Základy kryptografie I.
Šifrovat?…..Rozhodně Ano!

Kryptografie dneška

Jaroslav Pinkava

Rozsáhlé využívání výpočetní techniky vede ve svých důsledcích ke stále se zvětšujícímu objemu zpracovávaných a ukládaných informací. Roste objem přenášených elektronických dat, ať již prostřednictvím internetu či jiných přenosových prostředků. Vzrůstá zranitelnost těchto dat. Potenciální narušitelé se mohou dnes k informacím, které posléze zneužijí a přivodí Vám ekonomickou ztrátu, dostat celou řadou způsobů. Citlivé informace je třeba si chránit, to je dnes již samozřejmé. Jaké ale zvolit prostředky? Lze si vybírat z celé škály technických a programových prostředků. Dokonalá ochrana však stojí nemalé peníze. Nákup speciálně chráněné výpočetní techniky, budování separátních přenosových linek, to vše má smysl tehdy, jestliže se nám to samozřejmě vyplatí. Na druhé straně lze kýženého efektu dosáhnout často s vynaložením podstatně menších finančních nákladů. Velice efektivním prostředkem tohoto typu je šifrová ochrana. S její pomocí můžeme přenášet i ta nejcitlivější data prostřednictvím jinak tak málo bezpečného prostředku jako je internet. Data jsou ovšem přenesena v zašifrováné podobě.

Jakým prostředkem ochrany je šifrování, co s jeho pomocí lze zvládnout? Kryptografické prostředky slouží nejen k zakrytí obsahu přenášených informací, ale dokáží i zabezpečit, aby se mnou vyslaná informace dostala k mnou vybranému protějšku a dokonce zajistí, aby pouze on mohl číst tuto informaci. Přitom bude vědět (a nejen vědět - bude to mít zabezpečeno tzv. digitálním podpisem), že odesilatelem jsem byl právě já.

Aby toto vše zajistila, opírá se současná kryptografie o dva základní typy kryptografických algoritmů. Zejména k zabezpečení rychlého utajovaného přenosu většího objemu dat slouží tzv. symetrické šifry. U těchto šifer slouží jeden a tentýž klíč jak k zašifrování dat, tak i k jejich dešifraci. Symetrické šifry jsou dnes v praxi představovány především širokou třídou tzv. blokových šifer. Blokové šifry se jim říká vzhledem k tomu, že tyto algoritmy v zásadě zpracovávají otevřený text po větších blocích, obvykle po 64 bitech. Příklady těchto šifer jsou algoritmy **DES, 3-DES, IDEA, Blowfish, CAST** a celá řada dalších. Softwareová realizace těchto algoritmů zabezpečuje rychlé zašifrování i značně velkého objemu dat.

Druhým základním typem kryptografických algoritmů jsou asymetrické šifry. Také se jim říká šifry s veřejným klíčem. Základní význačnou charakteristikou, která je odlišuje od symetrických šifer, je existence dvou klíčů. Jeden klíč je použit při šifrování dat, druhý je pak použit při jejich dešifraci. Jak vyplývá z logiky věci, chráněný musí být především klíč sloužící k dešifrování dat. Je to také díky tomu, že tyto systémy jsou konstruovány tak, aby ze znalosti jednoho z těchto klíčů (např. šifrovacího) nešlo odvodit podobu klíče druhého (pro dešifrování). Tato vlastnost je nesmírně důležitá a tvoří podstatu bezpečnosti kryptosystémů s veřejným klíčem. Vzhledem k této vlastnosti je také složitější konstruovat takovéto šifrovací algoritmy (první známý algoritmus tohoto typu – **RSA** – byl zkonstruován teprve v roce 1978). Důsledkem toho je mj. skutečnost, že při šifrování jsou tyto algoritmy význačně pomalejší. Jsou proto

využívány s poněkud odlišnými úkoly než klasické symetrické šifry (užíváme je pro distribuci klíčů pro symetrickou šifru, digitální podpisy, autentizaci atd.).

Klíč, který u asymetrických algoritmů slouží k šifrování, může být tedy zveřejněn (většinou také je). Kdokoli může pomocí tohoto klíče šifrovat. Ovšen zpětnou transformaci – převod zašifrovaného textu na text otevřený – je schopen provést pouze vlastník dešifrovacího (tajného) klíče.

Významnými příklady systémů s veřejným klíčem jsou zmíněné RSA, dále v **DSA** (Digital Signature Algorithm – americká norma pro digitální podpis) použité El-Gamalovo schema. Blízkým schematem k RSA je Rabin-Williamsovo schema. Zejména díky možnostem význačně zkrátit nezbytnou délku klíčů jsou v současné době aktuální systémy s veřejným klíčem na bázi eliptických křivek. Pro výměnu klíčů je stále velmi populární rychlé Diffie-Hellmanovo schema.

Při posuzování výběru vhodného kryptografického algoritmu je nezbytné zabývat se kromě základních praktických vlastností (možnost softwareové resp. hardwareové realizace, rychlost této realizace, uživatelské vlastnosti – klíčové hospodářství, existence vhodných navazujících autentizačních protokolů atd.) i klíčovou otázkou bezpečnosti těchto schemat. Tímto je míněna zejména problematika odolnosti těchto schemat proti možným útokům potenciálních narušitelů. I tato problematika souvisí s ekonomickým náhledem na použité prostředky ochrany dat. Např. dnes je již všeobecně známo, že DES (Data Encryption Standard opublikovaný v roce 1977, měl původně sloužit po dobu deseti let) vzhledem ke krátké délce svého klíče (56 bitů) lze potenciálně luštit. Přesto je tento algoritmus široce používán dál. Souvisí to s tím, že právě ekonomické náklady potenciálního narušitele na kryptoanalýzu DES (získání odpovídajícího klíče a posléze dešifrací získání otevřených textů) jsou značně vysoké.

