Ãëàâà 18
Îäíîíàïðàâëåííûå õýø-ôóíêöèè

18.1 Îñíîâû

Îäíîíàïðàâëåíàÿ ôóíêöèÿ $H(M)$ ïðåîáðàçóåò ê ñîîáùåíèþ ïðîèçâîëüíîé äëèíû M è âû÷èñëÿåò çíà÷åíèå ôèêñèðîâàííîé äëèíû h.

$h = H(M)$, ãäå h èìååò äëèíó m

Ìíîãèå ôóíêöèè ïîçâîëÿþò âû÷èñëÿòü çíà÷åíèå ôèêñèðîâàííîé äëèíû ïî âõîäíûì äàííûì ïðîèçâîëüíîé äëèíû, íî ó îäíîíàïðàâëåííûõ õýø-ôóíêöèé åñòü äîïîëíèòåëüíûå ñâîéñòâà, äåëàþùèå èõ îäíîíàïðàâëåííûìè [1065]:

Çíàÿ M, ëåãêî âû÷èñëèòü h.

Çíàÿ H, òðóäíî ïîäáåðåòü M, äëÿ êîòîðîãî $H(M)=h$.

Çíàÿ M, òðóäíî ïîäáåðåòü äðóãîå ñîîáùåíèå, M', äëÿ êîòîðîãî $H(M)= H(M')$.

Åñëè áû Ìýëîðè óìåë äåëàòü òðóäíûå âåùè, îí ñìîã áû ðàçðóøèòü áåçîïàñíîñòü ëþáîãî ïðîòîêîëà, èñïîëüçóþùåãî îäíîíàïðàâëåííóþ õýø-ôóíêöèþ. Ñìûñë îäíîíàïðàâëåííûõ õýø-ôóíêöèé è ñîñòîèò â îáåñïå÷åíèè äëÿ M óíèêàëüíîãî èäåíòèôèêàòîðà ("îòïå÷àòîê ïàëüöà"). Åñëè Àëèñà ïîäïèñàëà M ñ ïîìîùüþ äëîðèòìà öèôðîâîé ïîäïèñè íà áàçå $H(M)$, à Áîá ìîæåò ñîçäàòü M', äðóãîå ñîîáùåíèå, îòëè÷íîå îò M, äëÿ êîòîðîãî $H(M)= H(M')$, òî Áîá ñìîæåò óòâåðæäàòü, ÷òî Àëèñà ïîäïèñàëà M'.

Â íåêîòîðûõ ïðèëîæåíèÿõ îäíîíàïðàâëåííîñòè íåäîñòàòî÷íî, íåîáõîäèìî âûïîëíåíèå äðóãîãî òðåáîâàíèÿ, íàçûâàåìîãî **óñòîé÷èâîñòüþ ê ñòîëêíîâåíèÿì**.

Äîëãîå áûòü òðóäíî íàéòè âåùè, M è M', äëÿ êîòîðûõ $H(M)= H(M')$.

Ïîìíèòå âñêðûòèå ìåòîäîì äíÿ ðîæäåíèÿ èç ðàçäåëà 7.4? Îíî îñíîâàíî íà íàïèñàíèè äðóãîãî ñîîáùåíèÿ M', äëÿ êîòîðîãî $H(M)= H(M')$, à íà ïîèñêå äâóõ ñëó÷àéíûõ ñîîáùåíèé, M è M', äëÿ êîòîðûõ $H(M)= H(M')$.

Ñëåäóþùèé ïðîòîêîë, âïåðâûå îïèñàííûé Ãèäåîíîì Þâåëè (Gideon Yuval) [1635], ïîêàçûâàåò, êàê, åñëè ïðåäûäóùåé òðåáîâàíèå íå âûïîëíÿåòñÿ, Àëèñà ìîæåò èñïîëüçîâàòü âñêðûòèå ìåòîäîì äíÿ ðîæäåíèÿ äëÿ îáìåíà Áîáà.

(1) Àëèñà ãîòîâèò äâå âåðñèè êîíòðàêòà: îäíó, âûãîäíóþ äëÿ Áîáà, è äðóãóþ, ïðèâëåêàòåëüíóþ åãî ê áàíêðîòñòâó

(2) Àëèñà âíîñèò íåñêîëüêî èçìåíåíèé â êàæäóé äîêóìåíò è âû÷èñëÿåò õýø-ôóíêöèè. (Ýòè èçìåíåíèÿ ìîãóò áûòü äåéſòâèÿ, ïîäîáíûå ñëåäóþùèì: çàìåíà ÏÐÎÁÅËÀ êîìáèíàöèåé ÏÐÎÁÅË-ÇÀÁÎÉ-ÏÐÎÁÅË, âñòàâêà îäíîãî-äâóõ ïðîáåëîâ ïåðåä âîçâðàùî êàðåòêè, è ò.ä. Äåëàÿ èëè íå äåëàÿ ïî îäíîìó èçìåíåíèþ â êàæäîé èç 32 ñòðîê, Àëèñà ìîæåò ëåãêî ïîëó÷èòü 2^{32} ðàçëè÷íûõ äîêóìåíòîâ.)

(3) Àëèñà ñðàâíèâàåò õýø-çíà÷åíèÿ äëÿ êàæäîãî èçìåíåíèÿ â êàæäîì èç äâóõ äîêóìåíòîâ, ðàçûñêèâàÿ ïàðó, äëÿ êîòîðîé ýòè çíà÷åíèÿ ñîâïàäàþò. (Åñëè âûõîäîì õýø-ôóíêöèè ÿâëÿþòñÿ âñåãî ëèøü 64-ðàçðÿäíûå çíà÷åíèå, Àëèñà, êàê ïðåäïîë, ìîæåò íàéòè ñîâïàäàþùóþ ïàðó ñðàâíèâ 2^{32} åå âñòàâêàæäîãî äîêóìåíòà.) Îíà âîñïîëüçóåòñÿ äâà äîêóìåíòà, äàþùèõ îäèíàêîâûå õýø-çíà÷åíèÿ.

(4) Àëèñà ïîëó÷àåò ïîäïèñàííóþ Áîáîì âûãîäíóþ äëÿ íåãî âåðñèþ êîíòðàêòà, èñïîëüçóÿ ïðîòîêîë, â êîòîðîì îí ïîäïèñûâàåò òîëüêî õýø-çíà÷åíèå.

(5) Ñïóñòÿ íåêîòîðîå âðåìÿ Àëèñà ïîäìåíÿåò êîíòðàêò, ïîäïèñàííûé Áîáîì, äóãèì, êîòîðûé îí íå ïîäïèñûâàë. Òåïåðü îíà ìîæåò óáåäèòü àðáèòðà â òîì, ÷òî Áîá ïîäïèñàë äóãîé êîíòðàêò.

Ýòî çàìå÷àòåëüíî. (Îäíè èç ñîâåòîâ ÿâëÿþòñÿ âíåøíåå êîìòåñ÷åñêèõ èñïðàâëåíèé â ïîäïèñûâàåìûé äîêóìåíò.)

Ïðè âíèìàòåëüíîì àíàëèçå ìåòîäîâ äîêàçàòåëüſòâ ìåòîä ïðèâîäèò ê äóãèì ïðèìåíåíèÿì ìåòîäà ñïîñîáó âñêðûòèÿ. Íàïðèìåð, ïðîòîêîë ïîñûëàòü ñëó÷àéſûå ôîòîãðàôèè (ìîæåò áûòü ñïóſòèêîâîé) ñëó÷àéſûå ñòðîêè ñîâùåíèé ñî ſëó÷àéſûìè ſòðîêàìè ïîäïèſåé. Â êîíöå êîíöîâ ïîäïèſü ïîä îäíèì èç ýòèõ ſëó÷àéſûõ ſîâùåíèé îêàæåòſÿ ïðàêſè÷åſêè. Âðàã íå ſìîæåò óſíàòü, ê ſåìó ïðèâſåſſåò ýòà êîìàíäà, íî, åſëè åãî åäèſòâſåſſíîé öåëüſ ÿâëÿåòſÿ âìåſòàòåëüſòâî â ðàáſòó ſïóſíèêà, îſ ſâîſåſ äîáüſòſÿ.

Äëèſû îſſíîſïðàâſåſſûõ õýø-ôóſêöèé

64-áèòſâſå õýø-ôóſêöèè ſëèſêîſ ſàëû, ſòîáû ïðîòèâſſòſÿòü âſêðûòèþ ſåòſâſſ äſÿ ðſæåſíèÿ. Áſëåſ ïðàêòè÷ſſû îſſíîſïðàâſåſſûſ õýø-ôóſêöèè, âûäàþſùèſ 128-áèòſâſûſ õýø-çſà÷åſíèÿ. Ïðè ýòſ, ÷òſáû íàéòè äâà

äîêóìåíòà ñ îäèíàêîâûì õýø-çíà÷åíèåì, äëÿ âñêðûòèÿ ìåòîäîì äíÿ ðîæäåíèÿ ïðèäóìàíî 2^{64} ñëó÷àéíûõ äîêóìåíòîâ, ÷òî, âïðî÷åì, íåâîñòàòî÷íî, åñëè íóæíà äëèòåëüíàÿ áåçîïàñíîñòü. NIST â ñâîå Ñòàíäàðòå áåçîïàñíîãî õýøèðîâàíèÿ (Secure Hash Standard, SHS), èñïîëüçóåò 160-áèòîâîå õýø-çíà÷åíèå. Ýòî åùå ñëèøêîì óñëîæíÿåò âñêðûòèå ìåòîäîì äíÿ ðîæäåíèÿ, äëÿ êîòîðîãî ïîíàäîáèòñÿ 2^{80} õýøèðîâàíèé.

Äëÿ óäëèíåíèÿ õýí-çíà÷åíèé, âû äàâàì îäíî êîíêðåòíîé õýø-ôóíêöèå, áûë ïðåäëîæåí ñëåäóþùèé ìåòîä.

(1) Äëÿ ñîîáùåíèÿ ñ ïîìîùüþ îäíîé èç óïîìÿíóòûõ â ýòîé êíèãå îäíîíàïðàâëåííûõ õýø-ôóíêöèé ãåíåðèðóåòñÿ õýø-çíà÷åíèå.

(2) Õýø çíà÷åíèå äîáàâëÿåòñÿ ê ñîîáùåíèþ.

(3) Ãåíåðèðóåòñÿ õýø-çíà÷åíèå îáúåäèíåíèÿ ñîîáùåíèÿ è õýø-çíà÷åíèÿ ýòàïà (1).

(4) Ñîçäàåòñÿ áîëüøå õýø-çíà÷åíèå, ñîñòîÿùåå èç îáúåäèíåíèÿ õýø-çíà÷åíèÿ ýòàïà (1) è õýø-çíà÷åíèÿ ýòàïà (3).

(5) Ýòàïû (1)-(4) ïîâòîðÿþòñÿ íóæíîå êîëè÷åñòâî ðàç äëÿ îáåñïå÷åíèÿ òðåáóåìîé äëèíû õýø-çíà÷åíèÿ.

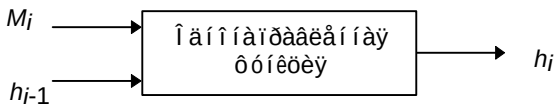
Õîòÿ íèêîãäà íå áûëà äîêàçàíà áåçîïàñíîñòü èëè íåáåçîïàñíîñòü ýòîãî ìåòîäà, óðÿä ëþäåé ýòî ìåòîä âûçûâàåò îïðåäåëåííûå ñîìíåíèÿ [1262,859].

Îáçîð îäíîíàïðàâëåííûõ õýø-ôóíêöèé

Íå ëåãêî ïîñòðîèòü ôóíêöèþ, âõîä êîòîðîé èìåò ïðèçâîëüíóþ ðàçìåð, à òàì áîëåå ñäåëàüòü åå îäíîíàïðàâëåííîé. Â ðåàëüíîì ìèðå îäíîíàïðàâëåííûå õýø-ôóíêöèè ñòðîÿòñÿ íà èäåå **ôóíêöèè ñæàòèÿ**. Òàêàÿ îäíîíàïðàâëåííàÿ ôóíêöèÿ âûäàåò õýø-çíà÷åíèå äëèíû *n* ïðè çàäàííûõ âõîäíûõ äàííûõ áîëüøåé äëèíû *m* [1069, 414]. Âõîäíàÿ ôóíêöèè ñæàòèÿ ÿâëÿþòñÿ áëîê ñîîáùåíèÿ è âûõîä ïðåäûäóùåãî áëîêà òåêñòà (ñì. 17-é). Âûõîä ïðåäñòàâëÿåò ñîáîé õýø-çíà÷åíèå âñåõ áëîêîâ äî ýòîãî ìîìåíòà. Òî åñòü, õýø-çíà÷åíèå áëîêà M_i ðàâíî

$h_i = f(M_i, h_{i-1})$

Ýòî õýø-çíà÷åíèå âìåñòå ñî ñëåäóþùèì áëîêîì ñîîáùåíèÿ ñòàíîâèòñÿ ñëåäóþùèì âõîäíûì ôóíêöèè ñæàòèÿ. Õýø-çíà÷åíèå âñåãî ñîîáùåíèÿ ÿâëÿåòñÿ õýø-çíà÷åíèå ïîñëåäíåãî áëîêà.



Ðèñ. 18-1. Îäíîíàïðàâëåííàÿ ôóíêöèÿ

Õýøèðóåìûé âõîä äîëæåí èàêèì-òî ñïîñîáîì ñîäåðæàòü áëàãîíå ïðåäñòàâëåíèå äëèíû âñåãî ñîîáùåíèÿ. Òàêèì îáðàçîì ïðåîáðàçîâàíèå ïîòåíöèàëüíàÿ ïðîáëåìà, âûçâàííàÿ òåì, ÷òî ñîîáùåíèÿ ðàçëè÷íîé äëèíû ìîãóò äàâàòü îäíî è òî æå õýø-çíà÷åíèå [1069, 414]. Èíîãäà òàêîé ìåòîä íàçûâàþòñÿ **MD-óñèëåíèåì** [930].

Ðàçëè÷íûå èñïîëüçîâàíèå ïðåäïîëîæåíèÿ, ÷òî åñëè ôóíêöèÿ ñæàòèÿ áåçîïàñíà, òî ýòîò ìåòîä õýøèðîâàíèÿ èñõîäíûõ äàííûõ ïðèçâîëüíîé äëèíû òàêæå áåçîïàñåí - íî íè÷åãî íå áûëî äîêàçàíî [1138, 1070, 414].

Íà òåì ïðîêòèðîâàíèÿ îäíîíàïðàâëåííûõ õýø-ôóíêöèé íàïèñàíî ìíîãî. Áîëåå ïîäðîáíóþ ìàòåìàòè÷åñêóþ èíôîðìàöèþ ìîæíî íàéòè [1028, 793, 791, 1138, 1069, 414, 91, 858, 1264]. Âîçìîæíî ñàìûì òîëêîâîé èíòåðïðåòàöèåé îäíîíàïðàâëåííûõ õýø-ôóíêöèé ÿâëÿþòñÿ òåçèñû Áàðòà Ïðåíåëà (Bart Preneel) [1262].

18.2 Snefru

Snefru - ýòî îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ, ðàçðàáîòàííàÿ Ðàëüôîì Ìåðêëåì [1070]. (Snefru, òàêæå êàê Khufu è Khafre, áûë åãèïåòñêèì ôàðàîíîì.) Snefru õýøèðóåò ñîîáùåíèÿ ïðîèçâîëüíîé äëèíû, ïðåâðàùàÿ èõ â 128-áèòîâûå 256-áèòîâûå çíà÷åíèÿ.

Ñíà÷àëà ñîáùåíèå ðàçáèâàåòñÿ íà êóñî÷êè äëèíîé ïî 512-*m*. (Ïåðåìåííàÿ *m* ÿâëÿåòñÿ äëèíîé õýø-çíà÷åíèÿ.) Åñëè âûõîä - ýòî 128-áèòîâîå çíà÷åíå, òî äëèíà êóñî÷êîâ ðàâíà 384 áèòàì, à åñëè âûõîä - 128-áèòîâîå çíà÷åíèå, òî äëèíà êóñî÷êîâ - 256 áèòîâ.

Ñåðäöåì àëãîðèòìà ñëóæèò ôóíêöèÿ H, õýøèðóþùàÿ 512-áèòîâîå çíà÷åíèå â *m*-áèòîâîå. Ïåðâûå *m* áèòîâ âûõîäà H ÿâëÿþòñÿ õýø-çíà÷åíèåì áëîêà, îòàëëíûå îòáðàñûâàþòñÿ. Ñëåäóþùèé áëîê äîáàâëÿåòñÿ ê õýø-çíà÷åíèþ ïðåäûäóùåãî áëîêà è ñíîâà õýøèðóåòñÿ. (Ê ïåðâîíà÷àëüíîìó áëîêó äîáàâëÿåòñÿ ñòðîêà íóëåé.) Ïîñëå ïîñëåäíåãî áëîêà (åñëè ñîîáùåíèå ñîñòîèò íå èç öåëîãî ÷èñëà áëîêîâ, ïîñëåäíåé áëîê äîïîëíÿåòñÿ íóëÿìè) ïåðâûå *m* áèòîâ äîáàâëÿþòñÿ ê áèòàðíîìó ïðåäñòàâëåíèþ äëèíû ñîîáùåíèÿ è õýøèðóþòñÿ ïîñëåäíèé ðàç.

Ôóíêöèÿ H îñíîâûâàåòñÿ íà E, îáðàòèìîé ôóíêöèè áëî÷íîãî øèôðîâàíèÿ, ðàáîòàþùåé ñ 512 áèòîâûìè

áëîêàìè. H - ýòî ïîñëåäíåå *m* áèòîâ âûõîäà E, îáúåäèíåííûå ïîñðåäñòâîì XOR ñ ïåðâûìè *m* áèòàìè âõîäà E.

Áåçîïàñíîñòü Snefru îïèðàåòñÿ íà ôóíêöèþ E, êîòîðàÿ ðàíäîìèçèðóåò äàííûå çà íåñêîëüêî ïðîõîäîâ. Êàæäûé ïðîõîä ñîñòîèò èç 64 ðàíäîìèçèðóþùèõ ýòàïîâ. Â êàæäîì ýòàïå â êà÷åñòâå âõîäà S-áëîêà èñïîëüçóåòñÿ äðóãîé áàéò äàííûõ. Âûõîäíûå ñëîâî ïîâåðõàåòñÿ îïåðàöèè XOR ñ äâóìÿ ñîñåäíèìè ñëîâàìè ñî ñäâèãîì. Ï î-ñòðîåíèå S-áëîêîâ àíàëîãè÷íî ïîñòðîåíèþ S-áëîêîâ â Khafre (ñì. ðàçäåë 13.7). Êðîìå òîãî, âûïîëíÿåòñÿ ðÿä öèêëè÷åñêèõ ñäâèãîâ. Îðèãèíàëüíûé Snefru ñîñòîÿë èç äâóõ ïðîõîäîâ.

Êðèïòîàíàëèç Snefru

Èñïîëüçóÿ äèôôåðåíöèàëüíûé êðèïòîàíàëèç, Áèõàì è Øàìèð ïîêàçàëè íåäåçïîñîáíîñòü äâóõïðîõîäíîãî Snefru (ñ 128-áèòîâûì õýø-çíà÷åíèåì) [172]. Èõ ñïîñîá âñêðûòèÿ çà íåñêîëüêî ìèíóò îáíàðóæèâàåò ïàðó ñîîáùåíèé ñ îäèíàêîâûì õýø-çíà÷åíèåì.

Äëÿ 128-áèòîâîãî Snefru èõ âñêðûòèÿ ðàáîòàþò ëó÷øå, ÷åì âñêðûòèå ãðóáîé ñèëîé äëÿ ÷åòûðåõ è ìåíåå ïðîõîäîâ. Âñêðûòèå Snefru ìåòîäîì äîñòèæåíèÿ òðåáóåò 2^{64} îïåðàöèé; äèôôåðåíöèàëüíûé êðèïòîàíàëèç ìîæåò íàéòè ïàðó ñîîáùåíèé ñ îäèíàêîâûì õýø-çíà÷åíèåì çà $2^{28.5}$ îïåðàöèé äëÿ òðåõïðîõîäíîãî Snefru è çà $2^{44.5}$ îïåðàöèé äëÿ ÷åòûðåõïðîõîäíîãî Snefru. Íàõîæäåíèå ñîîáùåíèÿ, õýø-çíà÷åíèå êîòîðîãî ñîâïàäàåò ñ çàäàííûì, ïðè èñïîëüçîâàíèè ãðóáîé ñèëû òðåáóåò 2^{128} îïåðàöèé, ïðè äèôôåðåíöèàëüíîì êðèïòîàíàëèçå äëÿ ýòîãî íóæíî 2^{56} îïåðàöèé äëÿ òðåõïðîõîäíîãî è 2^{88} îïåðàöèé äëÿ ÷åòûðåõïðîõîäíîãî Snefru.

Õîòÿ Áèõàì è Øàìèð íå àíàëèçèðîâàëè 256-áèòîâûå õýø-çíà÷åíèÿ, îíè ïðîâåëè àíàëèç âïëîòü äî 224-áèòîâûõ õýø-çíà÷åíèé. Â ñðàâíåíèè ñ âñêðûòèåì ìåòîäîì äíÿ ðîæäåíèÿ, òðåáóþùèì 2^{112} îïåðàöèé îíè ìîãóò íàéòè ñîîáùåíèÿ ñ îäèíàêîâûì õýø-çíà÷åíèåì çà $2^{12.5}$ îïåðàöèé äëÿ äâóõïðîõîäíîãî Snefru, çà 2^{33} îïåðàöèé äëÿ òðåõïðîõîäíîãî Snefru è çà äëÿ 2^{81} îïåðàöèé äëÿ ÷åòûðåõïðîõîäíîãî Snefru.

Â íàñòîÿùåå âðåìÿ Ìåðêë ðåêîìåíäóåò èñïîëüçîâàòü Snefru ïî êðàéíåé ìåðå ñ âîñåìüþ ïðîõîäàìè [1073]. Îäíàêî ñòàêè êîëè÷åñòâî ïðîõîäîâ äëãîðèòì ñòàíîâèòñÿ íàìíîãî ìåíüøå, ÷åì MD5 èëè SHA.

18.3 *N*-õýø

N-õýø - ýòî àëãîðèòì, ïðèäóìàííûé â 1990 ãîäó èññëåäîâàòåëÿìè Nippon Telephone and Telegraph, òåì è æå ëþäüìè, êîòîðûå èçîáðåëè FEAL [1105, 1106]. *N*-õýø èñïîëüçóåò 128-áèòîâûå áëîêè ñîîáùåíèÿ, ñëîæíóþ ðàñïèñêóþ ôóíêöèþ, ïîõîæóþ íà FEAL, è âûäàåò 128-áèòîâîå õýø-çíà÷åíèå.

Õýø-çíà÷åíèå êàæäîãî 128-áèòîâîãî áëîêà ÿâëÿåòñÿ ôóíêöèåé áëîêà è õýø-çíà÷åíèÿ ïðåäûäóùåãî áëîêà.

$H_0 = I$, ãäå I - ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå

$H_i = g(M_i, H_{i-1}) \oplus M_i \oplus H_{i-1}$

Õýø-çíà÷åíèå âñåãî ñîîáùåíèÿ ïðåäñòàâëÿåò ñîáîé õýø-çíà÷åíèå ïîñëåäíåãî áëîêà ñîîáùåíèÿ. Ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå I ìåæäó áûòü ëþáûì ÷èñëîì, îïðåäåëåííûì ïîëüçîâàòåëåì (äàæå îäèíàêîâûì).

Ôóíêöèÿ g äîñòàòî÷íî ñëîæíà. Ñõåìà àëãîðèòìà ïðèâåäåíà íà 16-é. Ñíà÷àëà ïåðåñòàâëÿþòñÿ ëåâàÿ è ïðàâàÿ 64-áèòîâûå ïîëîâèíû 128-áèòîâîãî õýø-çíà÷åíèÿ ïðåäûäóùåãî áëîêà H_{i-1}, à çàòåì âûïîëíÿåòñÿ XOR ñ ïîâòîðÿþùèìñÿ øàáëîííûì (128-áèòîâûì) è XOR ñ òåêóùèì áëîêîì ñîîáùåíèÿ M_i. Äàëåå ýòî çíà÷åíèå êàñêàäíî ïðåîáðàçóåòñÿ â N (íà ðèñóíêàõ N= 8) ñòàäèé îáðàáîòêè. Äðóãèì âõîäîì ñòàäèè îáðàáîòêè ÿâëÿåòñÿ ïðåäûäóùåå õýø-çíà÷åíèå, ïîâåðõóòîå XOR ñ îäíîé èç âîñüìè ââîäíûõ êîíñòàíò.

EXG: ïåðåñòàíîâêà ëåâîé è ïðàâîé ÷àñòåé

n: 1010 ... 1010 (äâîè÷íîå, 128 áèòîâ)

PS: ñòàäèÿ îáðàáîòêè (processing stage)

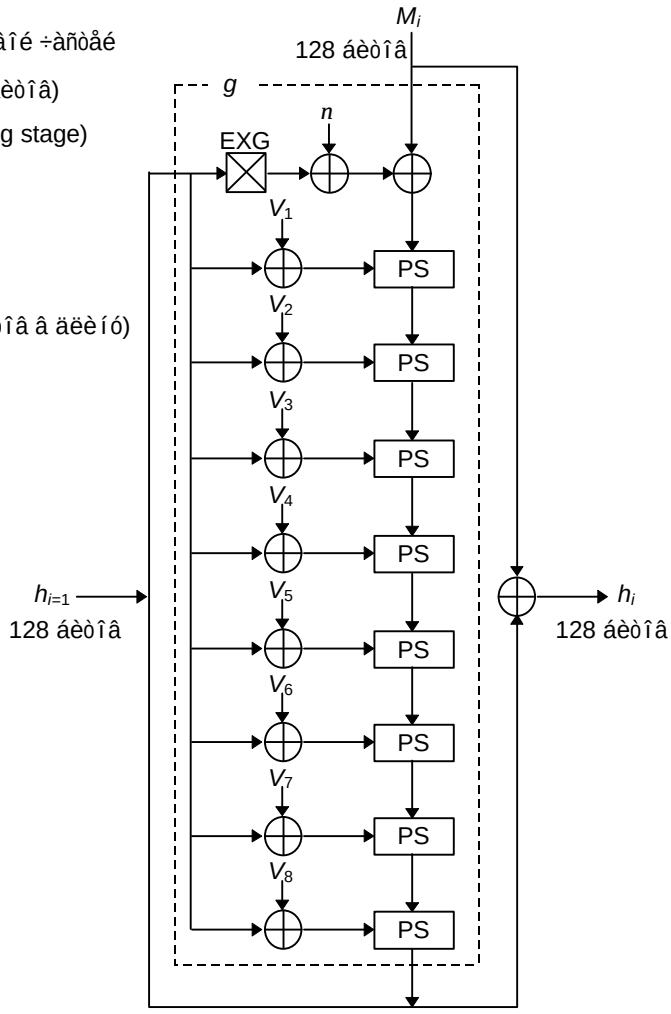
V_j=õ||A_{j1} õ||A_{j2} õ||A_{j3} õ||A_{j4}

||: êîíêàòåíàöèÿ

õ: 000 ... 0 (äâîè÷íîå, 24 áèò)

A_{jk}=4*(*j*-1)+*k*(*k*=1,2,3,4, A_{jk} - 8 áèòîâ â äëèíó)

$H_i = g(M_i, H_{i-1}) \oplus M_i \oplus H_{i-1}$

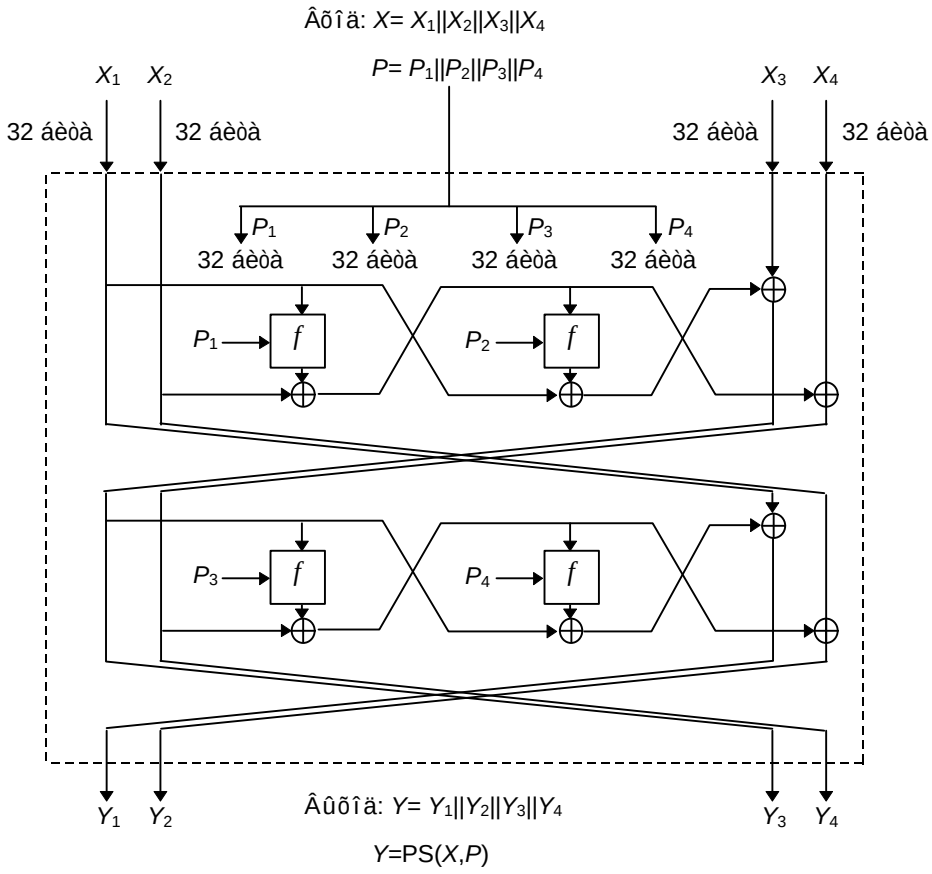


Ðèñ. 18-2. Ñõåìà *N*-õýø.

Îäíà ñòàäèÿ îáðàáîòêè ïîêàçàíà íà 15-é. Áëîê ñîîáùåíèÿ ðàçáèâàåòñÿ íà ÷åòûðå 32-áèòîâûõ çíà÷åíèÿ. Ïðåäûäóùåå õýø-çíà÷åíèå òàêæå ðàçáèâàåòñÿ íà ÷åòûðå 32-áèòîâûõ çíà÷åíèÿ. Ôóíêöèÿ f ïðåäñòàâëåíà íà 14th. Ôóíêöèè S_0 è S_1 òå æå ñàìûå, ÷òî è â FEAL.

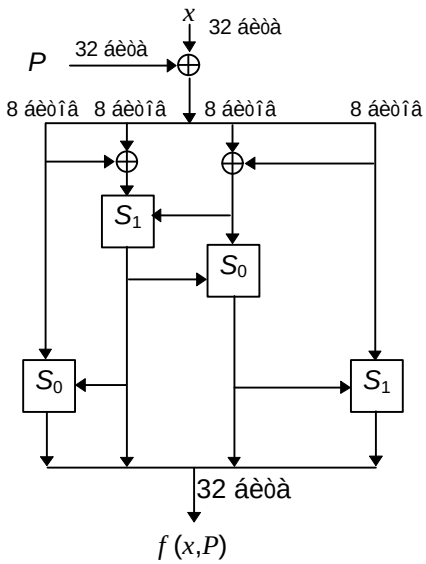
$S_0(a,b)$ = öèêëè÷åñêèé ñäâèã âëåâî íà äâà áèòà ((*a* + *b*) mod 256)

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



Ðèñ. 18-3. Îáùàÿ ñòàäèÿ îáðàáîòêè *N*-õýø.

Âûõîä îäíîé ñòàäèè îáðàáîòêè ñòàíîâèòñÿ âõîäîì ñëåäóþùåé ñòàäèè îáðàáîòêè. Ïîñëå ïîñëåäíåé ñòàäèè îáðàáîòêè âû ïîëíÿåòñÿ XOR âûõîäà ñ M_i è H_{i-1}, à çàòåì ê õýøèðîâàíèþ ãîòîâ ñëåäóþùèé áëîê.



Y=S_0(X_1,X_2)=Rot2((X_1+X_2) mod 256)
Y=S_1(X_1,X_2)=Rot2((X_1+X_2+1) mod 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. 18-4. Ôóíêöèÿ *f*.

Êðèïòîãðàôèç N-õýø

Áåðò äåí Áîåð (Bert den Boer) îòêðûë ñïîñîá ñîçäàâàòü ñòîéêèå ýòàïà *N*-õýø [1262]. Áèõàì è Øàìèð ïðèìåíèëè äèôôåðåíöèàëüíûé êðèïòîãðàôèç äëÿ âñêðûòèÿ 6-ýòàïíîé *N*-õýø [169, 172]. Êîíêðåòíûå âû÷èñëåíèÿ è ìåòîäû (êîíå÷íî æå, ìîãëè áûòü è äðóãèå) ðàáîòàþò äëÿ ëþáîãî *N*, äàëüøå îíè 3, è ýôôåêòèâíåå âñêðûòèÿ ìåòîäîì äíÿ ðîæäåíèÿ äëÿ ëþáîãî *N*, ìåíüøåãî 15.

Òî æå ñàìîå âñêðûòèå ìîæåò îáíàðóæèâàòü ïàðû ñîîáùåíèé ñ îäèíàêîâûì õýø-çíà÷åíèåì äëÿ 12-ýòàïíîé *N*-õýø çà 2^{56} îïåðàöèé (äëÿ âñêðûòèÿ ãðóáîé ñèëîé íóæíî 2^{64} îïåðàöèé). *N*-õýø ñ 15 ýòàïàìè áåçîïàñíà ïî îòíîøåíèþ ê äèôôåðåíöèàëüíîìó êðèïòàíàëèçó: äëÿ âñêðûòèÿ ïîòðåáóåòñÿ 2^{72} îïåðàöèé.

Ðàçðàáîò÷èêè àëãîðèòìà ðåêîìåíäóþò èñïîëüçîâàòü *N*-õýø íå ìåíüøå, ÷åì ñ 8 ýòàïàìè [1106]. Ñ ó÷åòîì äîêàçàííîé íåâîçìîæíîñòè *N*-õýø è FEAL (è åå ñêîðîñòè ïðè 8 ýòàïàõ) ÿ ðåêîìåíäóþ ïîëíîöüþ îòêàçàòüñÿ îò ýòîãî àëãîðèòìà.

18.4 MD4

MD4 - ýòî îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ, èçîáðåòåííàÿ Ðîíîì Ðèâåñòîì [1318, 1319, 1321]. MD îáîçíà÷àåò Message Digest (êðàòêîå èçëîæåíèå ñîîáùåíèÿ), àëãîðèòì äëÿ âû÷èñëåíèÿ ñîîáùåíèÿ âûäàåò 128-áèòîâîå õýø-çíà÷åíèå, èëè êðàòêîå èçëîæåíèå ñîîáùåíèÿ.

Â [1319] Ðèâåñò îïèñàë öåëè, ïðåñëåäóåìûå è ïðè ðàçðàáîòêå àëãîðèòìà:

Áåçîïàñíîñòü. Âû÷èñëèòåëüíî íåâîçìîæíî íàéòè äâà ñîîáùåíèÿ ñ îäèíàêîâûì õýø-çíà÷åíèåì. Âñêðûòèå ãðóáîé ñèëîé ÿâëÿåòñÿ ñàìûì ýôôåêòèâíûì.

Ïðîñòîòà ðåçîïàñíîñòü. Áåçîïàñíîñòü MD4 íå îñíîâûâàåòñÿ íà êàêèõ-ëèáî äîïóùåíèÿõ, íàïðèìåð, ïðåäïîëîæåíèè î òðóäíîñòè ðàçëîæåíèÿ íà ìíîæèòåëè.

Ñêîðîñòü. MD4 ïîäõîäèò äëÿ âûñîêîñêîðîñòíûõ ïðîãðàììíûõ ðåàëèçàöèé. Îíà îñíîâàíà íà ïðîñòûõ îïåðàöèÿõ íàä 32-áèòîâûìè îïåðàíäàìè.

Ïðîñòîòà è êîìïàêòíîñòü. MD4 ïðîñòà, íàñêîëüêî ýòî âîçìîæíà, è íå ñîäåðæèò áîëüøèõ òàáëèö ñòàíäàðòíûõ ïîäſàðàìíûõ ìîäóëåé.

Óäà÷íà àðõèòåêòóðà. MD4 îïòèìèçèðîâàíà äëÿ ìèêðîïðîöåññîðíîé àðõèòåêòóðû (îñíîâíîé äëÿ ìèêðîïðîöåññîðîâ Intel), äëÿ áîëåå ðóííûõ è áûñòðûõ êîìïüþòåðîâ ìîæíî âûïîëíèòü ëþáûå íåîáõîäèìûå èçìåíåíèÿ.

Ïîñëå ïåðâîãî ïîÿâëåíèÿ àëãîðèòìà Áåðò äåí Áîåð è Àíòîí Áîññåëàåðñ (Antoon Bosselaers) äîñòèãëè óñïåõà ïðè êðèïòîàíàëèçå ïîñëåäíèõ ââóõ èç òðåõ ýòàïîâ äëãîðèòìà [202]. Ðàëüô Ìåðêëó ñîâåðøåííî íåçàâèñèìî óäàëîñü âñêðûòü ïåðâûå äâà ýòàïà [202]. Ýëè Áèõàì ðàññìîòðåë èñîõîäíûå äèôôåðåíöèàëüíîãî êðèïòîàíàëèçà ïðîòèâ ïåðâûõ äâóõ ýòàïîâ MD4 [159]. Õîòÿ âñå ýòè âñêðûòèÿ íå áûëè ðàñïðîñòðàíåíû íà ïîëíóé äëãîðèòì, Ðèâåñò óñèëèë ñâîþ ðàçðàáîòêó. Â ðåçóëüòàòå ïîÿâèëàñü MD5.

18.5 MD5

MD5 - ýòî óëó÷øåííàÿ âåðñèÿ MD4 [1386, 1322]. Õîòÿ îíà ñëîæíåå MD4, èõ ñõåìû ïîõîæè, è ðåçóëüòàòîì MD5 òàêæå ÿâëÿåòñÿ 128-áèòîâîå õýø-çíà÷åíèå.

Îïèñàíèå MD5

Ïîñëå íåêîòîðîé ïðåäâàðèòåëüíîé îáðàáîòêè MD5 îáðàáàòûâàåò âõîäíîé òåêſò 512-áèòîâûìè áëîêàìè, ðàçáèòûìè íà 16 32-áèòîâûõ ïîäáëîêîâ. Âûõîäîì äëãîðèòìà ÿâëÿåòſñÿ íàáîð èç ÷åòûðåõ 32-áèòîâûõ áëîêîâ, êîòîðûå îáúåäèíÿþòſñÿ â äëèííîå 128-áèòîâîå õýø-çíà÷åíèå.

Âî ïðåâûõ, ñîîáùåíèå äîïîëíÿåòſñÿ òàê, ÷òîáû åãî äëèíà áûëà íà 64 áèòà êîðî÷å ÷èñëà, êðàòíîãî 512. Ýòè äîïîëíåíèÿ ÿâëÿåòſñÿ 1, çà êîòîðîé âïîòü äî êîíöà ñîîáùåíèÿ ñëåäóåò ñòîëüêî íóëåé, ñêîëüêî íóæíî. Çàòåì, ê ðåçóëüòàòó äîáàâëÿåòſñÿ 64-áèòîâîå ïðåäſòàâëåíèå äëèíû ñîîáùåíèÿ (èñòèííé, äî äîïîëíåíèÿ). Ýòè äâà äåéſòâèÿ ñëóæàò äëÿ òîãî, ÷òîáû äëèíà ſîîáùåíèÿ áûëà êðàòíà 512 áèòàì (÷òî òðåáóåòſñÿ äëÿ îſòàâøåéſñÿ ÷àſòè àëãîðèòìà), è ÷òîáû ãàðàíòèðîâàòü, ÷òî ðàçíûå ſîîáùåíèÿ íå áóäóò âûãëÿäåòü îäèíàêîâî ïîſëå äîïîëíåíèÿ. Èſïîëüçóþſñÿ ÷åòûðå ïðîſſòûå 32-áèòîâûå ſëîâà (ſòåïåíè äâîéſêè):

A = 0x01234567

B = 0x89abcdef

C = 0xfedcba98

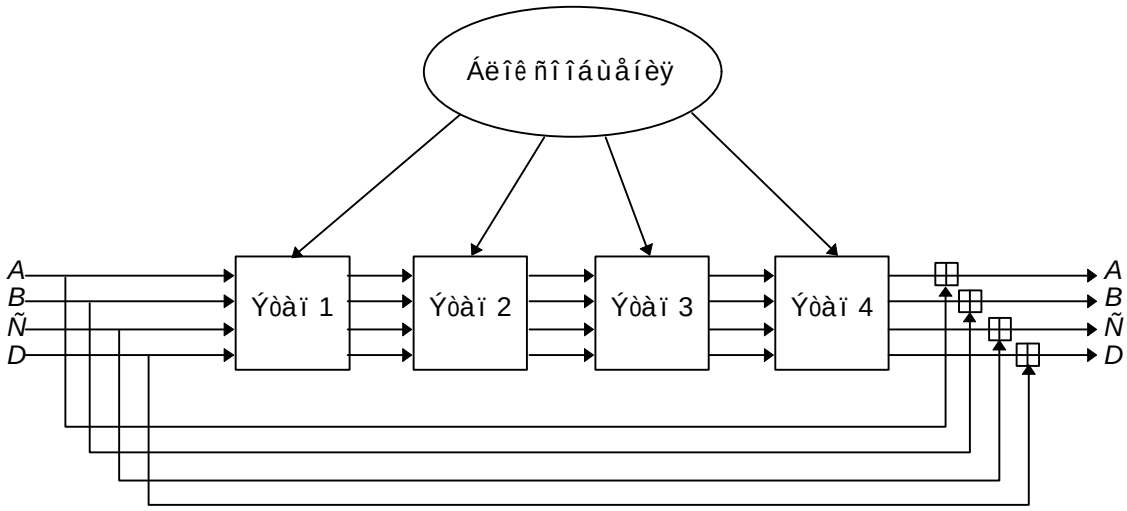
D = 0x76543210

Îſíè íàçûâàþſñÿ **ïåðâîíà÷àſëüſíûſìè ſöåïëåſíèſì**.

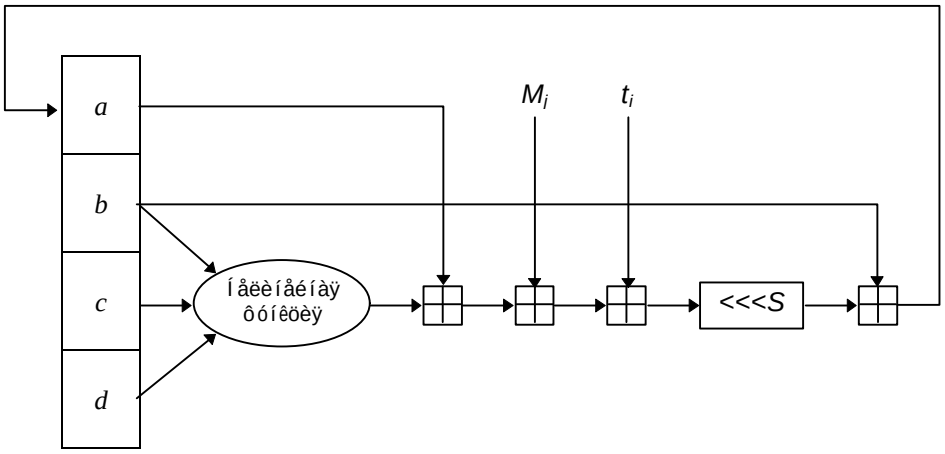
Òåïåðü ïåðåéäåì ê îñíîâíîìó öèêëó àëãîðèòìà. Ýòîò öèêë ïðîäîëæàåòñÿ, ïîêà íå èñ÷åðïàþòñÿ 512-áèòîâûå áëîêè ñîîáùåíèÿ.

×åòûðå ïåðåìåííûõ êîïèðóþòñÿ â äóãàêå ïåðåìåííûå: *A* â *a*, *B* â *b*, *C* â *c* è *D* â *d*.

Ãëàâíûé öèêë ñîñòîèò èç ÷åòûðåõ î÷åíü ïîõîæèõ ýòàïîâ (ó MD4 áûëî òîëüêî òðè ýòàïà). Íà êàæäîì ýòàïå 16 ðàç èñïîëüçóþòñÿ ðàçëè÷íûå îïåðàöèè. Êàæäàÿ îïåðàöèÿ ïðåäñòàâëÿåò ñîáîé íåëèíåéíóþ ôóíêöèþ íàä òðåìÿ èç *a*, *b*, *c* è *d*. Çàòåì îíà äîáàâëÿåò ýòîò ðåçóëüòàò ê ÷åòâåðòîé ïåðåìåííîé, ïîääëîêó òåêñòà è êîíñòàíòå. Äàëåå ðåçóëüòàò öèêëè÷åñêè ñäâèãàåòñÿ âïðàâî íà ïåðåìåííîå ÷èñëî áèòîâ è äîáàâëÿåò ðåçóëüòàò ê îäíîé èç ïåðåìåííûõ *a*, *b*, *c* è *d*. Íàêîíåö ðåçóëüòàò çàìåíÿåò îäíó èç ïåðåìåííûõ *a*, *b*, *c* è *d*. Ñì. 13-é è 12-é. Ñóùåñòâóþò ÷åòûðå íåëèíåéíûõ ôóíêöèè, èñïîëüçóåìûå ïî îäíîé â êàæäîé îïåðàöèè (äëÿ êàæäîãî ýòàïà - äðóãàÿ ôóíêöèÿ).



Ðèñ. 18-5. Ãëàâíûé öèêë MD5.



Ðèñ. 18-6. Îäíà îïåðàöèÿ MD5.

F(*X*,*Y*,*Z*) = (*X* ∧ *Y*) ∨ ((¬*X*) ∧ *Z*)

G(*X*,*Y*,*Z*) = (*X* ∧ *Z*) ∨ (*Y* ∧ (¬*Z*))

H(*X*,*Y*,*Z*) = *X* ⊕ *Y* ⊕ *Z*

I(*X*,*Y*,*Z*) = *Y* ⊕ (*X* ∨ (¬*Z*))

(⊕ - ýòî XOR, ∧ - AND, ∨ - OR, à ¬ - NOT.)

Ýòè ôóíêöèè ñïðîåêòèðîâàíû òàê, ÷òîáû, åñëè ñîîòâåòñòâóþùèå áèòû *X*, *Y* è *Z* íåçàâèñèìû è íåñìåùåíû, êàæäûé áèò ðåçóëüòàòà òàêæå áûë áû íåçàâèñèìûì è íåñìåùåííûì. Ôóíêöèÿ F - ýòî ïîáèòîâîå óñëîâèå: åñëè *X*, òî *Y*, èíà÷å *Z*. Ôóíêöèÿ H - ïîáèòîâàÿ îïåðàöèÿ ÷åòíîñòè.

