) <<< 2r}$

For step s = 0 to 7

$A = A \oplus (B + f_r(B, C, D) + S_{512r+8g+s})$

$TEMP = D$

$D = C$

$C = B$

$B = A <<< 5$

$A = TEMP$

$X_{(4g) <<< 2r} = A$

$X_{(4g+1) <<< 2r} = B$

$X_{(4g+2) <<< 2r} = C$

$X_{(4g+3) <<< 2r} = D$

(4) Ñîáðàòü îáúåäèíèòü X_0, X_1, X_2, ..., X_{255}, ïîëó÷àÿ øèôðîâàííûé.

Ôóíêöèè $f_r(B, C, D)$ àíàëîãè÷íû èñïîëüçóåìûì â MD5:

$f_0(B, C, D) = (B \wedge C) \vee ((\neg B) \wedge D)$

$f_1(B, C, D) = (B \wedge D) \vee (C \wedge (\neg D))$

$f_2(B, C, D) = B \oplus C \oplus D$

$f_3(B, C, D) = C \oplus (B \vee (\neg D))$

Äåøèôðîâàíèå ïðåäïîëàãàåò ñîáîé îáðàòíûé ïðîöåññ. Ãåíåðèðîâàíèå ïîäêëþ÷åé ÿâëÿåòñÿ íåïîñòîé çàäà÷åé. Âîò êàê ïî 80-áèòîâîìó êëþ÷ó K ìîæåò áûòü ñãåíåðèðîâàí ìàññèâ ïîäêëþ÷åé P.

(1) Ïðîèíèöèàëèçèðóéòå K_0, K_1, K_2, ..., K_9 10 áàéòàìè K.

(2) For i=10 to 255

$K_i = K_{i-2} \oplus K_{i-6} \oplus K_{i-7} \oplus K_{i-10}$

(3) For i=10 to 255, $P_i = i$

(4) m=0

(5) For *j*=0 to 1

For *i* = 256 to 1 step -1

$m = (K_{256-i} + K_{257-i}) \bmod i$

$K_{257-i} = K_{257-i} <<< 3$

Ïåðåñòàâèòü P_i è P_{i-1}

S-ìàññèâ èç 2048 32-áèòîâûõ ñëîâ ìîæåò áûòü ñãåíåðèðîâàí àíàëîãè÷íûì îáðàçîì ëèáî ïî òîìó æå 80-áèòîâîìó êëþ÷ó, ëèáî ïî äðóãîìó êëþ÷ó. Àâòîðû ïðåäóïðåæäàþò, ÷òî ýòè äâóõëè äîêàçàííûå "ðàññìàòðèâàòüñÿ òîëüêî â êà÷åñòâå ìîòèâàöèè, ìîãóò áûòü è äðóãèå ýôôåêòèâíûå ñõåìû, îáåñïå÷èâàþùèå ëó÷øóþ áåçîïàñíîñòü" [810].

Crab áûë ïðåäëîæåí êàê èñïûòàòåëüíûé ñòåíä äëÿ íîâûõ èäåé, à íå êàê ðàáî÷èé àëãîðèòì. Âî ìíîãîì îí èñïîëüçóåò òå æå ïðèìû, ÷òî è MD5. Áèòàì çàìåòèë, ÷òî î÷åíü áîëüøîé áëîê óïðîùàåò êðèïòîàíàëèç àëãîðèòìà [160]. Ñ äðóãîé ñòîðîíû Crab ìîæåò ïîçâîëÿòü ýôôåêòèâíî èñïîëüçîâàòü î÷åíü áîëüøîé êëþ÷. Â ýòîì ñëó÷àå "óïðîùåíèå êðèòèòàíàëèçà" ìîæåò íè÷åãî íå çíà÷èòü.

14.7 SXAL8/MBAL

Ýòî 64-áèòîâûé áëî÷íûé àëãîðèòì èç ßïîíèè [769]. SXAL8 - ýòî îñíîâíîé àëãîðèòì, à MBAL ïðåäñòàâëÿåò ñîáîé ðàñøèðåííóþ âåðñèþ ñ ïåðåìåííîé äëèíîé áëîêà. Òàê êàê âíóòðè MBAL âûïîëíÿåòñÿ ðÿä óíûõ äåéñòâèé, àâòîðû óòâåðæäàþò, ÷òî îíè ìîãóò îáåñïå÷èòü äîñòàòî÷íóþ áåçîïàñíîñòü çà ìàëûå ÷èñëî ðàóíäîâ. Ïðè äëèíå áëîêà 1024 áàéòà MBAL ïðèìåíí â 70 ðàç áûñòðåå, ÷åì DES. Ê íåñ÷àñòüþ â [1174] ïîêàçàíî, ÷òî MBAL ÷óâñòâèòåëåí ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó, à â [865] - ÷òî îí ÷óâñòâèòåëåí è ê ëèíåéíîìó êðèïòîàíàëèçó.

14.8 RC5

RC5 ïðåäñòàâëÿåò ñîáîé áëî÷íûé îêëüòð ñ áîëüøèì ÷èñëîì ïàðàìåòðîâ: ðàçìåðîì áëîêà, ðàçìåðîì êëþ÷à è êîëè÷åñòâîì ýòàïîâ. Î í áûë èçîáðåòåí Ðîíîì Ðèâåñòîì è ïðîàíàëèçèðîâàí â RSA Laboratories [1324, 1325].

Èñïîëüçóåòñÿ òðè äåéſòâèÿ: XOR, ñëîæåíèå è öèêëè÷åñêèå ñäâèãè. Íà áîëüøèíñòâå ïðîöåññîðîâ îïåðàöèè öèêëè÷åñêîãî ñäâèãà âûïîëíÿþòñÿ çà ïîñòîÿííûå âðåìÿ, ïðåìåííûå öèêëè÷åñêèå ñäâèãè ÿâëÿþòñÿ íåëèíåéíîé ôóíêöèåé. Ýòè öèêëè÷åñêèå ñäâèãè, çàâèñÿùèå è îò êëþ÷à, è îò äàííûõ, ïðåäñòàâëÿþò ñîáîé èíòåðåñíóþ îïåðàöèþ.

RC5 èñïîëüçóåò áëîê ïåðåìåííîé äëèíû, íî â ïðèâîäèìîì ïðèìåðå ìû îñòàíîâèìñÿ íà 64-áèòîâîì áëîêå äàííûõ. Ø èôðîâàíèå èñïîëüçóåò 2*r*+2 çàâèñÿùèõ îò êëþ÷à 32-áèòîâûõ ñëîâ - S_0, S_1, S_2, ... S_{2r+1} - ãäå *r* - ÷èñëî ýòàïîâ. Ýòè ñëîâà ìû ñãåíåðèðóåì ïîçäíåå. Äëÿ øèôðîâàíèÿ ñíà÷àëà ðàçäåëèì áëîê îòêðûòîãî òåêñòà íà äâà 32-áèòîâûõ ñëîâà: *A* è *B*. (RC5 ïðåäïîëàãàåò ñëåäóþ ùåå ñîãëàøåíèå ïî óïàêîâêå áàéòîâ â ñëîâà: ïåðâûé áàéò çàíèìàåò ìëàäøèå áèòû ðåãiñòðà *A*, è ò.ä.) Çàòåì:

$A = A + S_0$

$B = B + S_1$

For $i = 1$ to r:

$A = ((A \oplus B) <<< B) + S_{2i}$

$B = ((B \oplus A) <<< A) + S_{2i+1}$

Ðåçóëüòàò íàõîäèòñÿ â ðåãiñòðàõ *A* è *B*.

Äåøèôðîâàíèå òàêæå ïðîñòî. Ðàçáèòü áëîê îòêðûòîãî òåêſòà íà äâà ñëîâà, *A* è *B*, à çàòåì:

For $i = r$ down to 1:

$B = ((B - S_{2i+1}) >>> A) \oplus A$

$A = ((A - S_{2i}) >>> B) \oplus B$

$B = B - S_1$

$A = A - S_0$

Ñèìâîë ">>>" îáîçíà÷àåò öèêëè÷åñêèé ñäâèã íàïðàâî. Êîíå÷íî æå, âñå ñëîæíîñòè è âû÷èòàíèÿ âûïîëíÿþòñÿ ïî ìîäóëþ 2^{32}.

Ñîçäàíèå ìàññèâà êëþ÷åé áîëåå ñëîæíîé, íî òàêæå ïðÿìîëèíåéíî. Ñíà÷àëà, áàéòû êëþ÷à êîïèðóþòñÿ â ìàññèâ L èç c 32-áèòîâûõ ñëîâ, äîïîëíÿÿ ïðè íåîáõîäèìîñòè çàêëþ÷èòåëüíûå ñëîâ íóëÿìè. Çàòåì ìàññèâ S èíèöèàëèçèðóåòñÿ ïðè ïîìîùè ëèíåéíîãî êîíãðóýíòíîãî ãåíåðàòîðà ïî ìîäóëþ 2^{32}:

$S_0 = P$

for $i = 1$ to $2(r + 1) - 1$:

$S_i = (S_{i-1} + Q) \bmod 2^{32}$

P = 0xb7e15163 è Q = 0x9e3779b9, ýòè êîíñòàíòû îñíîâûâàþòñÿ íà äâîè÷íîì ïðåäñòàâëåíèè e è phi.

