ZÁKLADY ŠIFROVÁNÍ

(Petr Uřičář)

Věda zabývající se šifrováním, tedy utajováním informací, se nazývá kryptografie. Naproti tomu věda, která se zabývá luštěním šifer je kryptoanalýza. Nadřazeným pojmem pro oba dva obory je kryptologie. Šifrujeme tak, aby se útočníkovi nevyplatilo šifru prolomit. Musí platit tato nerovnost: NÁKLADY > ZISK Náklady útočníka na dešifrování by měly být větší než zisk, který by útočník měl v případě úspěšného dešifrování.

ZÁKLADNÍ POJMY

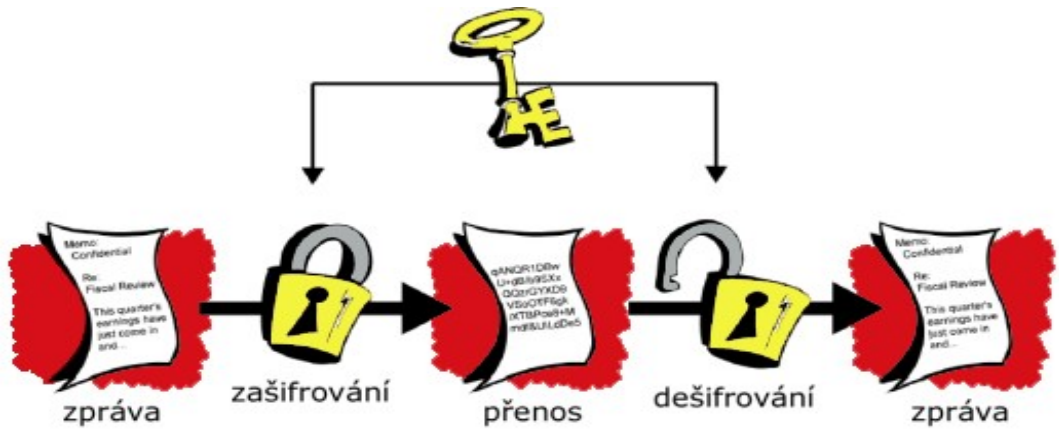
- ŠIFROVACÍ ALGORITMUS – matematická metoda použitá na zakódování či odkódování textu
- ŠIFROVACÍ KLÍČ — říká algoritmu **jak** (de)šifrovat (jakési heslo), vždy dostaneme výsledek – správnost závisí na zadaném klíči
- NEŠIFROVANÝ TEXT – text (nebo cokoli jiného), který chceme zašifrovat
- ŠIFROVANÝ TEXT – text po zašifrování
- SÍLA ŠIFRY – čím silnější šifra, tím větší usílí na její rozluštění – závisí na šifrovacím algoritmu
- DÉLKA KLÍČE — počet bitů, čím větší, tím více možných klíčů (při luštění hrubou silou), přidáním jednoho bitu se počet klíčů zdvojnásobí

DĚLENÍ

- PRVNÍ ROZDĚLENÍ
  - JEDNOSMĚRNÉ - z výsledku nelze získat originál, k ověřování nebo porovnávání (hash, dig. podpis)
  - OBOUSMŠRNÉ - při znalosti správného klíče jsme schopni dešifrovat výsledek a získat tak opět originál
- DRUHĚ ROZDĚLENÍ
  - S PRIVÁTNÍM KLÍČEM (SYMETRICKÉ)
    - BLOKOVÁ - zpracovávají více znaků (blok) otevřeného textu najednou
    - PROUDOVÁ - pokud chceme zašifrovat jen několik bitů otevřeného textu, nebo v případech, kdy jsou data získávána jako proud bitů a je potřeba je okamžitě šifrovat (RC4)
  - S VEŘEJNÝM KLÍČEM (ASYMETRICKÉ)

