MODERNÍ KRYPTOGRAFICKÉ METODY

Labyrint šifer v ráji počítačů

ROZVOJ POČÍTAČŮ, INTERNETU, ELEKTRONICKÉ POŠTY A MOBILNÍCH TELEFONŮ, ALE I NARŮSTAJÍCÍ OCHRANA DAT UVNITŘ ORGANIZACÍ ČI ZAČLEŇOVÁNÍ BEZPEČNOSTNÍCH FUNKCÍ DO OPERAČNÍCH SYSTÉMŮ, TO VŠE PŘINÁŠÍ STÁLE NOVÉ APLIKACE KRYPTOGRAFICKÝCH TECHNIK. VZNIKAJÍ NOVÉ PROTOKOLY A STANDARDY A MNOHDY JEŠTĚ NEZAŽITÉ POJMY JSOU UŽ BRÁNY JAKO SAMOZŘEJMOST. V PRÁVĚ ZAČÍNAJÍCÍM VOLNÉM SERIÁLU SE PROTO BUDEME VĚNOVAT JAK KLÍČOVÝM POJMŮM, TAK NEJPOUŽÍVANĚJŠÍM TECHNIKÁM A STANDARDŮM. ZAMĚŘÍME SE PŘITOM ZEJMÉNA NA MODERNÍ METODY A INTERNETOVOU KRYPTOGRAFII.

Nejprve si osvěžíme základní pojmy a principy z oblasti šifrování. Definice sice budeme uvádět bez nadbytečných formalismů, ale tak, aby bylo rozumět podstatě. Pro zájemce bude k dispozici dost literatury a dalších odkazů na zdroje, kde naleznou přesné matematické formulace, věty a důkazy. Mimochodem, v současné době existuje už několik desítek základních učebnic, příruček a knih, které se zabývají kryptografickými metodami – a přesto co autor, to jiná definice i u zcela základního pojmu. Kryptografie se totiž neustále rozvíjí, a tak dále vznikají nové metody i pojmy, zatímco některé „staré“ se dostávají do nových souvislostí.

NEZAMĚŇUJTE POJMY: KÓDOVÁNÍ JE PŘEVOD INFORMACE SE ZNÁMÝM ZPĚTNÝM POSTUPEM, **PŘI ŠIFROVÁNÍ JE K TOMU ALE POTŘEBA TAJNÝ KLÍČ.**

ALGORITMY A KLÍČE

Šifrovací algoritmus je transformace, která převádí otevřený text (otevřená data, plaintext) na šifrový text (zašifrovaná data, ciphertext) a naopak. Šifrovací algoritmus se tedy skládá ze dvou transformací: zašifrování a odšifrování. Při zašifrování je příslušná transformace řízena (parametrizována) **klíčem pro zašifrování** a při odšifrování pak **klíčem pro odšifrování**. U symetrických šifer jsou tyto klíče odvoditelné jeden z druhého (prakticky vždy jsou oba klíče totožné), zatímco u asymetrických šifer z jednoho klíče nelze zjistit druhý – je to výpočetně neproveditelné.

KÓDOVÁNÍ A ŠIFROVÁNÍ

Šifrování se často zaměňuje s pojmem kódování. Není divu, kódování je také proces převodu informace z jedné formy do druhé. Kódování k tomu ale nepoužívá žádnou utajovanou informaci – proces zakódování a dekódování je zcela veřejný a může ho provést každý; typickým příkladem jsou kódy ASCII, Latin 2 apod. U šifrovacího algoritmu ale vždy existuje „něco tajného“ – i když u asymetrických šifer (viz dále) si můžeme dovolit, aby jeden z klíčů byl veřejný. Ostatně, kdyby nic tajného v šifrovacím algoritmu nebylo, zašifrovat a odšifrovat data by mohl kdokoliv a smysl těchto operací by se zcela vytratil.

Obr. 1. Základní schéma šifrovacího algoritmu

SYMETRICKÉ ŠIFROVACÍ ALGORITMY

Jestliže klíč pro zašifrování je stejný jako klíč pro odšifrování (obecněji: pokud jeden můžeme odvodit z druhého), hovoříme o symetrickém šifrovacím algoritmu. Klasické symetrické algoritmy vidíte v tabulce I.

