Šifrovací standard AES

Představujeme kandidáty na AES: Šifra SERPENT

SERPENT je jedním z pěti kandidátů na Advanced Encryption Standard (AES). O celém výběrovém řízení se podrobněji dozvíte v úvodu k této sérii stručných popisů všech finalistů, a to v článku „Bitva o trůn vrcholí" v Chipu 10/99; zde se už věnujeme přímo technickému popisu šifry. Připomeňme jen, že AES se stane šifrovacím standardem pro příští století (nebo alespoň nějaká ta desetiletí) a bude mít dalekosáhlý vliv na počítačovou bezpečnost.

Blokovou šifru ***SERPENT*** přihlásili do soutěže Ross Anderson (UK), Eli Biham (Izrael) a Lars Knudsen (Norsko), známá esa světové kryptologie. Jako u všech kandidátů na AES je délka vstupního a výstupního bloku 128 bitů a podporované délky klíče 128, 192 a 256 bitů. SERPENT používá pevné substituční tabulky (osm S-boxů zobrazujících 4 bity na 4 bity) a pracuje v rundách podobně jako DES, má však dvojnásobný počet rund (32). Se 128bitovým blokem a 256bitovým klíčem je přibližně stejně rychlý jako DES, je ale bezpečnější než TripleDES.

Návrh šifry je dost konzervativní. Autoři nechtěli použít žádné nové prvky (datově závislé rotace, násobení nebo sčítání místo operace $\oplus$ apod.), a proto výhodně aplikovali osvědčené principy tak, aby se šifra dala dobře hardwarově i softwarově implementovat. Zejména, jak uvidíme dále, je kladen důraz na možnost paralelního zpracování jednotlivých bitů a možnost výpočtu rundovních klíčů za chodu („on-the-fly"). Díky tomu, že návrh je bitově orientovaný, umožňuje optimalizovat programový kód pro různé mikroprocesory. Odšifrování (je popsáno v hlavním dokumentu; viz infotipy) zde však probíhá trochu jinak než zašifrování, takže nelze použít stejný hardware jako u šifry MARS.

Postup při zašifrování

Před operací zašifrování nebo odšifrování anebo v jejím průběhu se vypočítá 33 rundovních klíčů. Jsou to 128bitové hodnoty K[i], i = 0..32, z nichž každou chápeme jako zřetězení čtyř 32bitových slov k_{4*i+0}, k_{4*i+1}, k_{4*i+2}, k_{4*i+3} (jejich výpočet popíšeme dále). Otevřený text se naplní do 128bitového bloku B[0] a v každé z 32 rund (i = 0..31) se z B[i] vypočte B[i+1]. Výsledný šifrový text je uložen v B[32]. Runda **i** se skládá z následujících kroků (viz též obrázek 1). Na vstupní 128bitový blok B[i] se „naxoruje" rundovní klíč K[i]. Obě proměnné jsou chápány jako čtyři 32bitová slova, takže také výsledek B[i] $\oplus$ K[i] je možné chápat jako čtyři 32bitová slova. Nyní se tato slova seřadí tak, že jejich bity vytvářejí „čtyřřad" (viz obr. 2), takže na prvním místě stojí za sebou první bity slov, na druhém místě druhé bity atd. Nyní aplikujeme substituční box S_i postupně na všech 32 popsaných čtveřic bitů (v i-té rundě použijeme jeden S-box S_i). Protože rund je 32 a S-boxů osm, používají se S-boxy „dokola", tedy $S_i = S_{i \bmod 8}$.

Vstup	$B[i] = (x_0, x_1, x_2, x_3)$
Maskování klíčem	$B[i] = B[i] \oplus K[i]$
Substituce	$(x_0, x_1, x_2, x_3) = S_i(B[i])$
Lineární transformace	
	$x_0 = x_0 <<< 13$
	$x_2 = x_2 <<< 3$
	$x_1 = x_0 \oplus x_1 \oplus x_2$
	$x_3 = x_3 \oplus x_2 \oplus (x_0 << 3)$
	$x_1 = x_1 <<< 1$
	$x_3 = x_3 <<< 7$
	$x_0 = x_0 \oplus x_1 \oplus x_3$
	$x_2 = x_3 \oplus x_2 \oplus (x_1 << 7)$
	$x_0 = x_0 <<< 5$
	$x_2 = x_2 <<< 22$
Výstup	$B[i+1] = (x_0, x_1, x_2, x_3)$

Pozn.: w<<r znamená posun slova w doleva o r bitů, přičemž zprava se doplní nuly.

Obr. 1. Jedna runda zašifrování.

Výstupem S-boxu jsou čtyři bity, které zase uložíme do čtyřřadu tak, jak byl seřazen vstup. Čtyři nově vzniklá 32bitová slova (tvořící ony čtyři řady) si označme x_0, x_1, x_2, x_3. Dosavadní operace pak můžeme zapsat ve tvaru $(x_0, x_1, x_2, x_3) = S_i(B[i] \oplus K[i])$. S novými hodnotami slov **x** nyní provedeme lineární transformaci L podle pseudokódu na obrázku 1 a obdržíme nové hodnoty 32bitových slov $x = L(x_0, x_1, x_2, x_3)$. Ty už tvoří výstup z i-té rundy $B[i+1] = (x_0, x_1, x_2, x_3)$. Ještě poznamenejme, že u 32. rundy je lineární transformace nahrazena operací XOR s rundovním klíčem K[32].

Příprava klíčů

Rundovní klíče se vytvářejí poměrně jednoduše. Pokud šifrovací klíč (128, 192 nebo 256 bitů) nemá délku 256 bitů, doplní se na ni bitem 1 a dále nulovými bity. Ten se naplní po řadě do osmi 32bitových proměnných w_{-8}, w_{-7}, ..., w_{-1} a ty se dále expandují až do w_{131} podle vzorce $w_i = (w_{i-8} \oplus w_{i-5} \oplus w_{i-3} \oplus w_{i-1} \oplus \phi \oplus i) <<< 11$, i = 0..131;

zde **w <<< r** znamená rotaci slova **w** o **r** bitů doleva a ϕ je hexadecimální konstanta *0x9e37799b* (autoři tvrdí, že tento vzorec vylučuje vznik slabých klíčů). Nyní na čtveřici slov (w_0, w_1, w_2, w_3) aplikujeme S-box (jako první použijeme S_3) stejným způsobem jako na obrázku 2 – vzniklá slova jsou už jednotlivá slova rundovního klíče $K[0] = (k_0, k_1, k_2, k_3)$. Další klíč $K[1] = (k_4, k_5, k_6, k_7)$ získáme aplikací boxu S_2 na (w_4, w_5, w_6, w_7) atd.

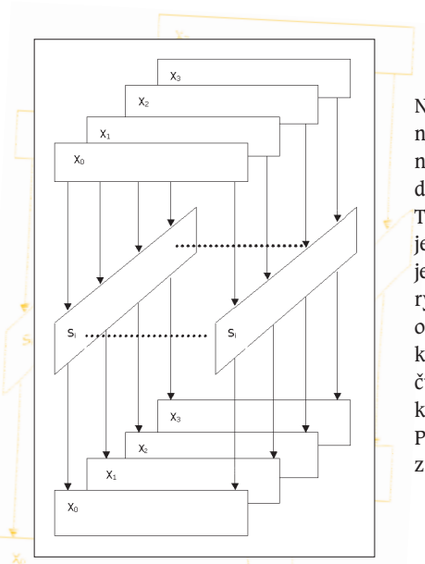
infotipy

Zdrojové kódy:
ftp://ftp.funet.fi/pub/crypt/cryptography/symmetric/SERPENT/
Úplný popis:
http://csrc.nist.gov/encryption/aes/aes_home.htm

(indexy u S-boxů se snižují o 1, modulo 8), až vytvoříme poslední rundovní klíč K[32] = (k_{128}, k_{129}, k_{130}, k_{131}). Ještě dodejme, že S-boxy jsou konstantní a byly vygenerovány tak, aby schéma co nejvíce odolávalo diferenciální a lineární kryptoanalýze (blíže viz základní dokument v infotipech).

Implementace a rychlost

Jak je zřejmé z definice zpracování klíče, rychlost šifry nezávisí na jeho délce. Dále je vidět, že rundovní klíče lze počítat za chodu. Zašifrování jednoho 128bitového bloku dat spotřebuje cca 1830 – 1940 instrukcí (je to pochopitelně závislé na typu procesoru). Navíc, díky bitově orientovanému návrhu, například 1940 instrukcí na Pentiu vyžaduje jen 1738 hodinových cyklů. Podstatné je, že na referenčním PC s 200MHz Pentiem Pro (při implementaci v jazyce C) autoři odhadují rychlost šifrování na 14,7 Mb/s. Na osmibitovém procesoru (například 3,5MHz 6805, používaném v čipových kartách) záleží na možnosti optimalizovat kód na úkor paměti. Tak například s využitím 1 KB paměti je možné dosáhnout rychlosti jen 12,8 Kb/s, zatímco s 2 KB paměti je to už 40,7 Kb/s.



Obr. 2. Průchod substitučními boxy.

Bezpečnost

Na základě pravděpodobností, vypočítaných pro potřeby diferenciální kryptoanalýzy, dospěli autoři k závěru, že 16rundovní SERPENT je stejně bezpečný jako TripleDES. Z bezpečnostních příčin však ještě zdvojnásobili počet rund na 32, což je z hlediska dlouhodobého používání šifry jistě velmi odpovědné. Pokud jde o odolnost vůči lineární a diferenciální kryptoanalýze a metodě příbuzných klíčů, je takový dotaz trochu jako přihrávka na smeč – jeden z autorů šifry SERPENT je totiž spoluobjevitelem dvou z těchto kryptoanalytických metod...

Závěr

SERPENT je konzervativní a silně bezpečnostně orientovaná šifra. To je bohužel zaplaceno její nejnižší rychlostí v porovnání s ostatními kandidáty na AES. Vhodná tedy bude zejména pro paralelní zpracování. Procesy šifrování a odšifrování jsou odolné vůči fyzickým typům útoků.

VLASTIMIL KLÍMA (*V.KLIMA@DECROS.CZ*)