SYMETRICKÉ ŠIFROVÁNÍ

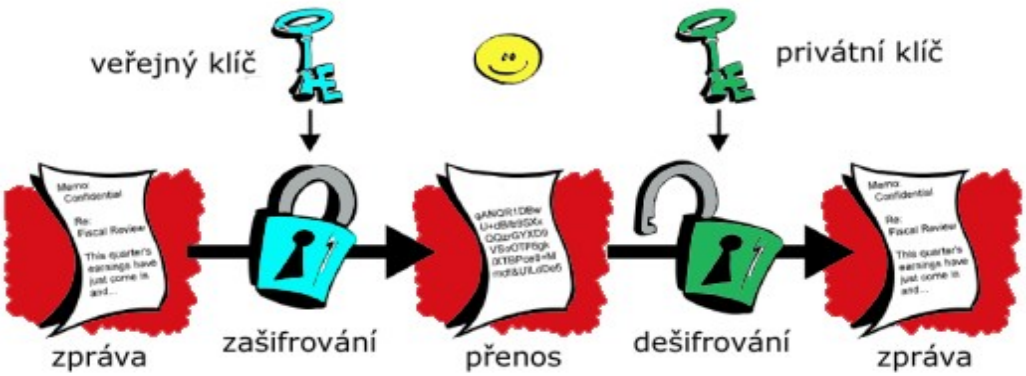
Symetrické (nebo konvenční) šifrování je metoda, při které je text zašifrován s pomocí jistého klíče a může být obnoven jen se znalostí tohoto klíče, což je zároveň jeho největší slabina. Symetrické kódy mají jako hlavní výhodu rychlost algoritmu. Na druhou stranu je nutné aby se příjemce i odesílatel dohodli na jednom klíči, který si musí nějakým bezpečným způsobem vyměnit a který budou znát *pouze* oni dva. Problémem je tedy distribuce klíče - jak dostat klíč k příjemci aniž by se ho chopil někdo nepovolaný? Samotné symetrické šifrování nemůže nikdy problém předání klíče vyřešit.



Kromě problému distribuce klíče má tento typ šifrování další nevýhodu: pokud je účastníků komunikace víc. Pokud chceme mít pro každou dvojici komunikujících stran jiný klíč, potřebujeme pro n účastníků $n(n-1)/2$ klíčů (jestliže je počet komunikujících malý, příliš to nevadí). Symetrické šifrování je mnohem jednodušší než asymetrické šifrování. Jednak nepotřebuje tak výkonné počítače, jednak je jednodušší jeho princip. Vzniklo mnohem dříve.

ASYMETRICKÉ ŠIFROVÁNÍ

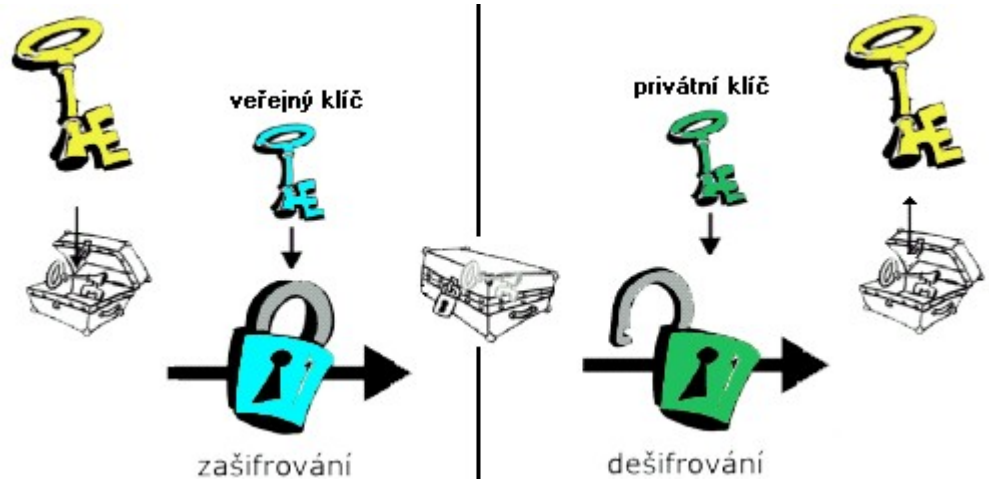
Asymetrické šifrování neboli kryptografie veřejného klíče je metoda vyvinutá Whitfieldem Diffiem a Martinem Hellmanem v roce 1975. Každý účastník komunikace má dva klíče. První z nich je **veřejný** (přístupný všem) a druhý je privátní (soukromý). Cokoli zašifrováno jedním klíčem, lze dešifrovat pouze druhým klíčem a naopak. Velkou výhodou tohoto přístupu je, že jeden z klíčů můžeme dát k dipozici komukoliv (tedy **zveřejnit** ho). Kdokoli nám pak chce napsat zprávu, použije k jejímu zašifrování tento veřejný klíč. Ani on sám, ani žádný jiný vlastník našeho veřejného klíče ji nebude schopen dešifrovat. Toho bude schopen pouze držitel druhého páru - privátního klíče, jímž bychom měli být pouze my. Chceme-li poté adresátovi poslat odpověď, nemůžeme ji zašifrovat svým privátním klíčem, neboť by ji byl schopen dešifrovat kdokoli, ale musíme použít veřejný klíč adresáta. Hlavní výhodou asymetrického šifrování je, že soukromé klíče jsou pouze u jejich majitelů a vně se pohybují pouze veřejné klíče. Asymetrické šifrování má jednu velkou nevýhodu - je velmi náročné na matematické operace, tedy i na výkon počítače.