Íàêîíåö, ïîäñòàâëÿåì L â S:

$i = j = 0$

$A = B = 0$

âûïîëíèòü n ðàç (ãäå n - ìàêñèìóì $2(r + 1)$ è c):

$A = S_i = (S_i + A + B) <<< 3$

$B = L_i = (L_i + A + B) <<< (A + B)$

$i = (i + 1) \bmod 2(r + 1)$

$j = (j + 1) \bmod c$

Ï î ñóòè, RC5 ïðåäñòàâëÿåò ñîáîé ñåìåéñòâî äëãîðèòìîâ. Òîëüêî ÷òî ìû ïîðåäëèëè RC5 ñ 32-áèòîâûì ñëîâîì è 64-áèòîâûì áëîêîì, íå ñóùåñòâóâ ïðè÷èí, çàïðåùàþùèõ èñïîëüçîâàòü òî æå äëãîðèì ñ 64-áèòîâûì ñëîâîì è 128-áèòîâûì. Äëÿ w = 64, P è Q ðàâíû 0xb7e151628aed2a6b è 0x9e3779b97f4a7c15, ñîîòâåòñòâåííî. Ðèâåñò îáîçíà÷èë ðàçëè÷íûå ðåâèçèè RC5 êàê RC5-*w*/*r*/*b*, ãäå w - ýòî ðàçìåð ñëîâà, r - ÷èñëî ýòàïîâ, à b - äëèíà êëþ÷à â áàéòàõ.

RC5 ÿâëÿåòñÿ íîâûì àëãîðèòìîì, íî RSA Laboratories ïîðïîëà äîñòàòî÷íî ìíîãî âðåìåíè, àíàëèçèðóÿ åãî ðàáîòó ñ 64-áèòîâûì áëîêîì. Ïîñëå 5 ýòàïîâ ñòàòèñòèêà âûãëÿäèò î÷åíü õîðîøî. Ïîñëå 8 ýòàïîâ êàæäûé áèò îòêðûòîãî òåêñòà âëèÿåò ìåðå íà îäèí öèêë÷åñêèé ñäâèã. Äèôôåðåíöèàëüíûå âñêðûòèå òðåáóåò 2^{24} âûáðàííûõ îòêðûòûõ òåêñòîâ äëÿ 5 ýòàïîâ, 2^{45} äëÿ 10 ýòàïîâ, 2^{53} äëÿ 12 ýòàïîâ è 2^{68} äëÿ 15 ýòàïîâ. Êîíå÷íî æå, ñóùåñòâóåò òî÷êà 2^{64} âîçìîæíûõ îòêðûòûõ òåêñòîâ, ïîýòîìó òàêîå âñêðûòèå íåïðèìåíèìî ïðîòèâ äëãîðèòìà ñ 15 è áîëåå ýòàïàìè. Îöåíêà äëÿ ëèíåéíîãî êðèïòîàíàëèçà ïîêàçûâàåò, ÷òî àëãîðèòì áåçîïàñåí ïîñëå 6 ýòàïîâ. Ðèâåñò ðåêîìåíäóåò èñïîëüçîâàòü íå ìåíüøå 12 ýòàïîâ, à ëó÷øå 16 [1325]. Ýòî ÷èñëî ìîæíî ìåíÿòüñÿ.

RSADSI â íàñòîÿùåå âðåìÿ ïàòåíóåò RC5, à ýòî íàçâàíèÿ çàÿâëåíî, êàê òîðãîâàÿ ìàðêà. Êîìïàíèÿ óòâåðæäàåò, ÷òî ïëàòà çà ëèöåíçèðîâàíèå áóäåò î÷åíü ìàëà, íî ýòî ëó÷øå ïðîâàðèòü.

14.9 Äðóãèå áëî÷íûå àëãîðèòìû

Ñóùåñòâóåò àëãîðèòì, íàçûâàåìûé â ëèòåðàòóðå CRYPTO-MECCANO [301], íî îí íå ÿâëÿåòñÿ áåçîïàñíûì. ×åòûðå ÿ÷åéêè êðèïòîãðàôà íà Eurocrypt '91 ïðåäñòàâëÿë àëãîðèòì, îñíîâàííûé íà õàîòè÷íûõ îòîáðàæåíèÿõ [687, 688], Áèõàì âûïîëíèë êðèïòîàíàëèç ýòîãî àëãîðèòìà íà òîé æå êîíôåðåíöèè [157]. Äðóãîé àëãîðèòì îïèðàåòñÿ íà ïîäìíîæåñòâà íåêîòîðîãî ìíîæåñòâà ñëó÷àéíûõ êîä [693]. Ñóùåñòâóåò ìíîæåñòâî àëãîðèòì, îñíîâàííûõ íà òåîðèè êîäîâ, èñïðàâëÿþùèõ îøèáêè: âàðèíò àëãîðèòìà ÌàêÝëèéñà (McEliece) (ñì. ðàçäåë 19.7) [786, 1290], àëãîðèòì Rao-Nam [1292, 733, 1504, 1291, 1056, 1057, 1058, 1293], âàðèàíòû àëãîðèòìà Rao-Nam [464, 749, 1503] è àëãîðèòì Li-Wang [964, 1561] - âñå îíè íåáåçîïàñíû. CALC òàêæå íåáåçîïàñåí [1109]. Àëãîðèòì TEA (Tiny Encryption Algorithm, Êðîøå-íûé àëãîðèòì øèôðîâàíèÿ) ñëèøêîì íîâ, ÷òîáû åãî êîìïëåòèðîâàòü [1592]. Äðóãèì àëãîðèòìîì ÿâëÿåòñÿ Vino [503]. MacGuffin, áëî÷íûé àëãîðèòì, ïðåäëîæåííûé Ìýòòîì Áëýéçîì è ìíîé, òàêæå íåáåçîïàñåí [189], îí áûë âçëîìàí íà òîé æå êîíôåðåíöèè, íà êîòîðîé îí áûë ïðåäëîæåí. BaseKing, ïîõîæèé ïîôèëîñîôèè íà 3-way, íî èñïîëüçóþùèé 192-áèòîâûé áëîê [385], ñëèøêîì íîâ, ÷òîáû åãî êîìïëåòèðîâàòü.

Êðîìå òîãî, ñóùåñòâóåò ìíîæåñòâî áëî÷íûõ àëãîðèòìîâ, ðàçðàáîòàííûõ âíå êðèïòîãðàôè÷åñêîãî ñîîáùåñòâà. Íåêîòîðûå èç íèõ èñïîëüçóþòñÿ ðàçëè÷íûìè âîâëå÷åííûìè è ïðàêòè÷åñêè íåïîíÿòíûìè îðãàíèçàöèÿìè. Ó ìåíÿ íåò äàííûõ î òàêèõ àëãîðèòìàõ. Ñóùåñòâóþò òàêæå äåñÿòêè ÷àñòíûõ êîìåð÷åñêèõ àëãîðèòìîâ. Íåêîòîðûå èç íèõ ìîãóò áûòü õîðîøè, íåêîòîðûå íåò. Åñëè êîìïàíèÿ ïðåäïîëàãàåò, ÷òî îïóáëèêîâàííûé àëãîðèòì íå áóäåò ñëóæèòü èíòåðåñàì êîìïàíèè, òî ëó÷øå ñîãëàñèòüñÿ ñ íåé è íå èñïîëüçîâàòü ýòè àëãîðèòìû.

14.10 Òåîðèÿ ïðîåêòèðîâàíèÿ áëî÷íîãî øèôðà

Â ðàçäåë 11.1 ÿ îïèñûâàë ïðèöèïû Øåííîíà äëÿ ñìåøåíèÿ è ðàññåÿíèÿ. Ñïóñòÿ ïÿòüäåñÿò ëåò ïîñëå òîãî, êàê ýòè ïðèöèïû áûëè âïåðâûå ñôîðìóëèðîâàíû, îíè ñòàþòñÿ êðàóãîëüíûì êàìíåì ïðåêðàñíîãî ïîíèìàíèÿ õîðî-

øåãî áëî÷íîãî øèôðà.

Ñìåøåíèå ñëóæèò äëÿ ìàñêèðîâêè âçàèìîñâÿçåé ìåæäó îòêðûòûì òåêñòîì, øèôðîâàëüíûì òåêñòîì è êëþ÷îì. Ïîíÿòíî, êàê äàæå íåçíà÷èòåëüíàÿ çàìåíà îäíîãî ñèìâîëà íà äðóãîé ïðè äëèíå áëîêà â 64 áèòà ïîçâîëÿåò ñîçäàâàòü ñòîéêèå øèôðû ñ îãðîìíûì ðàçìåðîì êëþ÷à? Õîðîøåå ñìåøèâàíèå óñëîæíÿåò ñòàòèñòèêó âçàèìîñâÿçåé, ÷òî íå ðàáîòàþò äàæå ìîùíûå êðèïòîãðàôè÷åñêèå ñðåäñòâà.

Äèôóçèÿ ðàñïðîñòðàíÿåò îäíîðîäíûõ áèòîâ îòêðûòîãî òåêñòà íà êàê ìîæíî áîëüøå êîëè÷åñòâî øèôðîâåñòà. Ýòî òàêæå ìàñêèðóåò ñòàòèñòè÷åñêèå âçàèìîñâÿçè è óñëîæíÿåò êðèïòîàíàëèç.