ASYMETRICKÉ ŠIFROVACÍ ALGORITMY

Jestliže z klíče pro zašifrování nelze odvodit klíč pro odšifrování, nebo naopak (přesněji: je to výpočetně neproveditelné), hovoříme o asymetrickém šifrovacím algoritmu. Tyto algoritmy bývají také nazývány **šifrovací algoritmy s veřejným klíčem**, protože jeden z klíčů je veřejný; ten druhý, k němu párový, se pak jmenuje klíč tajný (privátní, soukromý).

Pro utajení dat se používá klasický model: veřejným klíčem se zašifrovává, tajným klíčem se odšifrovává. Tak funguje zašifrování dat zejména pro přenos – odesílatel zašifruje data, která chce odeslat, veřejným klíčem příjemce. Výhodou je, že tento klíč je skutečně veřejně k dispozici, a tak každý může příjemci poslat něco zašifrovaného, aniž by potřeboval cokoli jiného. Příjemce pak data odšifruje svým tajným klíčem. Kouzlo utajení spočívá v tom, že nikdo jiný operaci od-

šifrování udělat nemůže, protože k tomu by už musel mít příjemcův tajný klíč.
Při podpisu dat naopak signatář při tvorbě podpisu používá svůj tajný klíč (vystupuje ve formě „podpisového“ klíče) a jistým způsobem ho „slučuje“ s podepisovanými daty. Výsledkem je tzv. *digitální podpis*, který může kdokoliv ověřit – použije k tomu veřejný klíč signatáře. Poznamenejme ještě, že v klasickém asymetrickém modelu, jakkoli to na první pohled vypadá podivně, se tajný (podepisovací) klíč používá při podepisování ve spojení s operací odšifrování (přestože při podpisu vlastně nejde o zašifrovaná data) a veřejný klíč (ověřovací) ve spojení s operací zašifrování – tedy stejně jako při šifrování dat.
Později ale vznikly speciální asymetrické **algoritmy pro digitální podpis**, které nepoužívají klasické operace zašifrování a odšifrování, ale operace *podepsání* a *verifikace*. Liší se od předchozích v tom, že pro tyto operace používají různé matematické metody. Zatímco tedy v klasickém případě byla operace zašifrování i odšifrování totožnou matematickou funkcí zpracovávající jednou veřejný a podruhé tajný klíč, v těchto nových algoritmech se používají dvě různé matematické funkce. Výsledkem operace podepsání pak jsou *data*, výsledkem operace ověření je odpověď *ANO/NE*.
Vznikly ještě další algoritmy, přesněji **kryptografické protokoly**, které definují vzájemnou činnost dvou nebo více stran (odtud označení *protokol*) k dosažení nějakého cíle. Využívají technik podobných asymetrickým algoritmům a mají různé účely (viz tab. 2). Nejpoužívanější je protokol umožňující dohodu nebo ustavení společného klíče zúčastněných stran pro přenosy dat přes komunikační kanál – nazýváme ho **algoritmus pro výměnu klíčů**. Protokoly ovšem existují nejen na bázi asymetrických, ale i symetrických šifer.

Kryptologie

Kryptologie je věda, která se zabývá šifrováním v celé šíři. Skládá se z kryptografie, vědy o tvorbě šifer, a z kryptoanalýzy, vědy o jejich luštění. **Kryptografie** kromě symetrických a asymetrických šifrovacích algoritmů studuje kryptografické nástroje, jako jsou generátory náhodných čísel, hašovací funkce, digitální podpisy, kryptografické protokoly apod.
Kryptoanalýza se zabývá nejen přímým luštěním, tj. hledáním klíčů nebo otevřených textů ze šifrových zpráv, ale v poslední době zejména odhalováním teoretických slabin šifer. Cílem je najít metody, které, i když nevedou přímo k otevřenému textu, ukazují, že šifra není tak silná, jak by měla teoreticky být. Takovým výsledkem může být třeba zjištění, že k útoku na šifru hrubou silou není zapotřebí 2^{56} klíčů, ale jen 2^{55} (například vlastnost komplementárnosti u DES), nalezení slabých nebo ekvivalentních klíčů, krátkých cyklů apod.

