Skipjack a KEA

Šifru v pytli neutajíš...

23. června 1998 ministerstvo obrany USA překvapivě oznámilo, že National Security Agency (NSA) odtajnila dva šifrovací algoritmy, jejichž tajemství dosud pečlivě střežila. Stalo se tak poprvé v celé historii této nejmocnější a nejhlídanější americké agentury. Podíváme se nyní, proč k tomu došlo a jak tyto šifry vypadají.

To, že jedna z nejproslulejších tajných služeb USA zveřejnila své utajované algoritmy, šokovalo kryptografickou komunitu na celém světě. Nechtělo se tomu ani věřit, vždyť za 50 let své existence NSA nic takového neudělala. Oznámení, které přišlo jako blesk z čistého nebe bez jakékoli předchozí přípravy veřejnosti, bylo však ve velmi krátké době oficiálně potvrzeno z více zdrojů. Nebylo pochyb o tom, že je to pravda. Zůstal jen údiv a nezodpovězená otázka „Proč?".

Skipjack a KEA už jsou veřejné

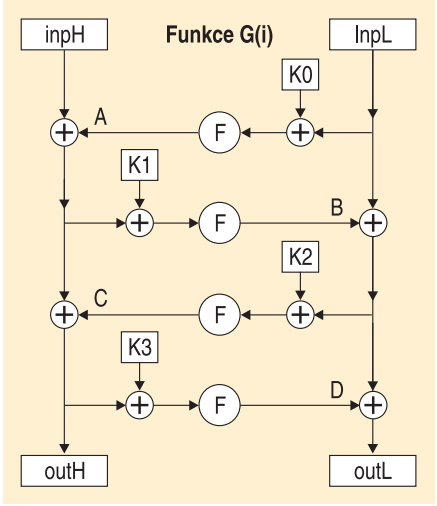
NSA zveřejnila všechny detaily klasické symetrické blokové šifry ***Skipjack*** pro šifrování dat a asymetrického algoritmu ***KEA*** (Key Exchange Algorithm) pro výměnu klíčů. Oba dva algoritmy byly až dosud realizovány pouze speciálně chráněným hardwarem (čipy Clipper, Capstone, Keystone, Regent, Krypton), aby se zabránilo jakémukoliv zpětnému inženýrství, a vlastně nikdy neměly být použity v softwaru.

K čemu měly tyto algoritmy vůbec sloužit? Před několika lety ministerstvo obrany USA potřebovalo zabezpečit svůj systém výměny elektronických zpráv DMS (Defense Message System), ve kterém se počítalo jak s desktopy, tak s přenosnými počítači. Šifrování však nešlo svěřit softwaru, neboť pak by se popis algoritmu mohl snadněji dostat na veřejnost, a tak tato práce musela být zabezpečena hardwarově. Hardware musel tuto úlohu splnit beze zbytku, a proto čipy vykonávající šifrovací operace byly speciálně chráněny fyzickými i jinými opatřeními proti zpětnému inženýrství. Náročné požadavky DMS nakonec splnil de facto jediný výrobek - PC karta ***Fortezza™*** (s variantou Fortezza™ Plus).