Äëÿ áåçîïàñíîñòè äîñòàòî÷íî îäíîãî ñìåøåíèÿ. Àëãîðèì, ñîñòîÿùèé èç åäèíñòâåííîé çàâèñÿùåé îò êëþ÷à òàáëèöû ñîîòâåòñòâèÿ 64 áèòîâ îòêðûòîãî òåêñòà 64 áèòàì øèôðîâåñòà áûë áû äîñòàòî÷íî ñëîæíûì. Ïðîáëåìà â òîì, ÷òî äëÿ òàêîé òàáëèöû ïðåäâû÷èñëåíèå áû ëëøèíñòâî ïàìÿòè: 1020 áàéòîâ. Ñì ûñë ñîçäàíèÿ áëî÷íîãî øèôðà è ñîñòîèò â ñîçäàíèè ÷åãî-òî ïîõîæåãî íà òàêóþ òàáëèöó, íî ïðåäúÿâëÿþùåãî ê ïàìÿòè áîëåå óìåðåííûå òðåáîâàíèÿ.

Ïðèì ñîñòîèò â òîì, ÷òîáû â îäíîì øèôðå â ðàçëè÷íûõ êîìáèíàöèÿõ ïåðåìåííûõ ïåðåìåæàòü ñìåøèâàíèå (ñ ãîðàçäî ìåíüøèì òàáëèöàìè) è äèôôóçèþ. Ýòî íàçûâàåòñÿ **ðàçíîòèïíûì øèôðîì**. Èíîãäà áëî÷íûé øèôð, êîòîðûé âêëþ÷àåò ïîñëåäîâàòåëüíûå ïðåîáðàçîâàíèÿ è ïîäñòàíîâêè, íàçûâàþò **ñåòü ïåðåñòàíîâîê-ïîäñòàíîâîê** (substitution-permutation network), èëè **SP-ñåòü**.

Âçàëýíèòå ñíîâà íà ôóíêöèþ f â DES. Ïðåðûâàíîâêà ñ ðàñøèðåíèåì è P-áëîê ðåàëèçóþò äèôóçèþ, à S-áëîêè - ñìåøåíèå. Ïåðåñòàíîâêà ñ ðàñøèðåíèåì è P-áëîê ëèíåéíû, S-áëîêè - íåëèíåéíû. Êàæäàÿ îïåðàöèÿ ñàìà ïî ñåáå î÷åíü ïðîñòà, íî âìåñòå îíè ðàáîòàþò î÷åíü õîðîøî.

Íà ïðèìåðå DES òàêæå ìîæíî ïîêàçàòü åùå íåñêîëüêî ïðèíöèïîâ ïðîåêòèðîâàíèÿ áëî÷íûõ øèôðà. Ïåðâûì ïðåäëîæèë áëî÷íûé øèôð, âêëþ÷àþùèé **èòåðàöèîííûé áëî÷íûé øèôð**. Ïðè ýòîì ïðåäïîëàãàåòñÿ, ÷òî ïðîñòàÿ ôóíêöèÿ óçåëêà ìó ñëåäîâàòåëüíî èñïîëüçîâàíà íåñêîëüêî ðàç. Äâóõýòàïíûé DES íå î÷åíü ñèëåí, ÷òîáû âñå áèòû ðåçóëüòàòà çàâèñåëè îò âñåõ áèòîâ êëþ÷à è âñåõ áèòîâ èñõîäíûõ äàííûõ, íóæíî 5 ýòàïîâ [1078, 1080]. 16-ýòàïíûé DES - ýòî ñèëüíûé àëãîðèòì, 32-ýòàïíûé DES åùå ñèëüíåå.

Ñåòè Ôåéñòåëà

Áîëüøèíñòâî áëî÷íûõ àëãîðèòìîâ ÿâëÿþòñÿ **ñåòÿìè Ôåéñòåëà** (Felstel networks). Ýòà èäåÿ äàòèðóåòñÿ íà÷àëî 70-õ ãîäîâ [552, 553]. Âîçüìèòå áëîê äëèíîé *n* è ðàçäåëèòå åãî íà äâå ïîëîâèíû äëèíîé *n*/2: L è R. Êîíå÷íî, *n* äîëæíî áûòü ÷åòíûì. Ì îæíî îðãàíèçîâàòü èòåðàöèîííûé áëî÷íûé øèôð, â êîòîðîì ðåçóëüòàò *j*-ãî ýòàïà îïðåäåëÿåòñÿ ðåçóëüòàòîì ïðåäûäóùåãî ýòàïà:

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

K_i - ýòî ïîäêëþ÷, èñïîëüçóåìûé íà *j*-îì ýòàïå, à f - ýòî ïðîèçâîëüíàÿ ôóíêöèÿ ýòàïà.

Ýòó êîíñòðóêöèþ ìîæíî óâåëè÷èòü, ÷òî ýòà ôóíêöèÿ ÿâëÿåòñÿ îáðàùàåìî. Òàê êàê äëÿ îáúåäèíåíèÿ ëåâîé ïîëîâèíû ñ ðåçóëüòàòîì ôóíêöèè ýòàïà îïåðàöèÿ XOR, ñëåäóþùåå âûðàæåíèå îáÿçàòåëüíî ÿâëÿåòñÿ èñòèííûì:

$L_{i-1} \oplus f(R_{i-1}, K_i) \oplus f(R_{i-1}, K_i) = L_{i-1}$

Ãàðàíòèðóåòñÿ, ÷òî øèôð, èñïîëüçóþùèé òàêóþ êîíñòðóêöèþ, îáðàòèì, åñëè ìîæíî âîññòàíîâèòü èñõîäíûå äàííûå f íà êàæäîì ýòàïå. Ñàìà ôóíêöèÿ f íåâàæíà, îí íå îáÿçàíà áûòü îáðàòèìîé. Ì û ìîæåì ñïðåêòðîâàòü f íàñòîëüêî ñëîæíîé, íàñêîëüêî çàõîòèì, è íàì íå ïîòðåáóåòñÿ ðàâåíñòâî äâà ðàçëè÷íûõ äëîáëåíèé ïðè øèôðîâàíèè, à äðóãîé äëÿ äåøèôðîâàíèÿ. Ñòðóêòóðà ñåòè Ôåéñòåëà àâòîìàòè÷åñêè ïîçâîëÿåò îá ýòîì.

Ïðîñòåéøèå ñîîòíîøåíèÿ

DES îáëàäàåò ñëåäóþùèì ñâîéñòâîì: åñëè $E_K(P) = C$, òî $E_K(P') = C'$, ãäå P', C' è K' - ïîáèòîâûå äîïîëíåíèÿ P, C è K. Ýòî ñâîéñòâî âäâîå óìåíüøàåò ñëîæíîñòü âñêðûòèÿ ãðóáîé ñèëîé. Ñâîéñòâà êîìïëåêñíîñòè ëåãêî îáúåäèíÿþòñÿ, è ìû ïîëó÷èì ñëåäóþùåå óòâåðæäåíèå: Ïóñòü $E_K(P) = C$, òî $E_{f(K)}(g(P,K)) = h(C,K)$

ãäå *f, g* è *h* - ïðîñòûå ôóíêöèè. Ïîä "ïðîñòûì ôóíêöèîíàëîì" ÿ ïîäðàçóìåâàþ ôóíêöèè, êîòîðûå âû÷èñëÿþòñÿ ëåãêî, íàìíîãî ëåã÷å, ÷åì âû÷èñëåíèå èòåðàöèè áëî÷íîãî øèôðà. Â DES f ïðåäñòàâëÿåò ñîáîé ïîáèòîâûå ëîãè÷åñêèå *K, g* - ïîáèòîâûå äîïîëíåíèå *P*, à *h* - ïîáèòîâûå äîïîëíåíèå *C*. Ýòî ÿâëÿåòñÿ ðåçóëüòàòîì âêðàïëåíèÿ êëþ÷à â ÷àñòü òåêñòà ñ ïîìîùüþ XOR.

Äëÿ õîðîøåãî áëî÷íîãî øèôðà íå ñóùåñòâóåò ïðîñòûõ ñîîòíîøåíèé. Ìåòîäû ïîèñêà íåêîòîðûõ èç ïîäîáíûõ ñëàáûõ ìåñò ìîæíî íàéòè â [917].

Ãðóïïîâàÿ ñòðóêòóðà

Ïðè èçó÷åíèè àëãîðèòìà âîçíèêàåò âîïðîñ, íå îáðàçóåò ëè îí ãðóïïó. Ýëåìåíòàìè ãðóïïû ÿâëÿþòñÿ áëîêè øèôðîòåêñòà äëÿ êàæäîãî âîçìîæíîãî êëþ÷à, à ãðóïïîâîé îïåðàöèåé ÿâëÿåòñÿ êîìïîçèöèÿ. Èçó÷åíèå ãðóïïîâîé ñòðóêòóðû àëãîðèòìà ïðåäñòàâëÿåò ñîáîé ïîïûòêó ïîíÿòü, íàñêîëüêî óâåëè÷èâàåòñÿ ïðîñòðàíñòâî øèôðîâàíèÿ ïðè ìíîæåñòâåííîì øèôðîâàíèè.