Blokové a proudové šifry

I když následující informace platí pro symetrické i asymetrické šifry, většinou se pojmy blokové a proudové šifry spojují se symetrickými algoritmy. U asymetrických šifer se totiž vždy implicitně předpokládá, že se jedná o blokovou šifru.

Blokové šifry

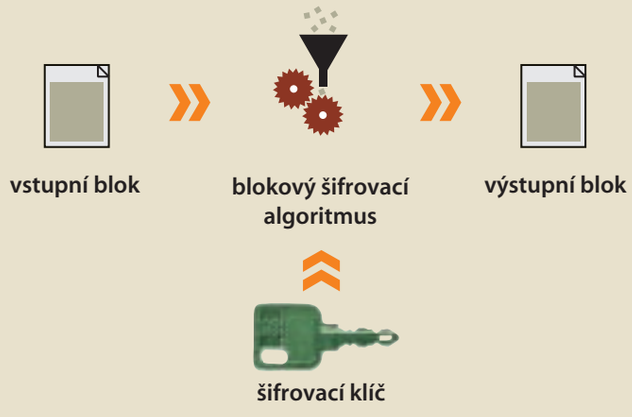
Blokové šifry zpracovávají více znaků otevřeného textu najednou. V současné době je to téměř výhradně blok 64 bitů, zatímco po přijetí standardu AES (viz tab. 1) to bude blok 128 bitů. V základním režimu činnosti bloková šifra zašifruje celý tento blok a vznikne tak stejně dlouhý blok šifrového textu. (Jistě je možné, aby šifrový blok byl delší, ale nepoužívá se to.) Protože se vlastně jedná o jakousi záměnu bloku za blok, nazývá se tento základní režim „elektronická kódová kniha“ *(ECB, Electronic Code Book)*. Vidíte, a už jsme zase u kódování! Jenže v tomto případě je kódová kniha pěkně dlouhá. Má 2^{64} nebo 2^{128} položek typu „otevřený blok – zašifrovaný blok“ a je „vygenerována“ tajným šifrovacím klíčem. Označíme-li šifrovací klíč K, otevřený text OT a šifrový text ŠT, pak zašifrování a odšifrování formálně zapisujeme jako $ŠT = E_K(OT)$ a $OT = D_K(ŠT)$; písmena E a D pocházejí z anglického *encrypt* a *decrypt*. Situaci znázorňuje obrázek 2.

Proudové šifry

Pokud chceme zašifrovat jen několik bitů či bajtů otevřeného textu, nebo v případech, kdy jsou data získávána jako proud bitů a je potřeba je okamžitě šifrovat, používají se proudové šifry. Nejpoužívanější proudové šifrovací algoritmy používají tzv. heslo *(running key, key stream)*, které je s otevřeným textem sloučeno nějakou jednoduchou operací bit po bitu nebo bajt po bajtu (nejčastěji je to operace XOR).

Kvalita šifer

Proudové i blokové šifrovací algoritmy mají tu výhodu, že k šifrování velkých objemů dat nepotřebují nijak dlouhý klíč. Musí ale zajistit, aby bez znalosti tohoto klíče nebylo možné



Obr. 2. Bloková šifra v modu ECB

Infotipy, tentokrát s poděkováním

Všechny citované články z Chipu (viz tabulky 1 a 2) i všechny moje články publikované v Chipu od r. 1992 jsou s laskavým souhlasem redakce k dispozici v elektronické formě. Pod mnemotechnickým označením *časopis-rok-strana(od)-strana(do).ext* je najdete na adrese *www.decros.cz/Security_Division/Crypto_Research/* nebo *ftp://ftp.decros.cz/pub/Archiv/Publications/*.
Chtěl bych touto cestou redakci Chipu také poděkovat za svolení k elektronickému vystavení všech mých článků – ne každý časopis je totiž k takovému kroku ochoten. Články z posledních let lze samozřejmě najít také na pravidelných Chip CD, která obsahují elektronickou formu časopisu.