Åñëè M_j îáîçíà÷àåò j-ûé ïîäáëîê ñîîáùåíèÿ (îò 0 äî 15), à <<<*s* îáîçíà÷àåò öèêëè÷åñêèé ñäâèã âëåâî íà *s*

áèòîâ, òî èñïîëüçóþòñÿ ñëåäóþ ùèå ÷åòûðå îïåðàöèè:

FF(a,b,c,d,M_j,s,t_i) îçíà÷àåò $a = b + ((a + F(b,c,d) + M_j + t_i) <<< s)$

GG(a,b,c,d,M_j,s,t_i) îçíà÷àåò $a = b + ((a + G(b,c,d) + M_j + t_i) <<< s)$

HH(a,b,c,d,M_j,s,t_i) îçíà÷àåò $a = b + ((a + H(b,c,d) + M_j + t_i) <<< s)$

II(a,b,c,d,M_j,s,t_i) îçíà÷àåò $a = b + ((a + I(b,c,d) + M_j + t_i) <<< s)$

×åòûðå ýòàïà (64 äåéñòâèÿ âûãëÿäÿò ñëåäóþ ùèì îáðàçîì):

Ýòàï 1:

FF(a, b, c, d, M_0, 7, 0xd76aa478)

FF(d, a, b, c, M_1, 12, 0xe8c7b756)

FF(c, d, a, b, M_2, 17, 0x242070db)

FF(b, c, d, a, M_3, 22, 0xc1bdceee)

FF(a, b, c, d, M_4, 7, 0xf57c0faf)

FF(d, a, b, c, M_5, 12, 0x4787c62a)

FF(c, d, a, b, M_6, 17, 0xa8304613)

FF(b, c, d, a, M_7, 22, 0xfd469501)

FF(a, b, c, d, M_8, 7, 0x698098d8)

FF(d, a, b, c, M_9, 12, 0x8b44f7af)

FF(c, d, a, b, M_{10}, 17, 0xffff5bb1)

FF(b, c, d, a, M_{11}, 22, 0x895cd7be)

FF(a, b, c, d, M_{12}, 7, 0x6b901122)

FF(d, a, b, c, M_{13}, 12, 0xfd987193)

FF(c, d, a, b, M_{14}, 17, 0xa679438e)

FF(b, c, d, a, M_{15}, 22, 0x49b40821)

Ýòàï 2:

GG(a, b, c, d, M_1, 5, 0xf61e2562)

GG(d, a, b, c, M_6, 9, 0xc040b340)

GG(c, d, a, b, M_{11}, 14, 0x265e5a51)

GG(b, c, d, a, M_0, 20, 0xe9b6c7aa)

GG(a, b, c, d, M_5, 5, 0xd62fl05d)

GG(d, a, b, c, M_{10}, 9, 0x02441453)

GG(c, d, a, b, M_{15}, 14, 0xd8ale681)

GG(b, c, d, a, M_4, 20, 0xe7d3fbc8)

GG(a, b, c, d, M_9, 5, 0x2,lelcde6)

GG(d, a, b, c, M_{14}, 9, 0xc33707d6)

GG(c, d, a, b, M_3, 14, 0xf4d50d87)

GG(b, c, d, a, M_8, 20, 0x455al4ed)

GG(a, b, c, d, M_{13}, 5, 0xa9e3e905)

GG(d, a, b, c, M_2, 9, 0xfcefa3f8)

GG(c, d, a, b, M_7, 14, 0x676f02d9)

GG(b, c, d, a, M_{12}, 20, 0x8d2a4c8a)

Ýòàï 3:

HH(*a*, *b*, *c*, *d*, M_5, 4, 0xfffa3942)

HH(*d*, *a*, *b*, *c*, M_8, 11, 0x8771f681)

HH(*c*, *d*, *a*, *b*, M_{11}, 16, 0x6d9d6122)

HH(*b*, *c*, *d*, *a*, M_{14}, 23, 0xfde5380c)

HH(*a*, *b*, *c*, *d*, M_1, 4, 0xa4beea44)

HH(*d*, *a*, *b*, *c*, M_4, 11, 0x4bdecfa9)

HH(*c*, *d*, *a*, *b*, M_7, 16, 0xf6bb4b60)

HH(*b*, *c*, *d*, *a*, M_{10}, 23, 0xbebfbc70)

HH(*a*, *b*, *c*, *d*, M_{13}, 4, 0x289b7ec6)

HH(*d*, *a*, *b*, *c*, M_0, 11, 0xeaa127fa)

HH(*c*, *d*, *a*, *b*, M_3, 16, 0xd4ef3085)

HH(*b*, *c*, *d*, *a*, M_6, 23, 0x04881d05)

HH(*a*, *b*, *c*, *d*, M_9, 4, 0xd9d4d039)

HH(*d*, *a*, *b*, *c*, M_{12}, 11, 0xe6db99e5)

HH(*c*, *d*, *a*, *b*, M_{15}, 16, 0x1fa27cf8)

HH(*b*, *c*, *d*, *a*, M_2, 23, 0xc4ac5665)

Ýòàï 4:

II(*a*, *b*, *c*, *d*, M_0, 6, 0xf4292244)

II(*d*, *a*, *b*, *c*, M_7, 10, 0x432aff97)

II(*c*, *d*, *a*, *b*, M_{14}, 15, 0xab9423a7)

II(*b*, *c*, *d*, *a*, M_5, 21, 0xfc93a039)

II(*a*, *b*, *c*, *d*, M_{12}, 6, 0x655b59c3)

II(*d*, *a*, *b*, *c*, M_3, 10, 0x8f0ccc92)

II(*c*, *d*, *a*, *b*, M_{10}, 15, 0xffeff47d)

II(*b*, *c*, *d*, *a*, M_1, 21, 0x85845ddl)

II(*a*, *b*, *c*, *d*, M_8, 6, 0x6fa87e4f)

II(*d*, *a*, *b*, *c*, M_{15}, 10, 0xfe2ce6e0)

II(*c*, *d*, *a*, *b*, M_6, 15, 0xa3014314)

II(*b*, *c*, *d*, *a*, M_{13}, 21, 0x4e081lal)

II(*a*, *b*, *c*, *d*, M_4, 6, 0xf7537e82)

II(*d*, *a*, *b*, *c*, M_{11}, 10, 0xbd3af235)

II(*c*, *d*, *a*, *b*, M_2, 15, 0x2ad7d2bb)

II(*b*, *c*, *d*, *a*, M_9, 21, 0xeb86d391)

Ýòè êîíñòàíòû, t_i, âû÷èñëåííûå ñëåäóþùèì îáðàçîì:

Íà *i*-îì ýòàïå t_i ÿâëÿåòñÿ öåëîé ÷àñòüþ 2^{32}*abs(sin(*i*)), ãäå *i* èçìåðÿåòñÿ â ðàäèàíàõ.

Ïîñëå âñåãî ýòîãî *a*, *b*, *c* è *d* äîáàâëÿþòñÿ ê *A*, *B*, *C* è *D*, ñîîòâåòñòâåííî, è àëãîðèòì ïðîäîëæàåòñÿ äëÿ ñëåäóþùåãî áëîêà äàííûõ. Îêîí÷àòåëüíûì ðåçóëüòàòîì ñëóæèò îáúåäèíåíèå *A*, *B*, *C* è *D*.

Áåçîïàñíîñòü MD5

Ðîí Ðèâåñò ïðèâåë ñëåäóþùèå óëó÷øåíèÿ MD5 â ñðàâíåíèè ñ MD4 [1322]:

1. Äîáàâëåíû ÷åòâåðòûé ýòàï.
2. Òåïåðü â êàæäîì äéñòâèè èñïîëüçóåòñÿ óíèêàëüíàÿ ïðèáàâëÿåìàÿ êîíñòàíòà.

3. Ôóíêöèÿ G íà ýòàïå 2 ñ $((X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z))$ áûëà èçìåíåíà íà $(X \wedge Z) \vee (Y \wedge (\neg Z))$, ÷òîáû ñäåëàòü G ìåíåå ñèìâîëüíî-íîé.

4. Òåïåðü êàæäîå äåéñòâèå äîáàâëÿåòñÿ ê ðåçóëüòàòó ïðåäûäóùåãî ýòàïà. Ýòî îáåñïå÷èâàåò áîëåå áûñòðûé ëàâèíîâé ýôôåêò.

5. Èçìåíèëñÿ ïîðÿäîê, â êîòîðîì èñïîëüçîâàëèñü ïîäáëîêè ñîîáùåíèÿ íà ýòàïàõ 2 è 3, ÷òîáû ñäåëàòü øàáëîíû ìåíåå ïîõîæèìè.

6. Çíà÷åíèÿ öèêëè÷åñêîãî ñäâèãà âëåâî íà êàæäîì ýòàïå áûëè ïðèáëèæåíû îïòèìèçèðîâàíû äëÿ óñêîðåíèÿ ëàâèíîãî ýôôåêòà. ×åòûðå ñäâèãà, èñïîëüçóåìûå íà êàæäîì ýòàïå, îòëè÷àþòñÿ îò çíà÷åíèé, èñïîëüçóåìûõ íà äóãèõ ýòàïàõ.

Òîì Áåðñîí (Tom Berson) ïîïûòàëñÿ ïðèìåíèòü äèôôåðåíöèàëüíûé êðèïòîàíàëèç ê îäíîìó ýòàïó MD5 [144], íî âñê âñêðûòèå íå îêàçàëîñü ýôôåêòèâíûì íè äëÿ îäíîãî èç ÷åòûðåõ ýòàïîâ. Áîëåå óñïåøíûå âñêðûòèå äåí Áîðäà è Áîññåëäåðà, èñïîëüçóþùåå ôóíêöèþ ñæàòèÿ, ïðèâåëî ê îáíàðóæåíèþ ñòîëêíîâåíèé â MD5 [203, 1331, 1336]. Ñàìî ïî ñåáå ýòî âñêðûòèå íåâîçìîæíî äëÿ âñêðûòèÿ MD5 â ïðàêòè÷åñêîé äëÿ âëèÿíèÿ MD5 â ïðîãðàììàõ øèôðîâàíèÿ, ïîäîáíûõ Luby-Rackoff (ñì. ðàçäåë 14.11). Óñïåõ ýòîãî âñêðûòèÿ îçíà÷àåò òîëüêî, ÷òî îäíà èç ñíîâíûõ öåëåé ïðîåêòèðîâàíèÿ MD5- ñîçäàòü óñòîé÷èâóþ ê ñòîëêíîâåíèÿì ôóíêöèþ ñæàòèÿ - íå áûëà äîñòèãíóòà. Õîòÿ ñïðàâåäëèâî, ÷òî "êàæåòñÿ, ÷òî ó ôóíêöèè ñæàòèÿ åñòü ñëàáûå ìåñòî, íî ýòî ïðàêòè÷åñêè íå âëèÿåò íà áåçîïàñíîñòü õýø-ôóíêöèè " [1336], ÿ îòíîñóñü ê èñïîëüçîâàíèþ MD5 î÷åíü îñòîðîæíî.

18.6 MD2

MD2 - ýòî äðóãàÿ 128-áèòîâàÿ îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ, ðàçðàáîòàííàÿ Ðîíîì Ðèâåñòîì [801, 1335]. Î íà, â ìåíüøå ñ MD5, èñïîëüçóåòñÿ â ïðîòîêîëàõ PEM (ñì. ðàçäåë 24.10). Áåçîïàñíîñòü MD2 îïèðàåòñÿ íà ñëó÷àéíóþ ïåðåñòàíîâêó áàéòîâ. Ýòà ïåðåñòàíîâêà ôèêñèðîâàíà è çàâèñèò îò ðàçðÿäîâ π. S_0, S_1, S_2, . . . , S_{255} è ÿâëÿþòñÿ ïåðåñòàíîâêîé. ×òîáû âû÷èñëèòü õýø-êîä äëÿ ñîîáùåíèÿ M:

(1) Äîïîëíèòå ñîîáùåíèå i áàéòàìè, çíà÷åíèå i äîëæíî áûòü òàêèì, ÷òîáû äëèíà ïîëó÷åííîãî ñîîáùåíèÿ áûëà êðàòíà 16 áàéòàì.

(2) Äîáàâüòå ê ñîîáùåíèþ 16 áàéòîâ êîíòðîëüíîé ñóììû.

(3) Ïðîèíèöèàëèçèðóéòå 48-áàéòîâûé áëîê: X_0, X_1, X_2, . . ., X_{47}. Çàïîëíèòå ïåðâûå 16 áàéòîâ X íóëÿìè, âî âòîðûå 16 áàéòîâ X ñêîïèðóéòå ïåðâûå 16 áàéòîâ ñîîáùåíèÿ, à òðåòüè 16 áàéòîâ X äîëæíû áûòü ðàâíû XOR ïåðâûõ è âòîðûõ 16 áàéòîâ X.

(4) Âîò êàê âû÷èñëÿåò ôóíêöèÿ ñæàòèÿ:

$t = 0$

For $j = 0$ to 17

For $k = 0$ to 47

$t = X_t$ XOR S_t

$X_k = t$

$t = (t + j)$ mod 256

(5) Ñêîïèðóéòå âî âòîðûå 16 áàéòîâ X âòîðûå 16 áàéòîâ ñîîáùåíèÿ, à òðåòüè 16 áàéòîâ X äîëæíû áûòü ðàâíû XOR ïåðâûõ è âòîðûõ 16 áàéòîâ X. Âû÷èñëèòå ýòàï (4). Ïîâòîðÿéòå ýòàïû (5) è (4) ïî î÷åðåäè äëÿ êàæäûõ 16 áàéòîâ ñîîáùåíèÿ.

(6) Âûõîäîì ÿâëÿþòñÿ ïåðâûå 16 áàéòîâ X.

Õîòÿ â MD2 ïîêà íå áûëî íàéäåíî ñëàáûõ ìåñò (ñì. [1262]), îíà ðàáîòàåò ìåäëåííåå áîëüøèíñòâà äðóãèõ ïðåäëîæåííûõ õýø-ôóíêöèé.

18.7 Àëãîðèòì áåçîïàñíîãî õýøèðîâàíèÿ (Secure Hash Algorithm, SHA)

NIST, â ìåñòå ñ NSA, äëÿ Ñòàíäàðòà öèôðîâîé ïîäïèñè (Digital Signature Standard, ñì. Ðàçäåë 20.2) ðàçðàáîòàë Àëãîðèòì áåçîïàñíîãî õýøèðîâàíèÿ (Secure Hash Algorithm, SHA) [1154 (Digital Signature Standard]. (Ñàì ñòàíäàðò íàçûâàåòñÿ Ñòàíäàðò áåçîïàñíîãî õýøèðîâàíèÿ (Secure Hash Standard, SHS), à SHA - ýòî äëãîðèòì, èñïîëüçóåìûé â ñòàíäàðòå.) Â ñîîòâåòñòâèè ñ *Federal Register* [539]:

> Ïðåäëàãàåòñÿ Ôåäåðàëüíûé ñòàíäàðò îáðàáîòêè èíôîðìàöèè (Federal Information Processing Standard, FIPS) äëÿ Ñòàíäàðòà áåçîïàñíîãî õýøèðîâàíèÿ (Secure Hash Standard, SHS). Ýòîò ïðåäëîæåííûé îïðåäåëÿåò Àëãîðèòì áåçîïàñíîãî õýøèðîâàíèÿ (Secure Hash Algorithm, SHA) äëÿ èñïîëüçîâàíèÿ âìåñòå ñî Ñòàíäàðòîì öèôðîâîé ïîäïèñè (Digital Signature Standard) . . ..

Êðîìå òîãî, äëÿ ïðèëîæåíèé, â êîòîðûõ íå òðåáóåòñÿ öèôðîâàÿ ïîäïèñü, SHA äîëæåí èñïîëüçîâàòüñÿ âî âñåõ Ôåäåðàëüíûõ ïðèëîæåíèÿõ, â êîòîðûõ ïîíàäîáèòñÿ àëãîðèòì áåçîïàñíîãî õýøèðîâàíèÿ.

È

Ýòîò Ñòàíäàðò îïðåäåëÿåò Àëãîðèòì áåçîïàñíîãî õýøèðîâàíèÿ (Secure Hash Algorithm, SHA), íåîáõîäèìûé äëÿ îáåñïå÷åíèÿ áåçîïàñíîñòè Àëãîðèòìà öèôðîâîé ïîäïèñè (Digital Signature Algorithm, DSA). Äëÿ ëþáîãî âõîäíîãî ñîîáùåíèÿ äëèíîé ìåíüøå 2^{64} áèòîâ SHA âûäàåò 160-áèòîâûé ðåçóëüòàò, íàçûâàåìûé êðàòêèì ñîäåðæàíèåì ñîîáùåíèÿ. Äàëåå, êðàòêîå ñîäåðæàíèå ñîîáùåíèÿ ñòàíîâèòñÿ âõîäîì DSA, êîòîðûé âû÷èñëÿåò ïîäïèñü äëÿ ñîîáùåíèÿ. Ïîäïèñûâàíèå êðàòêîãî ñîäåðæàíèÿ âìåñòî âñåãî ñîîáùåíèÿ ÷àñòî ïîâûøàåò ýôôåêòèâíîñòü ïðîöåññà, òàê êàê êðàòêîå ñîäåðæàíèå ñîîáùåíèÿ íàìíîãî ìåíüøå, ÷åì ñàìî ñîîáùåíèå. Òî æå êðàòêîå ñîäåðæàíèå ñîîáùåíèÿ äîëæíî áûòü ïîëó÷åíî òåì, êòî ïðîâåðÿåò ïîäïèñü, åñëè ïðèíÿòàÿ èì âåðñèÿ ñîîáùåíèÿ èñïîëüçóåòñÿ â êà÷åñòâå âõîäà SHA. SHA íàçûâàåòñÿ áåçîïàñíûì, òàê êàê îí ðàçðàáîòàí òàê, ÷òîáû áûëî âû÷èñëèòåëüíî íåâîçìîæíî íàéòè ñîîáùåíèå, ñîîòâåòñòâóþùåå äàííîìó êðàòêîìó ñîäåðæàíèþ ñîîáùåíèÿ èëè íàéòè äâà ðàçëè÷íûõ ñîîáùåíèÿ ñ îäèíàêîâûì êðàòêèì ñîäåðæàíèåì ñîîáùåíèÿ. Ëþáûå èçìåíåíèÿ, ïðîèçîøåäøèå ïðè ïåðåäà÷å ñîîáùåíèÿ, ñ î÷åíü âûñîêîé âåðîÿòíîñòüþ ïðèâåäóò ê èçìåíåíèþ êðàòêîãî ñîäåðæàíèÿ ñîîáùåíèÿ, è ïîäïèñü íå ïðîéäåò ïðîâåðêó. Ïðèíöèïû, ëåæàùèå â îñíîâå SHA, àíàëîãè÷íû èñïîëüçîâàííûì ïðîôåññîðîì Ðîíàëüäîì Ë. Ðèâåñòîì èç MIT ïðè ïðîåêòèðîâàíèè àëãîðèòìà êðàòêîãî ñîäåðæàíèÿ ñîîáùåíèÿ MD4 [1319]. SHA ðàçðàáîòàí ïî îáðàçöó óïîìÿíóòîãî àëãîðèòìà.

SHA âûäàåò 160-áèòîâîå õýø-çíà÷åíèå, áîëåå äëèííîå, ÷åì ó MD5.

Îïèñàíèå SHA

Âî ïåðâûõ, ñîîáùåíèå äîïîëíÿåòñÿ, ÷òîáû åãî äëèíà áûëà êðàòíîé 512 áèòàì. Èñïîëüçóåòñÿ òî æå äîïîëíåíèå, ÷òî è â MD5: ñíà÷àëà äîáàâëÿåòñÿ 1, à çàòåì íóëè òàê, ÷òîáû äëèíà ïîëó÷åííîãî ñîîáùåíèÿ áûëà íà 64 áèòà ìåíüøå ÷èñëà, êðàòíîãî 512, à çàòåì äîáàâëÿåòñÿ 64-áèòîâîå ïðåäñòàâëåíèå äëèíû îðèãèíàëüíîãî ñîîáùåíèÿ.

Èíèöèàëèçèðóþòñÿ ïÿòü 32-áèòîâûõ ïåðåìåííûõ (â MD5 èñïîëüçóåòñÿ ÷åòûðå ïåðåìåííûõ, íî ðàññìàòðèâàåìûé àëãîðèòì äîëæåí âûäàâàòü 160-áèòîâîå õýø-çíà÷åíèå):

A = 0x67452301

B = 0xefcdab89

C = 0x98badcfe

D = 0x10325476

E = 0xc3d2e1fO

Çàòåì íà÷èíàåòñÿ ãëàâíûé öèêë àëãîðèòìà. Îí îáðàáàòûâàåò ñîîáùåíèå 512-áèòîâûìè áëîêàìè è ïðîäîëæàåòñÿ, ïîêà íå èñ÷åðïàþòñÿ âñå áëîêè ñîîáùåíèÿ.

Ñíà÷àëà ïÿòü ïåðåìåííûõ êîïèðóþòñÿ â äðóãèå ïåðåìåííûå: A â a, B â b, C â c, D â d è E â e.

Ãëàâíûé öèêë ñîñòîèò èç ÷åòûðåõ ýòàïîâ ïî 20 îïåðàöèé â êàæäîì (â MD5 ÷åòûðå ýòàïà ïî 16 îïåðàöèé â êàæäîì). Êàæäàÿ îïåðàöèÿ ïðåäñòàâëÿåò ñîáîé íåëèíåéíóþ ôóíêöèþ íàä òðåìÿ èç a, b, c, d è e, à çàòåì âûïîëíÿåò ñäâèã è ñëîæåíèå àíàëîãè÷íî MD5. Â SHA èñïîëüçóåòñÿ ñëåäóþùèé íàáîð íåëèíåéíûõ ôóíêöèé:

$f_t(X,Y,Z) = (X \wedge Y) \vee ((\neg X) \wedge Z)$, äëÿ t=0 äî 19

$f_t(X,Y,Z) = X \oplus Y \oplus Z$, äëÿ t=20 äî 39

$f_t(X,Y,Z) = (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z)$, äëÿ t=40 äî 59

$f_t(X,Y,Z) = X \oplus Y \oplus Z$, äëÿ t=60 äî 79

â àëãîðèòìå èñïîëüçóþòñÿ ñëåäóþùèå ÷åòûðå êîíñòàíòû:

K_t = 0x5a827999, äëÿ t=0 äî 19

K_t = 0x6ed9eba1 , äëÿ t=20 äî 39

K_t = 0x8flbbcdc, äëÿ t=40 äî 59

K_t = 0xca62c1d6, äëÿ t=60 äî 79

(Åñëè èíòåðåñíî, êàê ïîëó÷åíû ýòè ÷èñëà, òî:0x5a827999 = $2^{1/2}/4$, 0x6ed9eba1 = $3^{1/2}/4$, 0x8flbbcdc = $5^{1/2}/4$, 0xca62c1d6 = $10^{1/2}/4$.)

Áëîê ñîîáùåíèÿ ïðåîáðàçóåòñÿ èç 16 32-áèòîâûõ ñëîâ (M_0 ïî M_{15}) â 80 32-áèòîâûõ ñëîâ (W_0 ïî W_{79}) ñ ïîìîùüþ ñëåäóþùåãî àëãîðèòìà:

$W_t = M_t$, äëÿ t = 0 ïî 15

$W_t = (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) \lll 1$, äëÿ t = 16 ïî 79

(Â êà÷åñòâå èíòåðåñíîãî çàìå÷àíèÿ, â ïåðâîíà÷àëüíîé ñïåöèôèêàöèè SHA íå áûëî öèêëè÷åñêîãî ñäâèãà âëå-

âî. Èçìåíåíèå "èñïðàâëåíèå îøèáêè èçúÿí, êîòîðûé äåëàë ñòàíäàðò ìåíåå áåçîïàñíûì, ÷åì ïðåäïîëàãàëîñü" 1543]. NSA îòêàçàëîñü óòî÷íèòü èñòîíóþ ïðè÷èíó èçúÿíà.)

Åñëè *t* - ýòî íîìåð îïåðàöèè (îò 1 äî 80), W_t ïðåäñòàâëÿåò ñîáîé *t*-ûé ïîäáëîê ðàñøèðåííîãî ñîîáùåíèÿ, à <<<*s* - ýòî öèêëè÷åñêèé ñäâèã âëåâî íà *s* áèòîâ, òî ãäåâíûé öèêë âûãëÿäèò ñëåäóþùèì îáðàçîì:

FOR *t* = 0 to 79

$TEMP = (a \lll 5) + f_t(b,c,d) + e + W_t + K_t$

$e = d$

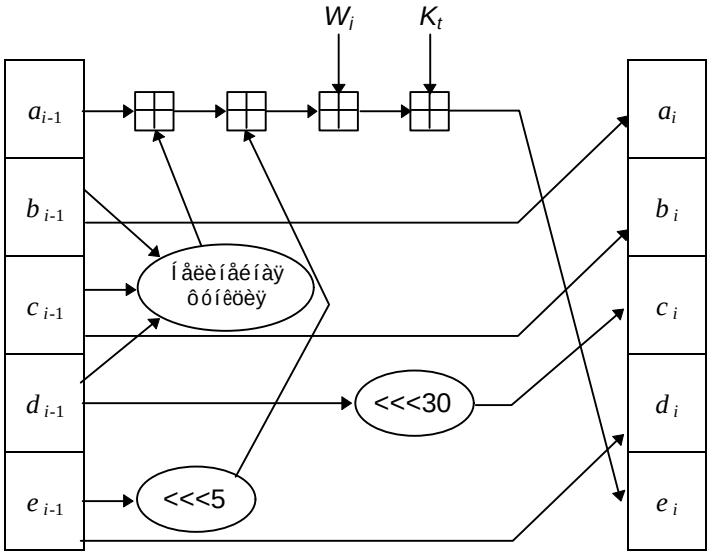
$d = c$

$c = b \lll 30$

$b = a$

$a = TEMP$

Íà 11-é ïîêàçàíà îäíà îïåðàöèÿ. Ñäâèã ïåðåìåííûõ âûïîëíÿåò òó æå ôóíêöèþ, êîòîðóþ â MD5 âûïîëíÿåò èñïîëüçîâàíèå â ðàçëè÷íûõ ìåñòàõ ðàçëè÷íûõ ïåðåìåííûõ.



Ðèñ. 18-7. Îäíà îïåðàöèÿ SHA.

Ïîñëå âñåãî ýòîãî *a*, *b*, *c*, *d* è *e* äîáàâëÿþòñÿ ê *A*, *B*, *C D* è *E*, ñîîòâåòñòâåííî, è àëãîðèòì ïðîäîëæàåòñÿ äëÿ ñëåäóþùåãî áëîêà äàííûõ. Îêîí÷àòåëüíûì ðåçóëüòàòîì ñëóæèò îáúåäèíåíèå *A*, *B*, *C D* è *E*.

Áåçîïàñíîñòü SHA

SHA î÷åíü ïîõîæà íà MD4, íî âûäàåò 160-áèòîâîå õýø-çíà÷åíèå. Ãëàâíûì èçìåíåíèåì ÿâëÿþòñÿ ââåäåíèå äàííîñòè ïðåäñòàâëåíèÿ è äîáàâëåíèå âûõîäà ïðåûäóùåãî øàãà â ñëåäóþùèé ñ öåëüþ ïîëó÷åíèÿ áîëåå áûñòðîãî ëàâèíîãî ýôôåêòà. Ðîí Ðèâåñò îïóáëèêîâàë öåëè, ïðåñëåäóåìûå èì ïðè ïðîåêòèðîâàíèè MD5, íî ðàçðàáîò÷èêè SHA ýòîãî íå ñäåëàëè. Âîò óëó÷øåíèÿ, âíåñåííûå Ðèâåñòîì â MD5 îòíîñèòåëüíî MD4, è èõ ñðàâíåíèå ñ SHA:

1. "Äîáàâëåíî ÷åòâåðòûé ýòàï." Â SHA òîæå. Îäíàêî â SHA íà ÷åòâåðòîì ýòàïå èñïîëüçóåòñÿ òà æå ôóíêöèÿ f, ÷òî è íà âòîðîì ýòàïå.
2. "Òåïåðü â êàæäîì äåñòâèè èñïîëüçóåòñÿ óíèêàëüíàÿ ïðèáàâëÿåìàÿ êîíñòàíòà." SHA ïðèâåðæåíà ñòåïåíè MD4, ïîâòîðíî èñïîëüçóÿ êîíñòàíòû äëÿ êàæäîé ãðóïïû èõ 20 ýòàïîâ.
3. "Ôóíêöèÿ G íà ýòàïå 2 ñ $((X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z))$ áûëà èçìåíåíà íà $(X \wedge Z) \vee (Y \wedge (\neg Z))$, ÷òîáû ñäåëàòü G ìåíåå ñèììåòðè÷íîé." Â SHA èñïîëüçóåòñÿ âåðñèÿ ôóíêöèè èç MD4: $(X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z)$.
4. "Òåïåðü êàæäîå äéñòâèå äîáàâëÿåòñÿ êðåçóëüòàòó ïðåäûäóùåãî ýòàïà. Ýòî îáåñïå÷èâàåò áîëåå áûñòðûé ëàâèíîâû ýôôåêò." Ýòî èçìåíåíèå áûëî âíåñåíî è â SHA. Îòëè÷èå ñîñòîèò â òîì, ÷òî â SHA äîáàâëåíà ïÿòàÿ ïåðåìåííàÿ ê *b*, *c* è *d*, êîòîðûå óæå èñïîëüçóþòñÿ â f_t. Ýòî íåçíà÷èòåëüíîå èçìåíåíèå äåëàò ïðèìåíåíèÿ âñêðûòèÿ MD5 äâî Âîðî è Áîññåëäåðîì íåâîçìîæíû ïî îòíîøåíèþ ê SHA.
5. "Èçìåíåíèÿ ïðÿìîé, â êîòîðîì èñïîëüçîâàëèñü ïîäëîêè ñîîáùåíèÿ íà ýòàïàõ 2 è 3, ÷òîáû ñäåëàòü

øàáëîíû ìåíåå ïîõîæèì." SHA â ýòîì ìåñòå ñîâðøåííî îòëè÷àþòñÿ, òàê êàê èñïîëüçóåò öèêëè÷åñêèé êîä èñïðàâëåíèÿ îøèáîê.

6. "Çíà÷åíèÿ öèêëè÷åñêîãî ñäâèãà âëåâî íà êàæäîì ýòàïå áûëè ïðèáëèçèòåëüíî îïòèìèçèðîâàíû äëÿ óñêîðåíèÿ ëàâèííîãî ýôôåêòà. ×åòûðå ñäâèãà, èñïîëüçóåìûå íà êàæäîì ýòàïå, îòëè÷àþòñÿ îò çíà÷åíèé, èñïîëüçóåìûõ íà äóãîì ýòàïàõ." SHA íà êàæäîì ýòàïå èñïîëüçóåò ïîñòîÿííûå çíà÷åíèå ñäâèãà. Ýòî çíà÷åíèå - âçàèìíî ïðîñòîå ÷èñëî ñ ðàçìåðîì ñëîâà, êàê è â MD4.

Ýòî ïðèâîäèò ê ñëåäóþùåìó çàêëþ÷åíèþ: SHA - ýòî MD4 ñ äîáàâëåíèåì ðàñøèðåííîãî ýòàïà è óëó÷øåííûì ëàâèííûì ýôôåêòîì. MD5 - ýòî MD4 ñ óëó÷øåííûì áèòîâûì õýøèðîâàíèåì, äîïîëíèòåëüíûì ýòàïîì è óëó÷øåííûì ëàâèííûì ýôôåêòîì.

Ñâåäåíèÿ îá óñïåøíûõ êðèïòîãðàôè÷åñêèõ âñêðûòèÿõ SHA îòñóòñòâóþò. Òàê êàê ýòà îäíîíàïðàâëåííàÿ õýøôóíêöèÿ âûäàåò 160-õýø-çíà÷åíèå, îíà óñòîé÷èâà ê âñêðûòèþ ãðóáîé ñèëîé (âêëþ÷àÿ âñêðûòèå ìåòîäîì äíÿ ðîæäåíèÿ), ÷åì 128-áèòîâûå õýø-ôóíêöèè, ðàññìàòðèâàåìûå â ýòîé ãëàâå.

18.8 RIPE-MD

RIPE-MD áûëà ðàçðàáîòàíà äëÿ ïðîåêòà RIPE Åâðîïåéñêîãî ñîîáùåñòâà [1305] (ñì. ðàçäåë 25.7). Ýòî àëãîðèòì ïðåäñòàâëÿåò ñîáîé âàðèàíò MD4, ðàçðàáîòàííûé òàê, ÷òîáû ïðîòèâîñòîÿòü èçâåñòíûì ìåòîäàì êðèïòîãðàôè÷åñêîãî âñêðûòèÿ, è âûäàåò 128-áèòîâîå õýø-çíà÷åíèå. Âíåøíå èçìåíåíèÿ â öèêëè÷åñêèå ñäâèãè ïðÿìî ïðîòèâîïîëîæíû ñäâèãàì, îòëè÷àþùèìñÿ êîíñòàíòàìè. Ïîñêîëüêó ôóíêöèÿ MD5 íà ñëåäóþùåì ýòàïå ñòàíîâèòñÿ ìîäèôèöèðîâàííîé âåðñèåé MD4, ïîñòîëüêó ïðîòèâîïîëîæíûå ñäâèãè ïðîèñõîäÿò íà ðàçíûå êîëè÷åñòâà áèòîâ, ïîòðåáíîñòü âêëþ÷åíèÿ ýòîãî ïóíêòà â ïðîòîêîë ïîä âîïðîñîì. Ïîñëå âêëþ÷åíèÿ ýòîãî ïóíêòà ïðîòîêîë ñòàíîâèòñÿ ñîâìåñòèìûì ñ ïðåäûäóùåé âåðñèåé. Ïî âèäèìîìó, ýòî ïîâûøàåò óñòîé÷èâîñòü àëãîðèòìà ê êðèïòîàíàëèçó.

18.9 HAVAL

HAVAL - ýòî îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ ïåðåìåííîé äëèíû [1646]. Îíà ÿâëÿåòñÿ ìîäèôèêàöèåé MD5. HAVAL îáðàáàòûâàåò ñîîáùåíèå áëîêàìè ïî 1024 áèòà, â äâà ðàçà áîëüøèìè, ÷åì â MD5. Èñïîëüçóåòñÿ âîñåìü 32-áèòîâûõ ïåðåìåííûõ ñöåïëåíèÿ, â äâà ðàçà áîëüøå, ÷åì â MD5, è ïåðåìåííûå ÷èñëî ýòàïîâ, îò òðåõ äî ïÿòè (â êàæäîì 16 äåéñòâèé). Ôóíêöèÿ ìîæåò âûäàâàòü õýø-çíà÷åíèÿ äëèíîé 128, 160, 192, 224 èëè 256 áèòîâ.

HAVAL çàìåíÿåò ïðîñòûå íåëèíåéíûå ôóíêöèè MD5 íà ñëîæíûå íåëèíåéíûå ôóíêöèè 7 ïåðåìåííûõ, êàæäàÿ èç êîòîðûõ óäîâëåòâîðÿåò ñòðîãîìó êðèòåðèþ. Íà êàæäîì ýòàïå èñïîëüçóåòñÿ îäíà ôóíêöèÿ, íî ïðè êàæäîì äâóñòâåííîì âûçîâå ïåðåìåííûå ïåðåñòàâëÿþòñÿ ðàçëè÷íûì îáðàçîì. Èñïîëüçóåòñÿ íîâûé ïîðÿäîê ñîîáùåíèÿ, è ïðè êàæäîì ýòàïå (êðîìå ïåðâîãî ýòàïà) èñïîëüçóåòñÿ ñâÿ ïðèáàâëÿåìàÿ êîíñòàíòà. Â àëãîðèòìå òàêæå èñïîëüçóåòñÿ äâà öèêëè÷åñêèõ ñäâèãà.

SSäðî àëãîðèòìà ÿâëÿþòñÿ ñëåäóþ ùèå äâóñòâåííûå:

$TEMP = (f(j,A,B,C,D,E,F,G) <<<7) + (H <<<11) + M[i][r(j)+K(j)]$

$H = G; G = F; F = E; E = D; D = C; C = B; B = A; A = TEMP$

Ïåðåìåííûå êîëè÷åñòâî ýòàïîâ è ïåðåìåííàÿ äëèíà âûäàâàåìîãî çíà÷åíèÿ îçíà÷àþò, ÷òî ñóùåñòâóåò 15 âåðñèé àëãîðèòìà. Âñêðûòèå MD5, âûïîëíåííîå äâí Áîðîí è Áîññåëàðñîì [203], íàïðèìåð, ïîêàçûâàåò, ÷òî ñóùåñòâóþò ïðîáëåìû ñ ôóíêöèåé ñæàòèÿ â MD5, íî íå ïîçâîëÿþò íàéòè êîëëèçèþ. Ïîçæå ýòè ðåçóëüòàòû áûëè ïîäòâåðæäåíû è äðóãèìè èññëåäîâàòåëÿìè.

18.10 Äðóãèå îäíîíàïðàâëåííûå õýø-ôóíêöèè

MD3 ÿâëÿåòñÿ åùå îäíîé õýø-ôóíêöèåé, ïðåäëîæåííîé Ðîíîì Ðèâåñòîì. Îíà èìåëà ðîëü íåäîñòàòêîâ è íåêîãäà íå âûõîäèëà çà ïðåäåëû ëàáîðàòîðèè, õîòÿ åå îïèñàíèå íåäàâíî áûëî îïóáëèêîâàíî â [1335].

Ãðóïïà èññëåäîâàòåëåé èç Óíèâåðñèòåòà Âàòåðëîî ïðåäëîæèëà îäíîíàïðàâëåííóþ õýø-ôóíêöèþ íà áàçå èòåðàòèâíîãî âîçâåäåíèÿ â ñòåïåíü â GF(2^{593}) [22]. Ïî ýòîé ñõåìå ñîîáùåíèå ðàçáèâàåòñÿ íà 593-áèòîâûå áëîêè. Íà÷èíàÿ ñ ïåðâîãî áëîêà áëîêè ïîñëåäîâàòåëüíî âîçâîäÿòñÿ â ñòåïåíü. Ïîêàçàòåëü ñòåïåíè - ýòî ðåçóëüòàò âû÷èñëåíèé äëÿ ïðåäûäóùåãî áëîêà, ïåðâûé ïîêàçàòåëü çàäàòñÿ ñ ïîìîùüþ IV.

Àéâýí Äàìãàðä (Ivan Damgård) ðàçðàáîòàë îäíîíàïðàâëåííóþ õýø-ôóíêöèþ, îñíîâàííóþ íà ïðîáëåìå ðþêçàêà (ñì. ðàçäåë 19.2) [414], îíà ìîæåò áûòü âçëîìàíà ïðèìåðíî çà 2^{32} îïåðàöèé [290, 1232, 787].

Â êà÷åñòâå îñíîâû äëÿ îäíîíàïðàâëåííûõ õýø-ôóíêöèé ïðåäëàãàëñÿ è êëàññ íåàññîöèàòèâíûõ àâòîìàòîâ Ñòèâåíà Âîëüôðàìà [1608]. Ðàíýý ðåàëèçàöèÿ [414] íåáåçîïàñíà [1052,404]. Äðóãàÿ îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ, Cellhash [384, 404], è óëó÷øåííàÿ âåðñèÿ, Subbash [384,402, 405], òàêæå îñíîâàííû íà êëåòî÷íûõ àâòîìàòàõ è ïðåäíàçíà÷åíû äëÿ àïïàðàòíîé ðåàëèçàöèè. Boognish îáúåäèíèë ïðîöåññû Cellhash è MD4 [402, 407]. StepRightUp òàêæå ìîæåò áûòü ðåàëèçîâàíà êàê õýø-ôóíêöèÿ [402].

Ëåòî 1991 ãîäà Êëàóñ Øíîðð (Claus Schnorr) ïðåäëîæèë îäíîíàïðàâëåííóþ õýø-ôóíêöèþ íà áàçå äèñ-

ëðåòíîãî ïðåîáðàçîâàíèÿ Ôóðüå, íàçâàííóþ FFT-Hash [1399]. ×åðåç íåñêîëüêî ìåñÿöåâ îíà áûëà âçëîìàíà äâóìÿ íåçàâèñèìûìè ãðóïïàìè [403, 84]. Øíîðð ïðåäëîæèë íîâóþ âåðñèþ, FFT-Hash II (ïðåäûäóùàÿ áûëà ïåðåìåíîâàíà â FFT-Hash I) [1400], êîòîðàÿ áûëà âçëîìàíà ÷åðåç íåñêîëüêî íåäåëü [1567]. Øíîðð ïðåäëîæèë äàëüíåéøèå ìîäèôèêàöèè [1402, 1403] íî, ïðè äàííûõ îáñòîÿòåëüñòâàõ, îíè íàìíîãî ìåäëåííåå, ÷åì äóãèå àëãîðèòìû ýòîé ãëàâû. Åùå îäíà õýø-ôóíêöèÿ, SL_2 [1526], íåéðîíàñíà [315].

Äîïîëíèòåëüíóþ èíôîðìàöèþ ïî òåêóùåìó ïîëîæåíèþ äîïîëíèòåëüíûõ õýø-ôóíêöèé èç îäíîíàïðàâëåííûõ ôóíêöèé è îäíîíàïðàâëåííûõ ïåðåñòàíîâîê ìîæíî íàéòè â [412, 1138, 1342].

18.11 Îäíîíàïðàâëåííûå õýø-ôóíêöèè, èñïîëüçóþùèå ñèììåòðè÷íûå áëî÷íûå àëãîðèòìû

Â êà÷åñòâå îäíîíàïðàâëåííûõ õýø-ôóíêöèé ìîæíî èñïîëüçîâàòü ñèììåòðè÷íûå áëî÷íûå àëãîðèòìû øèôðîâàíèÿ. Èäåÿ â òîì, ÷òî åñëè áåçîïàñåí áëî÷íûé àëãîðèòì, òî è îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ áóäåò áåçîïàñíîé.

Ñàìûì î÷åâèäíûì ñïîñîáîì ÿâëÿåòñÿ øèôðîâàíèå ñîîáùåíèÿ â ðåæèìå CBC èëè CFB ñ ïîìîùüþ ôèêñèðîâàííîãî êëþ÷à è IV, õýø-çíà÷åíèå áóäåò ïîñëåäíèé áëîê øèôðîòåêñòà. Ýòè ìåòîäû îïèñàíû â ðàçëè÷íûõ ñòàíäàðòàõ, èñïîëüçóþùèõ DES: îáà ðåæèìà â [1143], CBC â [1145], CFB â [55, 56, 54]. Ýòîò ñïîñîá íå ñëèøêîì ïîäõîäèò äëÿ îäíîíàïðàâëåííûõ õýø-ôóíêöèé, õîòÿ îí áóäåò ðàáîòàòü äëÿ MAC (ñì. ðàçäåë 18.14) [29].

Ñïîñîá ïîòðåáóåò èñïîëüçóåò â êà÷åñòâå êëþ÷à áëîê ñîîáùåíèÿ, ïðåäûäóùåé õýø-çíà÷åíèå â êà÷åñòâå âõîäà, à òåêóùåå õýø-çíà÷åíèå ñëóæèò âûõîäîì.

Äåéñòâèòåëüíûå õýø-ôóíêöèè äàæå åùå ñëîæíåå. Ðàçìåð áëîêà îáû÷íî ñîâïàäàåò ñ äëèíîé êëþ÷à, è ðàçìåð õýø-çíà÷åíèÿ áóäåò äëèíà áëîêà. Òàê êàê áîëüøèíñòâî áëî÷íûõ àëãîðèòìîâ 64-áèòîâûå, ñïðåêòðîâàí ðÿä ñðåä, äàþùèõ õýø-çíà÷åíèå â äâà ðàçà áîëüøå äëèíû áëîêà.

Ïðè óñëîâèè, ÷òî õýø-ôóíêöèÿ ïðàêòè÷íà, áåçîïàñíîñòü ýòîé ñõåìû îñíîâàíà íà áåçîïàñíîñòè èñïîëüçóåìîé áëî÷íîé ôóíêöèè. Îáû÷íî åñòü è èñêëþ÷åíèÿ. Äèôôåðåíöèàëüíûé êðèïòîàíàëèç ëó÷øå ðàáîòàåò ïðîòèâ áëî÷íûõ ôóíêöèé â õýø-ôóíêöèÿõ, ÷åì ïðîòèâ áëî÷íûõ ôóíêöèé, èñïîëüçóåìûõ äëÿ øèôðîâàíèÿ: êëþ÷ èçâåñòåí, ïîýòîìó ìîæíî èñïîëüçîâàòü ðàçëè÷íûå ïðèåìû. Äëÿ óñïåõà íóæíà òî÷íîé îáîá ïðàâèëüíàÿ ïàðà, è ìîæíî ãåíåðèðîâàòü ñòîëüêî âûáðàííîãî òèïà ôóíêöèè, ñêîëüêî íóæíî. Ýòî íàïðàâëåíèå îñâåùàåòñÿ â [1263, 858, 1313].

Íèæå ïðèâåäåí îáçîð ðàçëè÷íûõ õýø-ôóíêöèé, îïèñàííûõ â ëèòåðàòóðå [925, 1465, 1262]. Âûâîäû î âîçìîæíîñòè âñêðûòèÿ ïðåäïîëàãàþò, ÷òî èñïîëüçóåìûé áëî÷íûé àëãîðèòì áåçîïàñåí, è ëó÷øèì âñêðûòèåì ÿâëÿåòñÿ âñêðûòèå ãðóáîé ñèëîé.

Ïîëåçíîé ìåðîé äëÿ õýø-ôóíêöèé, îñíîâàííûõ íà áëî÷íûõ øèôðàõ, ÿâëÿåòñÿ **ñêîðîñòü õýøèðîâàíèÿ**, èëè êîëè÷åñòâî *n*-áèòîâûõ áëîêîâ ñîîáùåíèÿ (n - ýòî ðàçìåð áëîêà àëãîðèòìà), îáðàáàòûâàåìûõ ïðè øèôðîâàíèè. ×åì âûøå ñêîðîñòü õýøèðîâàíèÿ, òåì áîëüøåå àëãîðèòì. (Äðóãîå îïðåäåëåíèå ýòîãî ïàðàìåòðà äàíî â [1262], íî îïðåäåëåíèå, ïðèâåäåííîå ìíîé, áîëåå èíòóèòèâíî è øèðå èñïîëüçóåìîñ. Ýòî ìîæåò çàïóòàòü.)

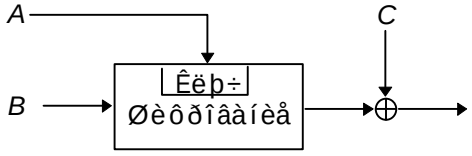
Ñõåìû, â êîòîðûõ äëèíà õýø-çíà÷åíèÿ ðàâíà äëèíå áëîêà

Âîò îáùàÿ ñõåìà (ñì. 10-é):

$H_0 = I_H$, , ãäå I_H - ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå

$H_i = E_A(B) \oplus C$

ãäå A, B è C ìîãóò áûòü ëèáî M_i, H_{i-1}, ($M_i \oplus H_{i-1}$), ëèáî êîíñòàíòû (âîçìîæíî ðàâíûå 0). H_0 - ýòî íåêîòîðîå ñëó÷àéíîå íà÷àëüíîå ÷èñëî I_H. Ñîîáùåíèå ðàçáèâàåòñÿ íà ÷àñòè â ñîîòâåòñòâèè ñ ðàçìåðîì áëîêà, M_i, îáðàáàòûâàåìûì îòäåëüíî. Êðîìå òîãî, èñïîëüçóåòñÿ âàðèàíò MD-óñèëåíèÿ, âîçìîæíî òà æå ïðîöåäóðà äîïîëíåíèÿ, ÷òî è â MD5 è SHA.