Ïîëåçíûì, îäíàêî, ÿâëÿåòñÿ íå âîïðîñ î òîì, äåéñòâèòåëüíî ëè àëãîðèòì ÿâëÿåòñÿ ãðóïïîé, à î òîì, íàñêîëüêî îí áëèçîê ê ãðóïïå. Åñëè íå õâàòàåò òîëüêî îäíîãî ýëåìåíòà, òî àëãîðèòì íå îáðàçóåò ãðóïïó, íî äâîéíîå øèôðîâàíèå áûëî áû - ñòàòèñòè÷åñêè ãîâîðÿ - ïðîñòîé ïîòåðåé âðåìåíè. Ðàáîòà íàä DES ïîêàçàëà, ÷òî DES î÷åíü äàëåê îò ãðóïïû. Ñóùåñòâóåò òàêæå ðÿä èíòåðåñíûõ âîïðîñîâ î ïîëóãðóïïå, ïîëó÷àåìîé ïðè øèôðîâàíèè DES. Ñîäåðæèò ëè îíà òîæäåñòâî, òî åñòü, íå îáðàçóåò ëè îíà ãðóïïó? Èíûìè ñëîâàìè, íå ãåíåðèðóåò ëè êîãäà-íèáóäü íåêîòîðàÿ êîìáèíàöèÿ îïåðàöèé øèôðîâàíèÿ (íå äåøèôðèðîâàíèÿ) òîæäåñòâåííóþ ôóíêöèþ? Åñëè òàê, íàñêîëüêî äëèííà ñàìàÿ êîðîòêàÿ òàêàÿ êîìáèíàöèÿ?

Öåëüþ èññëåäîâàíèÿ ÿâëÿåòñÿ îöåíêà ïðîñòðàíñòâà êëþ÷åé äëÿ òåîðåòè÷åñêîãî âñêðûòèÿ ãðóáîé ñèëîé, à ðåçóëüòàò ïðåäñòàâëÿåò ñîáîé íàèáîëüøóþ íèæíþþ ãðàíèöó ýíòðîïèè ïðîñòðàíñòâà êëþ÷åé.

Ñëàáûå êëþ÷è

Â õîðîøåì áëî÷íîì øèôðå âñå êëþ÷è îäèíàêîâî ñèëüíû. Îáû÷íî íåò ïðîáëåì è ïðè àëãîðèòìå ñ ìàëûì êîëè÷åñòâîì ñëàáûõ êëþ÷åé, òàêîì êàê DES. Âåðîÿòíîñòü ñëó÷àéíî âûáðàòü îäèí èç íèõ î÷åíü ìàëà, òàêîé êëþ÷ ëåãêî ïðîâåðèòü è ïðè íåîáõîäèìîñòè îòáðîñèòü. Îäíàêî, èíîãäà ýòè ñëàáûå êëþ÷è ìîãóò áûòü çàäåéñòâîâàíû, åñëè áëî÷íûé ôèëüòð èñïîëüçóåòñÿ êàê îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ (ñì. ðàçäåë 18.11).

Óñòîé÷èâîñòü ê äèôôåðåíöèàëüíîìó è ëèíåéíîìó êðèïòîàíàëèçó

Èññëåäîâàíèå äèôôåðåíöèàëüíîãî è ëèíåéíîãî êðèïòîàíàëèçà çíà÷èòåëüíî ïðîÿñíèëî òåîðèþ ïðîåêòèðîâàíèÿ õîðîøåãî áëî÷íîãî øèôðà. Àâòîðû IDEA ââåëè ïîíÿòèå **äèôôåðåíöèàëîâ**, îáîáùåíèå îñíîâíîé èäåè õàðàêòåðèñòèê [931]. Îíè óòâåðæäàëè, ÷òî ìîæíî ñîçäàâàòü áëî÷íûå øèôðû, óñòîé÷èâûå ê âñêðûòèþ ñ èñïîëüçîâàíèåì ýòîãî òèïà. Ðåçóëüòàòîì ïîäîáíîãî ïðîåêòèðîâàíèÿ è ÿâëÿåòñÿ IDEA [931]. Ïîçäíåå ýòî ïîíÿòèå áûëî ôîðìàëèçîâàíî â [1181, 1182], êîãäà Êàéñà Íèáåðã (Kaisa Nyberg) è Ëàðñ Êíóäñåí (Lars Knudsen) ïîêàçàëè, êàê ñîçäàâàòü áëî÷íûå øèôðû, äîêàçóåìî óñòîé÷èâûå ïî îòíîøåíèþ ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó. Ýòà òåîðèÿ áûëà ðàñøèðåíà íà äèôôåðåíöèàëû âûñøèõ ïîðÿäêîâ [702, 161, 927, 858, 860] è ÷àñòè÷íûå äèôôåðåíöèàëû [860]. Êàæåòñÿ, ÷òî äèôôåðåíöèàëû âûñøèõ ïîðÿäêîâ ïðèìåíèìû òîëüêî ê øèôðàì ñ ìàëûì ÷èñëîì ýòàïîâ, íî ÷àñòè÷íûå äèôôåðåíöèàëû ïðåêðàñíî îáúåäèíÿþòñÿ ñ äèôôåðåíöèàëàìè.

Ëèíåéíûé êðèïòîàíàëèç íîâåå, è îí âñå åùå ñîâåðøåíñòâóåòñÿ. Áûëè îïðåäåëåíû ïîíÿòèÿ êëàññèôèêàöèè êëþ÷åé [1019] è íåñêîëüêèõ ïðèáëèæåíèé [811, 812]. Åùå îäíî ðàñøèðåíèå êðèïòîàíàëèçà ìîæíî íàéòè â [1270]. Â [938] áûëà ïðåäïðèíÿòà ïîïûòêà îáúåäèíèòü äèôôåðåíöèàëüíûé è ëèíåéíûé êðèïòîàíàëèç â îäíîì âñêðûòèè. Ïîêà íåÿñíî, êàêàÿ ìåòîäèêà ïðîåêòèðîâàíèÿ ñìîæåò ïðîòèâîñòîÿòü ïîäîáíûì âñêðûòèÿì.

Êíóäñåí äîáèëñÿ íåêîòîðîãî óñïåõà, ðàññìàòðèâàÿ íåêîòîðûå íåîáõîäèìûå (íî, âîçìîæíî, íå äîñòàòî÷íûå) êðèòåðèè òîãî, ÷òî îí íàçâàë **ïðàêòè÷åñêè áåçîïàñíûìè ñåòÿìè Ôåéñòåëÿ** - øèôðîâ, óñòîé÷èâûõ êàê ê äèôôåðåíöèàëüíîìó, òàê è ê ëèíåéíîìó êðèïòîàíàëèçó [857]. Íèáåðã ââåë äëÿ ëèíåéíîãî êðèïòîàíàëèçà àíàëîã ïîíÿòèÿ äèôôåðåíöèàëîâ â äèôôåðåíöèàëüíîì êðèïòîàíàëèçå [1180].

Äîñòàòî÷íî èíòåðåñíîé êàæåòñÿ äâîéñòâåííîñòü äèôôåðåíöèàëüíîãî è ëèíåéíîãî êðèïòîàíàëèçà. Ýòà äâîéñòâåííîñòü ñòàíîâèòñÿ î÷åâèäíîé êàê ïðè ðàçðàáîòêå ìåòîäèêè ñîçäàíèÿ õîðîøèõ äèôôåðåíöèàëüíûõ õàðàêòåðèñòèê è ëèíåéíûõ ïðèáëèæåíèé [164, 1018], òàê è ïðè ðàçðàáîòêå êðèòåðèÿ ïðîåêòèðîâàíèÿ, îáåñïå÷èâàþùåãî óñòîé÷èâîñòü àëãîðèòìà ê îáîèì âñêðûòèÿì [307]. Ïîêà òî÷íî íåèçâåñòíî, êóäà çàâåäåò ýòî íàïðàâëåíèå èññëåäîâàíèé. Äëÿ íà÷àëà Äýéìåí ðàçðàáîòàë ñòðàòåãèþ ïðîåêòèðîâàíèÿ àëãîðèòìà, îñíîâàííóþ íà äèôôåðåíöèàëüíîì è ëèíåéíîì êðèïòîàíàëèçå [402].

Ïðîåêòèðîâàíèå S-áëîêîâ

Ñèëà áîëüøèíñòâà ñåòåé Ôåéñòåëÿ - è îñîáåííî èõ óñòîé÷èâîñòü ê äèôôåðåíöèàëüíîìó è ëèíåéíîìó êðèïòîàíàëèçó - íåïîñðåäñòâåííî ñâÿçàíà ñ èõ S-áëîêàìè. Ýòî ÿâèëîñü ïðè÷èíîé ïîòîêà èññëåäîâàíèé, ÷òî æå îáðàçóåò õîðîøèé S-áëîê.

S-áëîê - ýòî ïðîñòàÿ ïîäñòàíîâêà: îòîáðàæåíèå m-áèòîâûõ âõîäîâ íà n-áèòîâûå âûõîäû. Ðàíåå ÿ óïîìèíàë îá îäíîé áîëüøîé òàáëèöå îòîáðàæåíèÿ 64-áèòîâûõ âõîäîâ íà 64-áèòîâûå âûõîäû, òàêàÿ òàáëèöà ïðåäñòàâëÿëà áû ñîáîé S-áëîê ðàçìåðîì 64*64 áèòà. S-áëîê ñ *m*-áèòîâûì âõîäîì è n-áèòîâûì âûõîäîì íàçûâàåòñÿ **m*n-áèòîâûì S-áëîêîì**. S-áëîêè îáû÷íî ÿâëÿþòñÿ åäèíñòâåííûìè íåëèíåéíûìè äåéñòâèÿìè â àëãîðèòìå, èìåííî îíè

îáåñïå÷èâàþò áåçîïàñíîñòü áëî÷íîãî øèôðà. Â îáùåì ñëó÷àå ÷åì S-áëîêè áîëüøå, òåì ëó÷øå.