Obr. 3. Proudová šifra

luštit otevřený text. To na kvalitní šifrovací algoritmy klade vysoké nároky. Například u blokové šifry každý bit šifrového textu musí **složitě** záviset na **každém** bitu šifrovacího klíče a **každém** bitu otevřeného textu; navíc změna jediného z těchto bitů musí vést k nepredikovatelné změně v šifrovém textu apod. Vzhledem k pokrokům v oblasti kryptografie a kryptoanalýzy v posledních 30 letech jsou však už známy osvědčené postupy, jak tvořit kvalitní algoritmy, a hodně jich bylo také navrženo a je používáno. V současné době se proto dříve-

OD DOBRÉ ŠIFRY VYŽADUJEME, ABY **LUŠTITEL** ANI PŘI JEJÍ DOKONALÉ ZNALOSTI NEDOKÁZAL ZE ZAŠIFROVANÉHO TEXTU **ZÍSKAT ŽÁDNOU** UŽITEČNOU INFORMACI.

jší problém výběru kvalitního šifrovacího algoritmu přesouvá spíše k otázce jeho všeobecného používání z důvodu kompatibility, tj. na výběr standardu.

Požadavky na kvalitní šifrovací algoritmus

1. Návrh by měl pocházet od zkušených odborníků (nejlépe od týmu kryptografů a kryptoanalytiků s praktickými zkušenostmi).
2. Známé požadované teoretické kryptografické vlastnosti:
   statistické – vzájemná nekorelovanost otevřeného textu, šifrového textu a klíče, ...
   analytické – konfuze, difuze, úplnost, lavinovitost, ...
3. Odolnost proti všem známým kryptoanalytickým útokům. Předpokládá se, že případný útočník dokonale zná šifrovací algoritmus a jeho cílem je například otevřený text nebo šifrovací klíč.
4. Dostatečně dlouhý klíč.

Zveřejňování šifrovacích algoritmů

Z teoretického hlediska se zásadně uvažuje, že případný útočník šifrovací algoritmus zná. Je to nezbytný předpoklad, protože pokud se útočník na nějaký systém zaměří, s určitými náklady dokáže popis algoritmu vždy získat. Při návrhu algoritmů se proto s tím, že luštitel zná algoritmus, počítá jako se samozřejmostí.

Algoritmus	Používaná délka klíče	Typ šifry	Použití	Zdroj a další informace
AES	128 ,192, 256	bloková	připravovaný všeobecný standard (státní správa USA)	Chip 10/99, str. 40
CAST	40, 80, 128	bloková	státní správa (Kanada)	Chip 6/99, str. 56
DES	56	bloková	státní správa (USA)	Chip 5/93, str. 52
TripleDES	112, 168	bloková	všeobecný standard	Chip 5/93, str. 52
GOST	256	bloková	státní správa (Ruská federace)	Chip, 11/95, str. 170, Chip 12/95, str. 164
RC2	40, 128	bloková	internet	Internet Draft RFC 2268
Skipjack	80	bloková	státní správa (USA)	Chip 1/99, str. 46
RC4	40, 128	proudová	internet	Chip 9/99, str. 42
A5	54, 64	proudová	GSM	Chip 9/98, str. 148, Chip 2/00, str. 38

Tab. 1. Příklady symetrických šifer

V posledních letech se veřejnost algoritmu prosazuje v oblastech, kde jsou šifry široce veřejně používány (např. internetové prohlížeče apod.) – to je určitě správná tendence. Světová kryptografická veřejnost také očekává, že brzo bude možné používat bezpečný šifrovací algoritmus (viz AES) i v komerčních produktech, jako je právě komunikace na internetu nebo bankovní aplikace (což umožní zrušené embargo na vývoz amerického softwaru se silnou kryptografií).
Naproti tomu v uzavřených komunitách, jako jsou ozbrojené síly nebo vnitřní systémy bank a podobně, může být situace jiná. Utajování informací o algoritmech a jiných bezpečnostních opatřeních má za cíl znesnadnit případnému útočníkovi jeho činnost a zabránit útoku všemi možnými prostředky (jaký bankovní sejf banka používá, si také nechává pro sebe...). U ozbrojených sil je tomu podobně – ani zde se nezveřejňuje nic, co není nezbytně nutné. V těchto případech je tedy utajení algoritmu určitě na místě.
Tolik snad jako obecný úvod do problematiky. Nyní už přejdeme ke konkrétním algoritmům a chviličku se zastavíme u těch nejrozšířenějších internetových.