Odesilatel tedy zašifruje zprávu veřejným klíčem adresáta. Ten přijme zašifrovanou zprávu a dešifruje ji svým privátním klíčem. Protože je jediný, kdo má tento privátní klíč, zprávu nemůže nikdo cizí přečíst. (Při použití jiného klíče, který nepatří ke klíči, kterým se šifrovalo, dostaneme samozřejmě nesmysl). Při komunikaci více účastníků je potřeba celkem *2n klíčů*, tedy počet přímo úměrný počtu účastníků *n.*

HYBRIDNÍ ŠIFROVÁNÍ

Hybridní šifrování je kombinací obou výše zmíněných. Pomalé asymetrické algoritmy se použijí k výměně **symetrického klíče**, který slouží ke kódování další komunikace pomocí symetrických šifer. V praxi se proto používá kombinace symetrického a asymetrického šifrování. Tomuto způsobu se říká *„hybridní šifrování*". Využijeme výhod obou: rychlost symetrického šifrování a *„použitelnost*" asymetrického šifrování.



Odesilatel zvolí symetrický klíč, který zašifruje veřejným klíčem adresáta a pošle mu ho. Adresát tedy dostane asymetricky zašifrovaný symetrický klíč, který dešifruje svým privátním klíčem. Tím zaniká problém distribuce

klíče při symetrickém šifrování a zároveň se celý proces zrychlí. (Asymetrické šifrování je pro dlouhé zprávy pomalé).

HASHOVACÍ FUNKCE

Jednocestá funkce která vytvoří kratší "odraz" původních dat. Tyto nemohou žádným způsobem být navrácena v původní data, pouze lze takto ověřovat pravost dat. Součástí kryptologie jsou tzv. **výtahy zpráv** (message digest) označované jako kryptografické **hash kódy**. Nejvýstižnějším názvem je však **kryptografický kontrolní součet**. Jak jsem se již zmínil, jedná se o jednosměrné algoritmy - z výsledku nejsme schopni obnovit originál.

- ze vstupu proměnné délky vytváří malou hodnotu
- ze stejného vstupu vytváří vždy stejný výstup
- každé výsledné hodnotě by mělo odpovídat více vstupních kombinací
- algoritmus by neměl být snadno odvoditelný či invertovatelný
- malá změna na vstupu má za následek velké změny ve výstupu

Vytvoříme-li nějaký dokument (obecně jakýkoli soubor) a poté si uložíme i jeho výtah, můžeme později zkontrolovat zda aktuální verze našeho souboru nebyla změněna.

PŘÍKLADY ŠIFROVACÍCH ALGORITMŮ

Mezi algoritmy používající pouze privátní klíč patří např. DES a jeho vylepšené verze dvojitý či trojitý DES, IDEA, Skipjack, Blowfish, Twofish, CAST, RC2, RC4, AES a další.

