Základy kryptografie II.

Šifrovat?…..Rozhodně Ano!

Symetrické šifry

Jaroslav Pinkava

Minulá (úvodní) část seriálu seznámila čtenáře se základy šifrování. Byly objasněny některé základní pojmy a bylo řečeno, že dnešní kryptografie (nauka o navrhování šifrovacích algoritmů a způsobech jejich využívaní) se zabývá dvěma základními typy šifrovacích algoritmů: symetrickými a asymetrickými šiframi. Dnes budeme hovořit blíže o symetrických šifrovacích algoritmech resp. o jejich nejdůležitějších představitelích - o blokových šifrách.

Symetrické šifrovací algoritmy používají k šifrování i k dešifrování jeden a tentýž tajný klíč. V zásadě existují symetrické šifry dvou typů: proudové a blokové šifry.

Proudové šifry jsou šifrovací algoritmy, které mohou zpracovávat zprávu libovolné délky tak, že šifrují její jednotlivé prvky tj. bity či byty. Nemusí tedy shromáždit před šifrováním nejprve celý blok dat. Konstrukce proudových šifer je v zásadě jednoduchá. Sestává z náhodného generátoru, jehož výstupní hodnoty závisí na hodnotách tajného klíče. Výstupní posloupnost tohoto generátoru je pak nějakým jednoduchým způsobem kombinována s otevřeným textem. Obvykle je k tomu využíván součet modulo dva (XOR - exclusive OR).
Dešifrace pak probíhá analogickým způsobem. "Náhodným generátorem" (v závislosti na hodnotě tajného klíče) je opět generována pseudonáhodná posloupnost (říká se jí heslo) a sečtením modulo dva této posloupnosti a šifrového textu dostaneme zpět otevřený text. Při konstrukci příslušného generátoru hesla je samozřejmě třeba vycházet z podmínek definujících kryptologickou odolnost celého systému. Například je zcela reálné předpokládat, že v určitých situacích zná potenciální protivník jak šifrový text tak i jemu příslušející otevřený text (tzv. Known Plaintext Attack - útok při znalosti otevřeného textu). Potom jednoduchým způsobem získá "čisté" heslo a stojí před úlohou, jak získat k tomuto heslu příslušející tajný klíč. Pokud by tuto úlohu vyřešil, mohl by si pak vygenerovat příslušné heslo i pro úsek, kde adekvátní otevřený text jemu znám není. Samozřejmě kvalitně navržená šifra musí být schopná tomuto útoku odolat.
Ke konstrukci proudových šifer jsou obvykle využívány tzv. lineární registry (posuvné registry s lineární zpětnou vazbou) s nelineárním výstupem, resp. jsou přímo používány nelineární registry (již sama zpětná vazba těchto posuvných registrů je nelineární).
Poznámka: Obsah pojmu hesla v tomto odstavci se liší od obsahu tohoto pojmu v minulé části seriálu (pojem hesla využívaný jako označení pro posloupnost znaků např. při přihlášení se k počítači - anglicky password). Bohužel v české odborné terminologii již toto dvouznačné užívání pojmu hesla dosti pevně zakotvilo.

Blokové šifry zašifrovávají současně celý blok dat (obvykle 64 bitů, stejně veliký je i výstupní blok šifrového textu). Velikost vstupního bloku blokové šifry má základní význam pro bezpečnost celého algoritmu. Pokud by velikost tohoto bloku byla malá, pak by bylo možné

vytvořit "slovník", tj. sestavit kompletní seznam (při určitém klíči) vstupních a jim odpovídajích výstupních hodnot algoritmu. To by samozřejmě mělo velmi nepříznivý dopad na bezpečnost celého algoritmu. Proto je nezbytné volit velikost vstupního bloku "dostatečně velikou", tj. takovou, aby vytvoření takovéhoto slovníku bylo nereálné. V současnosti jsou používany převážně blokové šifry zpracovávající bloky o délce 64 bitů (odpovídající slovník by měl velikost 2^{64}). V rámci připravované normy pro 21. století (AES) jsou připravovány algoritmy zpracovávající bloky dat v délce 128 bitů.

Módy blokových šifer:

Pokud jeden a tentýž blok je dvakrát zašifrován tímtéž klíčem, obdržíme jako výsledný blok tentýž šifrový text (této metodě šifrování se říká elektronická kódová kniha - Electronic Code Book mode čili mód **ECB**). Takováto informace však může být užitečná pro potenciálního narušitele. V praxi by bylo proto výhodnější, aby týmž blokům otevřeného textu odpovídaly různé bloky šifrového textu. Všeobecně jsou užívány následující dvě metody:

- mód **CFB** (Cipher Feedback mode): blok šifrového textu je získán zašifrováním minulého bloku šifrového textu
(posledních 64 bitů) a přičtením části vzniklého šifrového textu (obvykle v délce 1 byte) modulo dva k stejně dlouhému bloku otevřeného textu.
- mód **CBC** (Cipher Block Chaining mode): blok šifrového textu je získán tak, že sečteme nejprve mod 2 blok otevřeného textu s minulým šifrovým textem a výsledek zašifrujeme.

Tyto způsoby šifrování vyžadují k započetí celého procesu určitou konkrétní hodnotu (inicializační vektor IV). Inicializační vektor se má dynamicky měnit, aby nebylo možné získat určité statistiky při opakujících se prvních blocích zpráv.

Pomocí módu **OFB** (Output Feedback mode) lze každou blokovou šifru využít jako zdroj binárního hesla a použít ji jako proudovou šifru.

Feistelova konstrukce blokových šifer je známá koncepce vytváření algoritmů blokových šifer. Horst Feistel pracoval v šedesátých a sedmdesátých letech pro IBM a tato konstrukci byla posléze použita při návrhu DES. V rámci Feistelovy konstrukce je vstupní blok nejprve rozdělen na dva bloky stejné délky. Jeden z těchto bloků je pak zpracován transformací opírající se o aktuální hodnoty klíče a následně je přičten modulo dva k druhému bloku. Pak druhý blok podstoupí analogickou transformaci. Toto je prováděno několikanásobně po sobě (např. pro DES je to šestnáctkrát). Výhodou Feistelovy konstrukce je, že prováděná transformace nemusí být invertibilní a přesto celý algoritmus umožňuje (při znalosti odpovídající hodnoty klíče) zpětnou dešifraci.

S problematikou blokových šifer úzce souvisí tzv. **hashovací funkce**. Vstupem (jednosměrné) hashovací funkce je blok proměnné délky (zpráva) a výstupem je blok pevné délky (obvykle 128 či 160 bitů) – hash. Při dané hodnotě hashe je výpočetně nemožné najít zprávu s tímto hashem, ve skutečnosti na základě znalosti hashe zprávy nemůžeme nic říci o obsahu vlastní zprávy. Pro některé jednosměrné hashovací funkce je výpočetně nemožné najít dvě různé zprávy s touž hodnotou hashe. Hashovací funkce jsou široce používány při vytváření tzv. otisku zprávy (message digest). Tento otisk je důležitý pro vytváření digitálních podpisů. Ale o tom zase až příště.

Slovník kryptologických pojmů:

Symetrická šifra: kryptografický algoritmus, který pro šifrování a dešifrování používá tentýž klíč (oproti tomu při asymetrickém šifrování se používá jiný klíč pro šifrování a jiný klíč pro dešifrování)

Proudová šifra: symetrická šifra zpracovávající otevřený text po jednotlivých prvcích (bitech, bytech)

Bloková šifra: symetrická šifra zpracovávající otevřený text po delších blocích (obvykle v délce 64 či 128 bitů).

Tajný klíč: klíč pro symetrickou šifru (utajovaný)

Délka klíče: počet bitů klíče. Pro symetrickou šifru je za bezpečnou (oproti hrubé síle = ozkoušení všech možných variant klíče) považována minimální délka v rozsahu 90-100 bitů.

S-Box: jeden ze základních stavebnách prvků moderní blokové šifry. V zásadě je to booleovská funkce převádějící binární vektor na jiný binární vektor. Pro kryptografické účely jsou tyto funkce studovány a jsou formulovány takové jejich vlastnosti, které poskytují záruky pro bezpečnost výsledné šifry. Tyto vlastnosti jsou obvykle statistického charakteru (např. tzv. kriterium laviny, anglicky Strict Avalanche Criterion, spočívá v požadavku, že při změně jednoho bitu vstupu do S-boxu se s pravděpodobností jedna polovina změní jednotlivé bity výstupu S-boxu).

Jednosměrná funkce: matematická funkce, kterou v jednom směru (přímém) lze snadno spočítat, zatímco v opačném směru (inverzní zobrazení) probíhají výpočty velmi obtížně.