Ukázalo se však, že takové řešení je dost drahé i na ministerstvo obrany, vzhledem k masovosti nasazení a pravděpodobně i nastalým technickým problémům. Oddalovat řešení však už nebylo možné, neboť státní správa trvala na co nejrychlejším nasazení. DMS navíc musí pracovat non-stop a má relativně velké množství koncových uživatelů. Všechny tyto faktory (čas, cena, mohutnost nasazení a různorodost podmínek použití) nakonec vedly k závěrům stručně zformulovaným v následujícím odstavci.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	A3	D7	09	83	F8	48	F6	F4	B3	21	15	78	99	B1	AF	F9
1x	E7	2D	4D	8A	CE	4C	CA	2E	52	95	D9	1E	4E	38	44	28
2x	0A	DF	02	A0	17	F1	60	68	12	B7	7A	C3	E9	FA	3D	53
3x	96	84	6B	BA	F2	63	9A	19	7C	AE	E5	F5	F7	16	6A	A2
4x	39	B6	7B	0F	C1	93	81	1B	EE	B4	1A	EA	D0	91	2F	B8
5x	55	B9	DA	85	3F	41	BF	E0	5A	58	80	5F	66	0B	D8	90
6x	35	D5	C0	A7	33	06	65	69	45	00	94	56	6D	98	9B	76
7x	97	FC	B2	C2	B0	FE	DB	20	E1	EB	D6	E4	DD	47	4A	1D
8x	42	ED	9E	6E	49	3C	CD	43	27	D2	07	D4	DE	C7	67	18
9x	89	CB	30	1F	8D	C6	8F	AA	C8	74	DC	C9	5D	5C	31	A4
Ax	70	88	61	2C	9F	0D	2B	87	50	82	54	64	26	7D	03	40
Bx	34	4B	1C	73	D1	C4	FD	3B	CC	FB	7F	AB	C6	3E	5B	A5
Cx	AD	04	23	9C	14	51	22	F0	29	79	71	7E	FF	8C	0E	E2
Dx	0C	EF	BC	72	75	6F	37	A1	EC	D3	8E	62	8B	86	10	E8
Ex	08	77	11	BE	92	4F	24	C5	32	36	9D	CF	F3	A6	BB	AC
Fx	5E	6C	A9	13	57	25	B5	E3	BD	A8	3A	01	05	59	2A	46

Substituční tabulka funkce *F*. Příklad v hexadecimálním vyjádření: *F(7A) = D6*.



Funkce G(i).

Za stávajícího stavu nelze trvat na původních bezpečnostních požadavcích. Do procesu výroby bude potřeba zainteresovat více výrobců a i sem vnést konkurenci. Bude potřeba disponovat širší škálou produktů a smířit se i se softwarovým řešením. To může přijít relativně rychle a operativněji, i když na nižší bezpečnostní úrovni. Šifrovací algoritmy se tedy musí dostat do softwaru mnoha uživatelů DMS i výrobců šifrovacích programů a zařízení. To ve svém důsledku naprosto jistě povede k jejich úniku na veřejnost. Logický závěr: je lépe to udělat sami a otevřeně. Odtud tedy i neočekávanost rozhodnutí – s možností zveřejnění se určitě počítalo jen jako s krajní variantou a čekalo se s ní pochopitelně až do poslední chvíle.

Příležitost pro komerční výrobce

Rozhodnutí NSA umožní rozvoj a použití komerčních levnějších řešení – alternativních Smart karet a softwarově orientovaných produktů, které by měly pokrýt ochranu citlivých (neutajovaných) národně bezpečnostních dat. Data z těchto systémů jsou však využívána i v systémech, které zpracovávají informace utajované. V těch se pro dosažení vyšší bezpečnosti používá speciální hardware (ať už pro ochranu šifrovacích klíčů nebo zajištění správného výkonu šifry, protokolu, spojení ap.). To však nebrání tomu, aby existovala datová kom-

patibilita se systémy nižších bezpečnostních úrovní, které jsou určeny pro masovější použití, jiné typy informací, a hlavně mohou být pořízeny levněji. Podmínkou je šifrování stejnými šiframi a NSA tedy používá algoritmy KEA a Skipjack i pro šifrování ve vyšších národně bezpečnostních systémech. A proč ne? Kvalita uvedených algoritmů musí být přece zajištěna tak jako tak!

NSA proto také oznámila otevřenost ke spolupráci s dalšími výrobci, aby urychlila vývoj příslušných aplikací. Uklidňující bylo přitom ujištění, že NSA nehodlá prosazovat Skipjack jako kandidáta na tvorbu nového šifrovacího standardu (viz např. Chip 11/97, str. 44; 12/98, str. 170). To uvolnilo nesmírné napětí, neboť kryptografická veřejnost se obávala, že zveřejnění Skipjacku je de facto zásahem NSA do výběru nového komerčního šifrovacího standardu AES (Advanced Encryption Standard), jak tomu bylo u DES před 25 lety.