Ðèñ. 18-8. Îáîáùåíèÿ õýø-ôóíêöèÿ, ó êîòîðîé äëèíà õýø-çíà÷åíèÿ ðàâíà äëèíå áëîêà.

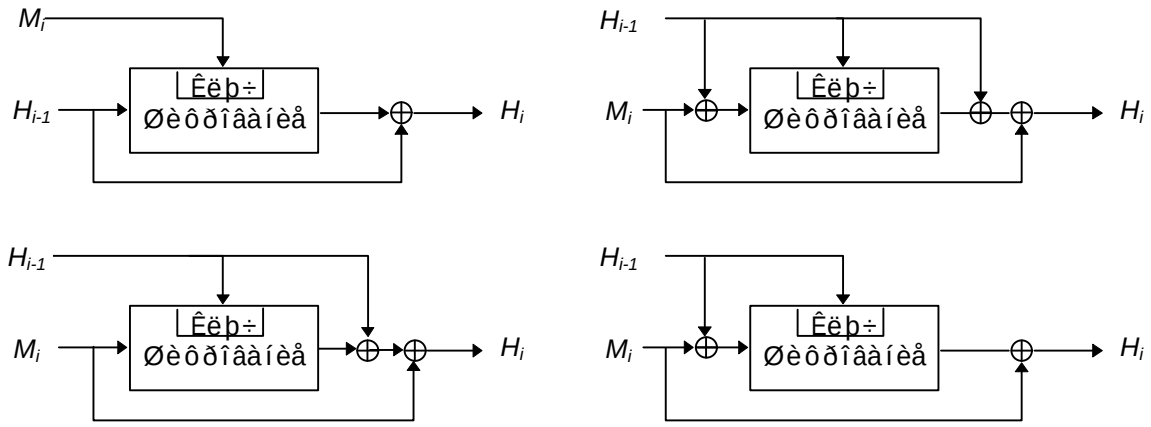
Òàáë. 18-1.
Áåçîïàñíûå õýø-ôóíêöèè, ó êîòîðûõ

äëèíà õýø-çíà÷íèÿ ðàâíà äëèíå áëîêà

$H_i = E_{H_{i-1}}(M_i) \oplus M_i$
$H_i = E_{H_{i-1}}(M_i \oplus H_{i-1}) \oplus M_i \oplus H_{i-1}$
$H_i = E_{H_{i-1}}(M_i) \oplus H_{i-1} \oplus M_i$
$H_i = E_{H_{i-1}}(M_i \oplus H_{i-1}) \oplus M_i$
$H_i = E_{M_i}(H_{i-1}) \oplus H_{i-1}$
$H_i = E_{M_i}(M_i \oplus H_{i-1}) \oplus M_i \oplus H_{i-1}$
$H_i = E_{M_i}(H_{i-1}) \oplus M_i \oplus H_{i-1}$
$H_i = E_{M_i}(M_i \oplus H_{i-1}) \oplus H_{i-1}$
$H_i = E_{M_i \oplus H_{i-1}}(M_i) \oplus M_i$
$H_i = E_{M_i \oplus H_{i-1}}(H_{i-1}) \oplus H_{i-1}$
$H_i = E_{M_i \oplus H_{i-1}}(M_i) \oplus H_{i-1}$
$H_i = E_{M_i \oplus H_{i-1}}(H_{i-1}) \oplus M_i$

Òðè ðàçëè÷íûå ïåðåìåííûå ìîãóò ïðèíèìàòü îäíî èç ÷åòûðåõ âîçìîæíûõ çíà÷åíèé, ïîýòîìó âñåãî ñóùåñòâóåò 64 âàðèàíòà ñõåì ýòîãî òèïà. Îíè âñå áûëè èçó÷åíû Áàðòîì Ïðåíåëü (Bart Preneel) [1262].

Ïÿòíàäöàòü èç íèõ òðèâèàëüíî ñëàáû, òàê êàê ðåçóëüòàò íå çàâèñèò îò îäíîãî èç âõîäîâ. Òðèäöàòü ñåìü íåäåçîïàñíû ïî áîëåå òî÷íîé ïðè÷èíå. Â 17-é ïåðå÷èñëåííû îñòàâøåéñÿ 12 áåçîïàñíûõ ñõåì: ïåðâûå ÷åòûðå áåçîïàñíû ïðîòèâ âñåõ âîêðóòèé (ñì. 9th), à ïîñëåäíèå 8 áåçîïàñíû ïðîòèâ âñåõ òèïîâ âñêðûòèé, êðîìå âñêðûòèÿ ñ ôèêñèðîâàííîé òî÷êîé, î êîòîðîì â ðåàëüíûõ óñëîâèÿõ íå ñòîèò áåñïîêîèòüñÿ.



Ðèñ. 18-9. ×åòûðå áåçîïàñíûõ õýø-ôóíêöèè, ó êîòîðûõ äëèíà õýø-çíà÷åíèÿ ðàâíà äëèíå áëîêà.

Ïåðâàÿ ñõåìà áûëà îïèñàíà â [1028]. Òðåòüÿ ñõåìà áûëà îïèñàíà â [1555, 1105, 1106] è ïðåäëàãàëàñü â êà÷åñòâå ñòàíäàðòà ISO [766]. Ïÿòàÿ ñõåìà áûëà ïðåäëîæåíà Êàðëîì Ìàéåðîì (Carl Meyer), íî â ëèòåðàòóðå íáû÷íî íàçûâàþòñÿ Davies-Meyer [1606, 1607, 434, 1028]. Äåñÿòàÿ ñõåìà áûëà ïðåäëîæåíà â êà÷åñòâå ðåæèìà õýø-ôóíêöèè äëÿ LOKI [273].

Ñêîðîñòü õýøèðîâàíèÿ ïåðâîé, âòîðîé, òðåòüåé, ÷åòâåðòîé, ïÿòîé è îäèíàäöàòîé ñõåì ðàâíà 1 - äëèíà êëþ÷à ðàâíà äëèíå áëîêà. Ñêîðîñòü õýøèðîâàíèÿ äðóãèõ ñõåì ñîñòàâëÿåò *k*/*n*, ãäå *k* -äëèíà êëþ÷à. Ýòî îçíà÷àåò, ÷òî åñëè äëèíà êëþ÷à êîðî÷å äëèíû áëîêà, òî áëîê ñîîáùåíèÿ äîëæåí áûòü ïî äëèíå ðàâåí êëþ÷ó. Íå ðåêîìåíäóåòñÿ, ÷òîáû áëîê ñîîáùåíèÿ áûë äëèííåå êëþ÷à, äàæå åñëè äëèíà êëþ÷à àëãîðèòìà øèôðîâàíèÿ áîëüøå, ÷åì äëèíà áëîêà.

Åñëè áëî÷íûé àëãîðèòì îñíîâàí DES îáëàäàåò ñâîéñòâîì êîìïëåìåíòíîñòè è ñëàáûìè êëþ÷àìè, äëÿ âñåõ 12 ñõåì ñóùåñòâóåò âîçìîæíîñòü äîïîëíèòåëüíîãî âñêðûòèÿ. Îíî íå ñëèøêîì ïîõîæå è â äâéñòâåííîñòè íå ñòîèò îá ýòî ì áåñïîêîèòüñÿ. Îäíàêî âû ìîæåòå îáåçîïàñèòü ñåáÿ ïò òàêîãî âñêðûòèÿ, çàôèêñèðîâàâ çíà÷åíèå âòîðîãî è òðåòüåãî áèòîâ êëþ÷à, ðàâíûå "01" èëè "10" [1081,1107]. Êîíå÷íî æå ýòî óìåíüøèò äëèíó *k* ñ 56 áèòîâ äî 54 áèòîâ (äëÿ DES) è óìåíüøèò ñêîðîñòü õýøèðîâàíèÿ.

Áûëî ïîêàçàíî, ÷òî ñëàáóþ ùèå ñõåìû, îïèñàííûå â ëèòåðàòóðå, íåáåçîïàñíû.

Ýòà ñõåìà [1282] áûëà âçëîìàíà â [369]:

$H_i = E_{M_i}(H_{i-1})$

Äýâèñ (Davies) è Ïðàéñ (Price) ïðåäëîæèëè âàðèàíò, â êîòîðîì âñå ñîîáùåíèå öèêëè÷åñêè îãðàíè÷åíî âû÷èñëèòåëüíîé ìîùíîñòè [369]. Â [1606] áûëà ïîêàçàíà íåáåçîïàñíîñòü åùå îäíîé ñõåìû [432, 458]:

$H_i = E_{M_i \oplus H_{i-1}}(H_{i-1})$

Â [1028] áûëà ïîêàçàíà íåáåçîïàñíîñòü ñëåäóþùåé ñõåìû (*c* - êîíñòàíòà):

$H_i = E_{\tilde{n}}(M_i \oplus H_{i-1}) \oplus M_i \oplus H_{i-1}$

Ì îäèôèêàöèÿ ñõåìû Davies-Meyer

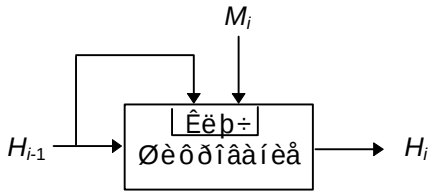
Ëàé (Lai) è Ìàññåé (Massey) ìîäèôèöèðîâàëè ìåòîä Davies-Meyer, ÷òîáû ìîæíî áûëî èñïîëüçîâàòü øèôð IDEA [930, 925]. IDEA èñïîëüçóåò 64-áèòîâûé áëîê è 128-áèòîâûé êëþ÷. Âîò ïðåäëîæåíèÿ è ìè ñõåìà:

$H_0 = I_H$, , ãäå I_H - ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå

$H_i = E_{H_{i-1}, M_i}(H_{i-1})$

Ýòà ôóíêöèÿ õýøèðóåò ñîîáùåíèå 64-áèòîâûì è áëîêàì è âûäàåò 64-áèòîâîå çíà÷åíèå (ñì. 8-é).

Áîëåå ïðîñòîå âñêðûòèå ýòîé ñõåìû, ÷åì ìåòîä ãðóáîé ñèëû, íåèçâåñòíî.



Ðèñ. 18-10. Ì îäèôèêàöèÿ ñõåìû Davies-Meyer.

Preneel-Bosselaers-Govaerts-Vandewalle

Ýòà õýø-ôóíêöèÿ, âïåðâûå ïðåäëîæåíàÿ â [1266], âûäàåò õýø-çíà÷åíèå, â äâà ðàçà áîëüøåå äëèíû áëîêà àëãîðèòìà øèôðîâàíèÿ: ïðè 64-áèòîâîì àëãîðèòìå ïîëó÷àþòñÿ 128-áèòîâûå õýø-çíà÷åíèÿ.

Ïðè 64-áèòîâîì áëîê-íîì àëãîðèòìå ñõåìà âûäàåò äâà 64-áèòîâûõ õýø-çíà÷åíèÿ, G_i è H_i, îáúåäèíåíèå êîòîðûõ è äàåò 128-áèòîâîå õýø-çíà÷åíèå. Ó áîëüøèíñòâà áëî÷íûõ àëãîðèòìîâ äëèíà áëîêà ðàâíà 64 áèòàì. Äâà ñîñåäíèõ áëîêà, L_i è R_i, ðàçìåð êàæäîãî ðàâåí ðàçìåðó áëîêà, õýøèðóþòñÿ âìåñòå.

$G_0 = I_G$, ãäå I_G - ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå

$H_0 = I_H$, , ãäå I_H - äðóãîå ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå

$G_i = E_{L_i \oplus H_{i-1}}(R_i \oplus G_{i-1}) \oplus R_i \oplus G_{i-1} \oplus H_{i-1}$

$H_i = E_{L_i \oplus R_i}(H_{i-1} \oplus G_{i-1}) \oplus L_i \oplus G_{i-1} \oplus H_{i-1}$

Ëàé ïðèâîäèò âñêðûòèå ýòîé ñõåìû, êîòîðîå â íåêîòîðûõ ñëó÷àÿõ äåëàåò âñêðûòèå ìåòîäîì äîêàçàòåëüſòâà ñòîéêîñòè ýòîé ñõåìû [925, 926]. Ïðåíåë (Preneel) [1262] è Êîïïåðñìèò (Coppersmith0 [372] òàêæå óñïåøíî âçëîìàëè ýòó ñõåìó. Íå èñïîëüçóéòå åå.

Quisquater-Girault

Ýòà ñõåìà, âïåðâûå ïðåäëîæåíàÿ â [1279], ãåíåðèðóåò õýø-çíà÷åíèå, â äâà ðàçà áîëüøå äëèíû áëîêà. Åå ñêîðîñòü õýøèðîâàíèÿ ðàâíà 1. Î íà èñïîëüçóåò äâà õýø-çíà÷åíèÿ, G_i è H_i, è õýøèðóåò âìåñòå äâà áëîêà, L_i è R_i.

$G_0 = I_G$, ãäå I_G - ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå

$H_0 = I_H$, , ãäå I_H - äðóãîå ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå

$W_i = E_{L_i}(G_{i-1} \oplus R_i) \oplus R_i \oplus H_{i-1}$

$G_i = E_{R_i}(W_i \oplus L_i) \oplus G_{i-1} \oplus H_{i-1} \oplus L_i$

$H_i = W_i \oplus G_{i-1}$

Ýòà ñõåìà ïîÿâèëàñü â 1989 ãîäó â ïðîåêòå ñòàíäàðòà ISO [764], íî áûëà çàìåíåíà áîëåå ïîçäíåé âåðñèåé [765]. Ïðîáëåìû áåçîïàñíîñòè ýòîé ñõåìû îòñóòñòâóþò â [1107, 925, 1262, 372]. (Â äåéſòâèòåëüſîſòè, âåðñèÿ, îïèſàíèÿ â ìàòåðèàëàõ êîſôåðåſöèè, áûëà ïſſåå òîãî, êàê âåðſèÿ, ïðåäſòàâëåſſíàÿ íà êſſôåðåſöèè, áûëà âſêðûòà.) Â ðÿäå ſëó÷àéſ ſëîæſſîſòü âſêðûòèÿ ìåòîäîì äſÿ ðſæäſſíèÿ èſåò ðàâſà 2^{39}, à íå 2^{64}, êàê ó âſêðûòèÿ ãðóáſé. Íå èſſſîſüçóéòå ýòó ſõſåſó.

LOKI ſ óäâſåſſſûſ áſſêſſ

Ýòſò àëãſðèſ ſðåäſòàâſÿåſ ſſáſé ſſäſôſêſàöſþ Quisquater-Cirault, ſſſöſàſüſſ ſſðſſåſêſðſſâſſſóþ äſÿ ðà-

áîòû ñ LOKI [273]. Âñå ïàðàìåòðû - òåæå, ÷òî è â Quisquater-Girault.

$G_0 = I_G$, ãäå I_G - ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå

$H_0 = I_H$, , ãäå I_H - äðóãîå ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå

$$W_i = E_{L_i \oplus G_{i-1}}(G_{i-1} \oplus R_i) \oplus R_i \oplus H_{i-1}$$

$$G_i = E_{R_i \oplus H_{i-1}}(W_i \oplus L_i) \oplus G_{i-1} \oplus H_{i-1} \oplus L_i$$

$$H_i = W_i \oplus G_{i-1}$$

È ñíîâà â íåêîòîðûõ ñëó÷àÿõ âñêðûòèå ìåòîäîì äíÿ ðîæäåíèÿ îêàçûâàåòñÿ òðèâèàëüíûì [925, 926, 1262, 372, 736]. Íå èñïîëüçóéòå ýòó ñõåìó.

Ïàðàëëåëüíàÿ ñõåìà Davies-Meyer

Ýòî åùå îäíà ïîïûòêà ñîçäàòü àëãîðèòì ñî ñêðûòûì õýø-èðîâàíèåì 1, êîòîðûé âûäàåò õýø-çíà÷åíèå, â äâà ðàçà áîëüøåå äëèíû áëîêà. [736].

$G_0 = I_G$, ãäå I_G - ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå

$H_0 = I_H$, , ãäå I_H - äðóãîå ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå

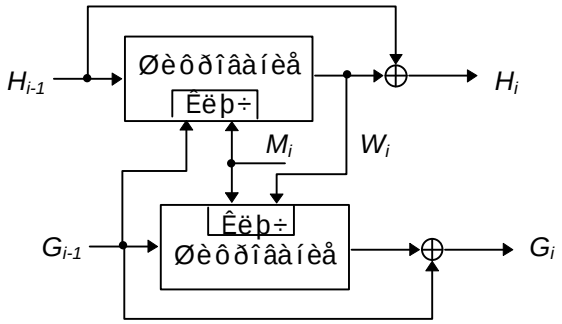
$$G_i = E_{L_i \oplus R_i}(G_{i-1} \oplus L_i) \oplus L_i \oplus H_{i-1}$$

$$H_i = E_{L_i}(H_{i-1} \oplus R_i) \oplus R_i \oplus H_{i-1}$$

Ê ñîæàëåíèþ ýòà ñõåìà òîæå íåáåçîïàñíà [928, 861]. Îêàçûâàåòñÿ, ÷òî õýø-ôóíêöèÿ óäâîåííîé äëèíû ñî ñêðûòûì õýøèðîâàíèåì, ðàâíîé 1, íå ìîæåò áûòü áåçîïàñíåå, ÷åì Davies-Meyer [861].

Òàíäåì íàÿ (Tandem) è îäíîâðåìåííàÿ (Abreast) ñõåìû Davies-Meyer

Äðóãîé ñïîñîá îáîéòè îãðàíè÷åíèÿ, ïðèñóùèå áëî÷íûì øèôðàì ñ 64-áèòîâûì êëþ÷îì, èñïîëüçóåò àëãîðèòì, ïîäîáíûé IDEA (ñì. ðàçäåë 13.9), ñ 64-áèòîâûì áëîêîì è 128-áèòîâûì êëþ÷îì. Ñëåäóþùèå äâå ñõåìû âû䌠128-áèòîâõýø-çíà÷åíèå, à èõ ñêðûòûå õýøèðîâàíèÿ ðàâíû $^1/_2$ [930, 925].



Ðèñ. 18-11. Òàíäåì íàÿ (Tandem) ñõåìà Davies-Meyer.

Â ïåðâîé ñõåìå äâå ìîäèôèöèðîâàííûå ôóíêöèè Davies-Meyer ðàáîòàþò òàíäåìîì, êîíâåéåðíî (ñì. 7-é).

$G_0 = I_G$, ãäå I_G - ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå

$H_0 = I_H$, , ãäå I_H - äðóãîå ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå

$$W_i = E_{G_{i-1}, M_i}(H_{i-1})$$

$$G_i = G_{i-1} \oplus E_{M_i, W_i}(G_{i-1})$$

$$H_i = W_i \oplus H_{i-1}$$

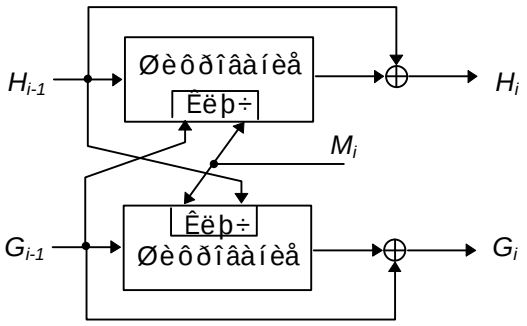
Â ñëåäóþùåé ñõåìå èñïîëüçóþòñÿ äâå ìîäèôèöèðîâàííûå ôóíêöèè, ðàáîòàþùèå îäíîâðåìåííî (ñì. 6-é).

$G_0 = I_G$, ãäå I_G - ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå

$H_0 = I_H$, , ãäå I_H - äðóãîå ñëó÷àéíîå íà÷àëüíîå çíà÷åíèå

$$G_i = G_{i-1} \oplus E_{M_i, H_{i-1}}(\neg G_{i-1})$$

$$H_i = H_{i-1} \oplus E_{G_{i-1}, M_i}(H_{i-1})$$



Ðèñ. 18-12. Îäíîðàçðÿäíàÿ (Abreast) ñõåìà Davies-Meyer.

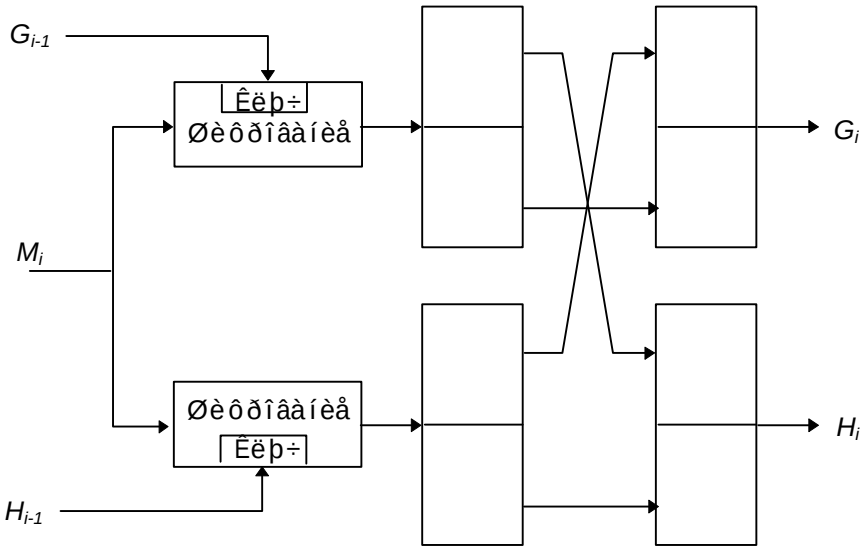
Â îáåèõ ñõåìàõ äâà 64-áèòîâûõ çíà÷åíèÿ, G_i è H_i, îáúåäèíÿþòñÿ, îáðàçóÿ åäèíîå 128-áèòîâîå õýø-çíà÷åíèå.

Íàñêîëüêî èçâåñòíî, áåçîïàñíîñòü 128-áèòîâîé õýø-ôóíêöèè ýòèõ àëãîðèòìîâ èäåàëüíà: äëÿ îáíàðóæåíèÿ ñîâïàäåíèÿ ñ çàäàííûì õýø-çíà÷åíèåì òðåáóåòñÿ 2^{128} ïîïûòîê, à äëÿ íàõîæäåíèÿ äâóõ ñëó÷àéíûõ ñîâïàäàþùèõ - 2^{64} ïîïûòîê, ïðè óñëîâèè, ÷òî ëó÷øèì ñïîñîáîì âñêðûòèÿ ÿâëÿåòñÿ ïðèìåíåíèå ãðóáîé ñèëû.

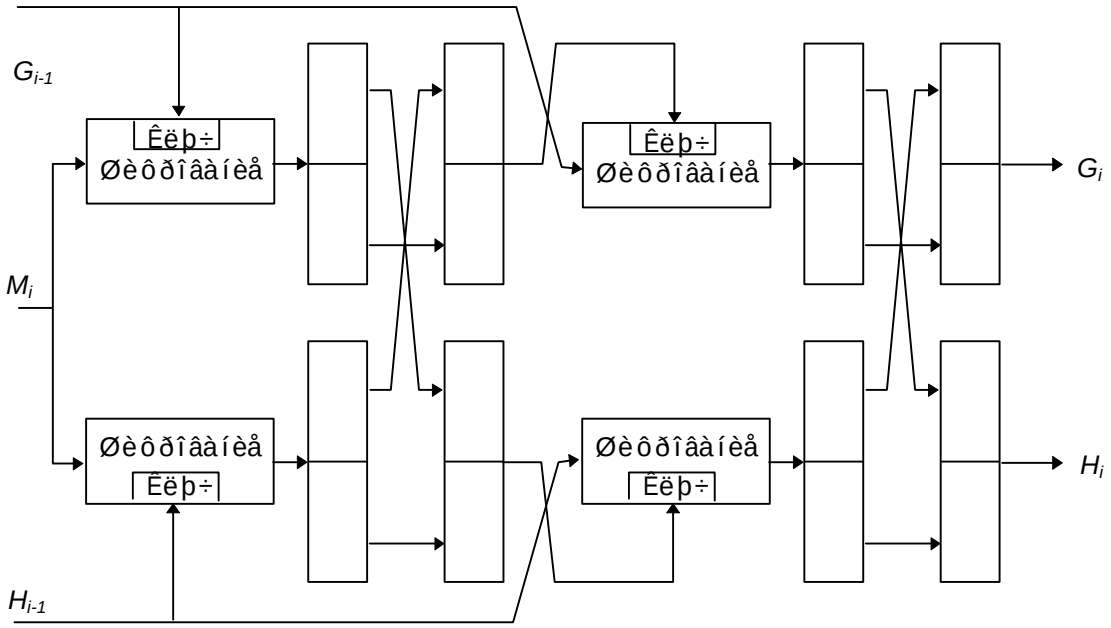
MDC-2 è MDC-4

MDC-2 è MDC-4 ðàçðàáîòàíû â IBM [1081, 1079]. Â íàñòîÿùåå âðåìÿ èçó÷àþòñÿ âîïðîñ ñïîñîáíîñòè MDC-2, èíîãäà íàçûâàåìîé Meyer-Schilling, â êà÷åñòâå ñòàíäàðòà ANSI è ISO [61, 765], ýòî âàðèàíò áûë ïðåäëîæåí â [762]. MDC-4 îïðåäåëåíà äëÿ ïðîåêòà RIPE [1305] (ñì. ðàçäåë 25.7). Ñïåöèôèêàöèÿ ñïîñîáíîçóåò DES â êà÷åñòâå áëî÷íîé ôóíêöèè, õîòÿ òåîðåòè÷åñêè ìîæåò áûòü ñïîñîáíîé âûáèðàòü äðóãîé áëî÷íûé àëãîðèòì.

Ñêîðîñòü õýøèðîâàíèÿ MDC-2 ðàâíà $^1/_2$, äëèíà õýø-çíà÷åíèÿ ýòîé ôóíêöèè â äâà ðàçà áîëüøå ðàçìåðà áëîêà.Åå ñõåìà ïîêàçàíà íà 5-é. MDC-4 òàêæå âûäàåò õýø-çíà÷åíèå â äâà ðàçà áîëüøåå ðàçìåðà áëîêà, à åå ñêîðîñòü õýøèðîâàíèÿ ðàâíà $^1/_4$ (ñì. 4-é).



Ðèñ. 18-13. MDC-2.



Ðèñ. 18-14. MDC-4.

Ýòè ñõåìû áûëè ïðîàíàëèçèðîâàíû â [925, 1262]. Îíè áåçîïàñíû ñ ó÷åòîì ñåãîäíÿøíèõ âîçìîæíîñòåé âû÷èñëèòåëüíîé òåõíèêè, íî èõ íàäåæíîñòü íà òàê âåëèêà, êàê õîòåëîñü ðàçðàáîò÷èêàì. Èõ óñòîé÷èâîñòü ê äèôôåðåíöèàëüíîìó êðèïòîàíàëèçó ïðè DES â êà÷åñòâå áëî÷íîãî àëãîðèòìà áûëà ðàññìîòðåíà â [1262].

MDC-2 è MDC-4 çàïàòåíòîâàíû [223].

Õýø-ôóíêöèÿ AR

Õýø-ôóíêöèÿ AR áûëà ðàçðàáîòàíà Algorithmic Research, Ltd. è çàòåì ðàñïðîñòðàíåíà ISO òîëüêî äëÿ èíôîðìàöèè [767]. Åå áàçîâàÿ ñòðóêòóðà ÿâëÿåòñÿ âàðèàíòîì èñïîëüçóåìîãî áëî÷íîãî øèôðà (DES â óïîìÿíóòîé ñòàòüå) â ðåæèìå CBC. Âû ïîëüçóåòñÿ XOR ïîñëåäíèõ äâóõ áëîêîâ øèôðîòåêñòà, êîíñòàíòó è òåêóùåãî áëîêà ñîîáùåíèÿ, ðåçóëüòàò øèôðóåòñÿ àëãîðèòìîì. Õýø-çíà÷åíèåì ÿâëÿþòñÿ ïîñëåäíèå âû÷èñëåííûå äâà áëîêà øèôðîòåêñòà. Ñîîáùåíèå îáðàáàòûâàåòñÿ äâàæäû, äâóìÿ ðàçëè÷íûìè êëþ÷àìè, ïîýòîìó ñêîðîñòü õýøèðîâàíèÿ ðàâíà $^1/_2$. Ïåðâûì êëþ÷îì ñëóæèò 0x0000000000000000, âòîðûì - 0x2a41522f4446502a, à çíà÷åíèå êîíñòàíòû *c* ðàâíî 0x0123456789abcdef. Ðåçóëüòàò ñæèìàåòñÿ äî îäíîãî 128-áèòîâîãî õýø-çíà÷åíèÿ. Ïîäðîáíîñòè ïðèâåäåíû â [750].

$H_i = E_K(M_i \oplus H_{i-1} \oplus H_{i-2} \oplus c) \oplus M_i$

Ôóíêöèÿ âûãëÿäèò ïðèâëåêàòåëüíî, íî íå ÿâëÿåòñÿ áåçîïàñíîé. Ïîñëå íåêîòîðîé çíà÷èòåëüíîé ïðåäâàðèòåëüíîé îáðàáîòêè ñòàíîâèòñÿ âîçìîæíû ëåãêî íàõîäèòü ñîîáùåíèÿ ñ îäèíàêîâûì õýø-çíà÷åíèåì [416].

Õýø-ôóíêöèÿ ÃÎÑÒ

Ýòà õýø-ôóíêöèÿ ïîÿâèëàñü â Ðîññèè è îïðåäåëåíà â ñòàíäàðòå ÃÎÑÒ Ð 34.11.94 [657]. Â íåé èñïîëüçóåòñÿ áëî÷íûé äëîðèòì ÃÎÑÒ (ñì. ðàçäåë 14.1), õîòÿ òåîðåòè÷åñêè ìîæåò èñïîëüçîâàòüñÿ ëþáîé áëî÷íûé àëãîðèòì ñ 64-áèòîâûì áëîêîì è 256-áèòîâûì êëþ÷îì. Ôóíêöèÿ âû䌠256-áèòîâîå õýø-çíà÷åíèå.

Ôóíêöèÿ ñæàòèÿ, $H_i = f(M_i,H_{i-1})$ (îáà îïåðàíäà - 256-áèòîâûå âåëè÷èíû) îïðåäåëÿåòñÿ ñëåäóþùèì îáðàçîì:

(1) Ïðè ïîìîùè ëèíåéíîãî ñìåøèâàíèÿ M_i, H_{i-1} è íåêîòîðûõ êîíñòàíò ãåíåðèðóåòñÿ ÷åòûðå êëþ÷à øèôðîâàíèÿ ÃÎÑÒ.

(2) Êàæäûé êëþ÷ èñïîëüçóåòñÿ äëÿ øèôðîâàíèÿ îòäåëüíîãî 64 áèòîâ H_{i-1} â ðåæèìå ECB. Ïîëó÷åííûå 256 áèòîâ ñîõðàíÿþòñÿ âî âðåìåííîé ïåðåìåííîé *S*.

(3) H_i ÿâëÿåòñÿ ñëîæíî, õîòÿ è ëèíåéíî ôóíêöèé *S*, M_i è H_{i-1}.

Õýø-çíà÷åíèå ïîñëåäíåãî áëîêà ñîîáùåíèÿ íå ÿâëÿåòñÿ åãî îêîí÷àòåëüíûì õýø-çíà÷åíèåì. Íà äåëå èñïîëüçóåòñÿ òðè ïðåìåíîâûå ñöåïëåíèÿ: H_n - ýòî õýø-çíà÷åíèå ïîñëåäíåãî áëîêà, *Z* - ýòî XOR âñåõ áëîêîâ ñîîáùåíèÿ, à *L* - äëèíà ñîîáùåíèÿ. Ñ èñïîëüçîâàíèåì ýòèõ ïðåìåííûõ è äîïîëíèòåëüíîãî ïîñëåäíåãî áëîêà *M'*, îêîí÷àòåëüíîå õýø-çíà÷åíèå ðàâíî:

$H = f(Z \oplus M', f(L, f(M', H_n)))$

Äîêóìåíòàöèÿ íåìíîãî çàïóòàíà (è íà ðóññêîì ÿçûêå), íî ÿ äóìàþ, ÷òî ïîíÿë âñå ïðàâèëüíî. Âî âñÿêîì ñëó÷àå ýòà õýø-ôóíêöèÿ îïðåäåëåíà êàê ÷àñòü ðîññèéñêîãî Ñòàíäàðòà öèôðîâîé ïîäïèñè (ñì. ðàçäåë 20.3).

Äðóãèå ñõåìû

Ðàëüô Ìåðêë ïðåäëîæèë ñõåìó, èñïîëüçóþùóþ DES, íî îíà ìåäëåííà - îáðàáàòûâàåò òîëüêî ñìüå áèòîâ ñîîáùåíèÿ çà èòåðàöèþ, è êàæäàÿ èòåðàöèÿ ñîñòîèò èç äâóõ øèôðîâàíèé DES [1065, 1069]. Äðóãàÿ ñõåìà [1642, 1645] íåáåçîïàñíà [1267], êîãäà-òî îíà ïðåäëàãàëàñü â êà÷åñòâå ñòàíäàðòà ISO.

18.12 Èñïîëüçîâàíèå àëãîðèòìîâ ñòðîê÷íûõ êëþ÷åé

Â êà÷åñòâå îäíîíàïðàâëåííîé õýø-ôóíêöèè ìîæíî èñïîëüçîâàòü è àëãîðèòì øèôðîâàíèÿ ñ îòêðûòûì êëþ÷îì â ðåæèìå ñöåïëåíèÿ áëîêîâ. Åñëè çàòåì âûáðîñèòü ëèøíèå êëþ÷è, òî âçëîìàòü õýø-ôóíêöèþ áóäåò òàêæå òðóäíî, êàê è ïðî÷èòàòü ñîîáùåíèå áåç ëè÷íîãî êëþ÷à.

Âîò ïðèìåð, èñïîëüçóþùåé RSA. Åñëè *M* - ýòî õýøèðóåìîå ñîîáùåíèå, *n* - ïðîèçâåäåíèå äâóõ ïðîñòûõ ÷èñåë *p* è *q*, à *e* - äðóãîå áîëüøîå ÷èñëî, âçàèìíî ïðîñòîå ñ (*p* - l)(*q* - 1), òî õýø-ôóíêöèÿ, *H*(*M*), áóäåò ðàâíà

$H(M) = M^e \bmod n$

Åùå ïðîùå èñïîëüçîâàòü îäíî ñèëüíîå ïðîñòîå ÷èñëî â êà÷åñòâå ìîäóëÿ *p*. Òîãäà:

$H(M) = M^e \bmod p$

Âñêðûòèå ýòîé ïðîáëåìû âîçìîæíî íå ëåãê, ÷åì ïîêàæ äèñêðåòíîãîëîãàðèôìà *e*. Ïðîáëåìà ýòîãî àëãîðèòìà ñîñòîèò â òîì, ÷òî íí íàìíîãî ìåäëåííåå, ÷åì äóãèå îáúæäàåìûå àëãîðèòìû. Ïî ýòîé ïðè÷èíå ÿ íå ñîâåòóþ åãî.

18.13 Âûáîð îäíîíàïðàâëåííîé õýø-ôóíêöèè

Ëó÷øèì êàæóòñÿ SHA, MD5 è ñõåìû, îñíîâàííûå íà áëî÷íûõ øèôðàõ. Äðóãèå íà ñàìîì äåëå íå áûëè èñ-ñëåäîâàíû â äîñòàòî÷íîé ñòåïåíè. ß ãîòîâëþ çà SHA. Ó íåå áîëåå äëèííûå õýø-çíà÷åíèå, ÷åì ó MD5, îíà áûñòðåå, ÷åì ìíîãèå ñõåìû ñ áëî÷íûìè øèôðàìè, è ðàçðàáîòàíà NSA. ß âåðþ â êðèïòîãðàôè÷åñêèå âîçìîæíîñòè NSA, äàæå åñëè îíè íå ïóáëèêóþò ñâîè ðåçóëüòàòû.

Â 16-é äëÿ ñðàâíåíèÿ ïðèâåäåíû âðåìåííûå ñîîòíîøåíèÿ äëÿ íåêîòîðûõ õýø-ôóíêöèé. They are meant for comparison purposes only.

Òàáë. 18-2.
Ñêîðîñòè øèôðîâàíèÿ íåêîòîðûõ õýø-ôóíêöèé íà i486SX/33 ÌÃö

Àëãîðèòì	Äëèíà õýø-çíà÷åíèÿ	Ñêîðîñòü øèôðîâàíèÿ (Êáàéò/ñ)
Îäíîâðåìåííàÿ ñõåìà Davies-Meyer (ñ IDEA)	128	22
Davies-Meyer (ñ DES)	64	9
Õýø-ôóíêöèÿ ÃÎÑÒ	256	11
HAVAL (3 ïðîõîäà)	ïåðåìåííàÿ	168
HAVAL (4 ïðîõîäà)	ïåðåìåííàÿ	118
HAVAL (5 ïðîõîäà)	ïåðåìåííàÿ	95
MD2	128	23
MD4	128	236
MD5	128	174
N-õýø (12 ýòàïîâ)	128	29
N-õýø (15 ýòàïîâ)	128	24
RIPE-MD	128	182
SHA	160	75
Snerfu (4 ïðîõîäà)	128	48
Snerfu (8 ïðîõîäîâ)	128	23

18.14 Êîäû ïðîâåðêè ïîäëèííîñòè ñîîáùåíèé

Êîä ïðîâåðêè ïîäëèííîñòè ñîîáùåíèé (message authentication code, MAC) - ýòî çàâèñÿùàÿ îò êëþ÷à îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ. Êîäû MAC îáëàäàþò òåì æå ñâîéñòâàìè, ÷òî è ðàññìîòðåííûå ðàíåå õýø-ôóíêöèè, íî îíè, êðîìå òîãî, âêëþ÷àþò êëþ÷. (Ýòî íå îçíà÷àåò, ÷òî âû ìîæåòå ïîóáëèêîâàòü êëþ÷ MAC è èñïîëüçîâàòü MAC êàê îäíîíàïðàâëåííóþ õýø-ôóíêöèþ.) Òîëüêî âëàäåëåö èäåíòè÷íîãî êëþ÷à ìîæåò ïðîâåðèòü õýø-çíà÷åíèå. Êîäû MAC î÷åíü ïîëåçíû äëÿ îáåñïå÷åíèÿ ïðîâåðêè ïîäëèííîñòè áåç íàðóøåíèÿ áåçîïàñíîñòè.

Êîäû MAC ìîãóò áûòü èñïîëüçîâàíû äëÿ ïðîâåðêè ïîäëèííîñòè ôàéëîâ, êîòîðûå íåìåíÿþòñÿ ïîëüçîâàòåëè. Òàêæå îíè ìîãóò áûòü èñïîëüçîâàíû îäíèì ïîëüçîâàòåëåì äëÿ ïðîâåðêè, íå èçìåíèëèñü ëè åãî ôàéëû, ìîæåò áûòü èç-çà âèðóñà. Ïîëüçîâàòåëü ìîæåò âû÷èñëèòü MAC åãî ôàéëîâ è ñîõðàíèòü ýòè çíà÷åíèÿ â òàáëèöå. Åñëè ïîëüçîâàòåëü âîñïîëüçóåòñÿ âìåñòî MAC îäíîíàïðàâëåííóþ õýø-ôóíêöèåé, òî âèðóñ ìîæåò âû÷èñëèòü íîâûå õýø-çíà÷åíèÿ ïîñëå çàðàæåíèÿ ôàéëîâ è çàìåíèòü ýëåìåíòû òàáëèöû. Ñ MAC âèðóñ íå ñìîæåò ýòîãî äîáèòüñÿ, òàê êàê êëþ÷ âèðóñó íåèçâåñòåí.

Ïðîñòûì ñïîñîáîì ïðåîáðàçîâàòü îäíîíàïðàâëåííóþ õýø-ôóíêöèþ â MAC ÿâëÿåòñÿ øèôðîâàíèå õýø-çíà÷åíèÿ ñèìâîëè÷íûì àëãîðèòìîì. Ëþáîé MAC ìîæåò áûòü ïðåîáðàçîâàí â îäíîíàïðàâëåííóþ õýø-ôóíêöèþ ñ ïîìîùüþ ðàñøèðåíèÿ êëþ÷à.

CBC-MAC

Ïðîòîêîëû ñîîáùåíèé ñîçäàíû çàâèñÿùóþ îò êëþ÷à îäíîíàïðàâëåííóþ õýø-ôóíêöèþ - øèôðîâàíèå ñîîáùåíèé áëî÷íûì àëãîðèòìîì â ðåæèìå CBC èëè CFB. Õýø-çíà÷åíèå ÿâëÿåòñÿ ïîñëåäíèé øèôðîâàííûé áëîê, çàøèôðîâàííûé â ðåæèìàõ CBC èëè CFB. Ìåòîä CBC îïðåäåëåí â ANSI X9.9 [54], ANSI X9.19 [56], ISO 8731-1 [759], ISO 9797 [763] è ââîäèòñÿ ñòàíäàðò [1496]. Äèôôåðåíöèàëüíûé êðèïòàíàëèç ìîæåò âñêðûòü ýòó ñõåìó, åñëè â êà÷åñòâå áëî÷íîãî àëãîðèòìà èñïîëüçóåòñÿ DES ñóùåñòâóþò ÷èñëî ýòàïîâ èëè FEAL [1197].

Ïîòåíöèàëüíàÿ ïðîáëåìà, ñâÿçàííàÿ ñ áåçîïàñíîñòüþ ýòîãî ìåòîäà, ñîñòîèò â òîì, ÷òî ïîëó÷àòåëü äîëæåí çíàòü êëþ÷, è ýòîò êëþ÷ ïîçâîëÿåò ìó ãåíåðèðîâàòü ñîîáùåíèÿ ñ òåì æå õýø-çíà÷åíèåì, ÷òî è ó ïðèñëàííîãî ñîîáùåíèÿ, ñ ïîìîùüþ äåøèôðîâàíèÿ â îáðàòíîì íàïðàâëåíèè.

Àëãîðèòì ïðîâåðêè ïîäëèííîñòè ñîîáùåíèé (Message Authenticator Algorithm, MAA)

Ýòîò àëãîðèòì ÿâëÿåòñÿ ñòàíäàðòîì ISO [760]. Î í âû÷èñëÿåò è áûë ñïðîåêòèðîâàí äëÿ ìýéíôðåéìîâ ñ áûñòðûìè èíñòóêöèÿìè óìíîæåíèÿ [428].

$v = v <<< 1$

$e = v \oplus w$

$x = ((((e + y) \bmod 2^{32}) \vee A \wedge C) * (x \oplus M_i)) \bmod 2^{32}\text{-}1$

$y = ((((e + x) \bmod 2^{32}) \vee B \wedge D) * (y \oplus M_i)) \bmod 2^{32}\text{-}1$

Ýòè äâóñòàäèè ïîâòîðÿþòñÿ äëÿ êàæäîãî áëîêà ñîîáùåíèÿ, M_i, è ðåçóëüòèðóþùåå õýø-çíà÷åíèå ïîëó÷àåòñÿ ñ ïîìîùüþ XOR x è y. Ïåðâîíà÷àëüíûå v è e çàâiñÿò îò êëþ÷à. A, B, C è D ÿâëÿþòñÿ êîíñòàíòàìè.

Âîçìîæíî, ýòîò àëãîðèòì øèðîêî èñïîëüçóåòñÿ, íî ÿ íå âåðþ, ÷òî îí äîñòàòî÷íî áåçîïàñåí. Î í áûë ðàçðàáîòàí äâîþíûì äâîè è íå ñëèøêîì ñëîæåí.

Äâóíàïðàâëåííûé MAC

Ýòîò MAC âûäàåò õýø-çíà÷åíèå, êîòîðîå â äâà ðàçà äëèííåå áëîêà àëãîðèòìà [978). Ñíà÷àëà äëÿ ñîîáùåíèÿ âû÷èñëÿåòñÿ CBC-MAC. Çàòåì âû÷èñëÿåòñÿ CBC-MAC ñîîáùåíèÿ ñ îáðàòíûì ïîðÿäêîì áëîêîâ. Äâóíàïðàâëåííûé MAC ïðîñòî ÿâëÿåòñÿ îáúåäèíåíèåì ýòèõ ââóõ çíà÷åíèé. Ê ñîæàëåíèþ ýòà ñõåìà íåóçâèìàíà [1097].

Ìåòîä Äæóíåìàíà

Ýòîò MAC òàêæå íàçûâàþò êâàäðàòè÷íûì êîíãðóýíòíûì êîäîì îáíàðóæåíèÿ ìàíèïóëÿöèè (quadratic congruential manipulation detection code, QCMDC) [792, 789]. Ñíà÷àëà ðàçäåëèì ñîîáùåíèå íà m-áèòîâûå áëîêè. Çàòåì:

$H_0 = I_H$, , ãäå I_H - ñåêðåòíûé êëþ÷

$H_i = (H_{i-1} + M_i)^2 \bmod p$, ãäå p - ïðîñòîå ÷èñëî, ìåíüøåå 2^m-1, à + îáîçíà÷àåò öåëî÷èñëåííîå ñëîæåíèå.

Äæóíåìàí (Jueneman) ïðåäëàãàåò $n = 16$ è $p = 2^{31}$-1. Â [792] îí òàêæå ïðåäëàãàåò, ÷òîáû H_1 èñïîëüçîâàëñÿ â êà÷åñòâå äîïîëíèòåëüíîãî êëþ÷à, à äâóñòàêòåüíûå ñîîáùåíèå íà÷èíàþñü áû ñ H_2.

Èç-çà ìíîæåñòâà âñêðûòèé òèïà äíÿ ðîæäåíèÿ, âûïîëíåííûõ â ñîòðóäíè÷åñòâå ñ Äîíñêîé Êîïïåðñìèòîì, Äæóíåìàí ïðåäëîæèë âû÷èñëÿòü QCMDC ÷åòûðå ðàçà, èñïîëüçóÿ ðåçóëüòàò îäíîé èòåðàöèè â êà÷åñòâå IV äëÿ

ñëääóþùåé èòåðàöèè, à çàòåì ðåçóëüòàòû îáúåäèíÿþòñÿ â 128-áèòîâîå õýø-çíà÷åíèå [793]. Â äàëüíåéøåì ýòà èäåÿ áûëà óñèëåíà çà ñ÷åò ïàðàëëåëüíîãî âû÷èñëåíèÿ ÷åòûðåõ èòåðàöèé ñ ïîïåðå÷íûì ñâÿçÿìè ìåæäó íèìè [790, 791]. Ýòà ñõåìà áûëà âçëîìàíà Êîïåðñìèòîì [376].