- DES (DATA ENCRYPTION STANDART) - byl vyvinut v IBM v polovině sedmdesátých let. DES kryptuje text po 64-bitových blocích. Přesto, že DES je dobře navrhnutý, jeho klíč je slabý vzhledem k dnešním potřebám a standardům. Proto byl vylepšen a zaveden tzv. Triple-DES. Triple-DES je DES který aplikuje na stejný blok dat 3 klíče. Triple DES je tedy 168-bitový a o něco pomalejší.

- IDEA (INTERNATIONAL DATA ENCRYPTION ALGORITHM) - bloková šifra, vymysleli ji v ETH v Curychu James L. Massey a Xuejia Lai v roce 1990. Původní jméno, pod kterým lze první verze vidět, je IPES - později změněno na nynější IDEA. Bohužel, na rozdíl od DES a CAST, IDEA není volně šiřitelná - je pod patentem.

- CAST - 128-bitová a velmi rychlá šifra. Je volně k použití. Jmenuje se po svých tvůrcích - Carlisle Adams a Stafford Tavares z Northern Telecom (Nortel). CAST je imunní vůči diferenciální i lineární kryptoanalýze. Tyto dvě metody jsou nejsilnější publikované metody. Obě byly úspěšné na DES.

Algoritmy používají veřejný klíč jsou náročné nejen na čas, ale i na vymyšlení, a neexistuje jich proto velké množství. Nejrozšířenější je bezpochyby RSA. Dalším známým je ElGamal. Existuje také algoritmus zvaný DSA, který byl vyvinut pro digitální podpisy, ale lze upravit pro potřeby šifrování. Jako poslední bych zmínil Diffie-Hellman, který je pro změnu zaměřen na výměnu kryptografických klíčů.

- RSA - algoritmus RSA je pojmenován podle počátečních písmen příjmení jeho autorů: Rivest, Shamir a Adleman. Vypracován byl v roce 1977 a je založen na neschopnosti lidského pokolení vymyslet rychlý algoritmus pro rozklad čísla na jeho prvočinitele. Algoritmus RSA je (zatím) velmi bezpečný, jelikož není znám žádný dostatečně rychlý postup na faktorizaci vysokého čísla. Ovšem nelze dokázat, že takovýto algoritmus neexistuje.

Pro vytváření kryptografických kontrolních součtů se používají např: MD2, MD5, SHA, HAVAL, SNEFRU, RIPEMD160 a jiné.

Některé způsoby rozluštění bez znalosti klíče

Rozluštění hrubou silou

Někteří útočníci spoléhají na hrubou sílu. Mechanicky zkoušejí všechny klíče a doufají, že se někdy trefí. V praxi to samozřejmě dělají počítače. Doba, kterou k tomu počítač potřebuje, se zdvojnásobí každým bitem klíče navíc. Délka klíče se tedy volí tak, aby luštění „hrubou silou" trvalo tak dlouho, než zpráva ztratí platnost.

Kryptoanalytika

Když je šifrovací metoda nedokonalá, je často rychlejší pro útočníka zkusit najít nějakou slabinu, periodu atd. Tím se zabývá kryptoanalytika. Kryptoanalytici hledají například něco, co se opakuje, nebo nějakou pravděpodobnost výskytu písmen, kterou pak porovnávají s pravděpodobností výskytu písmen v průměrném textu stejného jazyka.

*Tyto dvě metody používá k rozluštění podezřelých zpráv i CIA. V Americe bylo dlouho omezení na export šifrovacích programů. Délka klíče byla omezená na 56 bitů, aby Americká rozvědka dokázala dešifrovat co nejvíce zpráv.

Lidské selhání

Většina rozluštěných zpráv je však rozluštěna tak, že útočník získá nebo ukradne klíč. Často využije neopatrnosti vlastníka klíče. Jindy útočníkovi pomůže k získání klíče někdo "zevnitř" za finanční odměnu.

Zdroje

- www.strojsnv.sk
- www.pctuning.cz
- bobhy.wz.cz
- www.pgp.cz