NSA však šla ještě dále, když prohlásila, že bude plně respektovat vítěze výběrového řízení na AES a navíc umožní jeho začleňování do odpovídajících systémů ministerstva obrany (zde jde o neutajované, ale citlivé informace!). NSA se vytáhla. Všechny její kroky a postoje v tomto novém, bezprecendentním případu nelze kvalifikovat jinak, než jako otevřené, moderní a jednoznačně pozitivní rozhodnutí.

Vojenský rukopis se nezapře

Skipjack je 64bitová symetrická šifra s 80bitovým klíčem. Klíč je uložen v 10bajtovém zásobníku k[0], ..., k[9] a je používán tak, jak je uložen. V každé ze 32 „rund“ algoritmu se ze zásobníku vyčtou čtyři bajty klíče, přičemž z konce se automaticky přechází na začátek. Šifra tedy nemá žádnou inicializační fázi (přípravu klíče)! Způsob zašifrování znázorňují připojená schémata. Counter je čítač, který označuje číslo rundy (i = 1..32) a poprvé je použita hodnota i = 1. Otevřený text je uložen do čtyř slov *w1* až *w4* (po 16 bitech) a poté podroben osmi operacím typu A (i = 1..8), dále osmi operacím typu B (i = 9..16), znovu osmi operacím typu A (i = 17..24) a nakonec osmi operacím typu B (i = 25..32). Výsledek (zašifrovaný text) je uložen opět ve slovech *w1* až *w4*.

Schéma A i B myšlenkově vychází z posuvných registrů s nelineární zpětnou vazbou. Tato oblast je natolik různorodá a složitá, že nebyla ve veřejně přístupné literatuře prozkoumána tak dobře jako oblast lineárních posuvných registrů. Je to však doména vojenského výzkumu a Skipjack je jeho dítětem.

Popišme si ještě funkci *G(i)*. Ta je příkladem tzv. Feistelova schématu. Závislost funkce *G* na indexu rundy *i* je dána jen tím, že používá 4 bajty klíče, cyklicky vybíraného v dané rundě ze zásobníku. Ve funkci *G(i)* jsou použity tyto bajty klíče: *K0 = k[(4*i) mod 10]*, *K1 = k[(4*i+1) mod 10]*, *K2 = k[(4*i+2) mod 10]*, *K3 = k[(4*i+3) mod 10]* a pevná substituční tabulka *F* převádějící bajt na bajt. Označíme-li horní a dolní bajt vstupu funkce *G* jako *inpH a inpL a* podobně horní a dolní bajt výstupu funkce *G* jako *outH a outL*, pak výstup je definován těmito vztahy (bajty *A* až *D* jsou pomocné meziproměnné):

A = F(inpL xor K0),
B = F(inpH xor A xor K1),
C = F(inpL xor B xor K2),
D = F(inpH xor A xor C xor K3),
outH = inpH xor A xor C,
outL = inpL xor B xor D.

Funkce *F* je pevná substituce daná příslušnou tabulkou. Tím je popis Skipjacku úplný.

Hardwarová realizace Skipjacku: karta Fortezza.

Jak silný je Skipjack?

