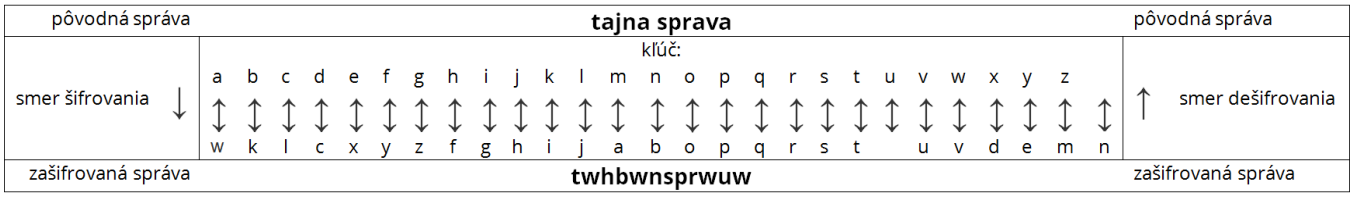
Súčasnosť šifrovania - symetrické a asymetrické šifry, DES, IDEA, RSA, PGP :)

UPOZORNENIE

S počítačmi prišla i nová éra šifrovania. Pôvodne postupy boli vďaka „obmedzenému“ množstvu možnosti zavrhnuté a hľadali sa postupy, ktoré by priniesli tak veľký počet kombinácií, že by ich počítač nedokázal rozlúštiť v reálnom čase. Súčasné šifry možno rozdeliť do dvoch základných kategórií:

Symetrické šifry - predstavujú kategóriu šifier, v ktorých sú šifrovacie kľúče pre šifrovanie a dešifrovanie rovnaké (resp. možno ich navzájom odvodiť). Tieto šifry sa označujú aj ako šifry tajného kľúča a vyžadujú, aby sa príjemca aj odosielateľ vopred dohodli na kľúči, ktorý budú používať a potom ho tajili. Ak sa ten istý kľúč používa dlhšiu dobu, vzniká nebezpečenstvo jeho prezradenia alebo v prípade mnohonásobného používania i dešifrovania (napr. prostredníctvom matematických výpočtov), preto sa kľúče často obmieňajú.

pôvodná správa	**tajna sprava**	pôvodná správa
smer šifrovania ↓	kľúč: Posuň písmená v abecede o 4 znaky	↑ smer dešifrovania
zašifrovaná správa	**xenredwtveze**	zašifrovaná správa



Medzi najjednoduchšie symetrické šifry patria zámeny písmen (substitučné šifry). Šípka smerom dole ukazuje smer šifrovania a šípka smerom hore ukazuje smer dešifrovania.

Asymetrické šifry - sú založené na myšlienke používania dvojice kľúčov – verejného a súkromného. Prostredníctvom jedného z nich sa správa zašifruje (napr. verejný kľúč), prostredníctvom druhého dešifruje (napr. súkromný kľúč). Príjemca správy nemusí poznať kľúč, prostredníctvom ktorého boli údaje zašifrované a odosielateľ nemusí (alebo dokonca nesmie) poznať kľúč, ktorý správu dešifruje. Majiteľ svoj verejný kľúč poskytne všetkým partnerom, s ktorými chce komunikovať a oni správy prostredníctvom neho zašifrujú. Dekódovať takto zašifrovanú správu možno už len prostredníctvom privátneho kľúča, ktorého jediným vlastníkom je prijímateľ správy. Sila tohto typu šifrovania spočíva v tom, že komunikujúci svoje kľúče nemusia poznať a z toho dôvodu ich nemôžu poskytnúť nikomu ďalšiemu.

V minulosti sa šifrovací algoritmus aplikoval na jednotlivé znaky, v súčasnosti pracuje s bitovými blokmi – naraz sa spracuje napr. 64 bitov textu (t.j. 8 znakov). Jednou z prvých šifier, ktorá mala neskôr vplyv na mnohé ďalšie, je symetrická šifra **DES** (*Data encryption standard* – štandard na zašifrovanie dát) prijatá v roku 1977 ako národná norma USA pre šifrovanie. Pôvodne pracovala so 64-bitovými blokmi, ktoré šifrovala pomocou 56-bitového kľúča. Jeho prelomenie je v súčasnosti otázkou krátkeho času, preto sa používajú rôzne kombinácie šifrovacích algoritmov – známy je napr. trojnásobný DES (*Triple DES*), ktorý používa dva DES-kľúče a na údaje trikrát aplikuje algoritmus DES.

Nástupcom DES sa stal algoritmus **IDEA** (*International data encryption algorithm*) publikovaný v roku 1991. Používa 128-bitový kľúč aplikovaný na 64-bitové bloky textu a je založený na používaní viacerých typov algebraických operácií, pričom okrem bezpečnosti predstihuje DES i v rýchlosti. Tento algoritmus je v súčasnosti považovaný za bezpečný.

Asymetrická kryptografia je založená na jednosmerných funkciách, ktorých charakteristickou črtou je rýchly výpočet výsledku a problematický až nemožný opačný postup – pre výsledok získať vstup do funkcie.

Typickým predstaviteľom tejto kategórie je algoritmus **RSA** (podľa iniciál autorov *Rivest*, *Shamir*, *Adleman*), ktorý náhodne generuje dve veľké prvočísla, z ktorých súčinu sa odvodí verejný kľúč. Z neho sa jednoduchou matematickou operáciou vypočíta súkromný kľúč. Súčasné prostriedky IT nie sú schopné získať z tohto súčinu pôvodné prvočísla v dostatočne krátkom čase a podvrhnúť súkromný alebo verejný kľúč.

Ak porovnáme účinnosť kryptovania symetrickou a asymetrickou šifrou, tak symetrická je považovaná za bezpečnejšiu a rýchlejšiu. Napríklad IDEA so 128-bitovým kľúčom je ekvivalentné sile 3000 bitov pri kryptovaní

s algoritmom RSA. Šifrovanie RSA s kľúčom menším než 1024 bitov sa momentálne nepovažuje za bezpečné. V praxi sa najčastejšie používa kombinácia symetrickej a asymetrickej kryptografie.

Za zmienku stojí ešte známy kryptografický systém **PGP** (P*retty good privacy*), ktorý v sebe implementuje asymetricko-symetrické šifrovanie spolu s digitálnymi podpismi a slúži prevažne na ochranu e-mailového systému na Internete.

História a princípy šifrovania - Scytale, Cézarova šifra, šifrovací disk, Vigenerova šifra, Cardanova šifra, Vernamova šifra, kľúč, substitučné a transpozičné šifry ↑

Steganografia ↓