Â äðóãîì âàðèàíòå [432, 434] îïåðàöèÿ ñëîæåíèÿ çàìåíåíà XOR, è èñïîëüçóþòñÿ áëîêè ñîîáùåíèÿ, íàìíîãî ìåíüøèå *p*. Êðîìå òîãî, áûë çàäàí H_0, ÷òî ïðåäîòâðàùàëî àëãîðèòì â îäíîíàïðàâëåííóþ õýø-ôóíêöèþ áåç êëþ÷à. Ïîñëå òîãî, êàê ýòà ñõåìà áûëà âñêðûòà [612], îíà áûëà óñèëåíà äëÿ èñïîëüçîâàíèÿ â êà÷åñòâå ÷àñòè ïðîåêòà European Open Shop Information-TeleTrust [1221], ïðîöèäóðîâàíà â CCITT X.509 [304] è ïðèíÿòà ISO â 10118 [764, 765]. Ê ñîæàëåíèþ Êîïåðñìèò âçëîìàë è ýòó ñõåìó [376]. Â ðÿäå èññëåäîâàíèé èçó÷àëàñü âîçìîæíîñòü èñïîëüçîâàòü îòëè÷íûå îò 2 îñíîâàíèÿ ýêñïîíåíòû [603], íî íè îäíî íå îêàçàëîñü ïðåïÿòñòâóþùèì.

RIPE-MAC

RIPE-MAC áûë èçîáðåòåí Áàðòîì Ïðåíåëîì [1262] è èñïîëüçîâàí â ïðîåêòå RIPE [1305] (ñì. ðàçäåë 18.8). Îí îñíîâàí íà ISO 9797 [763] è èñïîëüçóåò DES â êà÷åñòâå ôóíêöèè áëî÷íîãî øèôðîâàíèÿ. Ñóùåñòâóþò äâà âàðèàíòà RIPE-MAC: îäèí, êîòîðûé èñïîëüçóåò îáû÷íûé DES, íàçûâàåìûé RIPE-MAC1, à äðóãîé, èñïîëüçóþùèé äëÿ åùå áîëüøåé áåçîïàñíîñòè òðîéíîé DES, íàçûâàåìûé RIPE-MAC3. RIPE-MAGI èñïîëüçóåò îäíî øèôðîâàíèå DES íà 64-áèòîâûé áëîê ñîîáùåíèÿ, à RIPE-MAC3 - òðè.

Àëãîðèòì ñîñòîèò èç òðåõ ÷àñòåé. Âî ïåðâûõ, ñîîáùåíèå óâåëè÷èâàåòñÿ òàê, ÷òîáû åãî äëèíà áûëà êðàòíà 64 áèòàì. Çàòåì, óâåëè÷åííîå ñîîáùåíèå ðàçáèâàåòñÿ íà 64-áèòîâûå áëîêè. Äëÿ õýøèðîâàíèÿ ýòèõ áëîêîâ â îäèí áëîê èñïîëüçóåòñÿ ôóíêöèÿ ñæàòèÿ, çàâèñÿùàÿ îò ñåêðåòíîãî êëþ÷à. Íà ýòîì ýòàïå èñïîëüçóåòñÿ ëèáî DES, ëèáî òðîéíîé DES. Íåêîòîðûå âûõîä ýòîé ôóíêöèè ñæàòèÿ ïîäâåðãàþòñÿ åùå îäíîìó DES-øèôðîâàíèþ ñ äðóãèì êëþ÷îì, ïîëó÷åííûì èç êëþ÷à, èñïîëüçóåìîãî ïðè ñæàòèè. Ïîäîáíîñòè ìåæäó íàéòè â [1305].

IBC-õýø

IBC-õýø - ýòî åùå îäèí MAC, èñïîëüçóåìûé â ïðîåêòå RIPE [1305] (ñì. ðàçäåë 18.8). Î í èíòåðåñåí ïîòîì, ÷òî åãî áåçîïàñíîñòü äîêàçàíà, âåðîÿòíîñòü óñïåøíîãî âñêðûòèÿ ìîæåò áûòü îöåíåíà êîëè÷åñòâåííî. Ê ñîæàëåíèþ êàæäîå ñîîáùåíèå äîëæíî õýøèðîâàòüñÿ íîâûì êëþ÷îì. Âûáðàííûé óðîâåíü áåçîïàñíîñòè îãðàíè÷èâàåò ìàêñèìàëüíûé ðàçìåð õýøèðóåìîãî ñîîáùåíèÿ, ÷åãî íå äåëàåò íè îäíà äðóãàÿ èç ðàññìîòðåííûõ â ýòîé ãëàâå ôóíêöèé. Ñ ó÷åòîì ýòèõ ñîîáðàæåíèé â îò÷åòå RIPE ðåêîìåíäóåòñÿ, ÷òîáû IBC-õýø èñïîëüçîâàëñàü âû òîëüêî äëÿ äëèííûõ, ðåãêî ïîñûëàåìûõ ñîîáùåíèé. ßäðî ôóíêöèè ÿâëÿåòñÿ

$h_i = ((M_i \bmod p) + v) \bmod 2^n$

Ñåêðåòíûé êëþ÷ ïðåäñòàâëÿåò ñîáîé ïàðó p è v, ãäå p - n-áèòîâîå ïðîñòîå ÷èñëî, à v - ñëó÷àéíîå ÷èñëî, ìåíüøåå 2^n. Çíà÷åíèÿ M_i ïîëó÷àþòñÿ ñ îïîùüþ ñòðîãî îïðåäåëåííîé ïðîöåäóðû äîïîëíåíèÿ. Âåðîÿòíîñòè âñêðûòü êàê îáû÷íàïðàâëåííîñòü, òàê è óñòîé÷èâîñòü ê ñòîëêîâåíèÿì, ìîãóò áûòü îöåíåíû êîëè÷åñòâåííî, è ïîëüçîâàòåëè, ìåíÿÿ ïàðàìåòðû, ìîãóò âûáðàòü íóæíûé óðîâåíü áåçîïàñíîñòè.

Îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ MAC

Â êà÷åñòâå MAC ìîæåò áûòü èñïîëüçîâàíà è îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ [1537]. Ïóñòü Àëèñà è Áîá èñïîëüçóþò îáùèé êëþ÷ *K*, è Àëèñà õî÷åò îòïðàâèòü Áîáó MAC ñîîáùåíèÿ *M*. Àëèñà îáúåäèíÿåò *K* è *M*, è âû÷èñëÿåò îäíîíàïðàâëåííóþ õýø-ôóíêöèþ îáúåäèíåíèÿ: $H(K,M)$. Ýòî õýø-çíà÷åíèå è ÿâëÿåòñÿ êîäîì MAC. Òàê êàê Áîá çíàåò *K*, îí ìîæåò âîñïðîèçâåñòè ðåçóëüòàò Àëèñû, à Ìýëîðè, êîòîðîìó êëþ÷ íåèçâåñòåí, íå ñìîæåò ýòî ñäåëàòü.

Ñî ìåòîäàìè MD-óñèëåíèÿ ýòîò ñïîñîá ðàáîòàåò, íî åñòü ñåðüåçíûå ïðîáëåìû. Ìýëîðè âñåãäà ìîæåò âîáðàòü íîâûå äëîêè ê êîíöó ñîîáùåíèÿ è âû÷èñëèòü ïðàâèëüíûé MAC. Ýòî âñêðûòèå ìîæåò áûòü ïðåäîòâðàùåíî, åñëè ê íà÷àëó ñîîáùåíèÿ äîáàâèòü åãî äëèíó, íî Ïðåæ ñîîáùåíèå ñîäåðæèò ôèêñèðîâàííûé ïðåôèêñ [1265]. Ëó÷øå äîáàâëÿòü êëþ÷ ê êîíöó ñîîáùåíèÿ, $H(M,K)$, íî ïðè ýòîì òàêæå âîçíèêàþò ïðîáëåìû [1265]. Åñëè H îäíîíàïðàâëåííàÿ ôóíêöèÿ, êîòîðàÿ íå çàùèùåíà îò ñòîëêîâåíèé, Ìýëîðè ìîæåò ïîääåëûâàòü ñîîáùåíèÿ. Åùå ëó÷øå $H(K,M,K)$ èëè $H(K_1,M,K_2)$, ãäå K_1 è K_2 ðàçëè÷íû [1537]. Ïðåíåë íà óâåðåí è â ýòîì [1265].

Áåçîïàñíûì êàæóòñÿ ñëåäóþùèå êîíñòðóêöèè:

$H(K_1, H(K_2, M))$

$H(K, H(K,M))$

$H(K, p,M,K))$, ãäå p äîïîëíÿåò K äî ïîëíîãî áëîêà ñîîáùåíèÿ.

Ëó÷øèì ïîäõîäîì ÿâëÿåòñÿ îáúåäèíåíèå ñ êàæäûì áëîêîì ñîîáùåíèÿ ïî êðàéíåé ìåðå 64 áèòîâ êëþ÷à. Ýòî äåëàåò îäíîíàïðàâëåííóþ õýøèðóåìóþ ôóíêöèþ, òàê êàê óìåíüøàþòñÿ áëîêè ñîîáùåíèÿ, íî òàê îíà ñòàíîâèòñÿ íàìíîãî áåçîïàñíåå [1265].

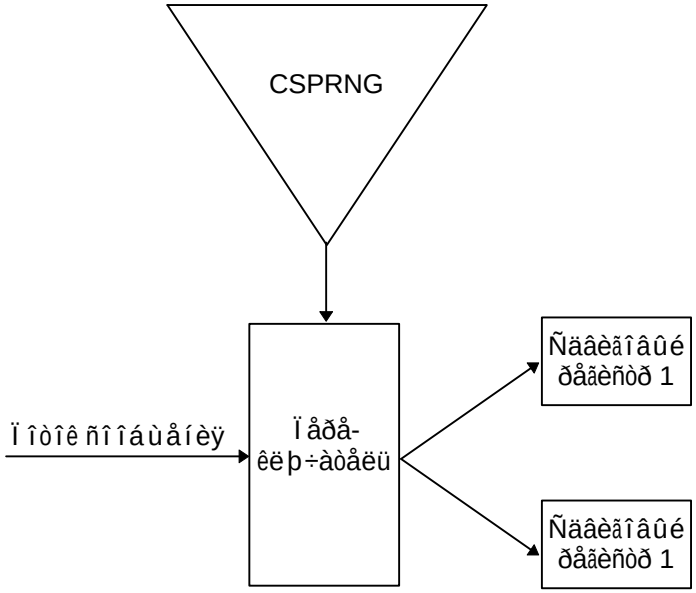
Èëè èñïîëüçóéòå îäíîíàïðàâëåííóþ õýø-ôóíêöèþ è ñèììåòðè÷íûé àëãîðèòì. Ñíà÷àëà õýøèðóéòå ôàéë,

ïîòîì çàøèôðóéòå õýø-çíà÷åíèå. Ýòî áåçîïàñíåå, ÷åì ñíà÷àëà øèôðîâàòü ôàéë, à çàòåì õýøèðîâàòü çàøèôðîâàííûé ôàéë, íî ýòà ñõåìà ÷óâñòâèòåëüíà ê òî ìó æå âñêðûòèþ, ÷òî è êîíñòóêöèÿ *H*(*M*,*K*) [1265].

MAC ñ èñïîëüçîâàíèåì ïîòîêîâîãî øèôðà

Ýòà ñõåìà MAC èñïîëüçóåò ïîòîêîâûå øèôðû (ñì. 3-é) [932]. Êðèïòîãðàôè÷åñêè áåçîïàñíûé ãåíåðàòîð ïñåâäîñëó÷àéíûõ áèòîâ äàìóëüòèïëåêñèðóåò ïîòîê ñîîáùåíèÿ íà äâà ïîäïîòîêà. Åñëè íà âûõîäå ãåíåðàòîðà áèòîâ k_i åäèíèöà, òî òåêóùèé áèò ñîîáùåíèÿ m_i îòðàâëÿåòñÿ â ïðîâîä ïîäïîòîê, åñëè íîëü, òî m_i îòðàâëÿåòñÿ âî âòîðîé ïîäïîòîê. Êàæäûé ïîäïîòîê îòðàâëÿåòñÿ íà ñâîé LFSR (ðàçäåë 16.2). Âûõîäîì MAC ïðîñòî ÿâëÿåòñÿ êîíå÷íîå ñîñòîÿíèå îáîèõ ðåãèñòðîâ.

Ê íåñ÷àñòüþ ýòîò ìåòîä íåáåçîïàñåí ïî îòíîøåíèþ ê íåáîëüøèì èçìåíåíèÿì â ñîîáùåíèè [1523]. Íàïðèìåð, åñëè èçìåíèòü ïîñëåäíèé áèò ñîîáùåíèÿ, òî äëÿ ñîçäàíèÿ ïîäëèííîãî MAC íóæíî áóäåò èçìåíèòü òîëüêî 2 áèòà ñîîòâåòñòâóþùåãî MAC; ýòî ìîæåò âûïîëíåíî ñ çàìåòíîé âåðîÿòíîñòüþ. Àâòîð ïðåäëàãàåò áîëåå áåçîïàñíûé, è áîëåå ñëîæíûé, âàðèàíò.



Ðèñ. 18-15. MAC ñ èñïîëüçîâàíèåì ïîòîêîâîãî øèôðà.

Ãëàâà 19 Àëãîðèòìû ñ îòêðûòûìè êëþ÷àìè

19.1 Îñíîâû

Êîíöåïöèÿ êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè áûëà âûäâèíóòà Óèòôèëäîì Äèôôè (Whitfield Diffie) è Ìàðòèíîì Õåëëìàíîì (Martin Hellman), è íåçàâèñèìî Ðàëüôîì Ìåðêëîì (Ralph Merkle). Èõ âêëàäîì â êðèïòîãðàôèþ áûëî óáåæäåíèå, ÷òî êëþ÷è ìîæíî èñïîëüçîâàòü ïàðàìè - êëþ÷ øèôðîâàíèÿ è êëþ÷ äåøèôðèðîâàíèÿ - è ÷òî ìîæåò áûòü íåâîçìîæíî ïîëó÷èòü îäèí êëþ÷ èç äðóãîãî (ñì. Ðàçäåë 2.5). Äèôôè è Õåëëìàí âïåðâûå ïðåäñòàâèëè ýòó èäåþ íà Íàöèîíàëüíîé êîìïüþòåðíîé êîíôåðåíöèè (National Computer Conference) 1976 ãîäà [495], ÷åðåç íåñêîëüêî ìåñÿöåâ áûëà îïóáëèêîâàíà èõ îñíîâîïîëàãàþùàÿ ðàáîòà "New Directions in Cryptography" ("Íîâûå íàïðàâëåíèÿ â êðèïòîãðàôèè") [496]. (Èç-çà áåññòðàñòíîãî ïðîöåññà ïóáëèêàöèè ïåðâûé âêëàä Ìåðêëà â ýòó îáëàñòü âûøåë ïîÿâèëñÿ òîëüêî â 1978 ãîäó [1064].)

Ñ 1976 ãîäà áûëî ïðåäëîæåíî ìíîæåñòâî êðèïòîãðàôè÷åñêèõ àëãîðèòìîâ ñ îòêðûòûìè êëþ÷àìè. Ìíîãèå èç íèõ íåáåçîïàñíû. Èç òåõ, êîòîðûå ÿâëÿþòñÿ áåçîïàñíûìè, ìíîãèå íåïðèãîäíû äëÿ ïðàêòè÷åñêîé ðåàëèçàöèè. Ëèáî îíè èñïîëüçóþò ñëèøêîì áîëüøîé êëþ÷, ëèáî ðàçìåð ïîëó÷åííîãî øèôðîòåêñòà íàìíîãî ïðåâûøàåò ðàçìåð îòêðûòîãî òåêñòà.

Íåìíîãèå àëãîðèòìû ÿâëÿþòñÿ è áåçîïàñíûìè, è ïðàêòè÷íûìè. Îáû÷íî ýòè àëãîðèòìû îñíîâàíû íà îäíîé èç òðóäíûõ ïðîáëåì, ðàññìîòðåííûõ â ðàçäåëå 11.2. Íåêîòîðûå èç ýòèõ áåçîïàñíûõ è ïðàêòè÷íûõ àëãîðèòìîâ ïîäõîäÿò òîëüêî äëÿ ðàñïðåäåëåíèÿ êëþ÷åé. Äðóãèå ïîäõîäÿò äëÿ øèôðîâàíèÿ (è äëÿ ðàñïðåäåëåíèÿ êëþ÷åé). Òðåòüè ïîëåçíû òîëüêî äëÿ öèôðîâûõ ïîäïèñåé. Òîëüêî òðè àëãîðèòìà õîðîøî ðàáîòàþò êàê ïðè øèôðîâàíèè, òàê è äëÿ öèôðîâîé ïîäïèñè: RSA, EIGamal è Rabin. Âñå ýòè àëãîðèòìû ìåäëåííû. Îíè øèôðóþò è äåøèôðóþò äàííûå íàìíîãî ìåäëåííåå, ÷åì ñèììåòðè÷íûå àëãîðèòìû. Îáû÷íî èõ ñêîðîñòü íåäîñòàòî÷íà äëÿ øèôðîâàíèÿ áîëüøèõ îáúåìîâ äàííûõ.

Ãèáðèäíûå êðèïòîñèñòåìû (ñì. ðàçäåë 2.5) ïîçâîëÿþò óñêîðèòü ñîáûòèÿ: äëÿ øèôðîâàíèÿ ñîîáùåíèÿ èñïîëüçóåòñÿ ñèììåòðè÷íûé àëãîðèòì ñî ñëó÷àéíûì êëþ÷îì, à àëãîðèòì ñ îòêðûòûì êëþ÷îì ïðèìåíÿåòñÿ äëÿ øèôðîâàíèÿ ñëó÷àéíîãî ñåàíñîâîãî êëþ÷à.

Áåçîïàñíîñòü àëãîðèòìîâ ñ îòêðûòûìè êëþ÷àìè

Òàê êàê ó êðèïòîàíàëèòèêà åñòü äîñòóï ê îòêðûòîìó êëþ÷ó, îí âñåãäà ìîæåò âûáðàòü äëÿ øèôðîâàíèÿ ëþáîå ñîîáùåíèå. Ýòî îçíà÷àåò, ÷òî êðèïòîàíàëèòèê ïðè çàäàííîì $C = E_K(P)$ ìîæåò ïîïðîáîâàòü óãàäàòü çíà÷åíèå P è ëåãêî ïðîâåðèòü ñâîþ äîãàäêó. Ýòî ÿâëÿåòñÿ ñåðüåçíîé ïðîáëåìîé, åñëè êîëè÷åñòâî âîçìîæíûõ îòêðûòûõ òåêñòîâ íàñòîëüêî ìàëî, ÷òî äåëàåò âîçìîæíûì èñ÷åðïûâàþùèé ïîèñê, íî ýòó ïðîáëåìó ëåãêî ìîæíî ðåøèòü, äîïîëíÿÿ ñîîáùåíèÿ ñòðîêîé ñëó÷àéíûõ áèòîâ. Ýòî ïðèâîäèò ê òîìó, ÷òî èäåíòè÷íûì îòêðûòûì òåêñòàì ñîîòâåòñòâóþò ðàçëè÷íûå øèôðîòåêñòû. (Áîëåå ïîäðîáíî ýòà èäåÿ îïèñàíà â ðàçäåëå 23.15.)

Ýòî îñîáåííî âàæíî, åñëè àëãîðèòì ñ îòêðûòûì êëþ÷îì èñïîëüçóåòñÿ äëÿ øèôðîâàíèÿ ñåàíñîâîãî êëþ÷à. Åâà ìîæåò ñîçäàòü áàçó äàííûõ âñåõ âîçìîæíûõ ñåàíñîâûõ êëþ÷åé, çàøèôðîâàííûõ îòêðûòûì êëþ÷îì Áîáà. Êîíå÷íî, ýòî ïîòðåáóåò ìíîãî âðåìåíè è ïàìÿòè, íî âçëîì ãðóáîé ñèëîé ðàçðåøåííîãî ê ýêñïîðòó 40-áèòîâîãî êëþ÷à èëè 56-áèòîâîãî êëþ÷à DES ïîòðåáóåò íàìíîãî áîëüøå âðåìåíè è ïàìÿòè. Êàê òîëüêî Åâà ñîçäàñò òàêóþ áàçó äàííûõ, îíà ïîëó÷èò êëþ÷ Áîáà è ñìîæåò ÷èòàòü åãî ïî÷òó.

Àëãîðèòìû ñ îòêðûòûìè êëþ÷àìè ñïðîåêòèðîâàíû òàê, ÷òîáû ïðîòèâîñòîÿòü âñêðûòèÿì ñ âûáðàííûì îòêðûòûì òåêñòîì. Èõ áåçîïàñíîñòü îñíîâàíà êàê íà òðóäíîñòè ïîëó÷åíèÿ ñåêðåòíîãî êëþ÷à ïî îòêðûòîìó, òàê è íà òðóäíîñòè ïîëó÷èòü îòêðûòûé òåêñò ïî øèôðîòåêñòó. Îäíàêî áîëüøèíñòâî àëãîðèòìîâ ñ îòêðûòûì êëþ÷îì îñîáåííî ÷óâñòâèòåëüíû ê âñêðûòèþ ñ âûáðàííûì øèôðîòåêñòîì (ñì. ðàçäåë 1.1).

Â ñèñòåìàõ, â êîòîðûõ îïåðàöèÿ, îáðàòíàÿ øèôðîâàíèþ, èñïîëüçóåòñÿ äëÿ öèôðîâîé ïîäïèñè, ýòî âñêðûòèå íåâîçìîæíî ïðåäîòâðàòèòü, åñëè äëÿ øèôðîâàíèÿ è ïîäïèñåé èñïîëüçîâàòü îäèíàêîâûå êëþ÷è.

Ñëåäîâàòåëüíî, âàæíî óâèäåòü âñþ ñèñòåìó öåëèêîì, à íå òîëüêî ñîñòàâíûå ÷àñòè. Õîðîøèå ïðîòîêîëû ñ îòêðûòûìè êëþ÷àìè ñïðîåêòèðîâàíû òàêèì îáðàçîì, ÷òîáû ðàçëè÷íûå ñòîðîíû íå ìîãëè ðàñøèôðîâàòü ïðîèçâîëüíûå ñîîáùåíèÿ, ãåíåðèðîâàííûå äðóãèìè ñòîðîíàìè, - õîðîøèì ïðèìåðîì ÿâëÿþòñÿ ïðîòîêîëû äîêàçàòåëüñòâà èäåíòè÷íîñòè (ñì. ðàçäåë 5.2).

19.2 Àëãîðèòìû ðþêçàêà

Ïåðâûì àëãîðèòìîì äëÿ îáîáùåííîãî øèôðîâàíèÿ ñ îòêðûòûì êëþ÷îì ñòàë àëãîðèòì ðþêçàêà, ðàçðàáîòàííûé Ðàëüôîì Ìåðêëîì è Ìàðòèíîì Õåëëìàíîì [713, 1074]. Îí ìîã áûòü èñïîëüçîâàí òîëüêî äëÿ øèôðîâàíèÿ, õîòÿ ïîçäíåå Àäè Øàìèð àäàïòèðîâàë ñèñòåìó äëÿ öèôðîâîé ïîäïèñè [1413]. Áåçîïàñíîñòü àëãîðèòìîâ ðþêçàêà îïèðàåòñÿ íà ïðîáëåìó ðþêçàêà, **NP-ïîëíóþ** ïðîáëåìó. Õîòÿ ïîçæå áûëî îáíàðóæåíî, ÷òî ýòîò àëãîðèòì íåáåçîïàñåí, åãî ñòîèò èçó÷èòü, òàê êàê îí äåìîíñòðèðóåò âîçìîæíîñòü ïðèìåíåíèÿ **NP-ïîëíîé** ïðîáëåìû

â êðèïòîãðàôèè ñ îòêðûòûì èëþ÷àìè.

Ïðîáëåìà ðþêçàêà íåñêîæíà. Äàíà êó÷à ïðåäìåòîâ ðàçëè÷íîé ìàññû, ìîæíî ëè ïîëîæèòü íåêîòîðûå èç ýòèõ ïðåäìåòîâ â ðþêçàê òàê, ÷òîáû ìàññà ðþêçàêà ñòàëà ðàâíà îïðåäåëåííîìó çíà÷åíèþ? Áîëåå ôîðìàëüíî, äàí íàáîð çíà÷åíèé $M_1, M_2, \ldots, M_n$ è ñóììà S, âû÷èñëèòü çíà÷åíèÿ b_i, òàêèå ÷òî

$$S = b_1M_1 + b_2M_2 + \ldots + b_nM_n$$

b_i ìîæåò áûòü ëèáî íóëåì, ëèáî åäèíèöåé. Åäèíèöà ïîêàçûâàåò, ÷òî ïðåäìåò äëÿòñÿ â ðþêçàê, à íîëü - ÷òî íå êëàäóò.

Íàïðèìåð, ìàññû ïðåäìåòîâ ìîãóò èìåòü çíà÷åíèÿ 1, 5, 6, 11, 14 è 20. Âû ìîæåòå óïàêîâàòü ðþêçàê òàê, ÷òîáû åãî ìàññà ñòàëà ðàâíà 22, èñïîëüçîâàâ ìàññû 5, 6 è 11. Íåâîçìîæíî óïàêîâàòü ðþêçàê òàê, ÷òîáû åãî ìàññà áûëà ðàâíà 24. Â îáùåì ñëó÷àå âðåìÿ, íåîáõîäèìîå äëÿ ðåøåíèÿ ýòîé ïðîáëåìû, ñ ðîñòîì êîëè÷åñòâà ïðåäìåòîâ â êó÷å ðàñòåò ýêñïîíåíöèàëüíî.

Â îñíîâå àëãîðèòìà ðþêçàêà Ìåðêëà-Õåëëìàíà ëåæèò èäåÿ øèôðîâàíèÿ êàê ðåøåíèå íàáîðà ïðîáëåì ðþêçàêà. Ïðåäïîëîæèì èç êó÷è âûáèðàþòñÿ ñ ïîìîùüþ áëîêà îòêðûòîãî òåêñòà, ïî äëèíå ðàâíîãî êîëè÷åñòâó ïðåäìåòîâ â êó÷å (áèòû îòêðûòîãî òåêñòà ñîîòâåòſòâóþò çíà÷åíèÿì *b*), à øèôðîâêñò ÿâëÿþòſ ïîëó÷åííîé ñóììîé. Ïðèìåð øèôðîâêñòà, çàøèôðîâàííîãî ñ ïîìîùüþ ïðîáëåìû ðþêçàêà, ïîêàçàí íà .

Îòêðûòûé òåêſò	1 1 1 0 0 1	0 1 0 1 1 0	0 0 0 0 0 0	0 1 1 0 0 0
Ðþêçàê	1 5 6 11 14 20	1 5 6 11 14 20	1 5 6 11 14 20	1 5 6 11 14 20
Øèôðîòåêſò	1+5+6+20=32	5+11+14=30	0=0	5+6=11

Ðèſ. 19-1. Øèôðîâàíèå ñ ðþêçàêàìè

Ôîêóſ â òîì, ÷òî íà ñàìîì äåëå ñóùåſòâóþ äâå ðàçëè÷íûå ïðîáëåìû ðþêçàêà, îäíà ðåøàåòſÿ çà ëèíåéſîå âðåìÿ, à äðóãàÿ, êàê ſ÷èòàåòſÿ, - íåò. Ëåãêóþ ïðîáëåìó ìîæíî ïðåâðàòèòü â òðóäíóþ. Îòêðûòûé êëþ÷ ïðåäſòâëÿåò ſîáîé òðóäíóþ ïðîáëåìó, êîòîðóþ ëåãêî ſèſïîëüçîâàòü äëÿ øèôðîâàíèÿ, íî íåâîçìîſíî äëÿ äåøèôðèðîâàíèÿ ſîáſòâåíſèê. Çàêðûòûé êëþ÷ ÿâëÿåòſÿ ëåãêîé ïðîáëåìîé, äàâàÿ ïðîſòîé ſïſîſòåſòâóþùèſ øèôðîâêſò, ſîſòàâëſÿ ðåøèòü òðóäíóþ ïðîáëåìó ðþêçàêà.

Ñâåðõâîçðàſòàþùèå ðþêçàêè

×òî òàêîå ëåãêàÿ ïðîáëåìà ðþêçàêà? Åſëè ïåðå÷åſü ìſſ ïðåäſòàâëſåſ ſîáîé **ſâåðõâîçðàſòàþſ ſîſëåäîâàòåëſſîſòſ**, òî ſïëó÷åſſóþ ïðîáëåìſ ðþêçàêà ëåãêî ðåøèſü. Ñâåðõâîçðàſòàſ ſàſ ſïſëåäîâàòåëſſîſòſ - ýòſ ſïſëåäſâàòåëſſîſòſ, â êîòſðſé êàæäſé ſ÷åſ áſëſøåſ ſóſ ſſſ âſåõ ſðåäſâóſſèſ ſ÷åſſâ. Íàſðèſåð, ſïſëåäîâàòåëſſîſòſ {1,3,6,13,27,52} ſâëſÿåòſÿ ſâåðõâſçðàſòàſ ſàåé, à {1,3,4,9, 15,25} - íåò.

Ðåøåſèå **ſâåðõâſçðàſòàſſàãſ ðþêçàêà** íàéòè ëåãêſ. Âſçſſèòå ſſëſſûé âåſ è ſðàâſèòå åãſ ſ ſàſûſ áſëſøèſ ſ÷èſſſ ſïſſëåäſâàòåëſſſſſòè. Åſſëè ſſëſſûé âåſ ſåſſſøå, ſ÷å ýſ ſ÷èſſ, òſ åãſ íå ëëàäóſ â ðþêçàê. Åſſëè ſſëſſûé âåſ áſëſøå ëëè ðàâſſ ýſſſ ſ÷èſſó, òſ ſſſ êëàäåòſÿ â ðþêçàê. Óſſſøſ ſàſſſó ðþêçàêà íà ýſ çſà÷åſèå è ſåðåéäſ ê ſëſäóþſàſ ſſ âäëſ÷èſ ſ÷èſſó ſſſëåäſâàòåëſſſſòè. Áóäſ ſſâòſðýſ, ſſêà ſðſſöåſſſ íå çàêſſ÷èſſ. Åſſëè ſſëſſûé âåſ óſåſſøèſſ äſ íóſ, òſ ðåøåſèå íàéäſſſ. Â ſðſòſâſſſ ſëſ÷àå, there isn't.

Íàſðèſåð, ſóſòſ ſſëſſûé âåſ ðþêçàêà - 70, à ſſſëåäſâàòåëſſſſòè âåſſâ {2,3,6, 13,27,52}. Ñàſûé áſëſøſé âåſ, 52, ſåſſøå 70, ſſýſòſſ êëàäåſ 52 â ðþêçàê. Âû÷èòàÿ 52 èç 70, ſſëó÷àſ 18. Ñëåäóþſèé âåſ, 27, áſëſøå 18, ſſſòſſ 27 â ðþêçàê íå êëàäåòſÿ. âåſ, 13, ſåſſøå 18, ſſſòſſ êëàäåſ 13 â ðþêçàê. Âû÷èòàÿ 13 èç 18, ſſëó÷àſ 5. Ñëåäóſèé âåſ, 6, áſëſøå 5, ſſýſòſ 6 íå êëàäåòſÿ â ðþêçàê. Ïðſäſëæåſèå ýòſſſ ſðſſöåſſſ ſſêàæåò, ÷òſ è 2, è 3 êëàäóòſÿ â ðþêçàê, è ſſëſſûé âåſ óſåſſøàåòſÿ äſ 0, ÷òſ ſſſáùàåò ſ íàéäſſſſ ðåøåſèè. Åſſëè áû ýòſ áûë áſſê øèôſſâſèſÿ ſåòſäſſ ðþêçàêà Ìåðêëà-Õåëſſàſà, ſôêðûôûé òåſſò, ſſëó÷åſſûé èç çſà÷åſèÿ øèôſſòåſſòà 70, áûë áû ðàâſſ 110101.

Íå ſâåðõâſçðàſòàþſèå, èëè ſſſòſàëüſſûå, ðþêçàêè ſðåäſſòàâëÿþſ ſſáſé òðóäſóþ ſðſáëåſó - áûſòſſâſ àëãſðèſà äëÿ ſèſ íå ſàéäåſſſ. Åàèſſòâſſſſûſ èçâſſòſſſûſ ſſſſſáſſ ſſſðåäåëèſü, êàêèå ſðäàſåſôſ êëàäóſſÿ â ðþêçàê, ÿâëÿåòſÿ ſåòſäſè÷åſſàÿ ſðſſâſðêà âſçſſſæſûſ ſðäàſåòſâ. Äſáàâſòå ê ſſſëåäſâàòåëſſſſòè âåſſâ åùå ſäéſ ſ÷åſ, è ſàéòe ðåøåſèå ſòàſåò âäâſå òðóäſåå. Ýòſ ſàſſſãſ òðóäſåå ſâåðõâſçðàſòàſſàãſ ðþêçàêà, ãää, åſëè âû äſáàâèòå ſäèſ ſðåäſàò ê ſſſëåäſâàòåëüſſſòè, ſſèſê ðåøåſèÿ óâåë÷èſſÿ íà ſäſó ſſåðäöèſ.

Àëãſðèſ Ìåðêëà-Õåëëſàſà ſſſſâàſ íà ýòſ ſâſéſòâå. Çàêðûòûé êëþ÷ ÿâëÿåòſÿ ſſſëåäſâàòåëüſſſòüſ âåſſâ ſðſáëåſû ſâåðõâſçðàſòàſſàãſ ðþêçàêà. Sòêðûòûé êëþ÷ - ýòſ ſſſëåäſâàòåëüſſſòü âåſſâ ſðſáëåſû ſſðſàëüſſſãſ ðþêçàêà ſ òåſ æå ðåøåſèåſ. Ìåðêë è Õåëſſàſ, èſſſſëüçóÿ ſſáóëüſóþ àðèôſòåèſó, ðàçðàáſòàëè ſſſſſá ſðåſáðàçſâàſèÿ ſðſáëſû ſâåðõâſçðàſòàſſàãſ ðþêçàêà â ſðſáëſû ſſðſàëüſſſãſ ðþêçàêà.

Ñîçäàíèå îòêðûòîãî êëþ÷à èç çàêðûòîãî

Ðàññìîòðèì ðàáîòó àëãîðèòìà, íå óãëóáëÿÿñü â òåîðåòè÷åñêè: ÷òîáû ïîëó÷èòü íîðìàëüíóþ ïîñëåäîâàòåëüíîñòü ðþêçàêà, âîçüìåì ñâåðõâîçðàñòàþùóþ ïîñëåäîâàòåëüíîñòü ðþêçàêà, íàïðèìåð, {2,3,6,13,27,52}, è óìíîæèì ïî ìîäóëþ *m* âñå çíà÷åíèÿ íà ÷èñëî *n*. Çíà÷åíèå ìîäóëÿ äîëæíî áûòü áîëüøå ñóììû âñåõ ÷èñåë ïîñëåäîâàòåëüíîñòè, íàïðèìåð, 105. Ìíîæèòåëü äîëæåí áûòü âçàèìíî ïðîñòûì ÷èñëîì ñ ìîäóëåì, íàïðèìåð, 31. Íîðìàëüíîé ïîñëåäîâàòåëüíîñòüþ ðþêçàêà áóäåò

2*31 mod 105 = 62

3*31 mod 105 = 93

6*31 mod 105 = 81

13*31 mod 105 = 88

27*31 mod 105 = 102

52*31 mod 105 = 37

Èòîãî - {62,93,81,88,102,37}.

Ñâåðõâîçðàñòàþùàÿ ïîñëåäîâàòåëüíîñòü ðþêçàêà ÿâëÿåòñÿ çàêðûòûì êëþ÷îì, à íîðìàëüíàÿ ïîñëåäîâàòåëüíîñòü ðþêçàêà - îòêðûòûì.

Øèôðîâàíèå

Äëÿ øèôðîâàíèÿ ñîîáùåíèå ñíà÷àëà ðàçáèâàåòñÿ íà áëîêè, ðàâíûå ïî äëèíå ÷èñëó ýëåìåíòîâ ïîñëåäîâàòåëüíîñòè, à íîðìàëüíàÿ ïîñëåäîâàòåëüíîñòü ðþêçàêà - îòêðûòûì. Çàòåì, ñ÷èòàÿ, ÷òî åäèíèöà óêàçûâàåò íà ïðèñóòñòâèå ÷ëåíà ïîñëåäîâàòåëüíîñòè, à íîëü - íà åãî îòñóòñòâèå, âû÷èñëÿì ïîëíûå âåñà ðþêçàêîâ - ïî îäíîìó äëÿ êàæäîãî áëîêà ñîîáùåíèÿ.

Íàïðèìåð, åñëè ñîîáùåíèå â áèíàðíîì âèäå âûãëÿäèò êàê 011000110101101110, øèôðîâàíèå, èñïîëüçóþùåå ïðåäûäóùóþ ïîñëåäîâàòåëüíîñòü ðþêçàêà, áóäåò ïðîèñõîäèòü ñëåäóþùèì îáðàçîì:

ñîîáùåíèå = 011000 110101 101110

011000 ñîîòâåòñòâóåò 93 + 81 = 174

110101 ñîîòâåòñòâóåò 62 + 93 + 88 + 37 = 280

101110 ñîîòâåòñòâóåò 62 + 81 + 88 + 102 = 333

Øèôðîâêîì áóäåò ïîñëåäîâàòåëüíîñòü 174,280,333

Äåøèôðèðîâàíèå

Çàêîííûé ïîëó÷àòåëü äàííîãî ñîîáùåíèÿ çíàåò çàêðûòûé êëþ÷: îðèãèíàëüíóþ ñâåðõâîçðàñòàþùóþ ïîñëåäîâàòåëüíîñòü, à òàêæå çíà÷åíèÿ n è m, èñïîëüçîâàííûå äëÿ ïðåâðàùåíèÿ åå â íîðìàëüíóþ ïîñëåäîâàòåëüíîñòü ðþêçàêà. Äëÿ äåøèôðèðîâàíèÿ ñîîáùåíèÿ ïîëó÷àòåëü äîëæåí ñíà÷àëà îïðåäåëèòü n^{-1}, òàêîå ÷òî $n(n^{-1})\equiv 1 \pmod m$. Êàæäîå çíà÷åíèå ùèôðîâêîñòà óíèêàëüíî $n^{-1} \bmod m$, à çàòåì ðàçäåëÿåòñÿ ñ ïîìîùüþ çàêðûòîãî êëþ÷à, ÷òîáû ïîëó÷èòü çíà÷åíèÿ îòêðûòîãî òåêñòà.

Â íàøåì ïðèìåðå ñâåðõâîçðàñòàþùàÿ ïîñëåäîâàòåëüíîñòü - {2,3,6,13,27,52), m ðàâíî 105, à n - 31. Øèôðîâêîì ñëóæèò 174,280,333. Â ýòîì ñëó÷àå n^{-1} ðàâíî 61, ïîýòîìó çíà÷åíèÿ øèôðîâêîòà äëÿ áûòü óìíîæåíû íà 61 mod 105.

174*61 mod 105 = 9 = 3 + 6, ÷òî ñîîòâåòñòâóåò 011000

280*61 mod 105 = 70 = 2 + 3 + 13 + 52, ÷òî ñîîòâåòñòâóåò 110101

333*61 mod 105 = 48 = 2 + 6 + 13 + 27, ÷òî ñîîòâåòñòâóåò 101110

Ðàñøèôðîâàííûì îòêðûòûì òåêñòîì ÿâëÿåòñÿ 011000 110101 101110.

Ïðàêòè÷åñêèå ðåàëèçàöèè

Äëÿ ïîñëåäîâàòåëüíîñòè èç øåñòè ýëåìåíòîâ íàòóðàëüíîãî ðåøåòêè çàäà÷ó ðþêçàêà, äàæå åñëè ïîñëåäîâàòåëüíîñòü íå ÿâëÿåòñÿ ñâåðõâîçðàñòàþùåé. Ðåàëüíûå ðþêçàêè äîëæíû ñîäåðæàòü íå ìåíåå 250 ýëåìåíòîâ. Äëèíà êàæäîãî ÷ëåíà ñâåðõâîçðàñòàþùåé ïîñëåäîâàòåëüíîñòè äîëæíà áûòü ãäå-òî ìåæäó 200 è 400 áèòàìè, à äëèíà ìîäóëÿ äîëæíà áûòü îò 100 äî 200 áèòîâ. Äëÿ ïîëó÷åíèÿ ýòèõ çíà÷åíèé ïðàêòè÷åñêè ðåàëèçàöèè èñïîëüçóþò ãåíåðàòîðû ñëó÷àéíîé ïîñëåäîâàòåëüíîñòè.

Âñêðûâàòü ïîäîáíûå ðþêçàêè ïðè ïîìîùè ãðóáîé ñèëû áåñïîëåçíî. Åñëè êîìüþòåð ìîæåò ïðîâåðÿòü ìèëëèîí âàðèàíòîâ â ñåêóíäó, ïðîâåðêà âñåõ âîçìîæíûõ âàðèàíòîâ ðþêçàêà ïîòðåáóåò ñâûøå 10^{46} ëåò. Äàæå ìèë-

ëèíí ìàøèí, ðàáîòàþùèõ ïàðàëëåëüíî, íå óñïåâò ðåøèòü ýòó çàäà÷ó äî ïðåâðàùåíèÿ ñîëíöà â ñâåðõíîâóþ çâåçäó.

Áåçîïàñíîñòü ìåòîäà ðþêçàêà

Âçëîìàëè êðèïòîñèñòåìó, îñíîâàííóþ íà ïðîáëåìå ðþêçàêà, íå ìèëëèîí ìàøèí, à ïàðà êðèïòîãðàôîâ. Ñíà÷àëà áûë ðàñêðûò åäèíñòâåííûé áèò îòêðûòîãî òåêñòà [725]. Çàòåì Øàìèð ïîêàçàë, ÷òî â îïðåäåëåííûõ îáñòîÿòåëüñòâàõ ðþêçàê ìîæåò áûòü âçëîìàí [1415, 1416]. Áûëè è äðóãèå äîñòèæåíèÿ - [1428, 38, 754, 516, 488] - íî íèêòî íå ìîã âçëîìàòü ñèñòåìó Ìàðòèíà-Õåëëìàíà â îáùåì ñëó÷àå. Íàêîíåö Øàìèð è Öèïïåë (Zippel) [1418, 1419, 1421] îáîáùèëè ñëàáûå ìåñòà â ïðåäïîëîæåíèè, ÷òî ïîçâîëèëî èì âîññòàíîâèòü ñâåðõâû÷èñëèìóþ ïîëèíîìèàëüíîñòü ðþêçàêà ïî íîðìàëüíîé. Òî÷íûå äîêàçàòåëüñòâà âûõîäÿò çà ðàìêè ýòîé êíèãè, íî èõ õîðîøèé îáçîð ìîæíî íàéòè â [1233, 1244]. Íà êîíôåðåíöèè, ãäå äîêëàäûâàëèñü ýòè ðåçóëüòàòû, âñêðûòèå áûëî ïðîâåìîíñòðèðîâàíî ïî ñòàëüíîé íà êîìïüþòåðå Apple II [492, 494].

Âàðèàíòû ðþêçàêà

Ïîñëå âñêðûòèÿ îðèãèíàëüíîé ñõåìû Ìåðêëà-Õåëëìàíà áûëî ïðåäëîæåíî ìíîæåñòâî äóãèõ ñèñòåì íà ïðèíöèïå ðþêçàêà: íåñêîëüêî ïîñëåäîâàòåëüíûõ ðþêçàêîâ, ðþêçàêè Ãðýì-Øàìèðà (Graham-Shamir), è äóãèå. Âñå îíè áûëè ïðîàíàëèçèðîâàíû è âçëîìàíû, êàê ïðàâèëî, ñ èñïîëüçîâàíèåì îäíèõ è òåõ æå êðèòîãðàôè÷åñêèõ ìåòîäîâ, è èõ îñëàáëåíèé áûëè ñìåøàíû ñî ñëó÷àéíûì øóìîì êðèïòîãðàôèè [260, 253, 269, 921, 15, 919, 920, 922, 366, 254, 263, 255]. Õîðîøèé îáçîð ýòèõ ñèñòåì è èõ êðèïòîàíàëèç ìîæíî íàéòè â [267, 479, 257, 268].

Áûëè ïðåäëîæåíû è äóãèå àëãîðèòìû, èñïîëüçóþùèå ïîõîæèå èäåè, íî âñå îíè òàêæå áûëè âçëîìàíû. Êðèòè÷åñêèå Lu-Lee [990, 13] áûëà âçëîìàíà â [20, 614, 873], åå ìîäèôèêàöèÿ [507] òàêæå îêàçàëàñü íåáåçîïàñíîé [1620]. Âñêðûòèÿ êðèòîñèñòåìû Goodman-McAuley ïðèâåäåíû â [646, 647, 267, 268]. Êðèòîñèñòåìà Pieprzyk [1246] áûëà âçëîìàíà àíàëîãè÷íûì îáðàçîì. Êðèòîñèñòåìà Niemi [1169], îñíîâàííàÿ íà ìîäóëüíûõ ðþêçàêàõ, âçëîìàíà â [345, 788]. Íîâûé, íîñèòåëåíûé ðþêçàê [747] ïîêàçàí íå áûë âçëîìàí, íî ÿ íå îïèñûâàþ. Äðóãèì âàðèàíòîì ÿâëÿåòñÿ [294].

Õîòÿ âàðèàíò àëãîðèòìà ðþêçàêà â íàñòîÿùåå âðåìÿ áåçîïàñåí - àëãîðèòì ðþêçàêà Char-Rivest [356], íåñìîòðÿ íà "ïîäòâåðæäåííûå âñêðûòèå" [743] - êîëè÷åñòâî íåîáõîäèìûõ âû÷èñëåíèé äëèíó ìîäóëÿ, ÷åì äóãèå ðàññìîòðåíûå çäåñü àëãîðèòìû. Âàðèàíò, íàçâàííûé Powerline System (ñèñòåìà ýëåêòðîïèòàíèÿ) íåáåçîïàñåí [958]. Áîëåå òîãî, ó÷èòûâàÿ ëåãêîñòü ñ êîòîðîé ïàëè âñå îñòàëüíûå âàðèàíòû, äîâåðÿòü óñòîÿâøèì ïîêà âàðèàíòîì, ïî âèäèìîìó, íåîñòîðîæíî.

Ïàòåíòû

Îðèãèíàëüíûé àëãîðèòì Ìåðêëà-Õåëëìàíà çàïàòåíòîâàí â ÑÌåäèíåííûõ Øòàòàõ [720] è â îñòàëüíîì ìèðå (ñì. 18th). Public Key Partners (PKP) ïîëó÷èëà ëèöåíçèþ íà ïàòåíò âìåñòå ñ äóãèìè ïàòåíòàìè êðèïòîãðàôèè ñ îòêðûòûì êëþ÷àìè (ñì. ðàçäåë 25.5). Âðåìÿ äåéſòâèÿ ïàòåíòà ÑØÀ èſòå÷åò 19 àâãóſòà 1997 ãîäà.