Â DES âîñåìü ðàçëè÷íûõ 6*4-áèòîâûõ S-áëîêîâ. Â Khufu è Khafre åäèíñòâåííûé 8*32-áèòîâûé S-áëîê, â LOKI 12*8-áèòîâûé S-áëîê, à â Blowfish è CAST 8*32-áèòîâûå S-áëîêè. Â IDEA S-áëîêîì ïî ñóòè ÿâëÿåòñÿ óìíîæåíèå ïî ìîäóëþ, ýòî 16*16-áèòîâûé S-áëîê. ×åì áîëüøå S-áëîê, òåì òðóäíåå îáíàðóæèòü ñòàòèñòè÷åñêèå îòêëîíåíèÿ, íóæíûå äëÿ âñêðûòèÿ ñ èñïîëüçîâàíèåì ëèíåéíîãî äèôôåðåíöèàëüíîãî, ëèíåéíîãî ëèíåéíîãî êðèïòîàíàëèçà [653, 729, 1626]. Êðîìå òîãî, õîòÿ ñëó÷àéíûå S-áëîêè îáû÷íî íå îïòèìàëüíû ñ òî÷êè çðåíèÿ óñòîé÷èâîñòè ê äèôôåðåíöèàëüíîìó è ëèíåéíîìó êðèïòîàíàëèçó, ñèëüíûå S-áëîêè ëåã÷å íàéòè ñðåäè S-áëîêîâ áîëüøåãî ðàçìåðà. Áîëüøèíñòâî ñëó÷àéíûõ S-áëîêîâ íåëèíåéíû, íåâûðîæäåíû è îáëàäàþò ñèëüíîé óñòîé÷èâîñòüþ ê ëèíåéíîìó êðèïòîàíàëèçó - è ñóùåñòâóþùèå ÷èñëà âõîäíûõ áèòîâ ýòà äîëÿ ñíèæàåòñÿ ìåäëåííî [1185, 1186, 1187].

Ðàçìåð *m* âàæíåå ðàçìåðà *n*. Óâåëè÷åíèå ðàçìåðà *n* ñíèæàåò ýôôåêòèâíîñòü äèôôåðåíöèàëüíîãî êðèïòîàíàëèçà, íî çíà÷èòåëüíî ïîâûøàåò ýôôåêòèâíîñòü äèôôåðåíöèàëüíîãî êðèïòîàíàëèçà. Äåéñòâèòåëüíî, åñëè $n \geq 2^m - m$, òî íàäåæíûå ñòàòèñòèêè ëåãêî äëÿ âõîäíûõ è âûõîäíûõ áèòîâ S-áëîêà. È åñëè $n \geq 2^m$, òî ëèíåéíàÿ çàâèñèìîñòü ñòàíîâèòñÿ òî÷íîé äëÿ âõîäíûõ áèòîâ [164].

Çàìåòíîé ÷àñòüþ ðàáîòû ïî ïðîâåòèðîâàíèþ S-áëîêîâ ÿâëÿåòñÿ èçó÷åíèå **ëîãè÷åñêèõ ôóíêöèé** [94, 1098, 1262, 1408]. Äëÿ îáåñïå÷åíèÿ áåçîïàñíîñòè áóëåâû ôóíêöèè, èñïîëüçóåìûå â S-áëîêàõ, äîëæíû îòâå÷àòü îïðåäåëåííûì óñëîâèÿì. Îíè íå äîëæíû áûòü íè ëèíåéíûìè, íè àôôèííûìè, íè äàæå áûòü áëèçêèìè ê ëèíåéíûì èëè àôôèííûì [9, 1177, 1178, 1188]. Êîëè÷åñòâî íóëåé è åäèíèö äîëæíî áûòü ñáàëàíñèðîâàííûì, è íå äîëæíî áûòü íèêàêèõ êîððåëÿöèé ìåæäó ðàçëè÷íûìè êîìáèíàöèÿìè áèòîâ. Ïðè èçìåíåíèè íà ïðîòèâîïîëîæíûé ëþáîãî âõîäíîãî áèòà âûõîäíûå áèòû äîëæíû âåñòè ñåáÿ íåçàâèñèìî. Ýòè êðèòåðèè ïðîâåòèðîâàíèÿ òàêæå ñâÿçàíû ñ èçó÷åíèåì **ôóíêöèé èçìåíà**: ôóíêöèé, êîòîðûå, êàê ìîæíî áûòü ïîêàçàíî, ÿâëÿþñÿ îïòèìàëüíî íåëèíåéíûìè. Õîòÿ íè îïðåäåëåíû ïðîñòî è åñòåñòâåííî, èõ èçó÷åíèå î÷åíü íåëåãêî [1344, 1216, 947, 905, 1176, 1271, 295, 296, 297, 149, 349, 471, 298].

Î÷åíü âàæíûì ñâîéñòâîì ïðåäñòàâëÿþùèõ ýôôåêò: ñêîëüêî âûõîäíûõ áèòîâ S-áëîêà èçìåíÿþòñÿ ïðè èçìåíåíèè íåêîòîðîãî ïîäìíîæåñòâà âûõîäíûõ áèòîâ. Íåòðóäíî çàäàòü äëÿ áóëåâûõ ôóíêöèé óñëîâèå, âûïîëíåíèå êîòîðûõ îáåñïå÷èâàåò îïðåäåëåííûé èäåàëüíûé ýôôåêò, íî ïðîåêòèðîâàíèå òàêèõ ôóíêöèé ÿâëÿþòñÿ áîëåå ñëîæíîé çàäà÷åé. **Ñòðîãèé ëàâèííûé êðèòåðèé** (strict avalanche criteria, SAC) îáåñïå÷èâàò, ÷òî ñ èçìåíåíèåì îäíîãî âõîäíîãî áèòà èçìåíÿþòñÿ ðîâíî ïîëîâèíà âûõîäíûõ áèòîâ [1586]. Ñì. òàêæå [982, 571, 1262, 399]. Â îäíîé èç ðàáîò ýòè êðèòåðèè ðàññìàòðèâàþòñÿ â òåðìèíàõ óòå÷êè èíôîðìàöèè [1640].

Íåñêîëüêî ëåò íàçàä êðèòîãðàôû ïðåäëîæèëè âûáðàòü S-áëîêè òàê, ÷òîáû òàáëèöà ðàñïðåäåëåíèÿ ðàçëè÷èé äëÿ êàæäîãî S-áëîêà áûëà ïîäîáíà ðàâíîìåðíîé. Ýòî îáåñïå÷èëî áû óñòîé÷èâîñòü ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó çà ñ÷åò ñäëàæèâàíèÿ äèôôåðåíöèàëîâ íà ëþáîì îòäåëüíîì ýòàïå [6, 443, 444, 1177]. Ïðèìåðîì òàêîãî ïðîåêòèðîâàíèÿ ÿâëÿþòñÿ LOKI. Îäíàêî òàêîé ïîäõîä èíîãäà ñîñòîÿòåëüíî óñëîæíÿåò àíàëèç, è çàâèñèìîñòü îò êëþ÷à. Â IDEA èñïîëüçóþòñÿ áîëüøèå çàâèñèìûå îò êëþ÷à S-áëîêè.

Âûáîð S-áëîêîâ - íå ïðîñòàÿ çàäà÷à, ñóùåñòâóþò íåæåëàòåëüíûå ðàçëè÷èìûå èäåè, êàê ëó÷øå ñäåëàòü

1. Ñëó÷àéíî âûáðàòü. ßñíî, ÷òî íåáîëüøèå ñëó÷àéíûå S-áëîêè íåáåçîïàñíû, íî áîëüøèå ñëó÷àéíûå S-áëîêè ìîãóò îêàçàòüñÿ äîñòàòî÷íî õîðîøè. Ñëó÷àéíûå S-áëîêè ñ âîñåìüþ è áîëåå âõîäàìè äîñòàòî÷íî ñèëüíû [1186, 1187]. Åùå ëó÷øå 12-áèòîâûå S-áëîêè. Óñòîé÷èâîñòü S-áëîêîâ âîçðàñòàåò, åñëè îíè îäíîâðåìåííî ÿâëÿþòñÿ è ñëó÷àéíûìè, è çàâèñÿùèìè îò êëþ÷à. Â IDEA èñïîëüçóþòñÿ áîëüøèå çàâèñÿùèå îò êëþ÷à S-áëîêè.
2. Âûáðàòü è ïðîâåðèòü. Â íåêîòîðûõ øèôðàõ ñâîéñòâà S-áëîêîâ, ãåíåðèðîâàííûõ ñëó÷àéíûì îáðàçîì, ïðîâåðÿþòñÿ. Ïðèìåðû òàêîãî ïîäõîäà ñîäåðæàòñÿ â [9, 729].
3. Ðàçðàáîòàòü âðó÷íóþ. Ïðè ýòîì ìàòåìàòè÷åñêèé àïïàðàò èñïîëüçóåòñÿ êðàéíå íåçíà÷èòåëüíî: S-áëîêè ñîçäàþòñÿ ñ èñïîëüçîâàíèåì èíòóèòèâíûõ ïðèíöèïîâ. Áàðò Ïðåíåë (Bart Preneel) çàÿâèë, ÷òî "... òåîðåòè÷åñêè èíòåðåñíûå êðèòåðèè íåäîñòàòî÷íû [äëÿ âûáîðà áóëåâûõ ôóíêöèé S-áëîêîâ] ...", è ÷òî "... íåîáõîäèìû ñïåöèàëüíûå êðèòåðèè ïðîåêòèðîâàíèÿ" [1262].
4. Ðàçðàáîòàòü ìàòåìàòè÷åñêè. S-áëîêè ñîçäàþòñÿ â ñîîòâåòñòâèè ñ ìàòåìàòè÷åñêèì çàêîíîì, ïîýòîìó íîâûå ìåòîäû ãàðàíòèðîâàííîé íàäåæíîñòè ïî îòíîøåíèþ ê äèôôåðåíöèàëüíîìó è ëèíåéíîìó êðèïòîàíàëèçó, à òàêæå õîðîøèì äèôôóçíûì ñâîéñòâàì. Ïðåêðàñíûé ïðèìåð òàêîãî ïîäõîäà ìîæíî íàéòè â [1179].

