Jak pašák zdokonalil AES

Nedávno se v diskusní skupině sci.crypt na Internetu objevil příspěvek, který oznamoval, že pisatel objevil novou nerozluštitelnou metodu. Tato oznámení chodí s železnou pravidelností stejně jako blázni do Matematického ústavu AV. Těmto lidem není možné vysvětlit jejich omyl často jiným způsobem než malým podvůdkem. Například vynálezcům trisekce úhlu se jejich metoda (která neexistuje) vyvrací tak, že se nadšeně účastníme jejich konstrukce na velké plachtě papíru na podlaze naší kanceláře, a tam nenápadně některou čáru nebo velké kružítko trochu přihneme, aby to nevyšlo. Pak s vynálezcem sdílíme krátké zamyšlení, proč to asi nevyšlo a opět velké nadšení, že kdyby se to ještě trochu zdokonalilo, tak to určitě vyjde. U šifer je to bohužel mnohem složitější.

Docela sympatická konstrukce

Ukážeme si jednu „pašáckou“ šifru („Pašák“ je v našich článcích ten, kdo všechno ví „a jde hned na věc“). Jednalo se o vývoj šifry, kdy bylo zadáno, že tam má být AES (Advanced Encryption Standard), ale aby tam byla ještě nějaká rezerva, kdyby AES „praskla“. Náš člověk se rozhodl použít TripleAES. Jenže ouha, omezené prostředí jednoduchého procesoru ukázalo, že k šifrování průchozích dat nelze použít ani jednoduchou AES, neboť není dost paměti na meziproměnné a na tzv. rundovní klíče. Šifra musela pracovat „na místě“, bez meziproměnných, zato mohla mít více iterací než AES, neboť času byl relativní dostatek. Náš vývojář věděl, že AES a všechny moderní šifry jsou vytvořeny ze substituce, permutace a přičítání rundovního klíče, a to iterovaně za sebou. Rundovní klíč však nebylo kam ukládat, proto se rozhodl ho vynechat a jako kompenzaci za to použil tajnou substituční tabulku a tajnou permutaci. Navíc použil tajný počet rund 10 + x, kde x je dolních pět bitů klíče (AES-128 má pouze 10 rund). Původní klíč posloužil pro zašifrování dvou konstant pomocí AES, přičemž první výstup se použil pro tajné naplnění substituční tabulky (*tabulka 1*) čtyřbitovými čísly 0–15 (dále jen „nibl“) a druhý pro tajné naplnění permutace čísel 0–15 (*tabulka 2*).

Rozbití statistik

V *tabulce 1* vidíme, jak se šifruje vstupní text „účet“ (hexadecimálně FA E8 65 74). Bajty jsou nejprve rozbity na nibly (F A E 8 6 5 7 4).

Každý nibl se pomocí tabulky zašifruje na dvojici niblů 02 00 31 10 30 23 03 33 (například první nibl F se zašifruje na 02). Potom se opět nibly rozpojí (0 2 0 0 3 1 1 0 3 0 2 3 0 3 3 3) a promíchají tajnou permutací.

Takže například nula z první pozice vstupu **0** 2 0 0 3 1 1 0 3 0 2 3 0 3 3 3 přejde podle *tabulky 2* na pozici 13, výsledek je 0 1 2 3 2 1 0 3 0 0 3 3 **0** 3 3 0. Nyní spojíme vždy lichý a sudý nibl, pocházející původně z různých míst: 01 23 21 03 00 33 03 30. Každá dvojice niblů je ukazatelem do substituční tabulky (první nibl ukazuje osu y a druhý osu x), čili ji nahradíme tím znakem v tabulce, na který ukazuje: 2 5 C 7 A 4 7 6. Uvědomíme si, že touto operací došlo k rozbití bajtů na nibly, jejich nahrazení za tajné hodnoty, promíchání jejich „půlpozic“ a převodu nově vzniklé pozice na nový znak. To je docela dobrý nápad a tvůrce předpokládal, že toto jistě rozruší statistické vlastnosti původního textu, nehledě na to, že příslušné operace závisí na klíči. Dále počítal s tím, že pokud uvedený postup bude opakovat mnohokrát za sebou, bude se míchání pozic a hodnot prohlubovat a zesložiťovat a vznikne silná šifra. Když si vypíšeme několik prvních iterací, zdá se skutečně, že iterace jsou náhodné a uvedený princip funguje.