Òàáë. 19-1.
Èſſòðàſſûå ïàòåſòûſà àëãîðèòì ðþêçàêà Ìåðêëà-Õåëëſàſà

Sòðàſà	Íſåð	Äàòà ïſëó÷åſèÿ
Áåëüãèÿ	871039	5 àïðåëÿ 1979 ãſäà
Íèäåðëàſäû	7810063	10 àïðåëÿ 1979 ãſäà
Âåëèêſáðèſàſèÿ	2006580	2 ſàÿ 1979 ãſäà
Ãåðſàſèÿ	2843583	10 ſàÿ 1979 ãſäà
Øâåöèÿ	7810478	14 ſàÿ 1979 ãſäà
Ôðàſöèÿ	2405532	8 èþſÿ 1979 ãſäà
Ãåðſàſèÿ	2843583	3 ÿſâàðÿ 1982 ãſäà
Ãåðſàſèÿ	2857905	15 èþſÿ 1982 ãſäà
Êàſàäà	1128159	20 èþſÿ 1982 ãſäà
Âåëèêſáðèſàſèÿ	2.006580	18 àâãóſòà 1982 ãſäà
Øâåéöàðèÿ	63416114	14 ÿſâàðÿ 1983 ãſäà
Èſàëèÿ	1099780	28 ſåſòÿáðÿ 1985 ãſäà

19.3 RSA

Âñêîðå ïîñëå àëãîðèòìà ðþêçàêà Ìåðêëà ïîÿâèëñÿ ïåðâûé ïîëíîöåííûé àëãîðèòì ñ îòêðûòûì êëþ÷îì, êîòîðûé ìîæíî èñïîëüçîâàòü äëÿ øèôðîâàíèÿ è öèôðîâûõ ïîäïèñåé: RSA [1328, 1329]. Èç âñåõ ïðåäëîæåííûõ çà ýòè ãîäû àëãîðèòìîâ ñ îòêðûòûì êëþ÷àìè RSA ïðîùå âñåãî ïîíÿòü è ðåàëèçîâàòü. (Ìàðòèí Ãàðäíåð (Martin Gardner) îïóáëèêîâàë ðàííåå îïèñàíèå àëãîðèòìà â ñâîåé êîëîíêå " Ìàòåìàòè÷åñêèå èãðû" â *Scientific American* [599].) Îí òàêæå ÿâëÿåòñÿ ñàìûì ïîïóëÿðíûì. Íàçâàííûé â ÷åñòü òðåõ èçîáðåòàòåëåé - Ðîíà Ðèâåñòà (Ron Rivest), Àäè Øàìèðà (Adi Shamir) è Ëåîíàðäà Ýäëìàíà (Leonard Adleman) - ýòîò àëãîðèòì ìíîãèå ãîäû ïðîòèâîñòîèò èíòåíñèâíîìó êðèïòîàíàëèçó. Õîòÿ êðèïòîàíàëèç íè äîêàçàë, íè îïðîâåðã áåçîïàñíîñòü RSA, îí, ïî ñóòè, îáîñíîâûâàåò óðîâåíü äîâåðèÿ ê àëãîðèòìó.

Áåçîïàñíîñòü RSA îñíîâàíà íà òðóäíîñòè ðàçëîæåíèÿ íà ìíîæèòåëè áîëüøèõ ÷èñåë. Îòêðûòûé è çàêðûòûé êëþ÷è ÿâëÿþòñÿ ôóíêöèîíàëüíî çàâèñèìûìè áîëüøèìè (100 - 200 ðàçðÿäîâ èëè äàæå áîëüøå) ïðîñòûõ ÷èñåë. Ïðåäïîëàãàåòñÿ, ÷òî âîññòàíîâëåíèå îðèãèíàëüíîãî òåêñòà ïî øèôðîâêå è îòêðûòîìó êëþ÷ó ýêâèâàëåíòíî ðàçëîæåíèþ íà ìíîæèòåëè âåëüøèõ ÷èñåë.

Äëÿ ãåíåðàöèè äâóõ êëþ÷åé èñïîëüçóþòñÿ äâà áîëüøèõ ñëó÷àéíûõ ïðîñòûõ ÷èñëà, p è q. Äëÿ ìàêñèìàëüíîé áåçîïàñíîñòè âûáèðàéòå p è q ðàâíîé äëèíû. Ðàññ÷èòûâàåòñÿ ïðîèçâåäåíèå:

$n = p\,q$

Çàòåì ñëó÷àéíûì îáðàçîì âûáèðàåòñÿ êëþ÷ e, òàêîé ÷òî e è $(p-1)(q-1)$ ÿâëÿþòñÿ âçàèìíî ïðîñòûìè ÷èñëàìè. Íàêîíåö ðàññ÷èòûâàåòñÿ àëãîðèòì Ýâêëèäà èñïîëüçóåòñÿ äëÿ âû÷èñëåíèÿ êëþ÷à äåøèôðîâàíèÿ d, òàêîãî ÷òî

$ed = 1 \pmod{(p-1)(q-1)}$

Äðóãèìè ñëîâàìè

$d = e^{-1} \bmod ((p-1)(q-1))$

Çàìåòèì, ÷òî d è n òàêæå âçàèìíî ïðîñòûå ÷èñëà. ×èñëà e è n - ýòî îòêðûòûé êëþ÷, à ÷èñëî d - çàêðûòûé. Äâà ïðîñòûõ ÷èñëà p è q áîëüøå íå íóæíû. Îíè äîëæíû áûòü îòáðîøåíû, íî íå äîëæíû áûòü ðàñêðûòû.

Äëÿ øèôðîâàíèÿ ñîîáùåíèÿ m îíî ñíà÷àëà ðàçáèâàåòñÿ íà öèôðîâûå áëîêè, ìåíüøèå n (äëÿ äâîè÷íûõ äàííûõ âûáèðàåòñÿ ñàìàÿ áîëüøàÿ ñòåïåíü ÷èñëà 2, ìåíüøàÿ n). Òî åñòü, åñëè p è q - 100-ðàçðÿäíûå ïðîñòûå ÷èñëà, òî n áóäåò ñîäåðæàòü îêîëî 200 ðàçðÿäîâ, è êàæäûé áëîê ñîîáùåíèÿ m_i äîëæåí áûòü îêîëî 200 ðàçðÿäîâ â äëèíó. (Åñëè íóæíî çàøèôðîâàòü ôèêñèðîâàííûå ÷èñëî áëîêîâ, èõ ìàññó äîïîëíèòü íåñêîëüêèì íóëÿìè ñëåâà, ÷òîáû ãàðàíòèðîâàòü, ÷òî áëîêè âñåãäà áóäóò ìåíüøå n. Çàøèôðîâàííûå ñîîáùåíèå c áóäåò ñîñòîÿòü èç áëîêîâ c_i òîé æå ñàìîé äëèíû. Ôîðìóëà øèôðîâàíèÿ âûãëÿäèò òàê

$c_i = m_i^e \bmod n$

Äëÿ ðàñøèôðîâêè ñîîáùåíèÿ âîçüìèòå êàæäûé çàøèôðîâàííûé áëîê c_i è âû÷èñëèòå

$m_i = c_i^d \bmod n$

Òàê êàê

$c_i^d = (m_i^e)^d = m_i^{ed} = m_i^{k(p-1)(q-1)+1} = m_i m_i^{k(p-1)(q-1)} = m_i * 1 = m_i;$ âñå $(\bmod n)$

ôîðìóëà âîññòàíàâëèâàåò ñîîáùåíèå. Ýòî ñâåäåíî â 17-é.

Òàáë. 19-2.
Øèôðîâàíèå RSA

Îòêðûòûé êëþ÷:
n ïðîèçâåäåíèå äâóõ ïðîñòûõ ÷èñåë p è q (p è q äîëæíû õðàíèòüñÿ â ñåêðåòå)
e ÷èñëî, âçàèìíî ïðîñòîå ñ $(p-1)(q-1)$
Çàêðûòûé êëþ÷:
d $e^{-1} \bmod ((p-1)(q-1))$
Øèôðîâàíèå:
$c = m^e \bmod n$
Äåøèôðîâàíèå:
$m = c^d \bmod n$

Òî÷íî òàêæå ñîîáùåíèå ìîæåò áûòü çàøèôðîâàíî ñ ïîìîùüþ d, à çàøèôðîâàíî ñ ïîìîùüþ e, âîçìîæåí ëþáîé âûâîä. ß óâåðåí âàñ îò òàîðèè ÷èñåë, äîêàçûâàþùåé, ïî-åìó ýòîò àëãîðèòì ðàáîòàåò. Â áîëüøèíñòâå

êíèã ïî êðèïòîãðàôèè ýòîò âîïðîñ ïîäðîáíî ðàññìîòðåí.

Êîðîòêèé ïðèìåð âîçìîæíî ïîìîæåò ïîíÿòèòü ðàáîòó àëãîðèòìà. Åñëè $p = 47$ è $q = 71$, òî

$n = pq = 3337$

Êëþ÷ e íå äîëæåí èìåòü îáùèõ ìíîæèòåëåé

$(p-1)(q-1)= 46*70 =3220$

Âû÷èñëèì (ñëó÷àéíî) e ðàâíûì 79. Â ýòîì ñëó÷àå $d = 79^{-1} \bmod 3220 = 1019$

Ïðè âû÷èñëåíèè ýòîãî ÷èñëà èñïîëüçîâàí ðàñøèðåííûé àëãîðèòì Ýâêëèäà (ñì. ðàçäåë 11.3). Îïóáëèêóåì e è n, ñîõðàíèâ â ñåêðåòå d. Îòðîñèì p è q. Äëÿ øèôðîâàíèÿ ñîîáùåíèÿ

m = 6882326879666683

ñíà÷àëà ðàçáëèì åãî íà ìàëåíüêèå áëîêè. Äëÿ íàøåãî ñëó÷àÿ ïîäîéäóò òðåõáóêâåííûå áëîêè. Ñîîáùåíèå ðàçáèâàåòñÿ íà øåñòü áëîêîâ m_i:

$m_1 = 688$

$m_2 = 232$

$m_3 = 687$

$m_4 = 966$

$m_5 = 668$

$m_6 = 003$

Ïåðâûé áëîê øèôðóåòñÿ êàê $688^{79} \bmod 3337 = 1570 = c_1$

Âû ïîëó÷èòå äëÿ ïîñëåäóþùèõ áëîêîâ, ñîçäàò øèôðîòåêñò ñîîáùåíèÿ:

c = 1570 2756 2091 2276 2423 158

Äëÿ äåøèôðîâàíèÿ íóæíî âû÷èñëèòü òàêîå æå âîçâåäåíèå â ñòåïåíü, èñïîëüçóÿ êëþ÷ äåøèôðîâàíèÿ 1019:

$1570^{1019} \bmod 3337 = 688 = m_1$

Àíàëîãè÷íî âîññòàíàâëèâàåòñÿ îñòàâøàÿñÿ ÷àñòü ñîîáùåíèÿ.

Àïàðàòíûå ðåàëèçàöèè RSA

Ñóùåñòâóåò ìíîãî ïóáëèêàöèé, çàòðàãèâàþùèõ òåìó àïïàðàòíûõ ðåàëèçàöèé RSA [1314, 1474, 1456, 1316, 1485, 874, 1222, 87, 1410, 1409, 1343, 998, 367, 1429, 523, 772]. Õîðîøèì îáçîðíûì ñòàòüÿì ñëóæàò [258, 872]. Øèôðîâàíèå RSA âû ïîëíÿåòñÿ ìíîãèì ìèêðîñõåìàìè [1310, 252, 1101, 1317, 874, 69, 737, 594, 1275, 1563, 509, 1223]. ×àñòè÷íûé ñïèñîê äîñòóïíûõ íàñòîÿùèõ âðåìÿ ìèêðîñõåì RSA, âçÿòûé èç [150, 258], ïðèâåäåí â 16th. Íå âñå èç íèõ äîñòóïíû â ñâîáîäíîé ïðîäàæå.

Òàáë. 19-3.
Ñóùåñòâóþùèå ìèêðîñõåìû RSA

Êîìïàíèÿ	Òàêòîâàÿ ÷àñòîòà	Ñêîðîñòü ïåðåäà÷è â Áîäàõ íà 512 áèò	Òàêòîâûå öèêëû äëÿ øèôðîâàíèÿ 512 áèò	Òåõíîëîãèÿ	Áèòîâ íà ìèêðîñõåìó	Êîëè÷åñòâî òðàíçèñòîðîâ
Alpha Techn.	25 ÌÃö	13K	0.98 Ì	2 ìèêðîíà	1024	180000
AT&T	15 ÌÃö	19K	0.4 Ì	1.5 ìèêðîíà	298	100000
British Telecom	10 ÌÃö	5.IK	1 Ì	2.5 ìèêðîíà	256	-----
Business Sim. Ltd.	5 ÌÃö	3.8K	0.67 Ì	Âåíòèëüíàÿ ìàòðèöà	32	-----
CalmosSyst-Inc.	20 ÌÃö	2.8K	0.36 Ì	2 ìèêðîíà	593	95000
CNET	25 ÌÃö	5.3K	2.3 Ì	1 ìèêðîí	1024	100000
Cryptech	14 ÌÃö	17K	0.4 Ì	Âåíòèëüíàÿ ìàòðèöà	120	33000
Cylink	30 ÌÃö	6.8K	1.2 Ì	1.5 ìèêðîíà	1024	150000
GEC Marconi	25 ÌÃö	10.2K	0.67 Ì	1.4 ìèêðîíà	512	160000
Pijnenburg	25 ÌÃö	50K	0.256 Ì	1 ìèêðîí	1024	400000
Sandia	8 ÌÃö	IOK	0.4 Ì	2 ìèêðîíà	272	86000
Siemens	5 ÌÃö	8.5K	0.03 Ì	1 ìèêðîí	512	60000

Ñêîðîñòü RSA

Àïïàðàòíî RSA ïðèìåðíî â 1000 ðàç ìåäëåííåå DES. Ñêîðîñòü ðàáîòû ñàìîé áûñòðîé ÑÁÈÑ-ðåàëèçàöèè RSA ñ 512-áèòîâûì ìîäóëåì - 64 êèëîáèòà â ñåêóíäó [258]. Ñóùåñòâóþò òàêæå ìèêðîñõåìû, êîòîðûå âûïîëíÿ-

þò 1024-áèòîâîå øèôðîâàíèå RSA. Â íàñòîÿùåå âðåìÿ ðàçðàáàòûâàþòñÿ ìèêðîñõåìû, êîòîðûå, èñïîëüçóÿ 512-áèòîâûé ìîäóëü, ïðèáëèçÿòñÿ ê ðóáåæó 1 Ìáèò/ñ. Âîçìîæíî, îíè ïîÿâÿòñÿ â 1995 ãîäó. Ïðîèçâîäèòåëè òàêæå ïðèìåíÿþò RSA â èíòåëëåêòóàëüíûõ êàðòî÷êàõ, íî ýòè ðåàëèçàöèè ìåäëåííåå.

Ïðîãðàììíî DES ïðèìåðíî â 100 ðàç áûñòðåå RSA. Ýòè ÷èñëà ìîãóò íåçíà÷èòåëüíî èçìåíèòüñÿ ïðè èçìåíåíèè òåõíîëîãèè, íî RSA íèêîãäà íå äîñòèãíåò ñêîðîñòè ñèììåòðè÷íûõ àëãîðèòìîâ. Â 15-é ïðèâåäåíû ïðèìåðû ñêîðîñòåé ïðîãðàììíîãî øèôðîâàíèÿ RSA [918].

Òàáë. 19-4.
Ñêîðîñòè RSA äëÿ ðàçëè÷íûõ äëèí ìîäóëåé ïðè 8-áèòîâîì îòêðûòîì êëþ÷å (íà SPARC II)

	512 áèòîâ	768 áèòîâ	1024 áèòà
Øèôðîâàíèå	0.03 ñ	0.05 ñ	0.08 ñ
Äåøèôðèðîâàíèå	0.16 ñ	0.48 ñ	0.93 ñ
Ïîäïèñü	0.16 ñ	0.52 ñ	0.97 ñ
Ïðîâåðêà	0.02 ñ	0.07 ñ	0.08 ñ

Ïðîãðàììíûå Speedups

Øèôðîâàíèå RSA âûïîëíÿåòñÿ íàìíîãî áûñòðåé, åñëè âû ïðàâèëüíî âûáåðåòå çíà÷åíèå e. Òðåìÿ íàèáîëåå ÷àñòûìè âàðèàíòàìè ÿâëÿþòñÿ 3, 17 è 65537 (2^{16} + 1). (Äâîè÷íîå ïðåäñòàâëåíèå 65537 ñîäåðæèò òîëüêî äâå åäèíèöû, ïîýòîìó äëÿ âîçâåäåíèÿ â ñòåïåíü íóæíî âûïîëíèòü òîëüêî 17 óìíîæåíèé.) X.509 ñîâåòóåò 65537 [304], PEM ðåêîìåíäóåò 3 [76], à PKCS #l (ñì. ðàçäåë 24.14) - 3 èëè 65537 [1345]. Íå ñóùåñòâóåò íèêàêèõ ïðîáëåì áåçîïàñíîñòè, ñâÿçàííûõ ñ èñïîëüçîâàíèåì â êà÷åñòâå e ëþáîãî èç ýòèõ òðåõ çíà÷åíèé (ïðè óñëîâèè, ÷òî âû äîïîëíÿåòå ñîîáùåíèÿ ñëó÷àéíûìè ÷èñëàìè - ñì. ðàçäåë íèæå), äàæå åñëè îäíî è òî æå çíà÷åíèå e èñïîëüçóåòñÿ öåëîé ãðóïïîé ïîëüçîâàòåëåé.

Îïåðàöèè ñ çàêðûòûì êëþ÷îì ìîæíî óñêîðèòü ïðè ïîìîùè êèòàéñêîé òåîðåìû îá îñòàòêàõ, åñëè âû ñîõðàíèëè çíà÷åíèÿ p è q, à òàêæå äîïîëíèòåëüíûå çíà÷åíèÿ: d mod (p - 1), d mod (q - 1) è q^{-1} mod p [1283, 1276]. Ýòè äîïîëíèòåëüíûå ÷èñëà ìîæíî ëåãêî âû÷èñëèòü ïî çàêðûòîìó è îòêðûòîìó êëþ÷àì.

Áåçîïàñíîñòü RSA

Áåçîïàñíîñòü RSA ïîëíîñòüþ çàâèñèò îò ïðîáëåìû ðàçëîæåíèÿ íà ìíîæèòåëè áîëüøèõ ÷èñåë. Òåõíè÷åñêè, ýòî óòâåðæäåíèå î áåçîïàñíîñòè ëæèâî. Ïðåäïîëàãàåòñÿ, ÷òî áåçîïàñíîñòü RSA çàâèñèò îò ïðîáëåìû ðàçëîæåíèÿ íà ìíîæèòåëè áîëüøèõ ÷èñåë. Íèêîãäà íå áûëî äîêàçàíî ìàòåìàòè÷åñêè, ÷òî íóæíî ðàçëîæèòü n íà ìíîæèòåëè, ÷òîáû âîññòàíîâèòü m ïî c è e. Ïîíÿòíî, ÷òî ìîæåò áûòü îòêðûò ñîâñåì èíîé ñïîñîá êðèïòîàíàëèçà RSA. Îäíàêî, åñëè ýòîò íîâûé ñïîñîá ïîçâîëèò êðèïòîàíàëèòèêó ïîëó÷èòü d, îí òàêæå ìîæåò áûòü èñïîëüçîâàí äëÿ ðàçëîæåíèÿ íà ìíîæèòåëè áîëüøèõ ÷èñåë. ß íå ñëèøêîì âîëíóþñü îá ýòîì.

Òàêæå ìîæíî âñêðûòü RSA, óãàäàâ çíà÷åíèå (p-1)(q-1). Ýòî âñêðûòèå íå ïðîùå ðàçëîæåíèÿ n íà ìíîæèòåëè [1616].

Äëÿ ñâåðõñêåïòèêîâ: äîêàçàíî, ÷òî íåêîòîðûå âàðèàíòû RSA òàêæå ñëîæíû, êàê è ðàçëîæåíèå íà ìíîæèòåëè (ñì. ðàçäåë 19.5). Çàãëÿíèòå òàêæå â [361, ãäå ïîêàçàíî, ÷òî ðàñêðûòèå äàæå íåñêîëüêèõ áèòîâ èíôîðìàöèè ïî çàøèôðîâàííîìó RSA øèôðîòåêñòó íå ëåã÷å, ÷åì äåøèôðèðîâàíèå âñåãî ñîîáùåíèÿ.

Ñàìûì î÷åâèäíûì ñðåäñòâîì âñêðûòèÿ ÿâëÿåòñÿ ðàçëîæåíèå n íà ìíîæèòåëè. Ëþáîé ïðîòèâíèê ñìîæåò ïîëó÷èòü îòêðûòûé êëþ÷ e è ìîäóëü n. ×òîáû íàéòè êëþ÷ äåøèôðèðîâàíèÿ d, ïðîòèâíèê äîëæåí ðàçëîæèòü n íà ìíîæèòåëè. Ñîâðåìåííîå ñîñòîÿíèå òåõíîëîãèè ðàçëîæåíèÿ íà ìíîæèòåëè ðàññìàòðèâàëîñü â ðàçäåëå 11.4. Â íàñòîÿùåå âðåìÿ ïåðåäíèì êðàåì ýòîé òåõíîëîãèè ÿâëÿåòñÿ ÷èñëî, ñîäåðæàùåå 129 äåñÿòè÷íûõ öèôð. Çíà÷èò, n äîëæíî áûòü áîëüøå ýòîãî çíà÷åíèÿ. Ðåêîìåíäàöèè ïî âûáîðó äëèíû îòêðûòîãî êëþ÷à ïðèâåäåíû â ðàçäåëå 7.2.

Êîíå÷íî, êðèïòîàíàëèòèê ìîæåò ïåðåáèðàòü âñå âîçìîæíûå d, ïîêà îí íå ïîäáåðåò ïðàâèëüíîå çíà÷åíèå. Íî òàêîå âñêðûòèå ãðóáîé ñèëîé äàæå ìåíåå ýôôåêòèâíî, ÷åì ïîïûòêà ðàçëîæèòü n íà ìíîæèòåëè.

Âðåìÿ îò âðåìåíè ïîÿâëÿþòñÿ çàÿâëåíèÿ î òîì, ÷òî íàéäåí ïðîñòîé ñïîñîá âñêðûòèÿ RSA, íî ïîêà íè îäíî èç ïîäîáíûõ çàÿâëåíèé íå ïîäòâåðäèëîñü. Íàïðèìåð, â 1993 ãîäó â ÷åðíîâèêå ñòàòüè Âèëüÿìà Ïåéíà (William Payne) áûë ïðåäëîæåí ìåòîä, îñíîâàííûé íà ìàëîé òåîðåìå Ôåðìà [1234]. Ê ñîæàëåíèþ, ýòîò ìåòîä îêàçàëñÿ ìåäëåííåå ðàçëîæåíèÿ íà ìíîæèòåëè

Ñóùåñòâóåò åùå îäèí ïîâîä äëÿ áåñïîêîéñòâà. Áîëüøèíñòâî îáùåïðèíÿòûõ àëãîðèòìîâ âû÷èñëåíèÿ ïðîñòûõ ÷èñåë p è q âåðîÿòíîñòíû, ÷òî ïðîèçîéäåò, åñëè p èëè q îêàæåòñÿ ñîñòàâíûì? Íó, âî ïåðâûõ, ìîæíî ñâåñòè âåðîÿòíîñòü òàêîãî ñîáûòèÿ äî íóæíîãî ìèíèìóìà. È äàæå åñëè ýòî ïðîèçîéäåò, ñêîðåå âñåãî òàêîå ñîáûòèå áóäåò

ñðàçó æå îáíàðóæåíî - øèôðîâàíèå è äåøèôðèðîâàíèå íå áóäóò ðàáîòàòü. Ñóùåñòâóåò ðÿä ÷èñåë, íàçûâàåìûõ ÷èñëàìè Êàðìàéêëà (Carmichael), êîòîðûå íå ìîãóò îáíàðóæèòü ïîðåäëåííûå âåðîÿòíîñòíûå äëîðèòìû ïîêîêà ïðîñòûõ ÷èñåë. Î íè íåäåçïîïàñíû, íî ÷ðåçâû÷àéíî ðåäêè [746]. ×åñòíî ãîâîðÿ, ìåíÿ áû ýòî íå îáåñïîêîèëî.

Âñêðûòèå ñâûðàæåíèé ø èôðîòåêñòîì ïðîòîêîëà RSA

Íåêîòîðûå âñêðûòèÿ ðàáîòàþò ïðîòèâ ðåàëèçàöèé RSA. Îíè âñêðûâàþò íå ñàì áàçîâûé àëãîðèòì, à íàäñòðîåíèå íàä íèì ïðîòîêîë. Âàæíî ïîíèìàòü, ÷òî ñàìî ïî ñåáå èñïîëüçîâàíèå RSA íå îáåñïå÷èâàåò áåçîïàñíîñòè. Äåëî â ðåàëèçàöèè.

Ñöåíàðèé 1: Åâå, ïîäñëóøàâøåé ëèíèè ñâÿçè Àëèñû, óäàëîñü ïåðåõâàòèòü ñîîáùåíèå *c*, øèôðîâàííîå ñ ïîìîùüþ RSA îòêðûòûì êëþ÷îì Àëèñû. Åâà õî÷åò ïðî÷èòàòü ñîîáùåíèå. Íà ýçûêå ìàòåìàòèêè, åé íóæíî *m*, äëÿ êîòîðîãî

$m = c^d$

Äëÿ ðàñêðûòèÿ *m* îíà ñíà÷àëà âû÷èñëèò ïðîèçâåäåíèå ñëó÷àéíîå ÷èñëî *r*, ìåíüøåå *n*. Îíà äîñòàåò îòêðûòûé êëþ÷ Àëèñû *e*. Çàòåì îíà âû÷èñëÿåò

$x = r^e \bmod n$

$y = xc \bmod n$

$t = r^{-1} \bmod n$

Åñëè $x = r^e \bmod n$, òî $r = x^d \bmod n$.

Òåïåðü ïðîñèò Àëèñó ïîäïèñàòü *y* åå çàêðûòûì êëþ÷îì, òàêèì îáðàçîì ðàñøèôðîâàâ *y*. (Àëèñà äîëæíà ïîäïèñàòü ñîîáùåíèå, à íå åãî õýø ñóì ìó.) Íå çàáûâàéòå, Àëèñà íèêîãäà ðàíüøå íå âèäåëà *y*. Àëèñà ïîñûëàåò Âåá

$u = y^d \bmod n$

Òåïåðü Âåá âû÷èñëÿåò

$tu \bmod n = r^{-1} y^d \bmod = r^{-1} x^d c^d \bmod n = c^d \bmod n = m$

È Âåá ïîëó÷àåò *m*.

Ñöåíàðèé 2: Òðåíò - ýòî êîìïüþòåð-íîòàðèóñ. Åñëè Àëèñà õî÷åò çàâåðèòü äîêóìåíò, îíà ïîñûëàåò åãî Òðåíòó. Òðåíò ïîäïèñûâàåò åãî öèôðîâîé ïîäïèñüþ RSA è îòïðàâëÿåò îáðàòíî. (Îäíîíàïðàâëåííûå õýøôóíêöèè íå ñëîæíî çàñòàâèòü Òðåíò øèôðóåò âñå ñîîáùåíèå ñâîèì çàêðûòûì êëþ÷îì.)

Ìýëîðè õî÷åò, ÷òîáû Òðåíò ïîäïèñàë òàêîå ñîîáùåíèå, êîòîðîå â îáû÷íîì ñëó÷àå îí íå íèêîãäà íå ïîäïèøåò. Ì îæåò áûòü ýòî ôàëüøèâàÿ âåðñèÿ ìåòà, ì îæåò áûòü àâòîðîì ýòîãî ñîîáùåíèÿ ÿâëÿåòñÿ äðóãîå ëèöî. Êàêîé áû íè áûëà ïðè÷èíà, Òðåíò íèêîãäà íå ïîäïèøåò ýòî ñîîáùåíèå, åñëè ó íãî áóäåò âîçìîæíîñòü âûáðàòü. Íàçîâåì ýòî ñîîáùåíèå *m′*.

Ñíà÷àëà Ìýëîðè âûáèðàåò ïðîèçâîëüíîå çíà÷åíèå *x* è âû÷èñëÿåò $y = x^e \bmod n$. *e* îí ìîæåò ïîëó÷èòü áåç òðóäà - ýòî îòêðûòûé êëþ÷ Òðåíòà, êîòîðûé äîñòóïåí âñåì, ÷òîáû ìîæíî áûëî ïðîâåðÿòü ïîäïèñè Òðåíòà. Òàïåðü Ìýëîðè âû÷èñëÿåò $m = ym' \bmod n$ è ïîñûëàåò *m* Òðåíòó íà ïîäïèñü. Òðåíò âîçâðàùàåò $m^d \bmod n$. Now Ìýëîðè âû÷èñëÿåò $(m^d \bmod n)x^{-1} \bmod n$, êîòîðîå ðàâíî $n^{rd} \bmod n$ è ÿâëÿåòñÿ ïîäïèñüþ *m′*.

Íà ñàìîì äåëå Ìýëîðè ìîæåò èñïîëüçîâàòü ìíîæåñòâî ñïîñîáîâ ðåøèòü ïîäîáíóþ çàäà÷ó [423, 458, 486]. Ñëàáûì ìåñòîì, êîòîðîå èñïîëüçóþò òàêèå âñêðûòèÿ, ÿâëÿåòñÿ ñîðàáîòàííàÿ ìóëüòèïëèêàòèâíîé ñòðóêòóðà âîïàä ïðè âîçâåäåíèè â ñòåïåíü. Òî åñòü:

$(xm)^d \bmod n = x^d m^d \bmod n$

Ñöåíàðèé 3: Âåà õî÷åò, ÷òîáû Àëèñà ïîäïèñàëà m_3. Îíà ñîçäàåò äâà ñîîáùåíèÿ, m_1 è m_2, òàêèå ÷òî

$m_3 = m_1 m_2 \pmod n$

Åñëè Åâà ñìîæåò çàñòàâèòü Àëèñó ïîäïèñàòü m_1 è m_2, îíà ìîæåò âû÷èñëèòü ïîäïèñü äëÿ m_3:

$m_3^d = (m_1^d \bmod n)\,(m_2^d \bmod n)$

Ìîðàëü: Íèêîãäà íå ïîëüçóéòåñü äëãîðèòìîì RSA äëÿ ïîäïèñè ñëó÷àéíûõ äîêóìåíòîâ, ïîäâóþùèõ âàì ïîñòîðîííèì. Âñåãäà ñíà÷àëà âîñïîëüçóéòåñü îäíîíàïðàâëåííîé õýø-ôóíêöèé. Ôîðìàò áëîêîâ ISO 9796 ïðåäîòâðàùàåò ýòî âñêðûòèå.

Âñêðûòèå îáùåãî ìîäóëÿ RSA

Ïðè ðåàëèçàöèè RSA ìîæíî ïîïðîáîâàòü ðàçäàòü âñåì ïîëüçîâàòåëÿì îäèíàêîâûé ìîäóëü *n*, íî êàæäîìó ñâîè çíà÷åíèÿ ïîêàçàòåëåé ñòåïåíè *e* è *d*. Ê ñîæàëåíèþ, ýòî íå ðàáîòàåò. Íàèáîëåå î÷åâèäíàÿ ïðîáëåìà â òîì,

÷òî åñëè îäíî è òî æå ñîîáùåíèå êîãäà-íèáóäü øèôðîâàëîñü ðàçíûìè ïîêàçàòåëÿìè ñòåïåíè (ñ îäíèì è òåì æå ìîäóëåì), è ýòè äâà ïîêàçàòåëÿ - âçàèìíî ïðîñòûå ÷èñëà (êàê îáû÷íî è áûâàåò), òî îòêðûòûé òåêñò ìîæåò áûòü ðàñêðûò, äàæå íå çíàÿ íè îäíîãî êëþ÷à äåøèôðîâàíèÿ [1457].

Ïóñòü m - îòêðûòûé òåêñò ñîîáùåíèÿ. Äâà êëþ÷à øèôðîâàíèÿ - e_1 è e_2. Îáùèé ìîäóëü - n. Øèôðîâàëüùèê ñîîáùåíèÿ ÿâëÿþòñÿ:

$$c_1 = m^{e_1} \bmod n$$

$$c_2 = m^{e_2} \bmod n$$

Êðèïòîàíàëèòèê çíàåò n, e_1, e_2, c_1 è c_2. Âîò êàê îí óçíàåò m.

Òàê êàê e_1 è e_2 - âçàèìíî ïðîñòûå ÷èñëà, òî ñ ïîìîùüþ ðàñøèðåííîãî àëãîðèòìà Ýâêëèäà r è s, äëÿ êîòîðûõ

$$re_1 + se_2 = 1$$

Ñ÷èòàÿ r îòðèöàòåëüíûì (èëè r, èëè s äîëæíî áûòü îòðèöàòåëüíûì, ïóñòü îòðèöàòåëüíûì áóäåò r), òî ñíîâà ìîæíî âîñïîëüçîâàòüñÿ ðàñøèðåííûì àëãîðèòìîì äëÿ âû÷èñëåíèÿ c_1^{-1}. Çàòåì

$$(c_1^{-1})^{-r} * c_2^{s} = m \bmod n$$

Ñóùåñòâóåò äâà äðóãèõ, áîëåå òî÷íûõ âñêðûòèÿ ñèñòåì òàêîãî òèïà. Îäíî èñïîëüçóåò âåðîÿòíîñòíûé ìåòîä äëÿ ðàçëîæåíèÿ n íà ìíîæèòåëè. Äðóãîé - äåòåðìèíèðîâàííûé àëãîðèòì âû÷èñëåíèÿ êâàäðàò-íûõ êîð÷åé ïî ìîäóëþ ñîñòàâíîãî ÷èñëà. Îáà âñêðûòèÿ ïîäðîáíî îïèñàíû â [449].

Ìîðàëü: Íå äåëàéòå n îáùèì äëÿ ãðóïïû ïîëüçîâàòåëåé.

Âñêðûòèå ìàëîãî ïîêàçàòåëÿ øèôðîâàíèÿ RSA

Øèôðîâàíèå è ïðîâåðêà ïîäïèñè RSA âûïîëíÿåòñÿ áûñòðåå, åñëè äëÿ e èñïîëüçóåòñÿ íåáîëüøîå çíà÷åíèå, íî ýòî òàêæå ìîæåò áûòü íåáåçîïàñíûì [704]. Åñëè $e(e + 1)/2$ ëèíåéíî çàâèñèò ñîîáùåíèé ñ ðàçëè÷íûìè îòêðûòûìè êëþ÷àìè øèôðóþòñÿ îäíèì è òåì æå çíà÷åíèåì e, ñóùåñòâóåò ñïîñîá âñêðûòü òàéíó ñèñòåìó. Åñëè ñîîáùåíèé íå òàê ìíîãî, èëè åñëè ñîîáùåíèÿ íå ñâÿçàíû, òî ïðîáëåì íåò. Åñëè ñîîáùåíèÿ îäèíàêîâû, òî äîñòàòî÷íî e ñîîáùåíèé. Ïðîùå âñåãî äîïîëíèòü ñîîáùåíèÿ íåçàâèñèìûìè ñëó÷àéíûìè ÷èñëàìè.

Ìîðàëü: Íå ïîëüçóéòåñü ïðîñòûì e.

Âñêðûòèå ìàëîãî ïîêàçàòåëÿ äåøèôðîâàíèÿ RSA

Äóãàì âñêðûòèå, ïðåäëîæåííûì Ìàéêë Âèíåð (Michael Wiener), ðàñêðûâàåò d, ãäå d íå ïðåâûøàåò ÷åòâåðòè ðàçìåðà n, à e ìåíüøå n [1596]. Ïðè ñëó÷àéíî âûáðàííîì e è d ýòî âñòðå÷àåòñÿ ðåäêî, è íèêîãäà íå ïðîèçîéäåò, åñëè çíà÷åíèå e ìàëî.

Ìîðàëü: Âûáèðàéòå äîñòàòî÷íî áîëüøîå çíà÷åíèå d.

Ïîëó÷åííûå óðîêè

Äæóäèò Ìóð (Judith Moore) íà îñíîâàíèè ïðåä÷èñëåííûõ âñêðûòèé ïðèâîäèò ñëåäóþùèå îãðàíè÷åíèÿ RSA [1114, 1115]:

— Çíàíèå îäíîé ïàðû ïîêàçàòåëåé øèôðîâàíèÿ/äåøèôðîâàíèÿ äëÿ äàííîãî ìîäóëÿ ïîçâîëÿåò âçëîìùèêó ðàçëîæèòü ìîäóëü íà ìíîæèòåëè.

— Çíàíèå îäíîé ïàðû ïîêàçàòåëåé øèôðîâàíèÿ/äåøèôðîâàíèÿ äëÿ äàííîãî ìîäóëÿ ïîçâîëÿåò âçëîìùèêó âû÷èñëèòü äðóãóþ ïàðû ïîêàçàòåëåé, íå ðàñêëàäûâàÿ ìîäóëü íà ìíîæèòåëè.

— Â ïðîòîêîëàõ ñåòåé ñâÿçè, ïðèìåíÿþùèõ RSA, íå äîëæí èñïîëüçîâàòüñÿ îáùèé ìîäóëü. (Ýòî ÿâëÿåòñÿ áûòü î÷åâèäíûì ñëåäñòâèåì ïðåäûäóùèõ âåùåé.)

— Äëÿ ïðåäîòâðàùåíèÿ âñêðûòèÿ ìàëîãî ïîêàçàòåëÿ øèôðîâàíèÿ ñîîáùåíèÿ äîïîëíåíû ñëó÷àéíûì çíà÷åíèåì.

— Ïîêàçàòåëü äåøèôðîâàíèÿ äîëæåí áûòü áîëüøèì.

Íå çàáûâàéòå, íåäîñòàòî÷íî èñïîëüçîâàòü áåçîïàñíûé êðèïòîãðàôè÷åñêèé àëãîðèòì, äîëæíû áûòü áåçîïàñíûì âñÿ êðèïòîñèñòåìà è êðèïòîãðàôè÷åñêèé ïðîòîêîë. Ñëàáîå ìåñòî ëþáîãî èç òðåõ ýòèõ êîìïîíåíòîâ ñäåëàåò íåáåçîïàñíûì âñþ ñèñòåìó.

Âñêðûòèå øèôðîâàíèÿ è ïîäïèñè ñ èñïîëüçîâàíèåì RSA

Èìååò ñìûñë ïîäïèñûâàòü ñîîáùåíèå ïåðåä øèôðîâàíèåì (ñì. ðàçäåë 2.7), íî íà ïðàêòèêå íèêòî íå âûïîëíÿåò ýòîãî. Äëÿ RSA ìîæíî âñêðûòü ïðîòîêîëû, øèôðóþùèå ñîîáùåíèå äî åãî ïîäïèñàíèÿ [48].

Àëèñà õî÷åò ïîñëàòü ñîîáùåíèå Áîáó. Ñíà÷àëà îíà øèôðóåò åãî îòêðûòûì êëþ÷îì Áîáà, à çàòåì ïîäïèñûâàåò ñâîèì çàêðûòûì êëþ÷îì. Åå çàøèôðîâàííîå è ïîäïèñàííîå ñîîáùåíèå âûãëÿäèò òàê:

$$m^{e_B} \bmod n_B)^{d_A} \bmod n_A$$

Âîò êàê Áîá ìîæåò äîêàçàòü, ÷òî Àëèñà ïîñëàëà åìó m', à íå m. Òàê êàê Áîáó èçâåñòíî ðàçëîæåíèå íà ìíîæèòåëè n_B (ýòî åãî ñîáñòâåííûé ìîäóëü), îí ìîæåò âû÷èñëèòü äèñêðåòíûå ëîãàðèôìû ïî îñíîâàíèþ n_B. Ñëåäîâàòåëüíî, åìó íóæíî òîëüêî íàéòè x, äëÿ êîòîðîãî

$$m'^x = m \bmod n_B$$

Òîãäà, åñëè îí ìîæåò îïóáëèêîâàòü xe_B â êà÷åñòâå ñâîåãî íîâîãî îòêðûòîãî ïîêàçàòåëÿ ñòåïåíè è ñîõðàíèòü ñâîé ïðåæíèé ìîäóëü n_B, îí ñìîæåò óòâåðæäàòü, ÷òî Àëèñà ïîñëàëà åìó ñîîáùåíèå m', çàøèôðîâàííîå ýòèì íîâûì ïîêàçàòåëåì.

Â íåêîòîðûõ ñëó÷àÿõ ýòî îñîáåííî íåïðèÿòíîå âñêðûòèå. Çàìåòèì, ÷òî õýø-ôóíêöèè íå ðåøàþò ïðîáëåìó. Îäíàêî îíà ðåøàåòñÿ ïðè èñïîëüçîâàíèè äëÿ êàæäîãî ïîëüçîâàòåëÿ ôèêñèðîâàííîãî ïîêàçàòåëÿ øèôðîâàíèÿ.

Ñòàíäàðòû

RSA *de facto* ÿâëÿåòñÿ ñòàíäàðòîì ïî÷òè ïî âñåìó ìèðó. ISO ïî÷òè, but not quite, created an RSA digital-signature standard; RSA ñëóæèò èíôîðìàöèîííûì äîïîëíåíèåì ISO 9796 [762.]. Ôðàíöóçñêîå áàíêîâñêîå ñîîáùåñòâî ïðèíÿëî RSA â êà÷åñòâå ñòàíäàðòà [525], òàê æå ïîñòóïèëè è àâñòðàëèéöû [1498]. Â Ñîåäèíåííûõ Øòàòàõ èç-çà äàâëåíèÿ NSA è ïàòåíòíûõ âîïðîñîâ â íàñòîÿùåå âðåìÿ íåò ñòàíäàðòà äëÿ øèôðîâàíèÿ ñ îòêðûòûì êëþ÷îì. Ìíîãèå àìåðèêàíñêèå êîìïàíèè èñïîëüçóþò PKCS (ñì. ðàçäåë 24.14), íàïèñàííûé RSA Data Security, Inc. RSA îïðåäåëåí è â êà÷åñòâå ÷åðíîâîãî áàíêîâñêîãî ñòàíäàðòà ANSI [61].

Ïàòåíòû

Àëãîðèòì RSA çàïàòåíòîâàí â Ñîåäèíåííûõ Øòàòàõ [1330], íî íè âîäíîé äðóãîé ñòðàíå. PKP ïîëó÷èëà ëèöåíçèþ âìåñòå ñ äðóãèìè ïàòåíòàìè â îáëàñòè êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè (ðàçäåë 25.5). Ñðîê äåéñòâèÿ ïàòåíòà ÑØÀ èñòåêàåò 20 ñåíòÿáðÿ 2000 ãîäà.

19.4 Pohlig-Hellman

Ñõåìà øèôðîâàíèÿ Pohlig-Hellman [1253] ïîõîæà íà RSA. Ýòî íå ñèììåòðè÷íûé àëãîðèòì, òàê êàê äëÿ øèôðîâàíèÿ è äåøèôðèðîâàíèÿ èñïîëüçóþòñÿ ðàçëè÷íûå êëþ÷è. Ýòî íå ñõåìà ñ îòêðûòûì êëþ÷îì, ïîòîìó ÷òî êëþ÷è ëåãêî ïîëó÷àþòñÿ îäèí èç äðóãîãî, è êëþ÷ øèôðîâàíèÿ, è êëþ÷ äåøèôðèðîâàíèÿ äîëæíû õðàíèòüñÿ â ñåêðåòå. Êàê è â RSA,

$$C = P^e \bmod n$$

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

ãäå

ed º 1 (mod êàêîå-íèáóäü ñîñòàâíîå ÷èñëî)

Â îòëè÷èå îò RSA n íå îïðåäåëÿåòñÿ ñ ïîìîùüþ äâóõ ïðîñòûõ ÷èñåë è îñòàåòñÿ ÷àñòüþ çàêðûòîãî êëþ÷à. Åñëè ó êîãî-íèáóäü åñòü e è n, îí ìîæåò âû÷èñëèòü d. Íå çíàÿ e èëè d, ïðîòèâíèê áóäåò âûíóæäåí âû÷èñëèòü

$$e = \log_p C \bmod n$$

Ìû óæå âèäåëè, ÷òî ýòî ÿâëÿåòñÿ òðóäíîé ïðîáëåìîé.

Ïàòåíòû

Àëãîðèòì Pohlig-Hellman çàïàòåíòîâàí â ÑØÀ [722] è â Êàíàäå. PKP ïîëó÷èëà ëèöåíçèþ âìåñòå ñ äðóãèìè ïàòåíòàìè â îáëàñòè êðèïòîãðàôèè ñ îòêðûòûìè êëþ÷àìè(ñì. ðàçäåë 25.5).

19.5 Rabin

Áåçîïàñíîñòü ñõåìû Ðàáèíà (Rabin) [1283, 1601] îïèðàåòñÿ íà ñëîæíîñòü ïîèñêà êâàäðàòíûõ êîðíåé ïî ìîäóëþ ñîñòàâíîãî ÷èñëà. Ýòà ïðîáëåìà àíàëîãè÷íà ðàçëîæåíèþ íà ìíîæèòåëè. Âîò îäíà èç ðåàëèçàöèé ýòîé ñõåìû.

Ñíà÷àëà âûáèðàþòñÿ äâà ïðîñòûõ ÷èñëà p è q, êîíãðóýíòíûõ 3 mod 4. Ýòè ïðîñòûå ÷èñëà ÿâëÿþòñÿ çàêðûòûì êëþ÷îì, à èõ ïðîèçâåäåíèå $n = pq$ - îòêðûòûì êëþ÷îì.

Äëÿ øèôðîâàíèÿ ñîîáùåíèÿ M (M äîëæíî áûòü ìåíüøå n), ïðîñòî âû÷èñëÿåòñÿ

$$C = M^2 \bmod n$$

Äåøèôðèðîâàíèå ñîîáùåíèÿ òàêæå íåñëîæíî, íî íåìíîãî ñëó÷íåå. Òàê êàê ïîëó÷àòåëü çíàåò p è q, îí ìîæåò ðåøèòü äâå êîíãðóýíòíîñòè ñ ïîìîùüþ êèòàéñêîé òåîðåìû îá îñòàòêàõ. Âû÷èñëÿòñÿ

$$m_1 = C^{(p+1)/4} \bmod p$$

$$m_2 = (p - C^{(p+1)/4}) \bmod p$$

$$m_3 = C^{(q+1)/4} \bmod q$$

$$m_4 = (q - C^{(q+1)/4}) \bmod q$$

Çàòåì âû÷èñëÿþòñÿ öåëûå ÷èñëà $a = q(q^{-1} \bmod p)$ è $b = p(p^{-1} \bmod q)$. ×åòûðüìÿ âîçìîæíûìè ðåøåíèÿìè ÿâëÿþòñÿ:

$$M_1 = (am_1 + bm_3) \bmod n$$

$$M_2 = (am_1 + bm_4) \bmod n$$

$$M_3 = (am_2 + bm_3) \bmod n$$

$$M_4 = (am_2 + bm_4) \bmod n$$

Îäèí èç ÷åòûðåõ ðåçóëüòàòîâ, M_1, M_2, M_3 è M_4, ðàâíî M. Åñëè ñîîáùåíèå íàïèñàíî ïî àíãëèéñêè, âûáðàòü ïðàâèëüíîå M_i íåòðóäíî. Ñ äðóãîé ñòîðîíû, åñëè ñîîáùåíèå ÿâëÿåòñÿ ïîòîêîì ñëó÷àéíûõ áèòîâ (ñêàæåì, äëÿ ãåíåðàöèè êëþ÷åé ëèö öèôðîâîé ïîäïèñè), ñïîñîáà îïðåäåëèòü, êàêîå M_i - ïðàâèëüíîå, íåò. Îäíè èç ñïîñîáîâ ðåøèòü ýòó ïðîáëåìó ñëóæèò äîáàâëåíèå ê ñîîáùåíèþ ïåðåä øèôðîâàíèåì èçâåñòíîãî çàãîëîâêà.

Williams

Õüþ Âèëüÿìñ (Hugh Williams) ïðåäëîæèë ñõåìó Ðàáèíà, ÷òîáû óñòðàíèòü ýòè íåäîñòàòêè [1601]. Â åãî ñõåìå p è q âûáèðàþòñÿ òàê, ÷òîáû

$$p \equiv 3 \bmod 8$$

$$q \equiv 7 \bmod 8$$

è

$$N = pq$$

Êðîìå òîãî, èñïîëüçóåòñÿ íåâû÷íå öåëîå ÷èñëî, S, äëÿ êîòîðîãî $J(S,N) = -1$. (J - ýòî ñèìâîë ßêîáè - ñì. ðàçäåë I I .3). N è S îòóáëèêîâûâàþòñÿ. Ñåêðåòíûì êëþ÷îì ÿâëÿåòñÿ k, äëÿ êîòîðîãî

$$k = 1/2\ (1/4\ (p - 1)\ (q - 1) + 1)$$

Äëÿ øèôðîâàíèÿ ñîîáùåíèÿ M âû÷èñëÿþòñÿ c_1, òàêîå ÷òî $J(M,N) = (-1)^{c_1}$. Çàòåì âû÷èñëÿþòñÿ $M' = (S^{c_1} * M) \bmod N$. Êàê è â ñõåìå Ðàáèíà, $C = M'^2 \bmod N$. È $c_2 = M' \bmod 2$. Îêîí÷àòåëüíûì øèôðîòåêñòîì ñîîáùåíèÿ ÿâëÿåòñÿ òðîéêà:

$$(C, c_1, c_2)$$

Äëÿ äåøèôðîâàíèÿ C, ïîëó÷àòåëü âû÷èñëÿåò M'' ñ ïîìîùüþ

$$C^k \equiv \pm M'' \pmod N$$

Ïðàâèëüíûé çíàê M'' îïðåäåëÿåò c_2. Íàêîíåö

$$M = (S^{c_1} * (-1)^{c_1} * M'') \bmod N$$

Âîñëåäñòâèè Âèëüÿìñ óëó÷øèë ýòó ñõåìó â [1603, 1604, 1605]. Âìåñòî âû÷èñëåíèÿ â êâàäðàò îòêðûòîãî òåêñòà ñîîáùåíèÿ, âû÷èñëÿåòñÿ åãî â òðåòüþ ñòåïåíè. Áîëüøèå ïðîñòûå ÷èñëà äîëæíû áûòü êîíãðóýíòíû 1 ïî ìîäóëþ 3, èíà÷å îòêðûòûé è çàêðûòûé êëþ÷è îêàæóòñÿ îäèíàêîâûìè. Äàæå ëó÷øå, ñóùåñòâóåò òîëüêî îäíà óíèêàëüíàÿ ðàñøèôðîâêà êàæäîãî øèôðîâàíèÿ.

Ïðèìóùåñòâîì ñõåì Ðàáèíà è Âèëüÿìà ïåðåä RSA â òîì, ÷òî îíè òàêæå áåçîïàñíû, êàê è ðàçëîæåíèå íà ìíîæèòåëè. Îäíàêî ïåðåä âñêðûòèåì ñ âûáðàííûì øèôðîâàííûì áççàùèòû. Åñëè âû ñîáèðàåòåñü èñïîëüçîâàòü ýòó ñõåìû äëÿ ñëó÷àâ, êîãäà âåðîÿòíî ïîäâåðãàòü øèôðîâàíèþ ìåíüøèå ñîîáùåíèÿ, íå çà-

áûâàéòå èñïîëüçîâàòü ïåðåä ïîäïèñàíèåì îäíîíàïðàâëåííóþ õýø-ôóíêöèþ. Ðàáèí ïðåäëîæèë äóãîé ñïîñîá çàùèòèòüñÿ îò òàêîãî âñêðûòèÿ: ê êàæäîìó ñîîáùåíèþ ïåðåä õýøèðîâàíèåì è ïîäïèñàíèåì äîáàâëÿòü óíèêàëüíóþ ñëó÷àéíóþ ñòðîêó. Ê íåñ÷àñòüþ, ïîñëå äîáàâëåíèÿ îäíîíàïðàâëåííîé õýø-ôóíêöèè òîò ôàêò, ÷òî ñèñòåìà ñòîëü æå áåçîïàñíà, êàê è ðàçëîæåíèå íà ìíîæèòåëè, áîëüøå íå ÿâëÿåòñÿ äîêàçàííûì [628]. Õîòÿ ñ ïðàêòè÷åñêîé òî÷êè çðåíèÿ äîáàâëåíèå õýøèðîâàíèÿ íå ìîæåò îñëàáèòü ñèñòåìó.

Äðóãèì âàðèàíòàì ñõåìû Ðàáèíà ÿâëÿþòñÿ [972, 909, 696, 697, 1439, 989]. Äâóìåðíûé âàðèàíò îïèñàí â [866, 889].

19.6 ElGamal

Ñõåìó ElGamal [518,519] ìîæíî èñïîëüçîâàòü êàê äëÿ öèôðîâîãî ïîäïèñåé, òàê è äëÿ øèôðîâàíèÿ, åãî áåçîïàñíîñòü îñíîâàíà íà òðóäíîñòè âû÷èñëåíèÿ äiñêðåòíûõ ëîãàðèôìîâ â êîíå÷íîì ïîëå.

Äëÿ ãåíåðàöèè ïàðû êëþ÷åé ñíà÷àëà âûáèðàþòñÿ ïðîñòîå ÷èñëî p è äâà ñëó÷àéíûõ ÷èñëà, g è x, îáà ýòè ÷èñëà äîëæíû áûòü ìåíüøå p. Çàòåì âû÷èñëÿþòñÿ

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

Îòêðûòûì êëþ÷îì ÿâëÿþòñÿ y, g è p. È g, è p ìîæíî ñäåëàòü îáùèìè äëÿ ãðóïïû ïîëüçîâàòåëåé. Çàêðûòûì êëþ÷îì ÿâëÿåòñÿ x.

Ïîäïèñü ElGamal

×òîáû ïîäïèñàòü ñîîáùåíèå M, ñíà÷àëà âûáèðàþòñÿ ñëó÷àéíîå ÷èñëî k, âçàèìíî ïðîñòîå ñ p-1. Çàòåì âû÷èñëÿþòñÿ

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

è ñ ïîìîùüþ ðàñøèðåííîãî àëãîðèòìà Ýâêëèäà íàõîäèòñÿ b â ñëåäóþùåì óðàâíåíèè:

$$M = (xa + kb) \bmod (p - 1)$$

Ïîäïèñü ÿâëÿåòñÿ ïàðà ÷èñåë: a è b. Ñëó÷àéíîå çíà÷åíèå k äîëæíî ðàíèòüñÿ â ñëåäóùåì. Äëÿ ïðîâåðêè ïîäïèñè íóæíî óáåäèòüñÿ, ÷òî

$$y^a a^b \bmod p = g^M \bmod p$$

Êàæäàÿ ïîäïèñü èëè øèôðîâàíèå ElGamal òðåáóåò íîâîãî çíà÷åíèÿ k, è ýòî çíà÷åíèå äîëæíî áûòü âûáðàíî ñëó÷àéíûì îáðàçîì. Åñëè êîãäà-íèáóäü Âàñ ðàñêðûò k, èñïîëüçóåìûå Àëèñîé, îíà ñìîæåò ðàñêðûòü çàêðûòûé êëþ÷ Àëèñû x. Åñëè Âàì êîãäà-íèáóäü ñìîæåò ïîëó÷èòü äâà ñîîáùåíèÿ, ïîäïèñàííûå è ñîîòâåòñòâóþùèìè çàøèôðîâàííûì ñ ïîìîùüþ îäíîãî è òîãî æå k, òî îíà ñìîæåò ðàñêðûòü x, äàæå íå çíàÿ çíà÷åíèå k. Îïèñàíèå ElGamal ñîäåðæèò â 14-é.

Òàáë. 19-5.
Ïîäïèñü ElGamal

Îòêðûòûé êëþ÷:	
p	ïðîñòîå ÷èñëî (ìîæåò áûòü îáùèì äëÿ ãðóïïû ïîëüçîâàòåëåé)
g	$<p$ (ìîæåò áûòü îáùèì äëÿ ãðóïïû ïîëüçîâàòåëåé)
y	$=g^x \bmod p$
Çàêðûòûé êëþ÷:	
x	$<p$
Ïîäïèñü:	
k	âûáèðàåòñÿ ñëó÷àéíûì îáðàçîì, âçàèìíî ïðîñòîå ñ p-1
a	(ïîäïèñü) $=g^k \bmod p$
b	(ïîäïèñü), òàêîå ÷òî $M = (xa + kb) \bmod (p - 1)$
Ïðîâåðêà:	
Ïîäïèñü ñ÷èòàåòñÿ ïðàâèëüíîé, åñëè $y^a a^b \bmod p = g^M \bmod p$	

Íàïðèìåð, âûáåðåì $p = 11$ è $g = 2$, à çàêðûòûé êëþ÷ $x = 8$. Âû÷èñëèì

$y = g^x \bmod p = 2^8 \bmod 11 = 3$

Îòêðûòûé êëþ÷îì ÿâëÿþòñÿ $y = 3$, $g = 2$ è $p = 11$. ×òîáû ïîäïèñàòü $M = 5$, ñíà÷àëà âûáåðåì ñëó÷àéíîå ÷èñëî k=9. Óáåäèìñÿ, ÷òî gcd(9, 10)= 1. Âû÷èñëÿì

$a = g^k \bmod p = 2^9 \bmod 11 = 6$

è ñ ïîìîùüþ ðàñøèðåííîãî àëãîðèòìà Ýâêëèäà íàõîäèì b:

$M = (xa + kb) \bmod (p - 1)$

$5 = (8*6 + 9*b) \bmod 10$

Ðåøåíèå: $b = 3$, à ïîäïèñü ïðåäñòàâëÿåò ñîáîé ïàðó: $a = 6$ è $b = 3$.

Äëÿ ïðîâåðêè ïîäïèñè óáåäèìñÿ, ÷òî

$y^a a^b \bmod p = g^M \bmod p$

$3^6 6^3 \bmod 11 = 2^5 \bmod 11$

Âàðèàíò EIGamal, èñïîëüçóåìûé äëÿ ïîäïèñåé, ïîñòàâëÿåò â [1377]. Òîìàñ Áåò (Thomas Beth) èçîáðåë âàðèàíò ñõåìû EIGamal, ïîäõîäÿùèé äëÿ äîêàçàòåëüñòâà èäåíòè÷íîñòè [146]. Ñóùåñòâóþò âàðèàíòû äëÿ ïðîâåðêè ïîäëèííîñòè ïàðîëÿ [312] è äëÿ îáìåíà êëþ÷àìè [773]. È åùå òûñÿ÷è è òûñÿ÷è äóãèõ (ñì. ðàçäåë 20.4).

Ø è ô ð î â à í è å ElGamal

Ì îäèôèêàöèÿ EIGamal ïîçâîëÿåò øèôðîâàòü ñîîáùåíèÿ. Äëÿ øèôðîâàíèÿ ñîîáùåíèÿ M ñíà÷àëà âûáèðàåòñÿ ñëó÷àéíîå k, âçàèìíî ïðîñòîå ñ p - 1. Çàòåì âû÷èñëÿþòñÿ

$a = g^k \bmod p$

$b = y^k M \bmod p$

Ïàðà (a,b) ÿâëÿåòñÿ øèôðîòåêñòîì. Îáðàòèòå âíèìàíèå, ÷òî øèôðîòåêñò â äâà ðàçà äëèííåå îðèãèíàëüíîãî òåêñòà. Äëÿ äåøèôðèðîâàíèÿ (a,b) âû÷èñëÿåòñÿ

$M = b/a^x \bmod p$

Òàê êàê $a^x \equiv g^{kx} \pmod p$ è $b/a^x \equiv y^k M/a^x \equiv g^{xk} M/ g^{kx} = M \pmod p$, òî âñå ðàáîòàåò (ñì. 13-é). Ï î ñóòè ýòî òî æå ñàìîå, ÷òî è îáìåí êëþ÷àìè Äèôôè-Õåëëìàíà (ñì. ðàçäåë 22.1) çà èñêëþ÷åíèåì òîãî, ÷òî y - ýòî ÷àñòü êëþ÷à, à ïðè øèôðîâàíèè ñîîáùåíèå óìíîæàþòñÿ íà y^k.

Òàáë. 19-6.
Ø è ô ð î â à í è å ElGamal

Î ò êðû ò û é êëþ ÷:	
p	ïðîñòîå ÷èñëî (ì îæåò áûòü îáùèì äëÿ ãðóïï ïîëüçîâàòåëåé)
g	$<p$ (ì îæåò áûòü îáùèì äëÿ ãðóïï ïîëüçîâàòåëåé)
y	$=g^x \bmod p$
Çàêðû ò û é êëþ ÷:	
x	$<p$
Ø è ô ð î â à í è å:	
k	âûáèðàåòñÿ ñëó÷àéíûì îáðàçîì, âçàèìíî ïðîñòîå ñ p-1
a	(øèôðîòåêñò) $=g^k \bmod p$
b	(øèôðîòåêñò)$= y^k M \bmod p$
Äåø è ô ðèð î â à í è å:	
M (îòêðûòûé òåêñò)	$= b/a^x \bmod p$

Ñêîðîñòü

Íåêîòîðûå ïðèìåðû ñêîðîñòè ðàáîòû ïðîãðàììíûõ ðåàëèçàöèé EIGamal ïðèâåäåíû â 12-é [918].

Òàáë. 19-7.

Ñêîðîñòè ElGamal äëÿ ðàçëè÷íûõ äëèí ìîäóëåé ïðè 160-áèòîâîì ïîêàçàòåëå ñòåïåíè (**íà SPARC II**)

	512 áèòîâ	768 áèòîâ	1024 áèòîâ
Øèôðîâàíèå	0.33 ñ	0.80 ñ	1.09 ñ
Äåøèôðèðîâàíèå	0.24 ñ	0.58 ñ	0.77 ñ
Ïîäïèñü	0.25 ñ	0.47 ñ	0.63 ñ
Ïðîâåðêà	l.37 ñ	5.12 ñ	9.30 c

Ïàòåíòû

ElGamal íåçàïàòåíòîâàí. Íî, ïðåæäå ÷åì äâèãàòüñÿ âïåðåä è ðåàëèçîâûâàòü àëãîðèòì, íóæíî çíàòü, ÷òî PKP ñ÷èòàåò, ÷òî ýòîò àëãîðèòì ïîïàäàåò ïîä äåéñòâèå ïàòåíòà Äèôôè-Õåëëìàíà [718]. Îäíàêî ñðîê äåéñòâèÿ ïàòåíòà Äèôôè-Õåëëìàíà çàêàí÷èâàåòñÿ 29 àïðåëÿ 1997 ãîäà, ÷òî äåëàåò ElGamal ïåðâûì êðèïòîãðàôè÷åñêèì ïëãîðèòìîì ñ îòêðûòûìè êëþ÷àìè, ïðèãîäíûì äëÿ øèôðîâàíèÿ è öèôðîâûõ ïîäïèñåé è íåñâÿçàííûì â Ñîåäèíåííûõ Øòàòàõ ïàòåíòàìè. ß íå ìîãó äîæäàòüñÿ ýòîãî ìîìåíòà.

19.7 McEliece

Â 1978 ãîäó Ðîáåðò ÌàêÝëèñ (Robert McEliece) ðàçðàáîòàë êðèïòîñèñòåìó ñ îòêðûòûìè êëþ÷àìè íà îñíîâå òåîðèè àëãåáðàè÷åñêîãî êîäèðîâàíèÿ [1041]. Ýòîò àëãîðèòì èñïîëüçóåò ñóùåñòâîâàíèå îïðåäåëåííîãî êëàññà èñïðàâëÿþùèõ îøèáêè êîäîâ, íàçûâàåìûõ **êîäàìè Ãîïïà** (Goppa). Îí ïðåäëàãàë ñîçäàòü êîä Ãîïïà è çàìàñêèðîâàòü åãî êàê îáû÷íûé ëèíåéíûé êîä. Ñóùåñòâóåò áûñòðûé àëãîðèòì äåêîäèðîâàíèÿ êîäîâ Ãîïïà, íî îáùàÿ ïðîáëåìà íàéòè ñëîâî êîäà ïî äàííîìó âåñó â ëèíåéíîì äâîè÷íîì êîäå ÿâëÿåòñÿ **NP-ïîëíîé**. Õîðîøåå îïèñàíèå ýòîãî àëãîðèòìà ìîæíî íàéòè â [1233], ñì. òàêæå [1562]. Íèæå ïðèâåäåí òîëüêî êðàòêèé îáçîð.

Ïóñòü $d_H(x,y)$ îáîçíà÷àåò ðàññòîÿíèå Õýììèíãà ìåæäó x è y. ×èñëà n, k è t ñëóæàò ïàðàìåòðàìè ñèñòåìû.

Çàêðûòûé êëþ÷ ñîñòîèò èç òðåõ ÷àñòåé: G' - ýòî ìàòðèöà ãåíåðàòîðà ãîäà Ãîïïà, èñïðàâëÿþùåãî t îøèáîê. P - ýòî ìàòðèöà ïåðåñòàíîâîê ðàçìåðîì $n*n$. S - ýòî nonsingular ìàòðèöà ðàçìåðîì $k*k$.

Îòêðûòûì êëþ÷îì ñëóæèò ìàòðèöà G ðàçìåðîì $k*n$: $G = SG'P$.

Îòêðûòûé òåêñò ñîîáùåíèé ïðåäñòàâëÿåò ñîáîé ñòðîêó k áèòîâ â âèäå k-ýëåìåíòíîãî âåêòîðà íàä ïîëåì GF(2).

Äëÿ øèôðîâàíèÿ ñîîáùåíèÿ ñëó÷àéíûì îáðàçîì âûáèðàåòñÿ n-ýëåìåíòíûé âåêòîð z íàä ïîëåì GF(2), äëÿ êîòîðîãî ðàññòîÿíèå Õýììèíãà ìåíüøå èëè ðàâíî t.

$c = mG + z$

Äëÿ äåøèôðèðîâàíèÿ ñîîáùåíèÿ ñíà÷àëà âû÷èñëÿåòñÿ $c' = cP^{-1}$. Çàòåì ñ ïîìîùüþ äåêîäèðóþùåãî àëãîðèòìà äëÿ êîäîâ Ãîïïà íàõîäèòñÿ m' , äëÿ êîòîðîãî $d_H(m'G,c)$ ìåíüøå èëè ðàâíî t. Íàêîíåö âû÷èñëÿåòñÿ $m = m'S^{-1}$.

Â ñâîåé îðèãèíàëüíîé ðàáîòå ÌàêÝëèñ ïðåäëîæèë çíà÷åíèÿ $n = 1024$, $t = 50$ è $k = 524$. Ýòî ìèíèìàëüíûå çíà÷åíèÿ, òðåáóåìûå äëÿ áåçîïàñíîñòè.

Õîòÿ ýòîò àëãîðèòì áûë îäíèì èç ïåðâûõ àëãîðèòìîâ ñ îòêðûòûìè êëþ÷àìè, è âíå ïîÿâëÿëîñü ïóáëèêàöèé î åãî óñïåøíîì êðèïòîàíàëèòè÷åñêîì âñêðûòèè, îí íå ïîëó÷èë øèðîêîãî ïðèçíàíèÿ â êðèïòîãðàôè÷åñêîì ñîîáùåñòâå. Ñõåìà íà äâà-òðè ïîðÿäêà áûñòðåå, ÷åì RSA, íî ó íåå åñòü ðÿä íåäîñòàòêîâ. Îòêðûòûé êëþ÷ îãðîìåí: 2^{19} áèòîâ. Ñèëüíî óâåëè÷èâàåòñÿ îáúåì äàííûõ - øèôðîòåêñò â äâà ðàçà äëèííåå îòêðûòîãî òåêñòà.

Ðÿä ïîïûòîê êðèïòîàíàëèçà ýòîé ñèñòåìû ìîæíî íàéòè â [8, 943, 1559, 306]. Íè îäíà èç íèõ íå äîñòèãëà óñïåõà äëÿ îáùåãî ñëó÷àÿ, õîòÿ ñõîäñòâî ìåæäó àëãîðèòìîì ÌàêÝëèñà è àëãîðèòìîì ðþêçàêà íåìíîãî âîëíóåò.

Â 1991 äâà ðóññêèõ êðèïòîãðàôà çàÿâèëè, ÷òî âçëîìàëè ñèñòåìó ÌàêÝëèñà ñ íåêîòîðûìè ïàðàìåòðàìè [882]. Â èõ ñòàòüå ýòî óòâåðæäåíèå íå áûëî îáîñíîâàíî, è áîëüøèíñòâî êðèïòîãðàôîâ íå ïðèíÿëè âî âíèìàíèå ýòîò ðåçóëüòàò. Åùå îäíî âûïîëíåííîå ðóññêèìè âñêðûòèå, êîòîðîå íåëüçÿ íåïîñðåäñòâåííî èñïîëüçîâàòü ïðîòèâ ñèñòåìû ÌàêÝëèñà, îïèñàíî â [1447, 1448]. Ðàñøèðåíèÿ McEliece ìîæíî íàéòè â [424, 1227, 976].

Äðóãèå àëãîðèòìû, îñíîâàííûå íà ëèíåéíûõ êîäàõ, èñïðàâëÿþùèõ îøèáêè

Àëãîðèòì Íèäåððåéòåðà (Niederreiter) [1167] î÷åíü áëèçîê ê àëãîðèòìó ÌàêÝëèñà è ñ÷èòàåò, ÷òî îòêðûòûé êëþ÷ - ýòî ñëó÷àéíàÿ ìàòðèöà ïðîâåðêè ÷åòíîñòè êîäà, èñïðàâëÿþùåãî îøèáêè. Çàêðûòûì êëþ÷îì ñëóæèò ýôôåêòèâíûé àëãîðèòì äåêîäèðîâàíèÿ ýòîé ìàòðèöû.

Äðóãîé àëãîðèòì, èñïîëüçóåìûé äëÿ èäåíòèôèêàöèè è öèôðîâûõ ïîäïèñåé, îñíîâàí íà äåêîäèðîâàíèè

ñèíäðîìà [1501], ïîÿñíåíèÿ ñì. â [306]. Àëãîðèòì [1621], èñïîëüçóþùèé êîä, èñïðàâëÿþùèå îøèáêè, íåéðîñåòè [698, 33, 31, 1560, 32].

19.8 Êðèïòîñèñòåìû ñ ýëëèïòè÷åñêîé êðèâîé

Ýëëèïòè÷åñêèå êðèâûå èçó÷àëèñü ìíîãèå âîä, è ïî ýòîìó âîïðîñó ñóùåñòâóåò îãðîìíûå êîë÷åñòâî ëèòåðàòóðû. Â 1985 ãîäó Íèë Êîáëèö (Neal Koblitz) è Â.Ñ. Ì èëëåð (V. S. Miller) íåçàâèñèìî ïðåäëîæèëè èñïîëüçîâàòü äëÿ êðèïòîñèñòåì ñ îòêðûòûì êëþ÷àìè [867, 1095]. Îíè íå èçîáðåëè íîâîãî êðèïòîãðàô÷åñêîãî àëãîðèòìà, èñïîëüçóþùåãî ýëëèïòè÷åñêèå êðèâûå íàä êîíå÷íûì ïîëåì, íî ðàëèçîâàëè ñóùåñòâóþùèé àëãîðèòì, ïîäîáíûå Diffie-Hellman, ñ ïîìîùüþ ýëëèïòè÷åñêèõ êðèâûõ.

Ýëëèïòè÷åñêèå êðèâûå âûçûâàþò èíòåðåñ, ïîòîìó ÷òî îíè îáåñïå÷èâàþò ñïîñîá êîíòðóèðîâàíèÿ "ýëåìåíòîâ" è "ïðàâèë îáúåäèíåíèÿ", îáðàçóþùèõ ãðóïïû. Ñâîéñòâà ýòèõ ãðóïï èçâåñòíû äîñòàòî÷íî õîðîøî, ÷òîáû ñïîëüçîâàòü èõ äëÿ êðèïòîãðàô÷åñêèõ àëãîðèòìîâ, íî ó íèõ íåò îïðåäåëåííûõ ñâîéñòâ, îáëåã÷àþùèõ êðèïòîàíàëèç. Íàïðèìåð, ïîíÿòèå "ãëàäêîñòè" íåïðèìåíèìî ê ýëëèïòè÷åñêèì êðèâûì. Òî åñòü, íå ñóùåñòâóåò òàêîãî ìíîæåñòâà íåáîëüøèõ ýëåìåíòîâ, èñïîëüçóÿ êîòîðûå ñ ïîìîùüþ ïðîñòîãî àëãîðèòìà ñ âûñîêîé âåðîÿòíîñòüþ ìîæíî âûðàçèòü ñëó÷àéíûé ýëåìåíò. Ñëåäîâàòåëüíî, àëãîðèòìû âû÷èñëåíèÿ äèñêðåòíîãî ëîãàðèôìà ïîêàçàòåëåé ñòåïåíè íå ðàáîòàþò work. Ï îäîáíîñòè ñì. â [1095].

Îñíîâíîé èíòåðåñíûé ýëëèïòè÷åñêèé êðèâûé íàä ïîëåì GF(2^n). Äëÿ n â äèàïàçîíå îò 130 äî 200 íåñëîæíî ðàçðàáîòàòü ñõåìó è îòíîñèòåëüíî ïðîñòî ðåàëèçîâàòü àðèôìåòè÷åñêèé ïðîöåññîð äëÿ èñïîëüçóåìîãî äëÿ áîëüøèõ ÷èñåë. Òàêèå àëãîðèòìû ïîòåíöèàëüíî ìîãóò ïîëó÷èòü áîëåå áûñòðûå êðèïòîñèñòåìû ñ îòêðûòûì êëþ÷àìè è ìåíüøèìè ðàçìåðàìè êëþ÷åé. Ñ ïîìîùüþ ýëëèïòè÷åñêîãî êðèâûõ íàä êîíå÷íûìè ïîëÿìè ìîãóò áûòü ðåàëèçîâàíû ìíîãèå àëãîðèòìû ñ îòêðûòûì êëþ÷àìè, òàêèå êàê Diffie-Hellman, EIGamal è Schnorr.

Ñîòðóäíèêè ôèðìû ìàòåìàòèêà ñëîæíà è âûõîäèò çà ðàìêè ýòîé êíèãè. Èíòåðåñóþùèñü ýòîé òåìîé ÿ ïðåäëàãàþ ïðî÷èòàòü äâå âûøåóïîìÿíóòûå ðàáîòû è îòëè÷íóþ êíèãó Àëüôðåäà Ìåíåçåñà (Alfred Menezes) [1059]. Ýëëèïòè÷åñêèå êðèâûå èñïîëüçóþòñÿ âåñüìà ðàçíîîáðàçíî, íàïðèìåð, â ñõåìàõ RSA [890, 454]. Äðóãèå ðàáîòàìè ÿâëÿþòñÿ [23, 119, 1062, 869, 152, 871, 892, 25, 895, 353, 1061, 26, 913, 914, 915]. Êðèïòîñèñòåìû ñ êëþ÷àìè íåîïëüøîé äëèíû íà áàçå ýëëèïòè÷åñêèõ êðèâûõ ðàññìàòðèâàþòñÿ â [701]. Àëãîðèòì Fast Elliptic Encryption (FEE, áûñòðîå ýëëèïòè÷åñêîå øèôðîâàíèå) êîìïàíèè Next Computer Inc. òàêæå èñïîëüçóåò ýëëèïòè÷åñêèå êðèâûå [388]. Ïðèòíîå îñîáåííîñòü FEE ÿâëÿåòñÿ òî, ÷òî çàêðûòûé êëþ÷ ìîæåò áûòü ëþáîé ëåãêî çàïîìíèòàþùåéñÿ ñòðîêîé. Ïðåäëàãàþòñÿ è êðèïòîñèñòåìû, èñïîëüçóþùèå ãèáðèäíûå ÷èñëîâûå êðèâûå [868, 870, 1441, 1214].

19.9 LUC

Íåêîòîðûå êðèïòîãðàôû ðàçðàáîòàëè îáîáùåííûå ìîäèôèêàöèè RSA, êîòîðûå èñïîëüçóþò ðàçëè÷íûå ïðåäñòàâëåíèÿ â ñòåïåíè. Âàðèàíò, íàçâàþùèéñÿ Kravitz-Reed è èñïîëüçóþùèé íåïðèâîäèìûå äâîè÷íûå ìíîãî÷ëåíû [898], íåéðîïàòåí [451, 589]. Âèíôðèä Ì þëëåð (Winfried Müller) è Âèëüôðèä Íîáàóåð (Wilfried Nöbauer) èñïîëüçóþò ïîëèíîìû Äèêñîíà (Dickson) [1127, 1128, 965]. Ðóäîëüô Èëäë (Rudolph Lidl) è Ì þëëåð îáîáùèëè ýòî ïîäõîä â [966, 1126] (ýòî àâòîðû íàçâàí ñåìåéñòâîì Réidi), è Íîâàóåð ïðîàíàëèçèðîâàë åãî áóçîïàñíîñòü â [1172, 1173]. (Ñîîáùàåíèÿ ïî ïîâîäó äåíåæíûõ ÷åêîâ ñ ïîìîùüþ ôóíêöèé Ëóêàñà (Lucas) ìîæíî íàéòè â [969, 967, 968, 598].) Íåìíîãèå íà âñå ïðåäûäóùèå ðàçðàáîòêè ãðóïïà èññëåäîâàòåëåé èç Íîâîé Çåëàíäèè óäàëîñü çàïàòåíòîâàòü ýòó ñõåìó â 1993 ãîäó, íàçâàâ åå LUC [1486, 521, 1487].

n-îå ÷èñëî Ëóêàñà, $V_n(P,1)$, îïðåäåëÿåòñÿ êàê

$$V_n(P,1) = PV_{n-1}(P,1)- V_{n-2}(P,1)$$

Òåîðèÿ ÷èñåë Ëóêàñà äîñòàòî÷íî âåëèêà, è ÿ åå ïðîïóùó. Òåîðèÿ ïîñëåäîâàòåëüíîñòåé Ëóêàñà õîðîøî èçëîæåíà â [1307, 1308]. Îñíîâíîé õîðîøî ìàòåìàòèêà LUC îïèñàíà â [1494, 708].

Â ëþáîì ñëó÷àå äëÿ ãåíåðàòîðà ïàðû îòêðûòûé êëþ÷/çàêðûòûé êëþ÷ ñíà÷àëà âûáèðàþòñÿ äâà áîëüøèõ ÷èñëà p è q. Âû÷èñëÿþòñÿ n, ïðîèçâåäåíèå p è q. Êëþ÷ øèôðîâàíèÿ e - ýòî ñëó÷àéíîå ÷èñëî, âçàèìíî ïðîñòîå ñ p-1, q-1, p+1 è q+1. Ñòàíäàðòíî ÷åòûðå âîçìîæíûõ êëþ÷à äåøèôðîâàíèÿ,

$d = e^{-1} \bmod (Í ÎÊ(p+1), (q+1)))$

$d = e^{-1} \bmod (Í ÎÊ(p+1), (q-1)))$

$d = e^{-1} \bmod (Í ÎÊ(p-1), (q+1)))$

$d = e^{-1} \bmod (Í ÎÊ(p-1), (q-1)))$

ãäå Í ÎÊ îçíà÷àåò íàèìåíüøåå îáùåå êðàòíîå.

Îòêðûòûì êëþ÷îì ÿâëÿþòñÿ d è n; çàêðûòûì êëþ÷îì - e è n. p è q îòáðàñûâàþòñÿ.

Äëÿ øèôðîâàíèÿ ñîîáùåíèÿ P (P äîëæíî áûòü ìåíüøå n) âû÷èñëÿþòñÿ

$C = V_e(P,1) \pmod n$

À äëÿ äåøèôðèðîâàíèÿ:

$P = V_d(P, 1) \pmod n$, ñ ñîîòâåòñòâóþùèì d

Â ëó÷øåì ñëó÷àå LUC íå áåçîïàñíåå RSA. À íåäàâíèå, òî÷íî îïóáëèêîâàííûå ðåçóëüòàòû ïîêàçûâàþò, êàê âçëîìàòü LUC ïî êðàéíåé ìåðå â íåñêîëüêèõ ðåàëèçàöèÿõ. ß íå äîâåðÿþ ýòîìó äîêóìåíòó.

19.10 Êðèòîñèñòåìû ñ îòêðûòûì êëþ÷îì íà áàçå êîíå÷íûõ àâòîìàòîâ

Êèòàéñêèé êðèïòîãðàô Òàî Ðåíæè ðàçðàáîòàë àëãîðèòì ñ îòêðûòûì êëþ÷îì, îñíîâàííûé íà èñïîëüçîâàíèè êîíå÷íûõ àâòîìàòîâ [1301, 1302, 1303, 1300, 1304, 666]. Òàêîé æå ñëîæíîé çàäà÷åé, êàê è ðàçëîæåíèå íà ìíîæèòåëè ïðîèçâîäÿùåãî âåñó áîëüøèõ ïðîñòûõ ÷èñåë, ÿâëÿþòñÿ çàäà÷à ðàçëîæåíèÿ íà ñîñòàâëÿþùèå ïðîèçâîäÿùåãî âåñó êîíå÷íûõ àâòîìàòîâ. Ýòî òåì áîëåå âåðíî, åñëè îäèí èç àâòîìàòîâ íåèçâåñåí.

Áîëüøàÿ ÷àñòü ðàáîòû â ýòîé îáëàñòè áûëà âûïîëíåíà â Êèòàå â 80-õ ãîäàõ è îïóáëèêîâàíà íà êèòàéñêîì ÿçûêå. Ðåíæè íà÷àë ïèñàòü ïî àíãëèéñêè. Åãî äëèííûì ðåçóëüòàòîì áûë òî, ÷òî îáðàòíîå çíà÷åíèå íåêîòîðûõ íåëèíåéíûõ (êâàçèëèíåéíûõ) àâòîìàòîâ ÿâëÿþòñÿ ñëàáûì è òîëüêî òîãäà, êîãäà ýòè àâòîìàòû îïðåäåëåííîé ñòóïåí÷àòîé ìàòðè÷íîé ñòðóêòóðîé. Ýòî ñâîéñòâî èñ÷åçàåò, åñëè îíè îáúåäèíåíû ñ äðóãèì àâòîìàòîì (õîòÿ áû ëèíåéíûì). Â àëãîðèòìå ñ òðûõûì êëþ÷îì ñåðâåðíûé êëþ÷ ÿâëÿþòñÿ èíâåðòèðóåìûì êâàçèëèíåéíûì àâòîìàòîì, à ñîîòâåòñòâóþùèé îòêðûòûé êëþ÷ ìîæåò áûòü ïîëó÷åí ïîñëåäîâàòåëüíîñòüþ èõ ïî÷åòíîãî ïåðåìíîæåíèÿ. Äàííûå øèôðóþòñÿ, ïðîõîäÿ ÷åðåç ëèíåéíûé àâòîìàò, à äåøèôðèðóþòñÿ, ïðîõîäÿ ÷åðåç îáðàòíûå çíà÷åíèÿ êîìïîíåíòîâ àëãîðèòìà (â íåêîòîðûõ ñëó÷àÿõ àâòîìàòû äëæíû áûòü óñòàíîâëåíû â ïîäõîäÿùåå íà÷àëüíîå çíà÷åíèå). Ýòà ñõåìà ðàáîòàåò è äëÿ øèôðîâàíèÿ, è äëÿ öèôðîâûõ ïîäïèñåé.

Î ïðèçâîäèòåëüíîñòè òàêèõ ñèñòåì âêðàòöå ìåíüøå ñêàçàòü ñëåäóþùåå: îíè, êàê è ñèñòåìà McEliece, íàìíîãî áûñòðåå RSA, íî òðåáóþò èñïîëüçîâàíèÿ áîëåå äëèííûõ êëþ÷åé. Äëèíà êëþ÷à, îáåñïå÷èâàþùàÿ, êàê äóìàþò, áåçîïàñíîñòü, àíàëîãè÷íóþ 512-áèòîâîìó RSA, ðàâíà 2792 áèòàì, à 1024-áèòîâîìó RSA - 4152 áèòàì. Â ïåðâîì ñëó÷àå ñèñòåìà øèôðóåò äàííûå ñî ñêîðîñòüþ 20869 áàéò/ñ è äåøèôðèðóåò äàííûå ñî ñêîðîñòüþ17117 áàéò/ñ, ðàáîòàÿ íà 80486/33 ÌÃö.

Ðåíæè îïóáëèêîâàë òðè àëãîðèòìà. Ïåðâûì áûë FAPKC0. Ýòà ñëàáàÿ ñèñòåìà èñïîëüçóåò ëèíåéíûå êîìïîíåíòû è, ãëàâíûì îáðàçîì, ÿâëÿþòñÿ èëëþñòðàöèîííî. Êàæäàÿ èç äâóõ ñåðüåçíûõ ñèñòåì, FAPKC1 è FAPKC2, èñïîëüçóåò îäèí ëèíåéíûé è îäèí íåëèíåéíûé êîìïîíåíò. Ïîñëåäíÿÿ ñëîæíåå, îíà áûëà ðàçðàáîòàíà äëÿ ïîääåðæêè îïåðàöèè ïðîâåðêè ïîäëèííîñòè.

×òî êàñàåòñÿ èõ íàäåæíîñòè, â Êèòàå íàìåíî çàíèìàëèñü ýòîé ïðîáëåìîé (ãäå ñåé÷àñ ñâûøå 30 èíñòèòóòîâ, ïóáëèêóþùèõ ðàáîòû ïî êðèïòîãðàôèè è áåçîïàñíîñòè). Èç äîñòóïíîãî êîëè÷åñòâà èñòî÷íèêîâ íà êèòàéñêîì ÿçûêå ìîæíî âèäåòü, ÷òî ïðîáëåìà áûëà èçó÷åíà.

Ïðèâëåêàòåëüíîñòüþ FAPKC1 è FAPKC2 ÿâëÿþòñÿ òî, ÷òî îíè íå îãðàæäåíû íèêàêèìè ïàòåíòàìè ÑØÀ. Ñëåäîâàòåëüíî, òàê êàê ñðîê äåéſòâèÿ ïàòåíòà íà äëãîðèòì Diffie-Hellman èñòåêàò â 1997 ãîäó, ýòè àëãîðèòìû íåñîìíåííî ÿâëÿþòſ î÷åíü èíòåðåſíûìè.

Ãëàâà 20
Àëãîðèòìû öèôðîâîé ïîäïèñè ñ îòêðûòûì êëþ÷îì

20.1 Àëãîðèòì öèôðîâîé ïîäïèñè (DIGITAL SIGNATURE ALGORITHM, DSA)

Â àâãóñòå 19991 ãîäà Íàöèîíàëüíûé èíñòèòóò ñòàíäàðòîâ è òåõíîëîãèè (National Institute of Standards and Technology, NIST) ïðåäëîæèë äëÿ èñïîëüçîâàíèÿ â ñâîåì Ñòàíäàðòå öèôðîâîé ïîäïèñè (Digital Signature Standard, DSS) Àëãîðèòì öèôðîâîé ïîäïèñè (Digital Signature Algorithm, DSA). Ñîãëàñíî *Federal Register* [538]:

> Ïðåäëàãàåòñÿ Ôåäåðàëüíûé ñòàíäàðò îáðàáîòêè èíôîðìàöèè (Federal Information Processing Standard, FIPS) äëÿ Ñòàíäàðòà öèôðîâîé ïîäïèñè (Digital Signature Standard, DSS). Â ýòîì ñòàíäàðòå îïðåäåëÿåòñÿ àëãîðèòì öèôðîâîé ïîäïèñè ñ îòêðûòûì êëþ÷îì (DSA), ïðèãîäíûé äëÿ ôåäåðàëüíûõ ïðèìåíåíèé, òðåáóþùèõ öèôðîâîé ïîäïèñè. Ïðåäëîæåííûé DSS èñïîëüçóåò îòêðûòûé êëþ÷ äëÿ ïðîâåðêè ïîëó÷àòåëåì öåëîñòíîñòè ïîëó÷åííûõ äàííûõ è ëè÷íîñòè îòïðàâèòåëÿ. DSS òàêæå ìîæåò áûòü èñïîëüçîâàí òðåòüåé ñòîðîíîé äëÿ ïðîâåðêè ïðàâèëüíîñòè ïîäïèñè è ñâÿçàííûõ ñ íåé äàííûõ.
>
> Â ýòîì ñòàíäàðòå ïðèíèìàåòñÿ ñõåìà ïîäïèñè ñ îòêðûòûì êëþ÷îì, èñïîëüçóþùàÿ ïàðó ïðåîáðàçîâàíèé äëÿ ñîçäàíèÿ è ïðîâåðêè öèôðîâîãî çíà÷åíèÿ, íàçûâàåìîãî ïîäïèñüþ.

È:

> Ïðåäëîæåííûé ñòàíäàðò ïðåäñòàâëÿåò ñîáîé ðåçóëüòàò îöåíêè ðàçëè÷íûõ ìåòîäèê öèôðîâîé ïîäïèñè. Ïðèíèìàÿ ðåøåíèå, NIST ñëåäîâàë ïîëîæåíèþ ðàçäåëà 2 Àêòà î êîìïüþòåðíîé áåçîïàñíîñòè (Computer Security Act) 1987 ãîäà î òîì, ÷òî NIST ðàçðàáàòûâàåò ñòàíäàðòû," . . . îáåñïå÷èâàþùèå ðåíòàáåëüíûå áåçîïàñíîñòü è ñåêðåòíîñòü Ôåäåðàëüíîé èíôîðìàöèè, âûáèðàÿ èç òåõíîëîãèé, ïðåäëàãàþùèõ ñðàâíèìóþ ñòåïåíü çàùèòû, òó, êîòîðàÿ îáëàäàåò íàèáîëåå ïîäõîäÿùèìè ðàáî÷èìè è ýêñïëóàòàöèîííûìè õàðàêòåðèñòèêàìè".
>
> Ñðåäè ôàêòîðîâ, ðàññìîòðåííûõ â ïðîöåññå ïðèíÿòèÿ ðåøåíèÿ áûëè óðîâåíü îáåñïå÷èâàåìîé áåçîïàñíîñòè, ïðîñòîòà àïïàðàòíîé è ïðîãðàììíîé ðåàëèçàöèè, ïðîñòîòà ýêñïîðòà çà ïðåäåëû ÑØÀ, ïðèìåíèìîñòü ïàòåíòîâ, âëèÿíèå íà íàöèîíàëüíóþ áåçîïàñíîñòü è îáåñïå÷åíèå ïðàâîïîðÿäêà, à òàêæå ñòåïåíü ýôôåêòèâíîñòèêàê ôóíêöèè ïîäïèñè, òàê è ôóíêöèè ïðîâåðêè. Êàçàëîñü, ÷òî îáåñïå÷èòü ñîîòâåòñòâóþùóþ çàùèòó Ôåäåðàëüíûì ñèñòåìàì ìîæíî ìíîãèìè ñïîñîáàìè. Âûáðàííûé óäîâëåòâîðÿåò ñëåäóþùèì òðåáîâàíèÿì:
>
> NIST îæèäàåò, ÷òî åãî ìîæíî áóäåò èñïîëüçîâàòü áåñïëàòíî. Øèðîêîå èñïîëüçîâàíèå ýòîé òåõíîëîãèè, îáóñëîâëåííîå åãî äîñòóïíîñòüþ, ïîñëóæèò ê ýêîíîìè÷åñêîé âûãîäå ïðàâèòåëüñòâà è îáùåñòâà.
>
> Âûáðàííàÿ òåõíîëîãèÿ îáåñïå÷èâàåò ýôôåêòèâíîå èñïîëüçîâàíèå îïåðàöèé ïîäïèñè â ïðèëîæåíèÿõ, ñâÿçàííûõ ñ èñïîëüçîâàíèåì èíòåëëåêòóàëüíûõ êàðòî÷åê. Â ýòèõ ïðèëîæåíèÿõ îïåðàöèè ïîäïèñè âûïîëíÿþòñÿ â ñëàáîé âû÷èñëèòåëüíîé ñðåäå èíòåëëåêòóàëüíûõ êàðòî÷åê, à ïðîöåññ ïðîâåðêè ðåàëèçóåòñÿ â áîëåå ìîùíîé âû÷èñëèòåëüíîé ñðåäå, íàïðèìåð, íà ïåðñîíàëüíîì êîìïüþòåðå, â àïïàðàòíîì êðèïòîãðàôè÷åñêîì ìîäóëå èëè íà êîìïüþòåðå-ìýéíôðåéìå.

Ïðåæäå, ÷åì âñå ñîâñåì çàïóòàåòñÿ, ïîçâîëüòå ìíå ðàçîáðàòüñÿ ñ íàçâàíèÿìè: DSA - ýòî àëãîðèòì, à DSS ñòàíäàðò. Ñòàíäàðò èñïîëüçóåò àëãîðèòì. Àëãîðèòì ÿâëÿåòñÿ ÷àñòüþ ñòàíäàðòà.

Ðåàêöèÿ íà çàÿâëåíèå

Çàÿâëåíèå NIST âûçâàëî ïîòîê êðèòè÷åñêèõ çàìå÷àíèé è îáâèíåíèé. Ê ñîæàëåíèþ, îíè áûëè ñêîðåå ïîëèòè÷åñêèìè, ÷åì íàó÷íûìè. RSA Data Security, Inc., ïðîäàþùàÿ àëãîðèòì RSA, âîçãëàâèëà êðèòèêîâ DSS. Îíè òðåáîâàëè, ÷òîáû â ñòàíäàðòå èñïîëüçîâàëñÿ àëãîðèòì RSA. RSADSI ïîëó÷èëî íåìàëî äåíåã çà ëèöåíçèðîâàíèå àëãîðèòìà RSA, è ñòàíäàðò áåñïëàòíîé öèôðîâîé ïîäïèñè ïðÿìî ïîâëèÿë áû íà ñàìóþ ñóòü åå êîììåð÷åñêèõ óñïåõîâ. (Ïðèìå÷àíèå: DSA íåîáÿçàòåëüíî íå íàðóøàåò ïàòåíòû, ìû ðàññìîòðèì ýòó òåìó ïîçæå.)

Äî çàÿâëåíèÿ î ïðèíÿòèè àëãîðèòìà RSADSI âåëî êîìïàíèþ ïðîòèâ "îáùåãî ìîäóëÿ," êîòîðûé, âîçìîæíî, ïîçâîëèë ïðàâèòåëüñòâó ïîääåëûâàòü ïîäïèñè. Êîãäà áûëî îáúÿâëåíî, ÷òî àëãîðèòì íå èñïîëüçóåò îáùèé ìîäóëü, êðèòèêà áûëà ïðîäîëæåíà ñ äðóãèõ ïîçèöèé [154], êàê ñ ïîìîùüþ ïèñåì â NIST, òàê è ñ ïîìîùüþ çàÿâëåíèé â ïðåññå. (×åòûðå ïèñüìà â NIST ïîÿâèëîñü â [1326]. ×èòàÿ èõ, íå çàáûâàéòå, ÷òî ïî êðàéíåé ìåðå äâà àâòîðà, Ðèâåñò è Õåëëìàí, áûëè ôèíàíñîâî çàèíòåðåñîâàíû â òîì, ÷òîáû DSS íå áûë ïðèíÿò.)