Hashovací funkce: Vstupem (jednosměrné) hashovací funkce je blok proměnné délky (zpráva) a výstupem je blok pevné délky (obvykle 128 či 160 bitů) – hash.

DES: kryptografický standard. Byl vyvinut firmou IBM v sedmdesátých letech. V roce 1977 se stal americkou vládní normou pro šifrování (certifikován NIST – National Institute of Standards and Technology - naposledy v roce 1993). Široce používán, avšak v současné době ho nelze považovat za perspektivní algoritmus.

IDEA: (International Data Encryption Algorithm) je algoritmus s délkou klíče 128 bitů. Pro svou značnou bezpečnost a vysokou rychlost je považován za vysoce kvalitní algoritmus. IDEA je patentována, majitelem patentu je firma Ascom-Tech.

Blowfish: algoritmus s proměnnou délkou klíče (32 – 448 bitů). Blowfish byl navržen v roce 1993 a opublikován v roce 1994 Bruce Scneierem.

CAST: CAST, navržený autory Carlisle Adams a Stafford Taverns, je moderní algoritmus (bloková šifra s délkou bloku 64 bitů). Jeho design je velmi podobný algoritmu Blowfish, obsahuje S-boxy závislé na klíči, dále neinvertibilní funkci f a má strukturu Feistelovy šifry. CAST je patentován firmou Entrust Technologies, která ho však postoupila pro volné užití.

Skipjack: Jádro kryptografického chipu Clipper. Pomocí klíče v délce 80 bitů je zpracováván blok otevřeného textu o délce 64 bitů. Vyvinut NSA (National Security Agency). Dlouho utajován, na nátlak veřejnosti byl v červnu 1998 zveřejněn. Algoritmus obsahuje určitá zadní vrátka umožňující zpětnou

rekonstrukci klíče. Pro tuto vlastnost (key recovery - možnost zpětného rozkrytí klíče) byl dosti kritizován.

AES: Advanced Encryption Standard - připravovaná norma blokové šifry. Kandidát této normy musí splňovat tyto minimální požadavky:

a) musí podporovat šifrování bloků o velikosti 128 bitů
b) musí podporovat využívaní klíčů v délkách 128, 192 a 256 bitů

V srpnu 1998 budou vyhlášeni přijatí kandidáti (přihlášených je cca jedenáct) – pro další odbornou analýzu.

SHA-1: SHA-1 (Secure hash algoritnm) je hashovací funkce odpovídající normě FIPS PUB 180-1. Vytvoří 160 bitů dlouhý kontrolní hash. Algoritmus byl vyvinut NIST jako součást SHS (Secure Hash Standard).

MD5: Algoritmus MD5 vyvinula společnost RSA Data Scurity Inc. Lze ho použít k vytvoření hashe v délce 128 bitů ze zprávy libovolné délky.

RIPEMD 160: Nejnovějším hashovacím algoritmem je RIPEMD-160, který byl navržen s cílem nahradit MD4 a MD5. Vytváří (jak vyplývá z jeho názvu) hash v délce 160 bitů. Byl vyvinut v rámci evropského projektu RIPE.

Některé zajímavé WWW stránky:

http://csrc.nist.gov/encryption/aes/aes_home.htm
příprava kryptografického standartu (pro blokovou šifru) pro 21.století

http://www.cs.auckland.ac.nz/~pgut001/links.html
Peter Gutmann (jeden z nejlépe zpracovaných přehledů webovských stránek týkajících se kryptologie - možná vůbec nejlepší)

http://www.cs.hut.fi/ssh/crypto
Tatu Ylönen (bohatý zdroj informací z kryptologické problematiky)

http://www.modeemi.cs.tut.fi/~avs/eu-crypto.html
politika, legislativa a technologie - Evropa

http://www.itl.nist.gov/div897/pubs/fip46-2.htm
americký kryptografický standart (DES)

http://www.program.com/source/crypto/blowfish.txt
algoritmus Blowfish

http://zensoft.com/pages/IDEA.html
algoritmus IDEA

http://www.entrust.com/resources/whitepapers.htm
algoritmus CAST

http://www.itl.nist.gov/div897/pubs/fip180-1.htm
hashovací funkce SHA-1

http://www.globecom.net/(sv)/ietf/rfc/rfc1321.shtml
hashovací funkce MD5

http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html
hashovací funkce RIPEMD 160