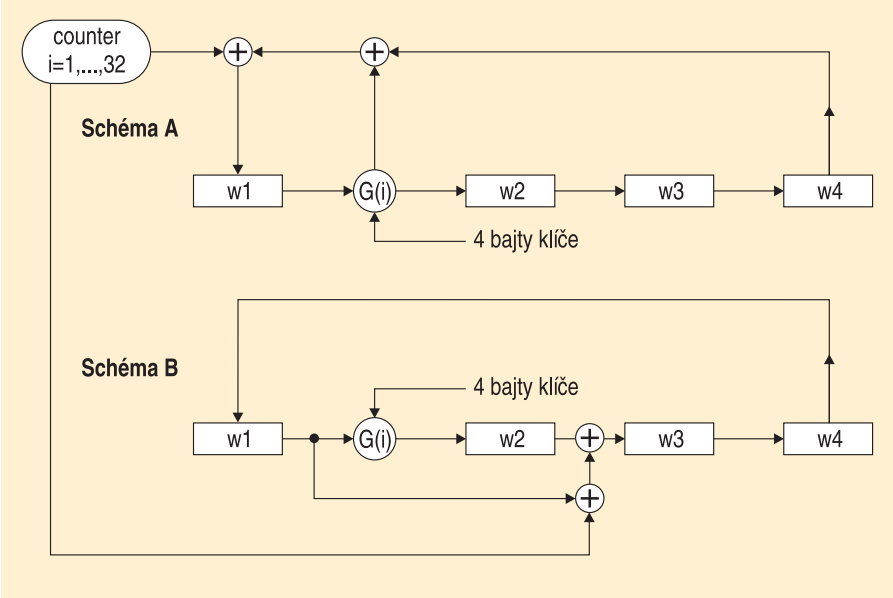
Na svůj armádní původ je Skipjack podle některých kryptologů dost „křehký”. Domnívají se, že jakékoliv oslabení kterékoliv části schématu by vedlo k jeho luštění, tj. nalezení (analytické) metody, která je účinnější než útok hrubou silou na 80bitový klíč. Taková metoda byla už také uplatněna na 31 rund Skipjacku (na konferenci Crypto´ 98 v USA), ale nikoli na plnohodnotných 32. Připomeňme paralelu s DES (návrh byl také korigován NSA), kdy se našla (analytická) metoda, účinnější než útok hrubou silou, ale pouze na 15, nikoli na 16 rund DES (pomineme-li vlastnost komplementárnosti). Říká se však, že NSA předběžně počítala s možností prozrazení šifry, a proto při jejím návrhu nepoužila své nejnovější know-how (to je sice pravděpodobné, ale přesto ho považuji za dostatečně bezpečný a silný algoritmus).

Kromě toho byly nalezeny další zajímavé vlastnosti. Je to např. existence takového vstupu funkce *G*, který jí prochází nezměněn. Ano, jak je vidět na schématu či na rovnicích, nastane to v případě, že *A = C* a *B = D*. To totiž po krátkém cvičení s rovnicemi dává vstup o hodnotách *inpH = K3 xor invF(K0 xor K2)*, *inpL = K0 xor invF(K1 xor K3)*, kde *invF* je tabulka inverzní k *F*, a ten je roven výstupu.

Jiné zajímavosti vás určitě napadnou při programové realizaci Skipjacku. Druhou známou vlastností je, že polovinu funkce *G*, tj. dvě feistelovské operace, lze nahradit tabulkou převádějící 16 bitů vstupu na 16 bitů výstupu. Je to velmi podobné metodě, která vedla k urychlení programové realizace DES. Klíč se jakoby „vytkne před operaci” (dvě rundy *G*) a zmíněná 128kilobajtová tabulka pak není závislá na klíči!

Závěr

Když před 25 lety NSA umožnila „vypuštění” DES na veřejnost, bylo to později interně považováno za jednu z jejích největších chyb. Dnes se připravuje nový standard AES, všemocná NSA stojí mimo tento proces, slibuje, že ho dokonce komerčně podpoří a publikuje i svůj standard. Zdá se, že se časy mění.



Šifrovací algoritmus Skipjack.

Do tohoto příspěvku už se nám nevejdou podrobnosti algoritmu výměny klíčů KEA, ale o něm si povíme příště. Pokud vás ke Skipjacku napadne cokoliv zajímavého, napište nám – rádi s tím seznámíme i ostatní čtenáře (a možná se jednou stanete slavnými kryptoanalytiky).

Vlastimil Klíma (*vklima@decros.cz*)