Ñóùåñòâóåò ðÿä ïðèçûâîâ îáúåäèíèòü "ìàòåìàòè÷åñêèé" è "ðó÷íîé" ïîäõîäû [1334], íî ðåàëüíî, ïî âèäèìîìó, êîíêóðèðóþò ñëó÷àíîì âûáðàííûå S-áëîêè è S-áëîêè ñ ïîðåäåëåííûìè ñâîéñòâàìè. Êîíå÷íî ïðèìóùåñòâî ïîëíîãî ïîäõîäà ÿâëÿåòñÿ îòíîñèòåëüíî ìàòåìàòè÷åñêèõ ïðîñòûõ ìåòîäîâ âñêðûòèÿ - äèôôåðåíöèàëüíîãî è ëèíåéíîãî êðèïòîàíàëèçà - íî îáñïå÷èâàåìàÿ ýòèì ïîäõîäîì ñòåïåíü çàùèòû îò íåèçâåñòíûõ ìåòîäîâ âñêðû-

òèÿ òàêæå íåèçâåñòíà. Ðàçðàáîò÷èêàì DES áûëî èçâåñòíî î äèôôåðåíöèàëüíîì êðèïòîàíàëèçå, è åãî S-áëîêè áûëè îïòèìèçèðîâàíû ñîîòâåòñòâóþùèì îáðàçîì. Ñêîðåå âñåãî, î ëèíåéíîì êðèïòîàíàëèçå îíè íå çíàëè, è S-áëîêè DES î÷åíü ñèëüíî ïî îòíîøåíèþ ê òàêîìó ñïîñîáó âñêðûòèÿ [1018]. Ñëó÷àéíî âûáðàííûå S-áëîêè â DES áûëè áû ñëàáåå ïðîòèâ äèôôåðåíöèàëüíîãî êðèïòîàíàëèçà, íî ñëèøêîì ïðîòèâ ëèíåéíîãî êðèïòîàíàëèçà.

Ñ äðóãîé ñòîðîíû ñëó÷àéíûå S-áëîêè ìîãóò íå áûòü îïòèìàëüíûìè ïî òî÷íîñòè ê äàííûì ñïîñîáàì âñêðûòèÿ, íî îíè ìîãóò áûòü äîñòàò÷íî áîëüøèìè è, ñëåäîâàòåëüíî, äîñòàòî÷íî íàäåæíûìè. Êðîìå òîãî, îíè, ñêîðåå âñåãî, áóäóò äîñòàòî÷íî óñòîé÷èâû è ïðîòèâ íåçâiñòíûõ ñïîñîáîâ âñêðûòèÿ. Ñïîð âñå åùå êèïèò, íî ëè÷íî ìíå êàæåòñÿ, ÷òî S-áëîêè äîëæíû áûòü òàêèìè áîëüøèìè, íàñêîëüêî ýòî âîçìîæíî, ñëó÷àéíûìè è çàâiñåòü îò êëþ÷à.

Ïðîåêòèðîâàíèå áëî÷íîãî øèôðà

Ïðîåêòèðîâàòü áëî÷íûé øèôð íåòðóäíî. Åñëè âû ðàññìàòðèâàåòå 64-áèòîâûé áëî÷íûé øèôð êàê ïåðåñòàíîâêó 64-áèòîâûõ ÷èñåë, ÿñíî, ÷òî ïî÷òè âñå ýòè ïåðåñòàíîâêè áåçïîëåçíû. Òðóäíîñòü ñîñòîèò â ïðîåêòèðîâàíèè áëî÷íîãî øèôðà, êîòîðûé íå òîëüêî áåçîïàñåí, íî òàêæå ìîæåò áûòü ëåãêî îïèñàí è ïðîñò ðåëèçîâàí.

Ëåãêî ìîæíî ñïðîåêòèðîâàòü áëî÷íûé øèôð, åñëè âû èñïîëüçóåòå ïàìÿòü, äîñòàòî÷íóþ äëÿ ðàçìåùåíèÿ S-áëîêîâ 48*32. Òðóäíî ñïðîåêòèðîâàòü íåáîëüøîé âàðèàíò DES, åñëè âû ñîáèðàåòåñü èñïîëüçîâàòü â íåì 128 ýòàïîâ. Ïðè äëèíå êëþ÷à 512 áèòîâ íå ñòîèò áåñïîêîèòüñÿ î òîì, íåò ëè êàêîé-ëèáî çàâèñÿùåé îò êëþ÷à êîìïëèìåíòíîñòè.

14.11 Èñïîëüçîâàíèå îäíîíàïðàâëåííûõ õýø-ôóíêöèé

Ñûëî ïðîñòî ñïîñîáîì èñïîëüçîâàòü äëÿ øèôðîâàíèÿ îäíîíàïðàâëåííóþ õýø-ôóíêöèþ ÿâëÿåòñÿ õýøèðîâàíèå ïðåäâàðèòåëüíîãî áëîêà øèôðîâàíèÿ, îáúåäèíåííîãî ñ êëþ÷îì, à çàòåì âûïîëíåíèå XOR ðåçóëüòàòà ñ òåêóùèì áëîêîì îòêðûòîãî òåêñòà:

$C_i = P_i \oplus H(K, C_{i-1})$

$P_i = C_i \oplus H(K, P_{i-1})$

Óñòàíîâèòå äëèíó áëîêà ðàâíîé äëèíå ðåçóëüòàòà îäíîíàïðàâëåííîé õýø-ôóíêöèè. Ïî ñóòè ýòî ïðèâîäèò ê èñïîëüçîâàíèþ îäíîíàïðàâëåííîé õýø-ôóíêöèè êàê áëî÷íîãî øèôðà â ðåæèìå CFB. Ïðè ïîìîùè àíàëîãè÷íîé êîíñòðóêöèè ìîæíî èñïîëüçîâàòü îäíîíàïðàâëåííóþ õýø-ôóíêöèþ è â ðåæèìå OFB:

$C_i = P_i \oplus S_i$; $S_i = H(K, C_{i-1})$

$P_i = C_i \oplus S_i = H(K, C_{i-1})$

Íàäåæíîñòü òàêîé ñõåìû îïðåäåëÿåòñÿ äåçïàñíîñòüþ îäíîíàïðàâëåííîé õýø-ôóíêöèè.

Karn

Ýòîò ìåòîä, èçîáðåòåííûé Ôèëîì Êàðíîì (Phil Karn) è îòêðûòûé èì äëÿ ñâîáîäíîãî èñïîëüçîâàíèÿ, ñîçäàò îáðàòèìûé áëîêîâûé øèôðîâàíèÿ èç îïðåäåëåííûõ îäíîíàïðàâëåííûõ õýø-ôóíêöèé.

Àëãîðèòì ðàáîòàåò ñ 32-áèòîâûìè áëîêàìè îòêðûòîãî òåêñòà è øèôðîâêè. Äëèíà êëþ÷à ìîæåò áûòü ïðèçâîëüíîé, õîòÿ îïðåäåëåííûå äëèíû êëþ÷åé áîëåå ýôôåêòèâíû äëÿ êîíêðåòíûõ îäíîíàïðàâëåííûõ õýø-ôóíêöèé. Äëÿ îäíîíàïðàâëåííûõ õýø-ôóíêöèé MD4 è MD5 ëó÷øå âñåãî ïîäõîäÿò 96-áèòîâûå êëþ÷è.

Äëÿ øèôðîâàíèÿ ñíà÷àëà ðàçáèòü òåêñò íà äâå 16-áèòîâûõ ïîëîâèíû: P_l è P_r. Çàòåì ðàçáèòü íà äâå 48-áèòîâûõ ïîëîâèíû êëþ÷: K_l è K_r.

$P = P_l , P_r$,

$K = K_l , K_r$

Äîáàâüòå K_l ê P_l è âûïîëíèòå õýøèðîâàíèå îäíîíàïðàâëåííîé õýø-ôóíêöèåé, çàòåì âûïîëíèòå XOR ðåçóëüòàò ñ P_r, ïîëó÷àÿ C_r, ïðåäâû ïîëíîìó øèôðîâêà. Çàòåì, äîáàâüòå K_r ê C_r âûïîëíèòå õýøèðîâàíèå îäíîíàïðàâëåííîé õýø-ôóíêöèåé. Âûïîëíèòå XOR ðåçóëüòàò ñ P_l , ïîëó÷àÿ C_l. Íàêîíåö, îáúåäèíèòå C_r è C_l , ïîëó÷àÿ øèôðîâêà.

$C_r = P_r \oplus H(P_l, K_l)$

$C_l = P_l \oplus H(C_r, K_r)$

$C = C_l, C_r$

Äëÿ äåøèôðîâàíèÿ ïðîñòî èíâåðòèðóéòå ïðîöåññ. Äîáàâüòå K_r ê *Cr*, âûïîëíèòå õýøèðîâàíèå è XOR ðåçóëüòàò ñ C_l , ïîëó÷àÿ P_l. Äîáàâüòå K_l ê P_l, âûïîëíèòå õýøèðîâàíèå è XOR ðåçóëüòàò ñ C_r , ïîëó÷àÿ P_r.