Tabulka 1 Tajná substituce

	0	1	2	3
0	A	2	F	7
1	8	0	3	D
2	B	C	1	5
3	6	E	9	4

Tabulka 2 Tajná permutace

1	2	3	4	5	6	7	8	9	10	11	12	13	19	15	16
3	7	11	15	2	6	10	14	4	8	12	16	1	5	9	13

Tabulka 3 Tři iterace podrobněji

0	ú	č	e	t
	FA	E8	65	74
	0200	3110	3023	0333
	0123	2103	0033	0330
	25	C7	A4	76
1	%	Ç	¤	v
	25	C7	A4	76
	0123	2103	0033	0330
	2033	1103	3330	0200
	B4	07	46	FA
2	'	□	F	ú
	B4	07	46	FA
	2033	1103	3330	0200
	3030	0132	3300	2130
	66	29	4A	C6
3	f	)	J	Ć

zruší se

zruší se

spojí se

Tabulka 4 Permutace řádu 6

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

Překvapení

Bylo to velké překvapení, když jsme Pašákovi sdělili, že kdyby použil třeba tisíc iterací, je to stejné, jako kdyby použil jednu. A navíc, že pro hodně klíčů tahle šifra vůbec nešifruje. Ono čertovo kopýtko je vidět, zapíšeme-li si dvě iterace za sebou (*tabulka 3*). Vidíme, že to, co jsme v poslední operaci předchozí iterace udělali, v první operaci následující iterace ihned vrátíme zpátky. Skutečně, na konci jedné iterace děláme převod dvojniblu na znak v tabulce (01 na 2, 23 na 5, atd.) a hned nato v další iteraci tento znak převádíme na dvojnibl. Substituci na konci jedné iterace a substituci na začátku další iterace tak vzájemně vyrušíme. Jedině úplně první a úplně poslední substituce se nemají vůči čemu zrušit, a proto zůstávají. Mezi nimi také zůstanou permutace ze všech iterací. Kolik iterací použijeme, tolik permutací se „setká uprostřed“. Ať jsou jakkoliv utajené, a i kdyby jich bylo tisíc, složíme-li je dohromady, dostaneme jen jednu jedinou permutaci. Tím se vysvětluje, že se celá šifra „scvrkne“ na jednu substituci úplně na začátku, jednu permutaci uprostřed a jednu substituci úplně na konci, čili na jedinou iteraci. Teď si ještě představme, že permutace uprostřed je identita. Pak se vlastně zruší i počáteční a závěrečná substituce vůči sobě a máme šifru, která nedělá nic. To nejlepší nakonec. Každá permutace, která pracuje nad konečným počtem prvků N (zde N = 16) se po několikerém složení zákonitě do identity dostane (pro nevěřící – viz pojem řád prvku permutační grupy). U nás je to po šesti složeních a *tabulka 4* ukazuje, kudy cestují jednotlivé číslice.

Pokud je klíč zrovna takový, že počet iterací vyjde jako násobek šesti, daná šifra vůbec nešifruje. Pašáci, kteří navrhují tyto a podobné šifry, i blázni, kteří se pravidelně vrací s kružítky a trojúhelníky, mají jedno společné. Po ukázce, že v jejich metodě je „drobná“ chyba, ji začnou vyspravovat novými drobnými krůčky a vylepšeními. Naše zkušenost je, že není příliš vhodné jim bránit v dalších nápadech, neboť je to pouze průvodní jev jejich veskrze kladné touhy vyřešit daný problém.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, tomas.rosa@rb.cz

LITERATURA

[1] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz