ŠIFROVACÍ STANDARD AES

Zvítězil Rijndael

Výměna „kreknutého“ amerického šifrovacího standardu DES za AES (Advanced Encryption Standard) dospěla do konečné fáze. Ve veřejné soutěži, trvající bezmála čtyři roky, byl za nový algoritmus vybrán Rijndael. Američané udělali gesto – národním, ale nepochybně i světovým šifrovacím standardem začátku třetího tisíciletí bude algoritmus od Belgičanů!

Pro světovou kryptografickou komunitu se letošní 2. říjen stal dnem, na který čekala skoro třicet let. Šifrovací standard DES bude po dlouhých tahanicích a nakonec i sestrojení DES-crackeru za soukromé peníze (viz infotipy) konečně nahrazen něčím bezpečným. Světový bankovní, telekomunikační a počítačový průmysl dostane nový šifrovací standard, o nějž se bude moci opřít! USA, v podobě standardizačního úřadu (NIST), udělaly historicky bezprecedenční gesto osvíceného panovníka a – bez zřejmého zásahu tajných služeb, jak tomu bylo doposud – ve veřejné soutěži (jednotlivé kandidáty jsme vám představili i v Chipu) vybraly algoritmus pro ochranu senzitivních informací ve státní správě. Čin o to osvícenější, že soutěž byla veřejná, dostatečně dlouhá na zjištění nedostatků a vítěz zahraniční – **Rijndael** (doporučená výslovnost tohoto slova je *rájndol*). Nos utřely velké organizace jako RSA, IBM a další a jejich algoritmy skončí pravděpodobně v zapomnění (škoda, osobně jsem fandil právě návrhu MARS od IBM...).

BUDE TO BYZNYS...

Teď půjde skutečně o velký byznys, který se dotkne i nás. Proč? Nastala situace, kdy se kombinuje několik zlomových událostí a faktorů. Prvním je rozvoj e-obchodu, bankovnictví, a vůbec „e-života“. Důležitou roli v něm hraje internet a ochrana informací (bankovní transakce, soukromí apod.), a tam všude je nutné šifrování a elektronický podpis. Druhým faktorem je neustálé vznikání nových aplikací, prostředků a služeb, a i tam je zapotřebí bezpečný standard, který je už k dispozici. Dalším faktorem je současná roztříštěnost – v řadě prostředků se používají navzájem nekompatibilní algoritmy, za které se mnohdy musí platit licenční poplatky (společnosti těžily z toho, že DES nebyl bezpečný a jeho varianta TripleDES pomalá). Svou roli nepochybně sehrál i ukončený vývoj nových standardů pro elektronický podpis a rozsáhlé rušení zákazu exportu silné kryptografie z USA.

Teď už si jistě dovedete představit, jak dobře všem zní, že od 2. 10. 2000 budou moci **zadarmo** implementovat nový, bezpečný a rychlý algoritmus Rijndael, který od obdržení razítka „standard AES“ dělí už jen měsíce (duben až červen 2001) a oficiální procedury (vypsání dokumentu FIPS PUB, připomínkové řízení, vyhlášení standardu).

SNADNÉ TO NEBUDE

Zdá se tedy, že všechno je naprosto ideální, ale nebude to tak jednoduché! Nový standard (mj. proto, aby byl odolný proti tzv. slovníkovým útokům a kolizím) zavádí i novou šířku dat, která zašifrovává a odšifrovává (najednou) místo původních 64 bitů nyní 128 bitů. Podobně je to s délkou klíče, která se povinně prodlužuje až na 256 bitů. Obojí dohromady (i zvlášť) je něco jako přestavba železnice na širokorozchodnou. Nejde totiž jen o nové aplikace – u těch starších to v mnoha případech nadělá v programech a protokolech velkou paseku, nemluvě o hardwarových zařízeních nebo čipových kartách, bankomatech, platebních terminálech...

Ale i tak to stojí za to! Bude se tedy, jak by asi řekl pan Werich, přeprogramovávat, vyvíjet, vyrábět, měnit a měnit. Staré a málo bezpečné za nové a bezpečnější. (K té bezpečnosti musím z povinnosti dodat: ... pokud nedojde k nějakému převratnému objevu, třeba v oblasti kvantových počítačů. Pak by se současné pojetí bezpečnosti zcela zhroutilo, ovšem nejen to...)

Domácí stránka amerického standardizačního úřadu NIST

infotipy

Citované články z Chipu naleznete také na
▸ *www.decros.cz/Security_Division/Crypto_Research/archiv.htm*
pod mnemotechnickým označením
časopis-rok-měsíc-strana(od-do).ext

[VK] Popis šifry Rijndael (podstatný extrakt):
Představujeme kandidáty na AES: Šifra RIJNDAEL, Chip 11/99, str. 64 – 65
[VK] Finále výběru kandidátů na AES a jejich základní charakteristiky:
Bitva o trůn vrcholí, Chip 10/99, str. 40 a 42
Sestrojení lušticího stroje na DES, odkazy, obrázky, dokumentace:
DES Cracker: Kladivo na DES, Chip 11/98, str. 74 – 75
[AES] Domácí stránka AES (všechny události a odkazy na související stránky):
▸ *http://csrc.nist.gov/encryption/aes/aes_home.htm*
[BG] Uznávané rychlostní testy kandidátů AES od Briana Gladmana:
▸ *http://www.btinternet.com/~brian.gladman/*
[TK] Tisková konference k oznámení vítěze AES a další odkazy:
▸ *http://www.nist.gov/public_affairs/releases/g00-176.htm*
[FAQ] Často kladené otázky a odpovědi (velmi dobré):
▸ *http://www.nist.gov/public_affairs/releases/aesq&a.htm*
[RI] Popis algoritmu, dokumentace, zdrojové kódy, testovací příklady:
▸ *ftp://ftp.funet.fi/pub/crypt/cryptography/symmetric/aes/*
▸ *http://csrc.nist.gov/encryption/aes/round2/r2algs.htm#Rijndael*

Technické informace

K algoritmu i k procesu jeho výběru existuje spousta užitečných, zejména technických informací, na které vás chceme upozornit. Je jich ovšem několik tisíc stran, a proto jsme je soustředili do komentovaných infotipů; pokud se jich budete držet, žádná důležitá informace vám neunikne. Především je dobré si přečíst často kladené otázky (viz [FAQ]). Jsou opravdu velmi dobře zpracované a manažerům plně postačí k orientaci. Dále je tu tisková konference k uvedení vítěze soutěže (viz [TK]) se zajímavými politickými a technickými aspekty, neboť vyhlášení vítěze se zúčastnili dost velcí pohlaváři. Pro programátory je tu i kompletní popis, zdrojové kódy a testovací vektory algoritmu (viz [RI]) a jeho český extrakt pro rychlejší orientaci ([VK]). Závěrečné kolo soutěže jsme popsali v článcích z minulého roku ([VK]), kde jsou i další informace.

Domácí stránka projektu AES

Shrnutí

Od vyhlášení soutěže na AES (2. I. 1997) do oznámení vítěze uplynulo tři a tři čtvrtě roku, tedy dost na to, aby se dala posoudit bezpečnostní kvalita kandidátů. Vítězem se stal belgický algoritmus Rijndael. Po oficiálním schválení se na dalších 20 až 30 let stane nejpoužívanější šifrou na světě a ovlivní bezpečnostní praxi v mnoha ohledech. Jeho úloha v novém tisíciletí je více než zřejmá – zvýšit důvěryhodnost elektronického obchodu, bankovnictví a „elektronického života“ vůbec.

Vlastimil Klíma • v.klima@decros.cz