$P_l = C_l \oplus H(C_r, K_r)$

$P_r = C_r \oplus H(P_l, K_l)$

$P = P_l, P_r$

Îáùàÿ ñòðóêòóðà Karn ñîâïàäàåò ñ ñòðóêòóðîé ìíîæåñòâà äóãèõ áëî÷íûõ àëãîðèòìîâ, ðàññìîòðåííûõ â ýòîì ðàçäåëå. Ó àëãîðèòìà òîëüêî äâà ýòàïà, òàê êàê åãî ñëîæíîñòü îïðåäåëÿåòñÿ îäíîíàïðàâëåííîé õýø-ôóíêöèåé. À, òàê êàê êëþ÷ èñïîëüçóåòñÿ òîëüêî êàê âòîðîé õýø-ôóíêöèè, îí íå ìîæåò áûòü ðàñêðûò äàæå ïðè ïîìùè âñêðûòèÿ ñ âûáðàííûì îòêðûòûì òåêñòîì, åñëè, êîíå÷íî, áåçîïàñíà èñïîëüçóåìàÿ îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ.

Luby-Rackoff

Ìàéêë Ëþáû (Michael Luby) è ×àðëüç Ðàêîôô (Charles Rackoff) ïîêàçàëè, ÷òî Karn íå ÿâëÿåòñÿ áåçîïàñíûì [992]. Ðàññìîòðèì äâà îäíîâðåìåííî ñîâùåíèÿ: *AB* è *AC*. Åñëè êðèïòîàíàëèòèê èçâëåêàåò èç øèôðîâêè ïðåôèêñ ïîáùåíèÿ, à òàêæå ïðåäïî÷òåíèÿ îòêðûòîãî òåêñòà âòîðîãî ñîîáùåíèÿ, òî îí ìîæåò ëåãêî âû÷èñëèòü âñå âòîðîå ñîîáùåíèå. Õîòÿ òàêîå âñêðûòèå ñ èçâåñòíûì îòêðûòûì òåêñòîì ðàáîòàåò òîëüêî ïðè îïðåäåëåííûõ óñëîâèÿõ, îíî ïðåäñòàâëÿåò ñîáîé ãëàâíóþ ïðîáëåìó â áåçîïàñíîñòè àëãîðèòìà.

Åå óäàëîñü èçáåæàòü ïðè ïîìùè òðåõýòàïíîãî àëãîðèòìà øèôðîâàíèÿ [992,1643,1644]. Îí èñïîëüçóåò òðè ðàçëè÷íûõ õýø-ôóíêöèè: H_1, H_2 è H_3. Äàëüíåéøèå èññëåäîâàíèÿ ïîêàçàëè, ÷òî H_1 ìîæåò ñîâïàäàòü ñ H_2, èëè H_2 ìîæåò ñîâïàäàòü ñ H_3, íî íå îäíîâðåìåííî [1193]. Êðîìå òîãî, H_1, H_2 è H_3 íå ìîãóò áûòü îñíîâàíû íà èòåðàöèîííîì øèôðîâàíèè [1643]. Â ëþáîì ñëó÷àå ïðè óñëîâèè, ÷òî $H(k,x)$ âäâåò ñåáÿ êàê ïñåâäîñëó÷àéíàÿ ôóíêöèÿ, òðåõýòàïíàÿ âåðñèÿ âûãëÿäèò ñëåäóþùèì îáðàçîì:

(1) Ðàçäåëèòå êëþ÷ íà äâå ïîëîâèíû: K_l è K_r.

(2) Ðàçäåëèòå áëîê îòêðûòîãî òåêñòà íà äâå ïîëîâèíû: L_0 è R_0.

(3) Îáúåäèíèòå K_l è L_0 è âûïîëíèòå õýøèðîâàíèå. Âûïîëíèòå XOR ðåçóëüòàòà õýøèðîâàíèÿ ñ R_0, ïîëó÷àÿ R_1:

$R_1 = R_0 \oplus H(K_l, L_0)$

(4) Îáúåäèíèòå K_r è R_1 è âûïîëíèòå õýøèðîâàíèå. Âûïîëíèòå XOR ðåçóëüòàòà õýøèðîâàíèÿ ñ L_0, ïîëó÷àÿ L_1

$L_1 = L_0 \oplus H(K_r, R_1)$

(5) Îáúåäèíèòå K_l è L_1 è âûïîëíèòå õýøèðîâàíèå. Âûïîëíèòå XOR ðåçóëüòàòà õýøèðîâàíèÿ ñ R_1, ïîëó÷àÿ R_2:

$R_2 = R_1 \oplus H(K_l, L_1)$

(6) Îáúåäèíèòå L_1 è R_2, ïîëó÷àÿ ñîîáùåíèå.

Øèôð êðàòêîãî ñîäåðæàíèÿ ñîîáùåíèÿ

Øèôð êðàòêîãî ñîäåðæàíèÿ ñîîáùåíèÿ(Message Digest Cipher, MDC), èçîáðåòåííûé Ïèòåðîì Ãóòìàííîì (Peter Cutmann) [676], ïðåäñòàâëÿåò ñîáîé ñïîñîá ïðåâðàùåíèÿ îäíîíàïðàâëåííûå õýø-ôóíêöèè â áëî÷íûé øèôð, ðàáîòàþùèé â ðåæèìå CFB. Øèôð ðàáîòàåò ïî÷òè òàêæå áûñòðî, êàê è õýø-ôóíêöèÿ, è ïî êðàéíåé ìåðå íàñòîëüêî æå áåçîïàñåí. Îñòàâøàÿñÿ ÷àñòü ýòîãî ðàçäåëà ïðåäïîëàãàåò çíàêîìñòâî ñ ãëàâîé 18.

Õýø ôóíêöèè, íàïðèìåð MD5 è SHA, èñïîëüçóþò 512-áèòîâûé òåñòîâûé áëîê äëÿ ïðåîáðàçîâàíèÿ âõîäíîãî çíà÷åíèÿ (128 áèòîâ â MD5, è 160 áèòîâ â SHA) â ðåçóëüòàò òîãî æå ðàçìåðà. Ýòî ïðåîáðàçîâàíèå íåîáðàòèìî, íî ïðèêðàñíî ïîäõîäèò äëÿ ðåæèìà CFB: è äëÿ øèôðîâàíèÿ, è äëÿ äåøèôðîâàíèÿ èñïîëüçóåòñÿ îäíà è òà æå îïåðàöèÿ.

Ðàññìîòðèì MDC ñ SHA. MDC èñïîëüçóåò 160-áèòîâûé áëîê è 512-áèòîâûé êëþ÷. Èñïîëüçóåòñÿ ïîáî÷íûé ýôôåêò õýø-ôóíêöèè, êîãäà â êà÷åñòâå ïðåäûäóùåãî õýø-çíà÷åíèÿ áåðåòñÿ âõîäíîé áëîê òòðûòîãî òåêñòà (160 áèòîâ), à 512-áèòîâûé âõîä õýø-ôóíêöèè èãðàåò ðîëü êëþ÷à (ñì. Ðèñ 14.5). Îáû÷íî ïðè èñïîëüçîâàíèè õýø-ôóíêöèè äëÿ õýøèðîâàíèÿ íåîòðîãî âõîäà 512-áèòîâûé âõîä ìåíÿåòñÿ ïðè õýøèðîâàíèè êàæäîãî íîâîãî 512-áèòîâîãî áëîêà. Í î â äàííîì ñëó÷àå 512-áèòîâûé âõîä ñòàíîâèòñÿ íåçìåíÿåìûì êëþ÷îì.

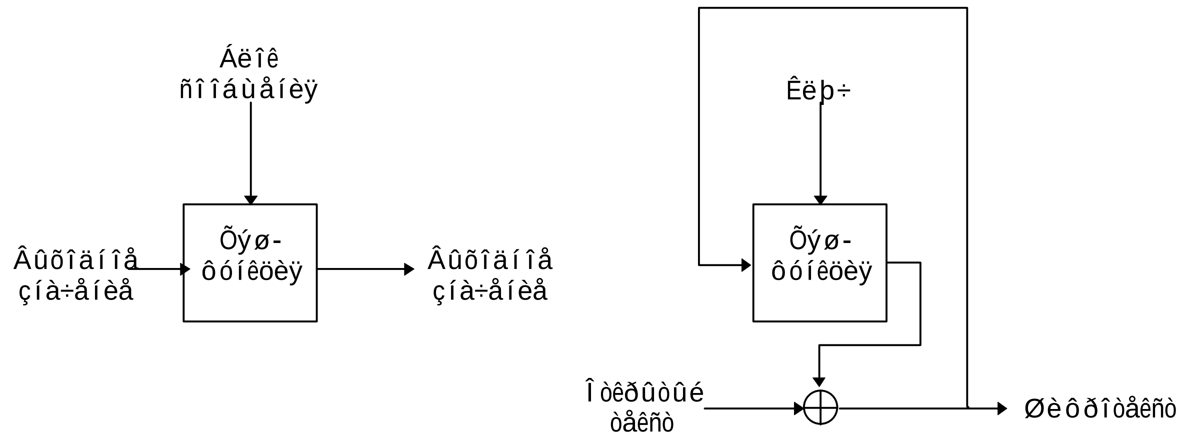
MDC ìîæíî èñïîëüçîâàòü ñ ëþáîé îäíîíàïðàâëåííîé õýø-ôóíêöèåé: MD4, MD5, Snefru, è ò.ä. Î íåçàâèñèòâàí è ìîæåò áûòü ñîâðåøåííî áåçîïàñíûì èñïîëüçîâàí êàê óãîäíî êîãäà óãîäíî è äëÿ ÷åãî óãîäíî [676].