RC2

Algoritmus RC2 byl publikován jako Internet Draft (RFC 2268) v roce 1977. Podobně jako DES a CAST je to 64bitová bloková šifra. Délku klíče lze volit v rozsahu 1 až 128 bajtů, nejčastěji se používá v délce 128 bitů (americké verze) a 40 bitů (exportní verze – doufejme, že už to nebude platit dlouho). Je široce používán na internetu, je například obsažen ve standardech S/MIME ver. 3.0 a SSL 3.1. Algoritmus navrhl R. Rivest pro společnost RSA.

RC4

Algoritmus RC4 je proudová šifra opět z dílny R. Rivesta. RC4 nebyl dodnes oficiálně publikován – přesto je jednou z nejčastějších proudových šifer na internetu. Popis byl zveřejněn neznámým hackerem v roce 1994, který disassembloval jeho kód z jednoho programu. Díky tomu je také algoritmus předmětem veřejných diskusí a výzkumu. Je obsažen v S/MIME ver. 3.0 i SSL ver. 3.0. Vedle DES je nejpoužívanějším algoritmem na internetu. Umožňuje volit délku klíče až 256 bajtů, nejpoužívanější je opět v délce 40 nebo 128 bitů. Je trochu anomální v tom, že nevyužívá tech-

Algoritmus	Popis	Zdroj a další informace
RSA	Rivest-Shamir-Adleman, algoritmus pro výměnu klíčů, digitální podpis, šifrování dat	Chip 4/95, str. 136
D-H	Diffie-Hellman, algoritmus pro výměnu klíčů (resp. ustavení společného klíče)	Chip 2/95, str. 126
DSA	Digital Signature Algorithm, algoritmus pro digitální podpis	Chip 5/99, str. 40
ElGamal	El-Gamalův algoritmus (varianty pro digitální podpis i pro šifrování)	
ECDSA	Algoritmus pro digitální podpis DSA, realizovaný na eliptických křivkách (EC)	

Tab. 2. Příklady asymetrických šifer

niku inicializačního vektoru, a proto se na každou zprávu musí generovat nový náhodný šifrovací klíč. Ten se pak komunikujícímu protějšku musí předat jinou bezpečnou cestou, například prostřednictvím asymetrického systému. O obou technikách si řekneme příště.

TripleDES

TripleDES je zkratka pro algoritmus, který využívá DES (viz tab. 1) jako stavební prvek, a to třikrát za sebou. Vzhledem k tomu zde vystupují tři klíče K1, K2 a K3, které mohou být různé. Nejčastěji se ale používá varianta známá jako „EDE“, a to se dvěma nebo třemi různými klíči. V prvním případě je vztah pro šifrování $ŠT = E_{K1}(D_{K2}(E_{K1}(OT)))$, v druhém případě $ŠT = E_{K3}(D_{K2}(E_{K1}(OT)))$. Přestože šifra DES už byla prolomena, TripleDES je považována (až na drobné teoretické nedostatky, jako je vlastnost komplementárnosti a slabé klíče) za spolehlivou a bezpečnou, i když pomalou šifru. Tam, kde menší rychlost není na závadu, je TripleDES v současné době bezpečným a oficiálním standardem. O tom, že bude ještě nějakou dobu aktuální, svědčí i právě nyní vyvinutý korejský „high-tech“ čip, šifrující rychlostí až 240 Mb/s! Obsahuje dva algoritmy – TripleDES a SEED.

CAST

Algoritmus CAST je velmi populární blokovou šifrou. Byl publikován na internetu jako RFC 2144 v květnu 1997 a jako freeware ho začalo používat mnoho firem ve svých produktech (včetně Microsoftu). Je tzv. Feistelovou šifrou a pracuje v rundách. Používá 40- až 128bitový klíč; při klíči do 80 bitů (včetně) se použije 12 rund, jinak 16 rund. Komerční produkty většinou podporují 80- a 128bitové klíče. V Kanadě byl CAST schválen pro ochranu dat ve státním sektoru až do stupně „vyhrazené“. Je to zcela ojedinělý případ, kdy byl nějaký veřejný algoritmus schválen pro ochranu utajovaných dat (i když nejnižšího stupně). Připomeňme, že algoritmy DES a GOST jsou sice také oficiálními standardy (americkým a ruským), ale pro ochranu pouze „senzitivních“, nikoli utajovaných dat.

Vlastimil Klíma
v.klima@decros.cz