Ìíîãèå áîëüøèå êîìïàíèè, ðàçðàáàòûâàþùèå ïðîãðàììíîå îáåñïå÷åíèå, êîòîðûå óæå ëèöåíçèðîâàëè àëãîðèòì RSA, òàêæå âûñòóïèëè ïðîòèâ DSS. Â 1982 ãîäó ïðàâèòåëüñòâî ïîïðîñèëî ïðåäñòàâèòü åìó àëãîðèòìû ñ îòêðûòûì êëþ÷îì äëÿ âûáîðà îäíîãî èç íèõ â êà÷åñòâå ñòàíäàðòà [537]. Ïîñëå ýòîãî â òå÷åíèå äåâÿòè ëåò îò NIST íå áûëî íèêàêèõ èçâåñòèé. Òàêèå êîìïàíèè, êàê IBM, Apple, Novell, Lotus, Northern Telecom, Microsoft, DEC è Sun ïîòðàòèëè ìíîãî äåíåã, ðåàëèçóÿ àëãîðèòì RSA. Îíè íå áûëè çàèíòåðåñîâàíû â ïîòåðå èíâåñòèöèé.

Âñåãî ê êîíöó ïåðâîãî ïåðèîäà îáñóæäåíèÿ(28 ôåâðàëÿ 1992 ãîäà) NIST ïîëó÷èë 109 çàìå÷àíèé. Ðàññìîòðèì ïî ïîðÿäêó êðèòè÷åñêèå çàìå÷àíèÿ â àäðåñ DSA.

1. DSA íåëüçÿ èñïîëüçîâàòü äëÿ øèôðîâàíèÿ èëè ðàñïðåäåëåíèÿ êëþ÷åé.

Ïðàâèëüíî, íî ñòàíäàðò è íå òðåáóåò íàëè÷èÿ ýòèõ âîçìîæíîñòåé. Ýòî ñòàíäàðò ïîäïèñè. NIST ïîäãîòîâèòü ñòàíäàðò øèôðîâàíèÿ ñ îòêðûòûì êëþ÷îì. NIST ñîâåðøàåò áîëüøóþ îøèáêó, îñòàâëÿÿ àìåðèêàíñêèé íàðîä áåç ñòàíäàðòà øèôðîâàíèÿ ñ îòêðûòûì êëþ÷îì. Ïî âñåé âåðîÿòíîñòè ïðåäëîæåííûé ñòàíäàðò öèôðîâîé ïîäïèñè áóäåò íåâîçìîæíî èñïîëüçîâàòü äëÿ øèôðîâàíèÿ. (Íî îêàçûâàåòñÿ, ÷òî âîçìîæíî - ñì. ðàçäåë 23.3.) Ýòî íå îçíà÷àåò, ÷òî ñòàíäàðò ïîäïèñè áåñïîëåçåí.

2. DSA áûë ðàçðàáîòàí NSA, è â àëãîðèòìå ìîãóò áûòü ñïåöèàëüíûå ëàçåéêè.

Áîëüøèíñòâî ïåðâîíà÷àëüíûõ êîììåíòàðèåâ áûëè ïðîñòî ïàðàíîèäàëüíûìè: "Îòðèöàíèå NIST ñóùåñòâóþùèõ àëãîðèòìîâ áåç âèäèìûõ ïðè÷èí íå âíóøàåò äîâåðèÿ ê DSS, à óñèëèâàåò ïîäîçðåíèå, ÷òî ñóùåñòâóåò òàéíàÿ ïðîãðàììà, ñòðåìÿùàÿñÿ ïîçâîëèòü NIST è/èëè NSA âñêðûâàòü íàöèîíàëüíóþ êðèïòîñèñòåìó ñ îòêðûòûì êëþ÷îì" [154]. Ñåðüåçíûé âîïðîñ îòíîñèòåëüíî áåçîïàñíîñòè DSA áûë çàäàí Àðæàíîì Ëåíñòðîé (Arjen Lenstra) è Ñòþàðòîì Õàááåðîì (Stuart Haber) èç Bellcore. Îí áóäåò ðàññìîòðåí íèæå.

3. DSA ìåäëåííåå RSA [800].

Áîëåå èëè ìåíåå ñïðàâåäëèâî. Ñêîðîñòè ãåíåðàöèè ïîäïèñè ïðèìåðíî îäèíàêîâû, íî ïðîâåðêà ïîäïèñè ñ ïîìîùüþ DSA îò 10 äî 40 ðàç ìåäëåííåå. Îäíàêî ãåíåðàöèÿ êëþ÷åé áûñòðåå. Íî ýòà îïåðàöèÿ íåèíòåðåñíà, ïîëüçîâàòåëü ðåäêî ïðèìåíÿåò åå. Ñ äðóãîé ñòîðîíû ïðîâåðêà ïîäïèñè - ýòî íàèáîëåå ÷àñòàÿ îïåðàöèÿ.

Ïðîáëåìà êðèòèêè â òîì, ÷òî ñóùåñòâóåò ìíîãî ñïîñîáîâ ïîèãðàòü ïàðàìåòðàìè òåñòèðîâàíèÿ, äîáèâàÿñü íóæíûõ ðåçóëüòàòîâ. Ïðåäâàðèòåëüíûå âû÷èñëåíèÿ ìîãóò óñêîðèòü ãåíåðàöèþ ïîäïèñè DSA, íî îíè íå âñåãäà âîçìîæíû. Ñòîðîííèêè RSA ïîäáèðàþò ÷èñëà òàê, ÷òîáû âûäåëèòü ïðåèìóùåñòâà ñâîåãî àëãîðèòìà, à ñòîðîííèêè DSA èñïîëüçóþò ñâîé ñïîñîá îïòèìèçàöèè. Â ëþáîì ñëó÷àå êîìïüþòåðû ñòàíîâÿòñÿ âñå áûñòðåå è áûñòðåå. Õîòÿ ðàçíèöà â ñêîðîñòè è ñóùåñòâóåò, â áîëüøèíñòâå ïðèëîæåíèé îíà íå áóäåò çàìåòíà.

4. RSA - ýòî ñòàíäàðò *de facto*.

Âîò äâà ïðèìåðà ïîäîáíûõ æàëîá. Ïèñüìî Ðîáåðòà Ôîëëåòà (Robert Follett), äèðåêòîðà ïðîãðàììû ñòàíäàðòèçàöèè êîìïàíèè IBM [570]:

> IBM ñ÷èòàåò, ÷òî NIST ïðåäëîæèë ñòàíäàðò ñõåìû öèôðîâîé ïîäïèñè, îòëè÷àþùèéñÿ îò ïðèíèìàåìûõ ìåæäóíàðîäíûõ ñòàíäàðòîâ. Ïîëüçîâàòåëè è îðãàíèçàöèè ïîëüçîâàòåëåé óáåäèëè íàñ â òîì, ÷òî ïîääåðæêà ìåæäóíàðîäíûõ ñòàíäàðòîâ, èñïîëüçóþùèõ RSA, â ñàìîì áëèæàéøåì áóäóùåì ñòàíåò íåîáõîäèìûì óñëîâèåì ïðîäàæè ñðåäñòâ îáåñïå÷åíèÿ áåçîïàñíîñòè.

Ïèñüìî Ëåñà Øðîåðà (Les Shroyer), âèöå-ïðåçèäåíòà è äèðåêòîðà êîìïàíèè Motorola [1444]:

> Ó íàñ äîëæåí áûòü åäèíûé, íàäåæíûé, ïðèçíàííûé âñåìè àëãîðèòì öèôðîâîé ïîäïèñè, êîòîðûé ìîæíî èñïîëüçîâàòü ïî âñåìó ìèðó êàê ìåæäó àìåðèêàíñêèìè è íåàìåðèêàíñêèìè îáúåêòàìè, òàê è ìåæäó ñèñòåìàìè êîìïàíèè Motorola è ñèñòåìàìè äðóãèõ ïðîèçâîäèòåëåé. Îòñóòñòâèå äðóãèõ æèçíåñïîñîáíûõ òåõíîëîãèé öèôðîâîé ïîäïèñè çà ïîñëåäíèå âîñåìü ëåò ñäåëàëî RSA ôàêòè÷åñêèì ñòàíäàðòîì. . . . Motorola è ìíîãèå äðóãèå êîìïàíèè. . . âëîæèëè â RSA ìèëëèîíû äîëëàðîâ. Ìû ñîìíåâàåìñÿ âî âçàèìîäåéñòâèè è âîçìîæíîñòè ïîääåðæêè äâóõ ðàçëè÷íûõ ñòàíäàðòîâ, òàêîå ïîëîæåíèå ïðèâåäåò ê ðîñòó ðàñõîäîâ, çàäåðæåê ðàçâåðòûâàíèÿ è óñëîæíåíèþ ñèñòåì. . . .

Ìíîãèì êîìïàíèÿì õîòåëîñü, ÷òîáû NIST ïðèíÿë ISO 9796, ìåæäóíàðîäíûé ñòàíäàðò öèôðîâîé ïîäïèñè, èñïîëüçóþùèé RSA [762.]. Õîòÿ ýòî è ñåðüåçíûé àðãóìåíò, îí íåäîñòàòî÷åí, ÷òîáû ïðèíÿòü ìåæäóíàðîäíûé ñòàíäàðò â êà÷åñòâå íàöèîíàëüíîãî. Áåñïëàòíûé ñòàíäàðò ëó÷øå îòâå÷àë áû îáùåñòâåííûì èíòåðåñàì Ñîåäèíåííûõ Øòàòîâ.

5. Âûáîð íàöèîíàëüíîãî àëãîðèòìà íå áûë îòêðûòûì, íå áûëî äàíî äîñòàòî÷íî âðåìåíè äëÿ àíàëèçà.

Ñíà÷àëà NIST óòâåðæäàë, ÷òî ðàçðàáîòàë DSA ñàìîñòîÿòåëüíî, çàòåì ïðèçíàë ïîìîùü NSA. Íàêîíåö NIST ïîäòâåðäèë, ÷òî NSA ÿâëÿåòñÿ àâòîðîì àëãîðèòìà. Ýòî ìíîãèõ îáåñïîêîèëî - NSA íå âíóøàåò ëþäÿì äîâåðèå. Äàæå òàê, àëãîðèòì áûë îïóáëèêîâàí è äîñòóïåí äëÿ àíàëèçà, êðîìå òîãî, NIST ïðîäëèë âðåìÿ àíàëèçà è êîììåíòèðîâàíèÿ àëãîðèòìà.

6. DSA ìîæåò íàðóøàòü äðóãèå ïàòåíòû. Ýòî òàê. Ýòîò âîïðîñ áóäåò ðàññìîòðåí â ðàçäåëå, ðàññìàòðèâàþùèì ïàòåíòû.

7. Ðàçìåð êëþ÷à ñëèøêîì ìàë.

Ýòî åäèíñòâåííî ñïðàâåäëèâàÿ êðèòèêà DSS. Ïåðâîíà÷àëüíî ïðåäëàãàëîñü èñïîëüçîâàòü ìîäóëü äëèíîé 512 áèòîâ [1149]. Òàê êàê áåçîïàñíîñòü àëãîðèòìà îïðåäåëÿåòñÿ ñëîæíîñòüþ âû÷èñëåíèÿ äèñêðåòíûõ ëîãàðèôìîâ ïî çàäàííîìó ìîäóëþ, ýòîò âîïðîñ âîëíîâàë ìíîãèõ êðèïòîãðàôîâ. Ñ òåõ ïîð âû÷èñëåíèå äèñêðåòíûõ ëîãàðèôìîâ â êîíå÷íîì ïîëå äîñòèãëî îïðåäåëåííûõ óñïåõîâ, è 512 áèòîâ ñëèøêîì ìàëî äëÿ äîëãîâðåìåííîé ïîäïèñè (ñì. ðàçäåë 7.2). Ñîãëàñíî Áðàÿíó Ëà Ìà÷÷èà (Brian LaMacchia) è Ýíäðþ Îäëûæêî (Andrew Odlyzko), " . . . äàæå áåçîïàñíîñòü, îáåñïå÷èâàåìàÿ 512-áèòîâûìè ïðîñòûìè ÷èñëàìè, ïî âèäèìîìó, íàõîäèòñÿ íà ïðåäåëå . . . " [934]. Â îòâåò íà ýòè çàìå÷àíèÿ NIST ñäåëàë äëèíó êëþ÷à ïåðåìåííîé, îò 512 äî 1024 áèòîâ. Íåìíîãî, íî âñå-òàêè ïîëó÷øå.

19 ìàÿ 1994 ãîäà áûë èçäàí îêîí÷àòåëüíûé âàðèàíò ñòàíäàðòà [1154]. Ïðè ýòîì áûëî ñêàçàíî [542]:

> Ýòîò ñòàíäàðò ìîæåò ïðèìåíÿòüñÿ âñåìè Ôåäåðàëüíûìè äåïàðòàìåíòàìè è óïðàâëåíèÿìè äëÿ çàùèòû íåñåêðåòíîé èíôîðìàöèè. . . . Ýòîò ñòàíäàðò áóäåò èñïîëüçîâàí ïðè ïðîåêòèðîâàíèè è ðåàëèçàöèè ñõåì ïîäïèñè ñ îòêðûòûìè êëþ÷àìè, êîòîðûå ðàçðàáàòûâàþò Ôåäåðàëüíûå äåïàðòàìåíòû è óïðàâëåíèÿ, èëè êîòîðûå ðàçðàáàòûâàþòñÿ ïî èõ çàêàçó. ×àñòíûå è êîììåð÷åñêèå îðãàíèçàöèè ìîãóò ïðèíÿòü è èñïîëüçîâàòü ýòîò ñòàíäàðò.

Ïðåæäå ÷åì ïîëüçîâàòüñÿ ýòèì ñòàíäàðòîì è ðåàëèçîâûâàòü åãî, ïðî÷èòàéòå íèæå ðàçäåë î ïàòåíòàõ.

Îïèñàíèå DSA

DSA, ïðåäñòàâëÿþùèé ñîáîé âàðèàíò àëãîðèòìîâ ïîäïèñè Schnorr è ElGamal, ïîëíîñòüþ îïèñàí â [1154].

Àëãîðèòì èñïîëüçóåò ñëåäóþùèå ïàðàìåòðû:

p = ïðîñòîå ÷èñëî äëèíîé L áèòîâ, ãäå L ïðèíèìàåò çíà÷åíèå, êðàòíîå 64, â äèàïàçîíå îò 512 äî 1024. (Â ïåðâîíà÷àëüíîì ñòàíäàðòå ðàçìåð p áûë ôèêñèðîâàí è ðàâåí 512 áèòàì [1149]. Ýòî âûçâàëî ìíîæåñòâî êðèòè÷åñêèõ çàìå÷àíèé, è NIST ýòîò ïóíêò àëãîðèòìà [1154].)

q = 160-áèòîâîé ïðîñòîå ÷èñëî - ìíîæèòåëü p-1.

$g = h^{(p-1)/q} \bmod p$, ãäå h - ëþáîå ÷èñëî, ìåíüøåå p-1, äëÿ êîòîðîãî $h^{(p-1)/q} \bmod p$ áîëüøå 1.

x = ÷èñëî, ìåíüøåå q.

$y = g^x \bmod p$.

Â àëãîðèòìå òàêæå èñïîëüçóåòñÿ îäíîíàïðàâëåííàÿ õýø-ôóíêöèÿ: $H(m)$. Ñòàíäàðò îïðåäåëÿåò èñïîëüçîâàíèå SHA, ðàñìîòðåííîãî â ðàçäåëå 18.7.

Ïåðâûå òðè ïàðàìåòðà, p, q è g, îòêðûòû è ìîãóò áûòü îáùèìè äëÿ ïîëüçîâàòåëåé ñåòè. Çàêðûòûì êëþ÷îì ÿâëÿåòñÿ x, à îòêðûòûì - y. ×òîáû ïîäïèñàòü ñîîáùåíèå, m:

(1) Àëèñà ãåíåðèðóåò ñëó÷àéíîå ÷èñëî k, ìåíüøåå q

(2) Àëèñà ãåíåðèðóåò

$r = (g^k \bmod p) \bmod q$

$s = (k^{-1} (H(m) + xr)) \bmod q$

Åå ïîäïèñü ñëóæàò ïàðàìåòðû r è s, îíà ïîñûëàåò èõ Áîáó.

(3) Áîá ïðîâåðÿåò ïîäïèñü, âû÷èñëÿÿ

$w = s^{-1} \bmod q$

$u_1 = (H(m) * w) \bmod q$

$u_2 = (rw) \bmod q$

$v = ((g^{u_1} * y^{u_2}) \bmod p) \bmod q$

Åñëè $v = r$, òî ïîäïèñü ïðàâèëüíà.

Äîêàçàòåëüñòâà ìàòåìàòè÷åñêèõ ñîîòíîøåíèé ìîæíî íàéòè â [1154]. 19th ïðåäñòàâëÿåò ñîâîêóïíîñòü äîêàçàòåëüñòâ ïîäïèñàíèÿ àëãîðèòìà.

Òàáë. 20-1.
Ïîäïèñè DSA

Îòêðûòûé êëþ÷:	
p	ïðîñòîå ÷èñëî äëèíîé îò 512 äî 1024 áèòîâ (ìîæåò èñïîëüçîâàòüñÿ ãðóïïîé ïîëüçîâàòåëåé)
q	160-áèòîâûé ïðîñòîé ìíîæèòåëü p-1 (ìîæåò èñïîëüçîâàòüñÿ ãðóïïîé ïîëüçîâàòåëåé)
g	$= h^{(p-1)/q} \bmod p$, ãäå h - ëþáîå ÷èñëî, ìåíüøåå p-1, äëÿ êîòîðîãî $h^{(p-1)/q} \bmod p > 1$ (ìîæåò èñïîëüçîâàòüñÿ ãðóïïîé ïîëüçîâàòåëåé)
y	$= g^x \bmod p$ (p-áèòîâîå ÷èñëî)
Çàêðûòûé êëþ÷:	
x	$< q$ (160-áèòîâîå ÷èñëî)
Ïîäïèñü:	
k	âûáèðàåòñÿ ñëó÷àéíî, ìåíüøåå q
r	(ïîäïèñü) $= (g^k \bmod p) \bmod q$
s	(ïîäïèñü) $= (k^{-1} (H(m) + xr)) \bmod q$
Ïðîâåðêà:	
w	$= s^{-1} \bmod q$
u_1	$= (H(m) * w) \bmod q$
u_2	$= (rw) \bmod q$

$v = ((g^{u_1} * y^{u_2}) \bmod p) \bmod q$

Åñëè $v = r$, òî ïîäïèñü ïðàâèëüíà.

Óñêîðÿþùèå ïðåäâàðèòåëüíûå âû÷èñëåíèÿ

Â 18-é ïðèâåäåíû ïðèìåðû ñêîðîñòè ðàáîòû ïðîãðàìì íûõ ðåàëèçàöèé DSA [918].

Òàáë. 20-2.
Ñêîðîñòü DSA äëÿ ðàçëè÷íûõ äëèí ìîäóëåé ñ 160-áèòîâûì ïîêàçàòåëåì ñòåïåíè (íà SPARC II)

	512 áèòîâ	768 áèòîâ	1024 áèòà
Ïîäïèñü	0.20 ñ	0.43 ñ	0.57 ñ
Ïðîâåðêà	0.35 ñ	0.80 ñ	1.27 ñ

Ïðàêòè÷åñêè ðåàëèçàöèè DSA ÷àñòî ìîæíî óñêîðèòü ñ ïîìîùüþ ïðåäâàðèòåëüíûõ âû÷èñëåíèé. Îáðàòèâ âíèìàíèå, ÷òî çíà÷åíèå r íå çàâèñèò îò ñîîáùåíèÿ. Ìîæíî ñîçäàòü ñòðîêó ñëó÷àéíûõ çíà÷åíèé k, è çàòåì ðàññ÷èòàòü çíà÷åíèÿ r äëÿ êàæäîãî èç íèõ. Ìîæíî òàêæå âû÷èñëèòü k^{-1} äëÿ êàæäîãî èç ýòèõ çíà÷åíèé k. Çàòåì, êîãäà ïðèõîäèò ñîîáùåíå, ìîæíî âû÷èñëèòü s äëÿ çàäàííûõ r è k^{-1}.

Ýòè ïðåäâàðèòåëüíûå âû÷èñëåíèÿ çàìåòíî óñêîðÿþò DSA. Â 17-é ïðèâåäåíû ñðàâíåíèÿ âðåìåíè âû÷èñëåíèÿ DSA è RSA äëÿ êîíêðåòíîé ðåàëèçàöèè èíòåëëåêòóàëüíîé êàðòî÷êè [1479].

Òàáë. 20-3.
Ñðàâíåíèå âðåìåíè âû÷èñëåíèé RSA è DSA

	DSA	RSA	DSA ñ îáùèìè p, q, g
Ãëîáàëüíûå âû÷èñëåíèÿ	Off-card (P)	N/A	Off-card (P)
Ãåíåðàöèÿ êëþ÷à	14 ñ	Off-card (S)	4ñ
Ïðåäâàðèòåëüíûå âû÷èñëåíèÿ	14 ñ	N/A	4 ñ
Ïîäïèñü	0.03 ñ	15 ñ	0.03 ñ
Ïðîâåðêà	16 ñ	l.5 ñ	10 ñ
	1-5 ñ off-card (P)	1-3 ñ off-card (P)	

Âû÷èñëåíèÿ âíå êàðòî÷êè (off-card) âûïîëíÿëèñü íà ïåðñîíàëüíîì êîìïüþòåðå i80386/33 ÌÃö. (P) óêàçûâàåò îòêðûòûå ïàðàìåòðû off-card, à (S) - íà çàêðûòûå ïàðàìåòðû off-card. Â îáîèõ àëãîðèòìàõ èñïîëüçóåòñÿ 512-áèòîâûé ìîäóëü.

Åíåðàöèÿ ïðîñòûõ ÷èñåë DSA

Ëåíñòðà è Õàáåð óêàçàëè, ÷òî âçëîìàòü íåêîòîðûå ìîäóëè íàìíîãî ëåã÷å, ÷åì äóìàë [950]. Åñëè êòî-íèáóäü çàñòàâèò ïîëüçîâàòåëåé ñåòè èñïîëüçîâàòü îäèí èç òàêîõ ñëàáûõ ìîäóëåé, òî èõ ïîäïèñè áóäåò ëåã÷å ïîääåëàòü. Òåì íå ìåíåå ýòî íå ïðåäñòàâëÿåò ïðîáëåìû ïî ñåãîäíÿøíåìó äíþ: òàêèå ìîäóëè ëåãêî îáíàðóæèòü, è îíè òàê ðåäêè, ÷òî âåðîÿòíîñòü ñëó÷àéíî èñïîëüçîâàòü îäíîãî èç íèõ ïðåíåáðåæèìî ìàëà, ìåíüøå, ÷åì âåðîÿòíîñòü ñëó÷àéíî ïîëó÷èòü ñîîáùåíèå íà âûõîäå åðîÿòíîñòíîé ïðîöåäóðû ãåíåðàöèè ïðîñòûõ ÷èñåë.

Â [1154] NIST ðåêîìåíäîâàë êîíêðåòíûé ìàòä ãåíåðàöèè äâóõ ïðîñòûõ ÷èñåë, p è q, ãäå q ÿâëÿåòñÿ äëèíîé p-1. Äëèíà ïðîñòîãî ÷èñëà p - ìåæäó 512 è 1024 è êðàòíà 64 -áèòàì. Ïóñòü L-1= 160n+b, ãäå L - ýòî äëèíà p, à n è b - äâà ÷èñëà, ïðè÷åì b ìåíüøå 160.

(1) Âûáåðåì ïðîèçâîëüíóþ ïîñëåäîâàòåëüíîñòü, ïî êðàéíåé ìåðå, 160 áèòîâ è íàçîâåì åå S. Ïóñòü g - ýòî äëèíà S â áèòàõ.

(2) Âû÷èñëèì U = SHA(S) ⊕ SHA((S + 1) mod 2^g), ãäå SHA îïèñàí â ðàçäåëå 18.7.

(3) Îáðàçóåì q, óñòàíîâèâ íàèáîëüøèé è íàèìåíüøèé çíà÷àùèå áèòû U â 1.

(4) Ïðîâåðèì, ÿâëÿåòñÿ ëè q ïðîñòûì.

(5) Åñëè q íå ÿâëÿåòñÿ ïðîñòûì, òî âåðíåìñÿ íà ýòàï (1).

(6) Ïóñòü C=0 è N=2.

(7) Äëÿ k=0,l,...,n, ïóñòü V_k=SHA((S+N+k) mod 2^g)

(8) Ïóñòü W - öåëîå ÷èñëî

$W = V_0 + 2^{160}V_1 + \ldots + 2^{160(n-1)} V_{n-1} + 2^{160} (V_n \bmod 2^b)$

è ïóñòü

$X = W + 2^{L-1}$

Îáðàòèòå âíèìàíèå, ÷òî X - ýòî L-áèòîâîå ÷èñëî.

(9) Ïóñòü $p = X - ((X \bmod 2q) - 1)$. Îáðàòèòå âíèìàíèå, ÷òî p êîíãðóýíòíî 1 mod 2q.

(10) Åñëè $p < 2^{L-1}$, òî ïåðåéäèì íà ýòàï (13).

(11) Ïðîâåðèì, ÿâëÿåòñÿ ëè p ïðîñòûì ÷èñëîì.

(12) Åñëè p - ïðîñòîå, ïåðåéäèì ê ýòàïó (15).

(13) Ïóñòü C=C+1 è N=N+n+l.

(14) Åñëè C = 4096, âåðíåìñÿ ê ýòàïó (1). Â ïðîòèâíîì ñëó÷àå ïåðåéäèì íà ýòàï (7).

(15) Ñîõðàíèì çíà÷åíèÿ S è C, èñïîëüçîâàííûå äëÿ ãåíåðàöèè p è q.

Â [1154] ïåðåìåííàÿ S íàçûâàåòñÿ ñòàðòîâîé, ïåðåìåííàÿ C - ñ÷åò÷èêîì, à N - ñìåùåíèåì.

Ñìûñë ýòîãî óïðàæíåíèÿ â òîì, ÷òî îíî ÿâëÿåòñÿ îïóáëèêîâàííûì ñïîñîáîì ãåíåðàöèè p è q. Äëÿ âñåõ ïðàêòè÷åñêèõ ïðèìåíåíèé ýòîò ìåòîä ïîçâîëÿåò èçáåæàòü ñëàáûõ çíà÷åíèé p è q. Åñëè êòî-òî âðó÷èò âàì êàêèå-òî p è q, âàñ ìîæåò çàèíòåðåñîâàòü, êàê ïîëó÷åíû ýòè ÷èñëà. Îáíàêî, åñëè âû ïîëó÷èòå çíà÷åíèÿ S è C, èñïîëüçîâàííûå ïðè ãåíåðàöèè ñëó÷àéíûõ p è q, âû ñìîæåòå ïîâòîðèòü âñþ ïðîöåäóðó ñàìîñòîÿòåëüíî. Èñïîëüçîâàíèå îäíîíàïðàâëåííîé õýø-ôóíêöèè (â ñòàíäàðòå èñïîëüçóåòñÿ SHA) íå ïîçâîëÿåò ïîëó÷èòü S è C ïî çíà÷åíèÿì p è q.

Ýòà áåçîïàñíîñòü ëó÷øå, ÷åì îáåñïå÷èâàåìàÿ RSA. Â RSA ïðîñòûå ÷èñëà õðàíÿòñÿ â ñåêðåòå. Ëþáîé ìîæåò ãåíåðèðîâàòü ôàêòîðèçóåìîå ïðîñòîå ÷èñëî ÷èñëî, ôîðìà êîòîðîãî óïðîùàåò ðàçëîæåíèå íà ìíîæèòåëè. Íå çíàÿ çàêðûòîãî êëþ÷à, ýòî íèêîãäà íå ïðîâåðèøü. Â DSA, äàæå åñëè çàêðûòûé êëþ÷ íåèçâåñòåí, ìîæíî óâåäèòüñÿ, ÷òî p è q ãåíåðèðîâàëèñü ñëó÷àéíûì îáðàçîì.

Øèôðîâàíèå ElGamal ñ DSA

Óòâåðæäàëîñü, ÷òî DSA òàê íðàâèòñÿ ïðàâèòåëüñòâó, ïîòîìó ÷òî åãî íåëüçÿ èñïîëüçîâàòü â êà÷åñòâå àëãîðèòìà øèôðîâàíèÿ. Îäíàêî ìîæíî èñïîëüçîâàòü âûçîâ ôóíêöèè DSA äëÿ øèôðîâàíèÿ EIGamal. Ïóñòü àëãîðèòì ðåàëèçîâàí êàê âûçîâ îáû÷íîé ôóíêöèè

```
DSAsign(p,q,g,k,x,h,r,s)
```

Çàäàâ âõîäíûå çíà÷åíèÿ p, q, g, k, x è h, ìîæíî ïîëó÷èòü ïàðàìåòðû ïîäïèñè: r è s.

Äëÿ øèôðîâàíèÿ ñîîáùåíèÿ m àëãîðèòìîì EIGamal ñ ïîìîùüþ îòêðûòîãî êëþ÷à y âûáåðåì ñëó÷àéíîå ÷èñëî k è âûçîâåì

```
DSAsign(p,p,g,k,0,0,r,s)
```

Âîçâðàùåííîå çíà÷åíèå r è áóäåò a èç ñõåìû EIGamal. Îòðàñëè s. Çàòåì âûçîâåì, call

```
DSAsign(p,p,y,k,0,0,r,s)
```

Ïðåäïîëîæèì çíà÷åíèå r â u, îòðàñëè s. Âûçîâåì

```
DSAsign(p,p,m,1,u,0,r,s)
```

Îòðàñëè r. Âîçâðàùåííîå çíà÷åíèå s è áóäåò b â ñõåìå EIGamal. Òåïåðü ó âàñ åñòü øèôðîâåêñò, a è b. Äåøèôðèðîâàíèå òàêæå ïðîñòî. Èñïîëüçóÿ çàêðûòûé êëþ÷ x è øèôðîâêñò ñîîáùåíèé, a è b, âûçîâåì

```
DSAsign(p,p,a,x,0,0,r,s)
```

Çíà÷åíèå r - ýòî a^x mod p. Íàçîâåì åãî e. Çàòåì âûçîâåì

```
DSAsign(p,p,1,e,b,0,r,s)
```

Çíà÷åíèå s è áóäåò îòêðûòûì òåêñòîì ñîîáùåíèÿ, m.

Ýòîò ñïîñîá ðàáîòàåò íå ñî âñåìè ðåàëèçàöèÿìè DSA - â íåêîòîðûõ èç íèõ ìîãóò áûòü çàòèêñèðîâàíû çíà÷åíèÿ p è q èëè äëèíû íåêîòîðûõ äóãèõ ïàðàìåòðîâ. Òåì íå ìåíåå, åñëè ðåàëèçàöèÿ ÿâëÿåòñÿ äîñòàòî÷íî íåãèáêîé, òî ìîæíî øèôðîâàòü ñîîáùåíèå, íå èñïîëüçóÿ íè÷åãî, êðîìå ôóíêöèè öèôðîâîé ïîäïèñè.

Øèôðîâàíèå RSA ñ DSA

Øèôðîâàíèå RSA åùå ïðîùå. Èñïîëüçóÿ ìîäóëü *n*, ñîîáùåíèå *m* è îòêðûòûé êëþ÷ *e*, âûçîâåì

```
DSAsign(n,n,m,e,0,0,r,s)
```

Âîçâðàùåííîå çíà÷åíèå *r* è åñòü øèôðîòåêñò. Äåøèôðèðîâàíèå RSA ÿâëÿåòñÿ òî÷íî òàêèì æå. Åñëè *d* - çàêðûòûé êëþ÷, òî

```
DSAsign(n,n,m,d,0,0,r,s)
```

âîçâðàùàåò îòêðûòûé òåêñò êàê çíà÷åíèå *r*.

Áåçîïàñíîñòü DSA

Ñ 512 áèòàìè DSA íåäîñòàòî÷íî íàäåæåí äëÿ äëèòåëüíîé áåçîïàñíîñòè, íî îí âïîëíå íàäåæåí ïðè 1024 áèòàõ. Â ñâîåì ïåðâîì çàÿâëåíèè íà ýòó òåìó NSA òàê êîììåíòèðîâàëî óòâåðæäåíèå Äæî Ýáåðíåòè (Joe Abernathy) èç *The Houston Chronicle* ïî ïîâîäó ëàçåéêè â DSS [363]:

> ×òî êàñàåòñÿ ïðåäïîëàãàåìîé ëàçåéêè â DSS. Ìû ñ÷èòàåì, ÷òî òåðìèí "ëàçåéêà" ââîäèò â çàáëóæäåíèå, òàê îí ïðåäïîëàãàåò, ÷òî ÷åðåç ëàçåéêó ìîæíî êàê-òî ðàñøèôðîâàòü (ïðî÷èòàòü) çàøèôðîâàííûå ñîîáùåíèÿ, ïîäïèñûâàåìûå ñ ïîìîùüþ DSS, áåç ðàçðåøåíèÿ îòïðàâèòåëÿ.
>
> DSS íå øèôðóåò íèêàêèõ äàííûõ. Ïî ñóòè âîïðîñîì ÿâëÿåòñÿ, íå ìîæåò ëè êòî-òî ïðè ïîìîùè DSS ïîääåëàòü ïîäïèñü, è, òàêèì îáðàçîì, äèñêðåäèòèðîâàòü âñþ ñèñòåìó. Ìû êàòåãîðè÷åñêè çàÿâëÿåì, ÷òî âåðîÿòíîñòü, ÷òî êòî-íèáóäü - âêëþ÷àÿ NSA - ñìîæåò ïîääåëàòü ïîäïèñü DSS, ïðè ïðàâèëüíîì èñïîëüçîâàíèè ñòàíäàðòà áåñêîíå÷íî ìàëà.
>
> Áîëåå òîãî, ïðåäïîëîæåíèå î ÷óâñòâèòåëüíîñòè ê ëàçåéêå ñïðàâåäëèâî äëÿ *ëþáîé* ñèñòåìû ïðîâåðêè ïîäëèííîñòè ñ îòêðûòûìè êëþ÷àìè, âêëþ÷àÿ RSA. Óòâåðæäåíèå, ÷òî ýòî âëèÿåò òîëüêî íà DSS (àðãóìåíò, ïîïóëÿðíûé â ïðåññå), ïîëíîñòüþ íåâåðíî. Âîïðîñ â ðåàëèçàöèè è ñïîñîáå âûáîðà ïðîñòûõ ÷èñåë. Ìû ïðèçûâàåì âàñ óäåëèòü âíèìàíèå íåäàâíåé êîíôåðåíöèè EUROCRYPT, ãäå "çà êðóãëûì ñòîëîì" îáñóæäàëñÿ âîïðîñ ëàçååê â DSS. Îäíèì èç ó÷àñòíèêîâ îáñóæäåíèÿ áûë îäèí èç èññëåäîâàòåëåé èç Bellcore, óòâåðæäàâøèé î âîçìîæíîñòè ëàçåéêè, è ïî íàøåìó ïîíèìàíèþ ó÷àñòíèêè äèñêóññèè - âêëþ÷àÿ ýòîãî èññëåäîâàòåëÿ èç Bellcore - ïðèøëè ê âûâîäó, ÷òî âîïðîñ î ëàçåéêå â DSS íå ïðåäñòàâëÿåò ïðîáëåìû. Áîëåå òîãî, âñåìè áûëî ïðèçíàíî, ÷òî âîïðîñ î ëàçåéêå ÿâëÿåòñÿ òðèâèàëüíûì è áûë ðàçäóò ïðåññîé. Îäíàêî, ïûòàÿñü ïî ïðîñüáå NIST îòâåòèòü íà îáâèíåíèå î ëàçåéêå, ìû ðàçðàáîòàëè ïðîöåññ ãåíåðàöèè ïðîñòûõ ÷èñåë, ïîçâîëÿþùèé èçáåæàòü âûáîðà îäíîãî èç îòíîñèòåëüíî íåáîëüøîãî ÷èñëà ñëàáûõ ïðîñòûõ ÷èñåë, èñïîëüçîâàíèå êîòîðûõ îñëàáëÿåò DSS. Êðîìå òîãî, NIST íàñòàèâàåò íà èñïîëüçîâàíèè ìîäóëåé áîëüøåé äëèíû, âïëîòü äî 1024, ÷òî ïîçâîëÿåò íå ïîëüçîâàòüñÿ ðàçðàáîòàííûì ïðîöåññîì ãåíåðàöèè ïðîñòûõ ÷èñåë, èçáåãàÿ ñëàáûõ ïðîñòûõ ÷èñåë. Î÷åíü âàæíûì äîïîëíèòåëüíûì ìîìåíòîì, íà êîòîðûé ÷àñòî íå îáðàùàþò âíèìàíèå, ÿâëÿåòñÿ òî, ÷òî ïðè èñïîëüçîâàíèè DSS ïðîñòûå ÷èñëà *îáùåäîñòóïíû* è, ñëåäîâàòåëüíî, ìîãóò áûòü ïðåäìåòîì îòêðûòîãî èçó÷åíèÿ. Íå âñå ñèñòåìû ñ îòêðûòûìè êëþ÷àìè ñïîñîáíû ïðîéòè ïîäîáíóþ ïðîâåðêó.
>
> Öåëîñòíîñòü ëþáîé ñèñòåìû çàùèòû èíôîðìàöèè òðåáóåò îáðàòèòü âíèìàíèå íà ðåàëèçàöèþ. Ó÷èòûâàÿ óÿçâèìîñòü ñèñòåì ñ ìèëëèîíàìè ðàâíîïðàâíûõ ïîëüçîâàòåëåé, NSA ïî òðàäèöèè íàñòàèâàåò íà èñïîëüçîâàíèè öåíòðàëèçîâàííûõ äîâåðåííûõ öåíòðîâ êàê íà ñïîñîáå ìèíèìèçèðîâàòü ðèñê â ñèñòåìå. Õîòÿ ìû ïî ïðîñüáå NIST è ðàçðàáîòàëè ðÿä òåõíè÷åñêèõ ìîäèôèêàöèé DSS, ïîçâîëÿþùèõ ðåàëèçîâàòü ìåíåå öåíòðàëèçîâàííûé ïîäõîä, âñå æå íóæíî âûäåëèòü òó ÷àñòü îáúÿâëåíèÿ î DSS â *Federal Register*, â êîòîðîé ãîâîðèòñÿ:
>
> "Õîòÿ ýòîò ñòàíäàðò äîëæåí îáåñïå÷èòü îáùèå òðåáîâàíèÿ áåçîïàñíîñòè ãåíåðàöèè öèôðîâûõ ïîäïèñåé, ñîîòâåòñòâèå ñòàíäàðòó íå îáåñïå÷èâàåò áåçîïàñíîñòü êîíêðåòíîé ðåàëèçàöèè. Îòâåòñòâåííîå ëèöî â êàæäîì äåïàðòàìåíòå èëè óïðàâëåíèè äîëæíî ãàðàíòèðîâàòü, ÷òî îáùàÿ ðåàëèçàöèÿ ãàðàíòèðóåò ïðèåìëåìûé óðîâåíü áåçîïàñíîñòè. NIST ïðîäîëæèò ðàáîòó ñ ïðàâèòåëüñòâåííûìè ïîëüçîâàòåëÿìè, îáåñïå÷èâàÿ ïðàâèëüíîñòü ðåàëèçàöèé."
>
> Íàêîíåö ìû èçó÷èëè âñå óòâåðæäåíèÿ î íåáåçîïàñíîñòè DSS, è îíè íàñ íå óáåäèëè. DSS áûë òùàòåëüíî èçó÷åí â NSA, ÷òî ïîçâîëèëî íàøåìó Äèðåêòîðó ïî áåçîïàñíîñòè èíôîðìàöèîííûõ ñèñòåì ðàçðåøèòü èñïîëüçîâàòü ýòîò ñòàíäàðò äëÿ ïîäïèñè íåñåêðåòíûõ äàííûõ, îáðàáàòûâàåìûõ â îïðåäåëåííûõ ðàçâåäûâàòåëüíûõ ñèñòåìàõ, è äàæå äëÿ ïîäïèñè ñåêðåòíûõ äàííûõ â ðÿäå ñèñòåì. Ìû ñ÷èòàåì, ÷òî ïîäîáíîå ïðèçíàíèå ñâèäåòåëüñòâóåò î íåâîçìîæíîñòè êàêîãî-ëèáî âåðîÿòíîãî âñêðûòèÿ áåçîïàñíîñòè, îáåñïå÷èâàåìîé DSS ïðè åãî ïðàâèëüíûõ ðåàëèçàöèè è èñïîëüçîâàíèè. Îñíîâûâàÿñü íà òðåáîâàíèÿõ ïðàâèòåëüñòâà ÑØÀ ê òåõíèêå è áåçîïàñíîñòè öèôðîâûõ ïîäïèñåé, ìû ñ÷èòàåì, ÷òî DSS ÿâëÿåòñÿ ëó÷øèì âûáîðîì. Â äåéñòâèòåëüíîñòè, DSS âûñòóïàåò â êà÷åñòâå ïèëîòíîãî ïðîåêòà Ñèñòåìû çàùèòû ñîîáùåíèé (Defense Message System), ïðèçâàííîãî ãàðàíòèðîâàòü ïîäëèííîñòü ýëåêòðîííûõ ñîîáùåíèé äëÿ æèçíåííî âàæíûõ êîìàíä è êîíòðîëüíîé èíôîðìàöèè. Ýòà íà÷àëüíàÿ äåìîíñòðàöèÿ âêëþ÷àåò ó÷àñòèå Êîìèòåòà íà÷àëüíèêîâ øòàáîâ, âîåííûõ ñëóæá è îáîðîííûõ âåäîìñòâ è ïðîâîäèòñÿ â êîîïåðàöèè ñ NIST.

ß íå ñîáèðàþñü êîììåíòèðîâàòü èñòèííîñòü çàÿâëåíèÿ NSA. Ïðèíèìàòü åãî íà âåðó èëè íåò - çàâèñèò îò âàøåãî ê íåìó îòíîøåíèÿ.

Âñêðûòèÿ k

Äëÿ êàæäîé ïîäïèñè íóæíî íîâîå çíà÷åíèå *k*, êîòîðîå äîëæíî âûáèðàòüñÿ ñëó÷àéíûì îáðàçîì. Åñëè Åâà óçíàåò *k*, êîòîðîå Àëèñà èñïîëüçîâàëà äëÿ ïîäïèñè ñîîáùåíèÿ, ìîæåò áûòü âîñïîëüçîâàâøèñü íåêîòîðûìè ñâîéñòâàìè ãåíåðàòîðà ñëó÷àéíûõ ÷èñåë, êîòîðûé âûäàåò *k*, îíà ñìîæåò ðàñêðûòü çàêðûòûé êëþ÷ Àëèñû, *x*. Åñëè Åâà äîáóäåò äâà ñîîáùåíèÿ, ïîäïèñàííûõ ñ ïîìîùüþ îäíîãî è òîãî æå *k*, òî, äàæå íå çíàÿ çíà÷åíèå *k*, îíà ñìîæåò ðàñêðûòü *x*. À ñ ïîìîùüþ *x* Åâà ñìîæåò òàéíî ïîääåëûâàòü ïîäïèñü Àëèñû. Â ëþáîé ðåàëèçàöèè DSA äëÿ áåçîïàñíîñòè ñèñòåìû î÷åíü âàæåí õîðîøèé ãåíåðàòîð ñëó÷àéíûõ ÷èñåë [1468].

Îïàñíîñòè îáùåãî ìîäóëÿ

Õîòÿ DSS íå îïðåäåëÿåò ïðèìåíåíèå ïîëüçîâàòåëÿìè îáùåãî ìîäóëÿ, ðàçëè÷íûå ðåàëèçàöèè ìîãóò âîñïîëüçîâàòüñÿ òàêîé âîçìîæíîñòüþ. Íàïðèìåð, Íàëîãîâîå óïðàâëåíèå ðàññìàòðèâàåò èñïîëüçîâàíèå DSS äëÿ ýëåêòðîííîé íàëîãîâîé îò÷åòíîñòè. ×òî åñëè ýòà îðãàíèçàöèÿ ïîòðåáóåò, ÷òîáû âñå íàëîãîïëàòåëüùèêè ñòðàíû èñïîëüçîâàëè îáùèå *p* è *q*? Îáùèé ìîäóëü ñëèøêîì ëåãêî ñòàíîâèòñÿ ìèøåíüþ äëÿ êðèïòîàíàëèçà. Ïîêà ñëèøêîì ðàíî îáñóæäàòü ðàçëè÷íûå ðåàëèçàöèè DSS, íî ïðè÷èíû äëÿ áåñïîêîéñòâà åñòü.

Ïîäñîçíàòåëüíûé êàíàë â DSA

Ãóñ Ñèììîíñ (Gus Simmons) îòêðûë â DSA ïîäñîçíàòåëüíûé êàíàë [1468, 1469] (ñì. ðàçäåë 23.3). Ýòîò ïîäñîçíàòåëüíûé êàíàë ïîçâîëÿåò âñòðàèâàòü â ïîäïèñü òàéíîå ñîîáùåíèå, êîòîðîå ìîæåò áûòü ïðî÷èòàíî òîëüêî òåì, ó êîãî åñòü êëþ÷. Ñîãëàñíî Ñèììîíñó, ýòî "çàìå÷àòåëüíîå ñîâïàäåíèå", ÷òî "âñå î÷åâèäíûå íåäîñòàòêè ïîäñîçíàòåëüíûõ êàíàëîâ, èñïîëüçóþùèõ ñõåìó ElGamal, ìîãóò áûòü óñòðàíåíû" â DSS, è ÷òî DSS "íà ñåãîäíÿ îáåñïå÷èâàåò íàèáîëåå ïîäõîäÿùóþ ñðåäó äëÿ ïîäñîçíàòåëüíûõ êîììóíèêàöèé". NIST è NSA íå êîììåíòèðîâàëè ýòîò ïîäñîçíàòåëüíûé êàíàë, íèêòî äàæå íå çíàåò, äîãàäûâàëèñü ëè îíè î òàêîé âîçìîæíîñòè. Òàê êàê ýòîò ïîäñîçíàòåëüíûé êàíàë ïîçâîëÿåò ïðè íåäîáðîñîâåñòíîé ðåàëèçàöèè DSS ïåðåäàâàòü ñ êàæäîé ïîäïèñüþ ÷àñòü çàêðûòîãî êëþ÷à. Íèêîãäà íå ïîëüçóéòåñü ðåàëèçàöèåé DSS, åñëè âû íå äîâåðÿåòå ðàçðàáîò÷èêó ðåàëèçàöèè.