Îäíàêî ëè÷íî ÿ íå âåðþ â ýòó ñõåìó. Ìîæíî ïîäîáðàòü òàêîé ñïîñîá âçëîìà, íà ïðîòèâîñòîÿùèé êîòîðîìó õýø-ôóíêöèÿ íå áûëà ðàññ÷èòàíà. Õýø-ôóíêöèè íå îáÿçàíû ïðîòèâîñòîÿòü âñêðûòèþ ñ âûáðàííûì îòêðûòûì òåêñòîì, êîãäà êðèïòîàíàëèòèê âûáèðàåò íåêîòîðûå íà÷àëüíûå 160-áèòîâûå çíà÷åíèÿ, ïîëó÷àåò èõ "çàøèôðîâàííûìè" îäíèì è òåì æå 512-áèòîâûì "êëþ÷îì" è ïîëüçóåòñÿ ýòèì äëÿ ïîëó÷åíèÿ íåêîòîðîé èíôîðìàöèè îá èñïîëüçóåìîì 512-áèòîâîì êëþ÷å. Òàê êàê ðàçðàáîò÷èêè õýø-ôóíêöèé íå äîëæíû áåñïîêîèòüñÿ î òàêîé âîçìîæíîñòè, ñ÷èòàòü âàø øèôð áåçîïàñíûì ïî îòíîøåíèþ ê ïðèâåäåííîìó ñïîñîáó âñêðûòèÿ - íå ëó÷-

øàÿ èäåÿ.

Áåçîïàñíîñòü øèôðîâ, îñíîâàííûõ íà îäíîíàïðàâëåííûõ õýø-ôóíêöèÿõ

Õîòÿ ýòè êîíñòðóêöèè è ìîãóò áûòü áåçîïàñíûìè, îíè çàâèñÿò îò èñïîëüçóåìîé îäíîíàïðàâëåííîé õýø-ôóíêöèè. Õîðîøàÿ îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ íå îáÿçàòåëüíî äàåò áåçîïàñíûé àëãîðèòì øèôðîâàíèÿ. Ñóùåñòâóþò ðàçëè÷íûå êðèïòîãðàôè÷åñêèå òðåáîâàíèÿ. Íàïðèìåð, ëèíåéíûé êðèïòîàíàëèç áåñïîëåçåí ïðîòèâ îäíîíàïðàâëåííûõ õýø-ôóíêöèé, íî äåéñòâåíåí ïðîòèâ àëãîðèòìîâ øèôðîâàíèÿ. Îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ, òàêàÿ êàê SHA, ìîæåò îáëàäàòü îïðåäåëåííûìè ëèíåéíûìè õàðàêòåðèñòèêàìè, êîòîðûå, íå âëèÿÿ íà åå áåçîïàñíîñòü êàê îäíîíàïðàâëåííîé õýø-ôóíêöèè, ìîãóò ñäåëàòü íåáåçîïàñíûì åå èñïîëüçîâàíèå â òàêîì àëãîðèòìå øèôðîâàíèÿ, êàê MDC. Ìíå íåèçâåñòíî íè î êàêèõ ðåçóëüòàòàõ êðèïòîàíàëèçà èñïîëüçîâàíèÿ êîíêðåòíîé îäíîíàïðàâëåííîé õýø-ôóíêöèè â êà÷åñòâå áëî÷íîãî øèôðà. Ïðåæäå ÷åì èñïîëüçîâàòü èõ äîæäèòåñü ïðîâåäåíèÿ ïîäðîáíîãî àíàëèçà.



(a) Õýø-ôóíêöèÿ (b) Õýø-ôóíêöèÿ êàê áëî÷íûé øèôð â ðåæèìå CFB

Ðèñ. 14-5. Øèôð êðàòêîãî ñîîáùåíèÿ (MDC).

14.12 Âûáîð áëî÷íîãî àëãîðèòìà

Ýòî î÷åíü òðóäíîå ðåøåíèå. DES ïî÷òè íàâåðíÿêà íåáåçîïàñåí ïðè èñïîëüçîâàíèè ïðîòèâ ïðàâèòåëüñòâ âåëèêèõ äåðæàâ, åñëè òîëüêî âû íå øèôðóåòå îãðîìíûìè êóñêàìè äàííûõ. Âîçìîæíî ýòî àëãîðèòì ïîêà íåïëîõ ïðîòèâ êîãî-íèáóäü äðóãîãî, íî âñêîðå è ýòî èçìåíèòñÿ. Ìàøèíû äëÿ âñêðûòèÿ êëþ÷à DES ãðóáîé ñèëîé ñêîðî ñòàíóò ïî êàðìàíó âñåì îðãàíèçàöèÿì.

Ïðåäëîæåííûå Áèõàìîì çàâèñèìûå îò êëþ÷à S-áëîêè DES áóäóò áåçîïàñíû â òå÷åíèå ïî êðàéíåé ìåðå íåñêîëüêèõ ëåò, ìîæåò áûòü çà èñêëþ÷åíèåì èñïîëüçîâàíèÿ ïðîòèâ ñàìûõ õîðîøî îáåñïå÷åííûõ ïðîòèâíèêîâ. Åñëè íåîáõîäèìàÿ áåçîïàñíîñòü äîëæíà áûòü îáåñïå÷åíà íà äåñÿòèëåòèÿ, èëè âû îïàñàåòåñü êðèïòîàíàëèòè÷åñêèõ óñèëèé ïðàâèòåëüñòâ âåëèêèõ äåðæàâ, âîñïîëüçóéòåñü òðîéíûì DES ñ òðåìÿ íåçàâèñèìûìè êëþ÷àìè.

Íåáåñïîëåçíû è äðóãèå àëãîðèòìû. Ìíå íðàâèòñÿ Blowfish, ïîòîìó ÷òî îí áûñòð, è ïîòîìó ÷òî ÿ åãî ïðèäóìàë. Íåïëîõî âûãëÿäèò 3-WAY, âîçìîæíî âñå â ïîðÿäêå è ñ ÃÎÑÒîì. Ïðîáëåìà ïîñîâåòîâàòü ÷òî-íèáóäü ñîñòîèò â òîì, ÷òî NSA ïî÷òè íàâåðíÿêà îáëàäàåò íàáîðîì ýôôåêòèâíûõ êðèïòîàíàëèòè÷åñêèõ ïðèåìîâ, êîòîðûå äî ñèõ ïîð çàñåêðå÷åíû, è ÿ íå çíàþ, êàêèå àëãîðèòìû ìîãóò áûòü âñêðûòû. Â Òàáë. 14.3 äëÿ ñðàâíåíèÿ ïðèâåäåíû âðåìåííûå ñîîòíîøåíèÿ äëÿ íåêîòîðûõ àëãîðèòìîâ.

Ìîé ëþáèìûé àëãîðèòì - IDEA. Åãî 128-áèòîâûé êëþ÷ â ñî÷åòàíèè ñ óñòîé÷èâîñòüþ ê îáùåèçâåñòíûì ñðåäñòâàì êðèïòîàíàëèçà - âîò èñòî÷íèê ìîåãî òåïëîãî è íåæíîãî ÷óâñòâà ê ýòîìó àëãîðèòìó. Ýòîò àëãîðèòì àíàëèçèðîâàëñÿ ðàçëè÷íûìè ãðóïïàìè, è íèêàêèõ ñåðüåçíûõ çàìå÷àíèé íå áûëî îïóáëèêîâàíî. Â îòñóòñòâèå íîâîñòåé êðèïòîàíàëèòè÷åñêèõ ïðîðûâîâ ÿ ñåãîäíÿ ñòàâëþ íà IDEA.

Òàáë. 14-3.
Ñêîðîñòè øèôðîâàíèÿ äëÿ íåêîòîðûõ áëî÷íûõ øèôðîâ íà i486SX/33 ÌÃö

Àëãîðèòì	Ñêîðîñòü øèôðîâàíèÿ (Êáàéò/ñ)	Àëãîðèòì	Ñêîðîñòü øèôðîâàíèÿ (Êáàéò/ñ)
Blowfish (12 ýòàïîâ)	182	MDC (ñ MD4)	186

Blowfish (16 ýòàï îâ)	135	MDC (ñ MD5)	135
Blowfish (20 ýòàï îâ)	110	MDC (ñ SHA)	23
DES	35	NewDES	233
FEAL-8	300	REDOC II	1
FEAL-16	161	REDOC III	78
FEAL-32	91	RC5-32/8	127
Ã Î ÑÒ	53	RC5-32/12	86
IDEA	70	RC5-32/16	65
Khufu (16 ýòàï îâ)	221	RC5-32/20	52
Khufu (24 ýòàï îâ)	153	SAFER (6 ýòàï îâ)	81
Khufu (32 ýòàï îâ)	115	SAFER (8 ýòàï îâ)	61
Luby-Rackoff (ñ MD4)	47	SAFER (10 ýòàï îâ)	49
Luby-Rackoff (ñ MD5)	34	SAFER (12 ýòàï îâ)	41
Luby-Rackoff (ñ SHA)	11	3-Way	25
Lucifer	52	Òðîéíîé DES	12