Základní je ovšem snaha používat především bezpečné algoritmy. Pro blokové šifry to znamená:

1) využívat algoritmy, které mají dostatečnou délku klíče. Za tu se dnes považuje délka 90-100 bitů.
2) opírat se o algoritmy konstruované tak, aby byly odolné oproti dalším potenciálním kryptoanalytickým metodám. Význačným představitelem takovýchto postředků jsou diferenciální a lineární kryptoanalýza.

Z těchto hledisek IDEA i Blowfish představují dnes vysoce kvalitní algoritmy.

Odlišně jsou konstruovány systémy s veřejným klíčem. Pro RSA (resp. Rabin-Williamsovo schema) je základem bezpečnosti zhodnocení protivníkových možností faktorizovat velké číslo. Pro schemata, jejichž bezpečnost je založena na úloze diskrétního logaritmu (El-Gamalovo schema, Diffie-Hellmanův systém pro výměnu klíčů) je to zhodnocení protivníkových možností spočítat tento diskrétní logaritmus. Analogicky pro systémy na bázi eliptických křivek to jsou protivníkovy možnosti spočítat eliptický diskrétní logaritmus. Možnosti současné výpočetní techniky proto vedou k odhadům dolní délky parametrů bezpečných kryptosystémů s veřejným klíčem. Pro RSA je uváděná hranice 768-1024 bitů pro číslo n, které je součinem dvou velkých prvočísel. Obdobná hranice je uváděna pro velikost použitého pole v systémech na bázi diskrétního logaritmu. Pro kryptosystémy opírající se o eliptické křivky (vhodně konstruované) je kritickou hodnotou největší prvočíslo v rozkladu řádu použité eliptické křivky. Toto číslo by mělo mít délku minimálně 160-180 bitů.

Kryptografie probíhá v posledních desetiletích neustálým bouřlivým vývojem. Objevují se stále nová kryptoschemata, objevují se ale i nové kryptoanalytické metody. Při volbě prakticky používaného algoritmu je potřebné k tomuto vývoji přihlížet. Je např. vhodné volit algoritmus, který je již relativně delší období posuzován v široké odborné kryptologické veřejnosti. Pro takovýto algoritmus máme pak svým způsobem další záruku jeho kryptologické odolnosti. Na pravidelně probíhajících kryptologických konferencích (mj. každoroční konference CRYPTO, EUROCRYPT) jsou tyto algoritmy předmětem odborných analýz.

Slovník kryptologických pojmů:

kryptografie- zabývá se navrhováním kryptografických algoritmů a způsoby jejich využívání
kryptoanalýza - zabývá se metodami umožňujícími získat ze šifrového textu text otevřený (bez znalosti klíče),
zkoumá odolnost (bezpečnost) a naopak zranitelnost jednotlivých kryptosystémů
kryptologie – vědní disciplína zahrnující kryptografii i kryptoanalýzu
kryptografický algoritmus (také šifrovací algoritmus, kryptosystém, kryptoschema, méně přesně šifra) –
matematický postup, který přetváří otevřený text do takové podoby, kdy původní informace se stává nečitelnou a obráceně, postup , který přetváří šifrový text do podoby otevřeného textu.
klíč – parametr kryptografického algoritmu (obvykle utajovaný), bezpečnost kryptosystému záleží na bezpečnosti (dešifrovacího) klíče
otevřený text – řetězec znaků, který bude šifrován
šifrový text – řetězec znaků, který je výsledkem šifrování
šifrování – použití šifrovacího algoritmu
dešifrování – získání otevřeného textu ze šifrového textu pomocí šifrovacího algoritmu a (dešifrovacího) klíče
bloková šifra – kryptografický algoritmus převádějící otevřený text po blocích (obvykle v délce 64 resp. 128 bitů)
proudová šifra – kryptografický algoritmus, při jehož užití probíhá šifrování po jednotlivých bitech
symetrická šifra – kryptografický algoritmus, který pro šifrování i dešifrování používá tentýž klíč
asymetrická šifra – kryptografický algoritmus, který používá dva odlišné klíče, jeden pro šifrování a jeden pro dešifrování
veřejný klíč – jeden z dvojice klíčů asymetrického šifrovacího algoritmu, obvykle slouží k šifrování a nemusí být utajován
RSA – jeden z prvních (1978) kryptosystémů s veřejným klíčem založený na umocňování v modulární aritmetice
heslo – řetězec znaků (obvykle v délce 8 – 16 bytů) sloužící k ověření uživatelovy identity
hashovací funkce - vytváří ke zprávě jedinečný blok (říká se mu hash či digitální otisk (message digest). Jedinečný proto, neboť je (z výpočetního hlediska) prakticky nemožné nalézt druhou (odlišnou) takovou zprávu, která by měla shodný takový hash..

Některé zajímavé webové stránky:

http://www.io.com/~ritter/GLOSSARY.HTM
rozsáhlý slovník kryptologických pojmů
http://www.iks-jena.de/mitarb/lutz/security/cryptfaq/
odpovědi na časté otázky z kryptologické problematiky (německy)
http://www.netmeg.net/faq/science/cryptography/cryptography-faq/
odpovědi na časté otázky z kryptologické problematiky (anglicky)
http://www.netmeg.net/faq/science/cryptography/rsa/01.html
obdobně
ftp://idea.sec.dsi.unimi.it/pub/security/crypt
algoritmy, programy, dokumenty…
http://www.jya.com/crypto.htm
nejnovější zprávy ze světa, které se týkají kryptologie