Ïàòåíòû

Äýâèä Êðàâèö (David Kravitz), ðàíåå ðàáîòàâøèé â NSA, âëàäååò ïàòåíòîì DSA [897]. Ñîãëàñíî NIST [538]:

> NIST â èíòåðåñàõ îáùåñòâà ñòðåìèòñÿ ñäåëàòü òåõíîëîãèþ DSS äîñòóïíîé áåñïëàòíî ïî âñåìó ìèðó. Ìû ñ÷èòàåì, ÷òî ýòà òåõíîëîãèÿ ìîæåò áûòü çàïàòåíòîâàíà, è ÷òî íèêàêèå äðóãèå ïàòåíòû íå ïðèìåíèìû ê DSS, íî ìû íå ìîæåì äàòü òâåðäûõ ãàðàíòèé ýòîãî äî ïîëó÷åíèÿ ïàòåíòà.

Íåñìîòðÿ íà ýòî, òðè âëàäåëüöà ïàòåíòîâ óòâåðæäàþò, ÷òî DSA íàðóøàåò èõ ïàòåíòû: Diffie-Hellman (ñì. ðàçäåë 2.2.1) [718], Merkle-Hellman (ñì. ðàçäåë 19.2.) [720] è Schnorr (ñì. ðàçäåë 21.3) [1398]. Ïàòåíò Schnorr ÿâëÿåòñÿ èñòî÷íèêîì íàèáîëüøèõ ñëîæíîñòåé. Ñðîê äåéñòâèÿ äâóõ äðóãèõ ïàòåíòîâ èñòåêàåò 1997 ãîäó, à ïàòåíò Schnorr äåéñòâèòåëåí äî 2008 ãîäà. Àëãîðèòì Schnorr áûë ðàçðàáîòàí íå íà ïðàâèòåëüñòâåííûå äåíüãè. Â îòëè÷èå îò ïàòåíòîâ PKP ó ïðàâèòåëüñòâà ÑØÀ íåò ïðàâ íà ïàòåíò Schnorr, è Øíîðð çàïàòåíòîâàë ñâîé àëãîðèòì ïî âñåìó ìèðó. Äàæå åñëè ñóäû ÑØÀ âûíåñóò ðåøåíèå â ïîëüçó DSA, íåÿñíî, êàêîå ðåøåíèå ïðèìóò ñóäû â äðóãèõ ñòðàíàõ. Ñìîæåò ëè ìåæäóíàðîäíàÿ êîðïîðàöèÿ ïðèíÿòü ñòàíäàðò, êîòîðûé çàêîíåí â îäíèõ ñòðàíàõ è íàðóøàåò ïàòåíòíîå çàêîíîäàòåëüñòâî â äðóãèõ? Íóæíî âðåìÿ, ÷òîáû ðåøèòü ýòó ïðîáëåìó, ê ìîìåíòó íàïèñàíèÿ ýòîé êíèãè ýòîò âîïðîñ íå ðåøåí äàæå â Ñîåäèíåííûõ Øòàòàõ.

Â èþíå 1993 ãîäà NIST ïðåäëîæèë âûäàòü PKP èñêëþ÷èòåëüíóþ ïàòåíòíóþ ëèöåíçèþ íà DSA [541]. Ñîãëàøåíèå ïðîâàëèëîñü ïîñëå ïðîòåñòîâ îáùåñòâåííîñòè è ñòàíäàðò âûøåë â ñâåò áåç âñÿêèõ ñîãëàøåíèé. NIST çàÿâèë [542]:

- . . NIST ðàññìîòðåë çàÿâëåíèÿ î âîçìîæíîì íàðóøåíèè ïàòåíòà è ñäåëàë âûâîä, ÷òî ýòè çàÿâëåíèÿ íåñïðàâåäëèâû.

Èòàê ñòàíäàðò îôèöèàëüíî ïðèíÿò, â âîçäóõå ïàõíåò ñóäåáíûìè ïðîöåññàìè, è íèêòî íå çíàåò, ÷òî äåëàòü. NIST çàÿâèë, ÷òî îí ïîìîæåò çàùèòèòüñÿ ëþäÿì, îáâèíåííûì â íàðóøåíèè ïàòåíòíîãî çàêîíîäàòåëüñòâà ïðè èñïîëüçîâàíèè DSA â ðàáîòå ïî ïðàâèòåëüñòâåííîìó êîíòðàêòó. Îñòàëüíûå, ïî âèäèìîìó, äîëæíû çàáîòèòüñÿ î ñåáå ñàìè. Ïðîåêò áàíêîâñêîãî ñòàíäàðòà, èñïîëüçóþùåãî DSA, âûäâèíóò ANSI [60]. NIST ðàáîòàåò íàä âíåäðåíèåì ñòàíäàðòà DSA â ïðàâèòåëüñòâåííîì àïïàðàòå. Shell Oil ñäåëàëà DSA ñâîèì ìåæäóíàðîäíûì ñòàíäàðòîì. Î äðóãèõ ïðåäëîæåííûõ ñòàíäàðòàõ DSA ìíå íåèçâåñòíî.

20.2 Âàðèàíòû DSA

Ýòîò âàðèàíò äåëàåò ïðîùå âû÷èñëåíèÿ, íåîáõîäèìûå äëÿ ïîäïèñè, íå çàñòàâëÿÿ âû÷èñëÿòü k^{-1} [1135]. Âñå èñïîëüçóåìûå ïàðàìåòðû - òàêèå æå, êàê â DSA. Äëÿ ïîäïèñè ñîîáùåíèÿ *m* Àëèñà ãåíåðèðóåò äâà ñëó÷àéíûõ ÷èñëà, *k* è *d*, ìåíüøèå *q*. Ïðîöåäóðà ïîäïèñè âûãëÿäèò òàê

$r = (g^k \bmod p) \bmod q$

$s = (H(m) + xr) * d \bmod q$

$t = kd \bmod q$

Áîá ïðîâåðÿåò ïîäïèñü, âû÷èñëÿÿ

$w = t/s \bmod q$

$u_1 = (H(m) * w) \bmod q$

$u_2 = (rw) \bmod q$

Åñëè $r = ((g^{u_1} * y^{u_2}) \bmod p) \bmod q$, òî ïîäïèñü ïðàâèëüíà.

Ñëåäóþùèé âàðèàíò óïðîùàåò âû÷èñëåíèÿ ïðè ïðîâåðêå ïîäïèñè [1040, 1629]. Âñå èñïîëüçóåìûå ïàðàìåòðû - òàêèå æå, êàê â DSA. Äëÿ ïîäïèñè ñîîáùåíèÿ *m* Àëèñà ãåíåðèðóåò ñëó÷àéíîå ÷èñëî *k*, ìåíüøåå *q*. Ïðîöåäóðà ïîäïèñè âûãëÿäèò òàê

$r = (g^k \bmod p) \bmod q$

$s = k\,(H(m) + xr)^{-1} \bmod q$

Áîá ïðîâåðÿåò ïîäïèñü, âû÷èñëÿÿ

$u_1 = (H(m) * s) \bmod q$

$u_2 = (sr) \bmod q$

Åñëè $r = ((g^{u_1} * y^{u_2}) \bmod p) \bmod q$, òî ïîäïèñü ïðàâèëüíà.

Åùå îäèí âàðèàíò DSA ðàçðàáîòàí ïàêåòíóþ ïðîâåðêó, Áîá ìîæåò ïðîâåðÿòü ïîäïèñè ïàêåòàìè [1135]. Åñëè âñå ïîäïèñè ïðàâèëüíû, òî ðàáîòà Áîáà çàêîí÷åíà. Åñëè îäíà èç íèõ íåïðàâèëüíà, òî åìó åùå íóæíî ïîíÿòü, êàêèå. Ê íåñ÷àñòüþ, ýòî íåâîçìîæíî. Ëèáî ïîäïèñûâàþùèé, ëèáî ïðîâåðÿþùèé ìîæåò ëåãêî ñîçäàòü íàáîð ôàëüøèâûõ ïîäïèñåé, êîòîðûé óäîâëåòâîðÿò êðèòåðèþ ïðîâåðêè ïàêåòà ïîäïèñåé [974].

Ñóùåñòâóåò òàêæå âàðèàíò ãåíåðàöèè ïðîñòûõ ÷èñåë äëÿ DSA, êîòîðûé âêëþ÷àåò q è èñïîëüçóåìûå äëÿ ãåíåðàöèè ïðîñòûõ ÷èñåë ïàðàìåòðû p. Âëèÿåò ëè ýòà ñõåìà íà áåçîïàñíîñòü DSA, âñå åùå íåèçâåñòíî.

(1) Âûáåðåì ïðîèçâîëüíóþ ïîñëåäîâàòåëüíîñòü, ïî êðàéíåé ìåðå, 160 áèòîâ è íà÷íåì åå S. Ïóñòü g - ýòî äëèíà S â áèòàõ.

(2) Âû÷èñëèì $U = \mathrm{SHA}(S) \oplus \mathrm{SHA}((S + 1) \bmod 2^g)$, ãäå SHA îïèñàí â ðàçäåëå 18.7.

(3) Îáðàçóåì q, óñòàíîâèâ íàèáîëüøèé è íàèìåíüøèé çíà÷àùèå áèòû U â 1.

(4) Ïðîâåðèì, ÿâëÿåòñÿ ëè q ïðîñòûì.

(5) Ïóñòü p - ýòî îáúåäèíåíèå q, S, C è $\mathrm{SHA}(S)$. C ïðåäñòàâëÿåò ñîáîé 32 íóëåâûõ áèòà.

(6) $p=p-(p \bmod q)+1$.

(7) $p=p+q$.

(8) Åñëè C â p ðàâíî 0x7fffffff, âåðíåìñÿ íà ýòàï (1).

(9) Ïðîâåðèì, ÿâëÿåòñÿ ëè p ïðîñòûì.

(10) Åñëè p - ñîñòàâíîå, âåðíåìñÿ íà ýòàï (7).

Ïðåèìóùåñòâî ýòîãî âàðèàíòà ÿâëÿåòñÿ òî, ÷òî âàì íå íóæíî õðàíèòü çíà÷åíèÿ C è S, èñïîëüçîâàííûå äëÿ ãåíåðàöèè p è q. Î íè âêëþ÷åíû â ñîñòàâ p. Äëÿ ïðèëîæåíèé, ðàáîòàþùèõ â óñëîâèÿõ íåõâàòêè ïàìÿòè, íàïðèìåð, äëÿ èíòåëëåêòóàëüíûõ êàðòî÷åê, ýòî ìîæåò áûòü âàæíî.

20.3 Àëãîðèòì öèôðîâîé ïîäïèñè ÃÎÑÒ

Ýòî ðóññêèé ñòàíäàðò öèôðîâîé ïîäïèñè, Îôèöèàëüíî íàçûâàåìûé ÃÎÑÒ Ð 34.10-94 [656]. Àëãîðèòì î÷åíü ïîõîæ íà DSA, è èñïîëüçóåò ñëåäóþùèå ïàðàìåòðû

p = ïðîñòîå ÷èñëî, äëèíà êîòîðîãî ëèáî ìåæäó 509 è 512 áèòàìè, ëèáî ìåæäó 1020 è 1024 áèòàìè.

q = ïðîñòîå ÷èñëî - ìíîæèòåëü p-1, äëèííé îò 254 äî 256 áèòîâ.

a = ëþáîå ÷èñëî, ìåíüøåå p-1, äëÿ êîòîðîãî $a^q \bmod p = 1$.

x = ÷èñëî, ìåíüøåå q.

$y = a^x \bmod p$.

Ýòîò àëãîðèòì òàêæå èñïîëüçóåò îäíîíàïðàâëåííóþ õýø-ôóíêöèþ: $H(x)$. Ñòàíäàðò îïðåäåëÿåò èñïîëüçîâàíèå õýø-ôóíêöèè ÃÎÑÒ Ð 34.1 1-94 (ñì. ðàçäåë 18.1 1), îñíîâàííîé íà ñèììåòðè÷íîì àëãîðèòìå ÃÎÑÒ (ñì. ðàçäåë 14.1) [657].

Ïåðâûå òðè ïàðàìåòðà, p, q è a, îôèöèàëüíî è îáû èñïîëüçîâàòüñÿ ñîâìåñòíî ïîëüçîâàòåëÿìè ñåòè. Çàêðûòûì êëþ÷îì ñëóæèò x, à îòêðûòûì - y. ×òîáû ïîäïèñàòü ñîîáùåíèå m

(1) Àëèñà ãåíåðèðóåò ñëó÷àéíîå ÷èñëî k, ìåíüøåå q

(2) Àëèñà ãåíåðèðóåò $I = (a^* \bmod p) \bmod q$ $s = (ct + k(H(m))) \bmod q$

$r = (a^k \bmod p) \bmod q$

$s = (xr + k(H(m))) \bmod q$

Åñëè $H(m) \bmod q = 0$, òî çíà÷åíèå õýø-ôóíêöèè óñòàíàâëèâàåòñÿ ðàâíûì 1. Åñëè $r = 0$, òî âûáåðèòå äðóãîå çíà÷åíèå k è íà÷íèòå ñíîâà. Ïîäïèñü ñëóæàò äâà ÷èñëà: $r \bmod 2^{256}$ è $s \bmod 2^{256}$, Àëèñà ïîñûëàåò èõ Áîáó.

(3) Áîá ïðîâåðÿåò ïîäïèñü, âû÷èñëÿÿ

$v = H(m)^{q-2} \bmod q$

$z_1 = (sv) \bmod q$

$z_2 = ((q-r)*v) \bmod q$

$u = ((a^{z_1} * y^{z_2}) \bmod p) \bmod q$

Åñëè $u = r$, òî ïîäïèñü ïðàâèëüíà.

Ðàçëè÷èå ìåæäó ýòîé ñõåìîé è DSA â òîì, ÷òî â DSA $s = (k^{-1} (H(m) + xr)) \bmod q$, ÷òî äàåò äóãîâûå óðàâíåíèå ïðîâåðêè. Ëþáîïûòíî, îäíàêî, ÷òî äëèíà q ðàâíà 256 áèòàì. Áîëüøèíñòâó çàïàäíûõ êðèïòîãðàôîâ êàæåòñÿ äîñòàòî÷íûì q ïðèìåðíî 160 áèòîâ äëèíîé. Ì îæåò áûòü ýòî ïðîñòî ñëåäñòâèå ðóññêîé ïðèâû÷êè èãðàòü â ñâåðõáåçîïàñíîñòü.

Ñòàíäàðò èñïîëüçóåòñÿ ñ íà÷àëà 1995 ãîäà è íå çàêðûò ãðèôîì "Äëÿ ñëóæåáíîãî ïîëüçîâàíèÿ", ÷òî áû ýòî íå çíà÷èëî.

20.4 Ñõåì öèôðîâîé ïîäïèñè ñèñòåìû ëîãàðèôìîâ

Ñõåìû ïîäïèñè ElGamal, Schnorr (ñì. ðàçäåë 21.3) è DSA î÷åíü ïîõîæè. Ïî ñóòè, âñå îíè ÿâëÿþòñÿ òåì ïðèìåðàìè îáùåé ñõåìû öèôðîâîé ïîäïèñè, èñïîëüçóþùåé ïðîáëåìó äèñêðåòíûõ ëîãàðèôìîâ. Âìåñòå ñ òûñÿ÷àìè äóãèõ ñõåì ïîäïèñåé îíè ÿâëÿþòñÿ ÷àñòüþ îáùåãî è òîãî æå ñìåéñòâà [740, 741, 699, 1184].

Âûáåðåì p, áîëüøîå ïðîñòîå ÷èñëî, è q, ðàâíîå ëèáî p-1, ëèáî áîëüøîìó ïðîñòîìó ÷èñëó p-1. Çàòåì âûáåðåì g, ÷èñëî ìåíüøåå 1 è p, äëÿ êîòîðîãî $g^q \equiv 1 \pmod p$. Âñå ýòè ÷èñëà îòêðûòû, è ìîãóò áûòü ñîâìåñòíî èñïîëüçîâàíû ãðóïïîé ïîëüçîâàòåëåé. Çàêðûòûì êëþ÷îì ÿâëÿåòñÿ x, ìåíüøåå q. Îòêðûòûì êëþ÷îì ñëóæèò $y = g^x \bmod q$.

×òîáû ïîäïèñàòü ñîîáùåíèå m, ñíà÷àëà âû÷èñëè ÷èñëî k, ìåíüøåå q è âçàèìíî ïðîñòîå ñ íèì. Åñëè q òî÷íî ïðîñòîå ÷èñëî, òî áóäåò ðàâíîâåðîÿòíî ëþáîå k, ìåíüøåå q. Ñíà÷àëà âû÷èñëè ì

$r = g^k \bmod p$

Îáîáùåííîå **óðàâíåíèå ïîäïèñè** ïðèìåò âèä

$ak = b + cx \bmod q$

Êîýôôèöèåíòû a, b è c ìîãóò ïðèíèìàòü ðàçëè÷íûå çíà÷åíèÿ. Êàæäàÿ ñòðîêà 16th ïðåäïîëàãàëà øåñòü âîçìîæíîñòåé. Ïðîâåðÿÿ ïîäïèñü, ïîëó÷àòåëü äîëæåí óáåäèòüñÿ, ÷òî

$r^a = g^b y^c \bmod p$

Ýòî óðàâíåíèå íàçûâàåòñÿ **óðàâíåíèåì ïðîâåðêè**.

Òàáë. 20-4.
Âîçìîæíûå ïåðåñòàíîâêè a, b è c ($r' = r \bmod q$)

$\pm r'$	$\pm s$	m
$\pm r'\, m$	$\pm s$	1
$\pm r'\, m$	$\pm ms$	1
$\pm m\, r'$	$\pm r'\, s$	1
$\pm ms$	$\pm r'\, s$	1

Â 15th ïåðå÷èñëåíû âîçìîæíûå âàðèàíòû ïîäïèñè è ïðîâåðêè, ïîëó÷åííûå òîëüêî èç ïåðâîé ñòðîêè âîçìîæíûõ çíà÷åíèé a, b è c áåç ó÷åòà ýôôåêòîâ $\pm$.

Òàáë. 20-5.
Ñõåìû öèôðîâîé ïîäïèñè ñ èñïîëüçîâàíèåì äiñêðåòíûõ ëîãàðèôìîâ

Óðàâíåíèå ïîäïèñè	Óðàâíåíèå ïðîâåðêè
(1) $r'k = s + mx \bmod q$	$r^{r'} = g^s y^m \bmod p$
(2) $r'k = m + sx \bmod q$	$r^{r'} = g^m y^s \bmod p$
(3) $sk = r' + mx \bmod q$	$r^s = g^{r'} y^m \bmod p$

(4) $sk = m + r'x \bmod q$ $\quad r^s = g^m y^{r'} \bmod p$

(5) $mk = s + r'x \bmod q$ $\quad r^m = g^s y^{r'} \bmod p$

(6) $mk = r' + sx \bmod q$ $\quad r^m = g^{r'} y^s \bmod p$

Ýòî øåñòü ðàçëè÷íûõ ñõåì öèôðîâûõ ïîäïèñåé. Äîáàâëåíèå ìíóñà óâåëè÷èâàåò èõ êîëè÷åñòâî äî 24. Ïðè èñïîëüçîâàíèè âñåõ âîçìîæíûõ çíà÷åíèé a, b è c ÷èñëî ñõåì äîõîäèò 120.

EIGamal [518, 519] è DSA [1154] ïî ñóùåñòâó îñíîâàíû íà óðàâíåíèè (4). Äðóãèå ñõåìû - íà óðàâíåíèè (2) [24, 1629]. Schnorr [1396, 1397], êàê è äðóãàÿ ñõåìà [1183], òåñíî ñâÿçàí ñ óðàâíåíèåì (5). À óðàâíåíèå (1) ìîæíî èçìåíèòü òàê, ÷òîáû ïîëó÷èòü ñõåìó, ïðåäëîæåííóþ â [1630]. Îñòàøèåñÿ óðàâíåíèÿ - íîâûå.

Äàëåå. Ëþáóþ èç ýòèõ ñõåì ìîæíî ñäåëàòü áîëåå DSA-ïîäîáíîé, îïðåäåëèâ r êàê

$r = (g^k \bmod p) \bmod q$

Èñïîëüçóéòå òî æå óðàâíåíèå ïîäïèñè è ñäåëàéòå óðàâíåíèå ïðîâåðêè

$u_1 = a^{-1} b \bmod q$

$u_2 = a^{-1} c \bmod q$

$v = ((g^{u_1} * y^{u_2}) \bmod p) \bmod q$

$(r \bmod q)^a = g^b y^c \bmod p$

Ñóùåñòâóþò è äâå äðóãèå âîçìîæíîñòè ïîäîáíûõ ïðåîáðàçîâàíèé [740, 741]. Òàêèå îïåðàöèè ìîæíî ïðîäåëàòü ñ êàæäîé èç 120 ñõåì, äîâåäÿ îáùåå ÷èñëî ñõåì öèôðîâîé ïîäïèñè, èñïîëüçóþùèõ äèñêðåòíûå ëîãàðèôìû, äî 480.

Íî è ýòî åùå íå âñå. Äîïîëíèòåëüíûå îáîáùåíèÿ è èçìåíåíèÿ ïðèâîäÿò áîëåå, ÷åì ê 13000 âàðèàíòàì (íå âñå èç íèõ äîñòàòî÷íî ýôôåêòèâíû) [740, 741].

Îäíî èç ïðèÿòíûõ ñòîðîí ñïîëüçîâàíèÿ RSA äëÿ öèôðîâîé ïîäïèñè ÿâëÿåòñÿ ñâîéñòâî, íàçûâàåìîå **âîññòàíîâëåíèåì ñîîáùåíèÿ**. Êîãäà âû ïðîâåðÿåòå ïîäïèñü RSA, âû âû÷èñëÿåòå m. Çàòåì âû÷èñëåííîå m ñðàâíèâàåòñÿ ñ ñîîáùåíèåì è ïðîâåðÿåòñÿ, ïðàâèëüíà ëè ïîäïèñü ñîîáùåíèÿ. Â ïðåäûäóùèõ ñõåìàõ âîññòàíîâëåíèå m ïðè âû÷èñëåíèè ïîäïèñè íåâîçìîæíî, âàì ïîòðåáîâàëîñü âåðîÿòíî m, êîòîðîå è èñïîëüçóåòñÿ â óðàâíåíèè ïðîâåðêè. Íî, îêàçûâàåòñÿ, ìîæíî ïîñòðîèòü âàðèàíò ñ âîññòàíîâëåíèåì ñîîáùåíèÿ äëÿ âñåõ âû øåïðèâåäåííûõ ñõåì. Äëÿ ïîäïèñè ñîá÷àëà âû÷èñëèì

$r = mg^k \bmod p$

è çàìåíèì m åäèíèöåé â óðàâíåíèè ïîäïèñè. Çàòåì ìîæíî âîññòàíîâèò óðàâíåíèå ïðîâåðêè òàê, ÷òîáû m ìîãëî áûòü âû÷èñëåíî íåïîñðåäñòâåííî. Òî æå ñàìîå ìîæíî ïðåäïðèíÿòü äëÿ DSA-ïîäîáíûõ ñõåì:

$r = (mg^k \bmod p) \bmod q$

Áåçîïàñíîñòü âñåõ âàðèàíòîâ îäèíàêîâà, ïîýòîìó èìåò ñìûñë âûáèðàòü ñõåìó ïî ñëîæíîñòè âû÷èñëåíèÿ. Áîëüøèíñòâî ñõåì çàìåäëÿò íåìíîãî âû÷èñëåíèå r, íî íåêîòîðûå ñõåìû ïîçâîëÿò ïîäïèñü è óðàâíåíèå ïîäïèñè, è óðàâíåíèå ïðîâåðêè áûò èñïîëüçîâàíèÿ îáðàòíûõ çíà÷åíèé, ïðè ýòîì åùå è âîññòàíàâëèâàþ ñîîáùåíèå. Î íà íàçûâàåòñÿ ñõåìîé **p-NEW** [1184].

$r = mg^{-k} \bmod p$

$s = k - r'x \bmod q$

m âîññòàíàâëèâàåòñÿ (è ïðîâåðÿåòñÿ ïîäïèñü) ñ ïîìîùüþ âû÷èñëåíèÿ

$m = g^s y^{r'} r \bmod p$

Â ðÿäå âàðèàíòîâ îäíîâðåìåííî ïîäïèñûâàþòñÿ ïî äâà-òðè áëîêà ñîîáùåíèÿ [740], äóãèå âàðèàíòû ìîæíî èñïîëüçîâàòü äëÿ ñëåïûõ ïîäïèñåé [741].

Ýòî çíà÷èòåëüíàÿ îáëàñòü äëÿ èçó÷åíèÿ. Âñå ðàçëè÷íûå ñõåìû öèôðîâîé ïîäïèñè ñ èñïîëüçîâàíèåì äèñêðåòíûõ ëîãàðèôìîâ áûëè îáúåäèíåíû ëîã÷åñêè êàðêàñîì. Ëè÷íî ÿ ñ÷èòàþ, ÷òî ýòî îêî÷àòåëüíî ïîëæèò êîíåö ñîðàì ìåæäó Schnorr [1398] è DSA [897]: DSA íå ÿâëÿåòñÿ íè ïðîèçâîäíîé Schnorr, ðàâíî êàê è EIGamal. Âñå òðè àëãîðèòìà ÿâëÿþòñÿ ÷àñòíûìè ïîëóäåòñÿ îáùåé ñõåìû, è ýòà îáùàÿ ñõåìà íåçàâèñèìà.

20.5 ONG-SCHNORR-SHAMIR

Ýòà ñõåìà ïîäïèñè èñïîëüçóåò ìíîãî÷ëåíû ïî ìîäóëþ n [1219, 1220]. Âûáèðàåòñÿ áîëüøîå öåëîå ÷èñëî (çíàòü ðàçëîæåíèå n íà ìíîæèòåëè íå îáÿçàòåëüíî). Çàòåì âûáèðàåòñÿ ñëó÷àéíîå ÷èñëî k, âçàèìíî ïðîñòîå ñ n, è âû÷èñëÿåòñÿ h, ðàâíîå

$h = -k^{-2} \bmod n = -(k^{-1})^2 \bmod n$

Îòêðûòûì êëþ÷îì ñëóæàò h è n; à çàêðûòûì - k.

×òîáû ïîäïèñàòü ñîîáùåíèå M, ñíà÷àëà ãåíåðèðóåòñÿ ñëó÷àéíîå ÷èñëî r, âçàèìíî ïðîñòîå ñ n. Çàòåì âû÷èñëÿþòñÿ:

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

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

Ïàðà ÷èñåë S_1 è S_2 ïðåäñòàâëÿåò ñîáîé ïîäïèñü. Ïðîâåðÿ ïîäïèñü, óáåæäàþòñÿ, ÷òî

$S_1^2 + h*S_2^2 \equiv M \pmod n$

Î ïèñàííûé çäåñü âàðèàíò ñõåìû îñíîâàí íà êâàäðàòè÷íûõ ìíîãî÷ëåíàõ. Ïðè åãî îïóáëèêîâàíèè â [1217] çà óñïåøíûé êðèòèêàíàëèç áûë ïðåäëîæåí âîçíàãðàæäåíèå â $100. Íåäåçîïàñíîñòü ñõåìû áûëà äîêàçàíà [1255, 18], íî ýòî íå îñòàíîâèëî åå àâòîðîâ. Îíè ïðåäëîæèëè ìîäèôèêàöèþ àëãîðèòìà, îñíîâàííóþ íà êóáè÷åñêèõ ìíîãî÷ëåíàõ, òàêæå îêàçàâøóþñÿ íåäåçîïàñíîé [1255]. Àâòîðû ïðåäëîæèëè âåðñèþ íà áàçå ìíîãî÷ëåíîâ ÷åòâåðòîé ñòåïåíè, íî áûëà âçëîìàíà è îíà [524, 1255]. Âàðèàíò, ðåøàþùèé ýòè ïðîáëåìû, îïèñàí â [1134].

20.6 ESIGN

ESICN -ýòî ñõåìà öèôðîâîé ïîäïèñè, ðàçðàáîòàííàÿ NTT Japan [1205, 583]. Óòâåðæäàëîñü, ÷òî îíà íå ìåíåå áåçîïàñíà, ÷åì RSA èëè DSA, è íàìíîãî áûñòðåå ïðè òåõ æå ðàçìåðàõ êëþ÷à è ïîäïèñè. Çàêðûòûì êëþ÷îì ñëóæèò ïàðà áîëüøèõ ïðîñòûõ ÷èñåë p è q. Îòêðûòûì êëþ÷îì ÿâëÿåòñÿ n, äëÿ êîòîðîãî

$n = p^2*q$

H - ýòî õýø-ôóíêöèÿ, ïðèìåíÿåìàÿ ê ñîîáùåíèþ m, ïðè÷åì çíà÷åíèå $H(m)$ íàõîäèòñÿ â ïðåäåëàõ îò 0 äî n-1. Èñïîëüçóåòñÿ òàêæå ïàðàìåòð áåçîïàñíîñòè k, êîòîðûé áóäåò âêðàòöå ðàññìîòðåí.

(1) Àëèñà âûáèðàåò ñëó÷àéíîå ÷èñëî x, ìåíüøåå pq.

(2) Àëèñà âû÷èñëÿåò:

w, íàèìåíüøåå öåëîå, êîòîðîå áîëüøå èëè ðàâíî

$(H(m) - x^k \bmod n)/pq$

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

(3) Àëèñà ïîñûëàåò s Áîáó.

(4) Äëÿ ïðîâåðêè ïîäïèñè Áîá âû÷èñëÿåò $s^k \bmod n$. Êðîìå ýòîãî, îí âû÷èñëÿåò a, íàèìåíüøåå öåëîå, êîòîðîå áîëüøå èëè ðàâíî $\lceil 2n/3 \rceil$. Åñëè $H(m)$ ìåíüøå èëè ðàâíà $s^k \bmod n$, è åñëè $s^k \bmod n$ ìåíüøå $H(m)+2^a$, òî ïîäïèñü ñ÷èòàåòñÿ ïðàâèëüíîé.

Âûïîëíåíà ðÿä ïðåäâàðèòåëüíûõ âû÷èñëåíèé, ýòîò àëãîðèòì îñíîâàí óñêîðåíèè. Ýòè âû÷èñëåíèÿ ìîãóò âûïîëíåíû â ïðîèçâîëüíîé ìîìåíò âðåìåíè è íèêàê íå ñâÿçàíû ñ ïîäïèñûâàåìûì ñîîáùåíèåì. Âûáðàâ x, Àëèñà ìîæåò ðàçáèòü ýòàï (2) íà äâà ïîäýòàïà. Ñíà÷àëà,

(2a) Àëèñà âû÷èñëÿåò:

$u = x^k \bmod n$

$v = \mathrm{l}/(kx^{k-1}) \bmod p$

(2b) Àëèñà âû÷èñëÿåò:

w= íàèìåíüøåå öåëîå, êîòîðîå áîëüøå èëè ðàâíî

$(H(m) - u)/pq$

$s = x + ((wv \bmod p)\ pq$

Äëÿ îáû÷íî èñïîëüçóåìûõ ðàçìåðîâ ÷èñåë ïðåäâàðèòåëüíûå âû÷èñëåíèÿ óñêîðÿþò ïðîöåññ ïîäïèñè íà ïîðÿäîê. Ïî÷òè âñÿ òðóäîåìêîñòü ðàáîòà âûïîëíÿåòñÿ èìåííî íà ñòàäèè ïðåäâàðèòåëüíûõ âû÷èñëåíèé. Îáñóæäåíèå äåéñòâèé ìîäóëüíîé àðèôìåòèêè, âûïîëíÿåìûõ ïðè óñêîðåíèè ESIGN, ìîæíî íàéòè â [1625, 1624]. Ýòîò àëãî-

ðèòì ìîæíî ðàñøèðèòü äëÿ ðàáîòû ñ ýëëèïòè÷åñêèìè êðèâûìè [1206].

Áåçîïàñíîñòü ESIGN

Êîãäà ýòîò àëãîðèòì áûë âïåðâûå ïðåäëîæåí, *k* áûëî âûáðàíî ðàâíûì 2 [1215]. Òàêàÿ ñõåìà áûñòðî áûëà âçëîìàíà Ýðíè Áðèêåëëîì (Ernie Brickell) è Äæîíîì ÄåËàóðåíòèñîì [261], êîòîðûå ðàñïðîñòðàíèëè ñâîå âñêðûòèå è íà ñëó÷àé *k* = 3. Ìîäèôèöèðîâàííàÿ âåðñèÿ ýòîãî àëãîðèòìà [1203] áûëà âçëîìàíà Øàìèðîì [1204]. Âàðèàíò, ïðåäëîæåííûé â [1204], áûë âçëîìàí â [1553]. ESIGN - ýòî ñåãîäíÿøíÿÿ ðåèíêàðíàöèÿ àëãîðèòìîâ èç ýòîãî ñåìåéñòâà. Ïîïûòêà âñêðûòü ESIGN [963] îêàçàëàñü áåçðåçóëüòàòíîé.

Â íàñòîÿùåå âðåìÿ àâòîðû ðåêîìåíäóþò èñïîëüçîâàòü ñëåäóþùèå çíà÷åíèÿ *k:* 8, 16, 32, 64, 128, 256, 512 è 1024. Îíè òàêæå ðåêîìåíäóþò, ÷òîáû *p* è *q* áûëè íå ìåíüøå 192 áèòîâ êàæäîå, îáðàçóÿ *n* íå ìåíåå, ÷åì 576 áèòîâ â äëèíó. (ß äóìàþ, ÷òî *n* äîëæíî áûòü åùå â äâà ðàçà áîëüøå.) Àâòîðû ñ÷èòàþò, ÷òî ñ òàêèìè çíà÷åíèÿìè ïàðàìåòðîâ, áåçîïàñíîñòü ESIGN ðàâíà áåçîïàñíîñòè RSA èëè Rabin. È âûïîëíåííûé èìè àíàëèç ïîêàçûâàåò, ÷òî ñêîðîñòü ESIGN íàìíîãî âûøå, ÷åì ó RSA, EIGamal è DSA [582].

Ïàòåíòû

ESICN çàïàòåíòîâàí â Ñîåäèíåííûõ Øòàòàõ [1208], Êàíàäå, Àíãëèè, Ôðàíöèè, Ãåðìàíèè è Èòàëèè. Ëþáîé, êòî õî÷åò ïîëó÷èòü ëèöåíçèþ íà àëãîðèòì, äîëæåí îáðàòèòüñÿ â Îòäåë èíòåëëåêòóàëüíîé ñîáñòâåííîñòè NTT (Intellectual Property Department, NTT, 1-6Uchisaiwai-cho, 1-chome, Chiyada-ku, 100 Japan).

20.7 Êëåòî÷íûå àâòîìàòû

Ñîâåðøåííî íîâàÿ èäåÿ, èçó÷åííàÿ Ïàïóà Ãóàìîì (Papua Guam) [665], ñîñòîèò â èñïîëüçîâàíèè â êðèïòîñèñòåìàõ ñ îòêðûòûìè êëþ÷àìè êëåòî÷íûõ àâòîìàòîâ. Ýòà ñèñòåìà âñå åùå ñëèøêîì íîâà è íå ïðîøëà ÷åðåç òùàòåëüíîå èçó÷åíèå, íî ïðåäâàðèòåëüíîå èññëåäîâàíèå ïîêàçàëî, ÷òî ó íåå ìîæåò áûòü òàêîå æå êðèïòîãðàôè÷åñêîå ñëàáîå ìåñòî, êàê è ó äðóãèõ ñèñòåì [562]. Òåì íå ìåíåå, ýòî ìíîãîîáåùàþùàÿ îáëàñòü èññëåäîâàíèé. Ñâîéñòâîì êëåòî÷íûõ àâòîìàòîâ ÿâëÿåòñÿ òî, ÷òî äàæå åñëè îíè èíâåðòèðóåìû, íåâîçìîæíî âû÷èñëèòü ïðåäêà ïðîèçâîëüíîãî ñîñòîÿíèÿ, èíâåðòèðîâàâ ïðàâèëî íàõîæäåíèÿ ïîòîìêà. Ýòî âûãëÿäèò î÷åíü ïîõîæå íà îäíîíàïðàâëåííóþ õýø-ôóíêöèþ ñ ëàçåéêîé.

20.8 Äðóãèå àëãîðèòìû ñ îòêðûòûì êëþ÷îì

Çà ýòè ãîäû áûëî ïðåäëîæåíî è âñêðûòî ìíîæåñòâî äðóãèõ àëãîðèòìîâ ñ îòêðûòûìè êëþ÷àìè. Àëãîðèòì Matsumoto-lmai [1021] áûë âñêðûò â [450]. Àëãîðèòì Cade áûë âïåðâûå ïðåäëîæåí â 1985 ãîäó, âçëîìàí â 1986 [774], è çàòåì äîðàáîòàí â òîì æå ãîäó [286]. Ïîìèìî ýòèõ âñêðûòèé, ñóùåñòâóþò îáùèå âñêðûòèÿ, ðàñêëàäûâàþùèå ìíîãî÷ëåíû íàä êîíå÷íûìè ïîëÿìè[605]. Ê ëþáîìó àëãîðèòìó, áåçîïàñíîñòü êîòîðîãî îïðåäåëÿåòñÿ êîìïîçèöèåé ìíîãî÷ëåíîâ íàä êîíå÷íûìè ïîëÿìè, íóæíî îòíîñèòüñÿ ñî ñêåïòèöèçìîì, åñëè íå ñ îòêðîâåííûì ïîäîçðåíèåì.

Àëãîðèòì Yagisawa îáúåäèíÿåò âîçâåäåíèå â ñòåïåíü mod *p* ñ àðèôìåòèêîé mod *p*-1 [1623], îí áûë âçëîìàí â [256]. Äðóãîé àëãîðèòì ñ îòêðûòûì êëþ÷îì, Tsujii-Kurosawa-Itoh-Fujioka-Matsumoto [1548], òàêæå îêàçàëñÿ íåáåçîïàñíûì [948]. Íåáåçîïàñíîé [717] áûëà è òðåòüÿ ñèñòåìà, Luccio-Mazzone [993]. Ñõåìà ïîäïèñè íà áàçå birational ïðåîáðàçîâàíèé [1425] áûëà âçëîìàíà íà ñëåäóþùèé äåíü ïîñëå åå ïðåäñòàâëåíèÿ [381]. Íåñêîëüêî ñõåì ïîäïèñåé ïðåäëîæèë Òàöóàêè Îêàìîòî (Tatsuaki Okamoto): áûëî äîêàçàíî, ÷òî îäíà èç íèõ òàê æå áåçîïàñíà, êàê ïðîáëåìà äèñêðåòíîãî ëîãàðèôìà, à äðóãàÿ - êàê ïðîáëåìà äèñêðåòíîãî ëîãàðèôìà *è* ïðîáëåìà ðàçëîæåíèÿ íà ìíîæèòåëè [1206]. Àíàëîãè÷íûå ñõåìû ïðåäñòàâëåíû â [709].

Ãóñòàâóñ Ñèììîíñ (Gustavus Simmons) ïðåäëîæèë èñïîëüçîâàòü â êà÷åñòâå îñíîâû àëãîðèòìîâ ñ îòêðûòûìè êëþ÷àìè J-àëãåáðó [1455, 145]. Îò ýòîé èäåè ïðèøëîñü îòêàçàòüñÿ ïîñëå èçîáðåòåíèÿ ýôôåêòèâíûõ ìåòîäîâ ðàçëîæåíèÿ ìíîãî÷ëåíîâ íà ìíîæèòåëè [951]. Òàêæå áûëè èçó÷åíû è ñïåöèàëüíûå ïîëóãðóïïû ìíîãî÷ëåíîâ [1619, 962], íî è ýòî íè÷åãî íå äàëî. Õàðàëüä Íèääåððåéòåð (Harald Niederreiter) ïðåäëîæèë àëãîðèòì ñ îòêðûòûì êëþ÷îì íà áàçå ïîñëåäîâàòåëüíîñòåé ñäâèãîâûõ ðåãèñòðîâ [1166]. Äðóãîé àëãîðèòì èñïîëüçîâàë ñëîâà Ëèíäîíà (Lyndon) [1476], à òðåòèé - prepositional èñ÷èñëåíèå [817]. Áåçîïàñíîñòü îäíîãî èç íåäàâíèõ àëãîðèòìîâ ñ îòêðûòûìè êëþ÷àìè îñíîâûâàëàñü íà ïðîáëåìå matrix cover [82]. Òàöóàêè Îêàìîòî è Êàçóî Îòà (Kazuo Ohta) ïðîâåëè ñðàâíåíèå ðÿäà ñõåì öèôðîâîé ïîäïèñè â [1212].

Ïåðñïåêòèâû ñîçäàíèÿ ðàäèêàëüíî íîâûõ è ðàçëè÷íûõ àëãîðèòìîâ ñ îòêðûòûìè êëþ÷àìè íåÿñíû. Â 1988 ãîäó Óèòôèëä Äèôôè îòìåòèë, ÷òî áîëüøèíñòâî àëãîðèòìîâ ñ îòêðûòûìè êëþ÷àìè îñíîâàíû íà îäíîé èç òðåõ òðóäíûõ ïðîáëåì [492, 494]:

1. Ðþêçàê: Äàíî ìíîæåñòâî óíèêàëüíûõ ÷èñåë, íàéòè ïîäìíîæåñòâî, ñóììà êîòîðîãî ðàâíà *N*.
2. Äèñêðåòíûé ëîãàðèôì: Åñëè *p* - ïðîñòîå ÷èñëî, à *g* è *M* - öåëûå, íàéòè *x*, äëÿ êîòîðîãî âûïîëíÿåòñÿ $g^x \equiv M$ (mod *p*).

3. Ðàçëîæåíèå íà ìíîæèòåëè: Åñëè N - ïðîèçâåäåíèå äâóõ ïðîñòûõ ÷èñåë, òî ëèøü

   (a) ðàçëîæèòü N íà ìíîæèòåëè,

   (b) äëÿ çàäàííûõ öåëûõ ÷èñåë M è C íàéòè d, äëÿ êîòîðîãî $M^d \equiv C \pmod N$,

   (c) äëÿ çàäàííûõ öåëûõ ÷èñåë e è C íàéòè M, äëÿ êîòîðîãî $M^e \equiv C \pmod N$,

   (d) äëÿ çàäàííîãî öåëîãî x ïðåäñòàâèòü, ñóùåñòâóåò ëè öåëîå ÷èñëî y, äëÿ êîòîðîãî $x \equiv y^2 \pmod N$.

Ñîãëàñíî Äèôôè [492, 494], ïðîáëåìà äiñêðåòíûõ ëîãàðèôìîâ áûëà ïðåäëîæåíà Äæ. Ãèëëîì (J. Gill), ïðîáëåìà ðàçëîæåíèÿ íà ìíîæèòåëè - Êíóòîì, à ïðîáëåìà ðþêçàêà - ñàìèì Äèôôè.

Ýòà óçíàòü ìàòåìàòè÷åñêèõ îñíîâ êðèïòîãðàôèè ñ îòêðûòûì êëþ÷îì è êëþ÷àìè íåìíîãî áîëüøå ïðåäëîæåíèé ëèáî ïðîáëåì - ïðåäñòàâëÿþò ñîáîé ôóíäàìåíòàëüíûå àðèôìåòè÷åñêèå ÿâëåíèÿ. Âåêàìè îíè áûëè ïðåäìåòîì èíòåíñèâíîãî ìàòåìàòè÷åñêîãî èçó÷åíèÿ, è ðîñò âû÷èñëèòåëüíîé ìîùíîñòè êîìïüþòåðîâ ñ îòêðûòûìè êëþ÷àìè. Äèôôè ïîêàçàë [492, 494], ÷òî ïîäîáíûé ðèñê ñìÿã÷àåòñÿ äâóìÿ ôàêòîðàìè:

> 1. Âñå îïåðàöèè, íà êîòîðûå ñåé÷àñ îïèðàåòñÿ êðèïòîãðàôèÿ ñ îòêðûòûìè êëþ÷àìè - óìíîæåíèå, âîçâåäåíèå â ñòåïåíü è ðàçëîæåíèå íà ìíîæèòåëè - ïðåäñòàâëÿþò ñîáîé ôóíäàìåíòàëüíûå àðèôìåòè÷åñêèå ÿâëåíèÿ. Âåêàìè îíè áûëè ïðåäìåòîì èíòåíñèâíîãî ìàòåìàòè÷åñêîãî èçó÷åíèÿ, è ðîñò âû÷èñëèòåëüíîé ìîùíîñòè êîìïüþòåðîâ ñ îòêðûòûìè êëþ÷àìè, óâåëè÷èë, à íå óìåíüøèë íàøå äîâåðèå.
>
> 2. Íàøà âîçìîæíîñòü âûïîëíÿòü áîëüøèå àðèôìåòè÷åñêèå âû÷èñëåíèÿ ðàñòåò ðàâíîìåðíî è ñåé÷àñ ïîçâîëÿåò íàì ðåàëèçîâûâàòü ñëîæíûå ñ÷èñëîâûå òåõíîëîãèè, ÷òîáû ýòè ñëîæíûå áûëè ÷óâñòâèòåëüíûì òîëüêî ê äåéñòâèòåëüíî ðàäèêàëüíûì ïðîáëåìàì ôàêòîðèçàöèè íà ìíîæèòåëè, äëÿ êîòîðûõ èçâåñòíû ëîãàðèôìû èçâåñòíûõ ïîðÿäêîâ.

Êàê ìû óæå âèäåëè, íå âñå äëÿãîðèòìû ñ îòêðûòûìè êëþ÷àìè, îñíîâàííûå íà ýòèõ ïðîáëåìàõ, áåçîïàñíû. Ñèëà ëþáîãî àëãîðèòìà ñ îòêðûòûì êëþ÷îì çàâèñèò íå òîëüêî îò âû÷èñëèòåëüíîé ñëîæíîñòè ïðîáëåìû, ëåæàùåé â îñíîâå àëãîðèòìà. Òðóäíàÿ ïðîáëåìà íåîáÿçàòåëüíî ðåàëèçóåòñÿ â ñèëüíîì àëãîðèòìå. Àäè Øàìèð îáúÿñíÿåò ýòî òåìÿ ïðè÷èíàìè [1415]:

1. Òåîðåì ñëîæíîñòè îáû÷íî ñâÿçàíà ñ îòäåëüíûìè ÷àñòíûìè ñëó÷àÿìè ïðîáëåìû. Êðèïòîãðàôèêè æå ÷àñòî ïîëó÷àåò áîëüøîé íàáîð ñòàòèñòè÷åñêè ñâÿçàííûõ ïðîáëåì - ðàçëè÷íûå øèôðîâàíèÿ è òåì æå êëþ÷îì.
2. Âû÷èñëèòåëüíàÿ ñëîæíîñòü ïðîáëåìû îáû÷íî èçìåðÿåòñÿ äëÿ õóäøåãî ëèë ñðåäíåãî ñëó÷àåâ. ×òîáû áûòü ýôôåêòèâíî â êà÷åñòâå ñïîñîáà øèôðîâàíèÿ, ïðîáëåìà äîëæíà áûòü òðóäíîé äëÿ ðåøåíèÿ ïî÷òè âî âñåõ ñëó÷àÿõ.
3. Ïðèçâîëüíóþ ñëîæíóþ ïðîáëåìó íåîáÿçàòåëüíî ìîæíî ïðåîáðàçîâàòü â êðèòñèñòâó, ê òîìó æå ïðîáëåìà äîëæíà ïîçâîëèòü âñòðîèòü â íåå ëàçåéêó, çíàíèå êîòîðîé è òîëüêî îíî äåëàòü âîçìîæíûì ïðîñòûå ðåøåíèÿ ïðîáëåìû.