### Symetrické šifry

Jde o šifry používající stejný šifrovací klíč jak pro zašifrování, tak pro dešifrování. Tato výhoda použití jediného klíče pro všechny úkony se zpracovávanými daty se projevuje i vyšší rychlostí práce počítače při šifrování. Výhoda na jedné straně je ale nevýhodou na straně druhé, neboť v okamžiku prozrazení, jsou vlastně odkryta všechna kdy jím zašifrovaná data. V praxi se symetrické šifry využívají především pro zašifrování zálohovaných dat.

Velmi jednoduchou a známou aplikací symetrického klíče je tzv. *Caesarova šifra.* Její princip spočívá v tom, že je provedeno abecední posunutí po písmenech a klíčem je číslo, které určuje právě toto posunutí.

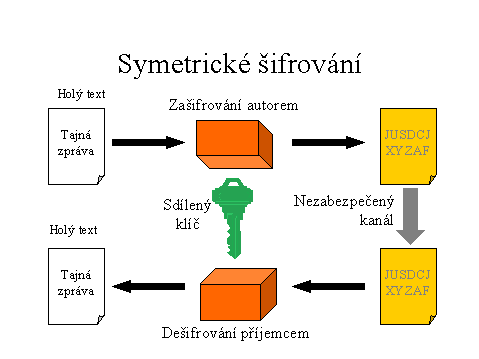
**Příklad :**

Klíč = 3

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Tedy AHOJ = DKRM



**Symetrické šifry můžeme rozdělit na:**

***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).

***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 264). 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.

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.

**Použitá literatura:**

HÁK, Igor. *Moderní počítačové viry* [online]. [cit. 2013-02-03]. Dostupné z: <http://www.cmsps.cz/~marlib/bezpecnost/viry/velka_kniha_o_virech.pdf>

PINKAVA, Jaroslav. Základy kryptografie I. [online]. [cit. 2013-02-03]. Dostupné z: <http://crypto-world.info/pinkava/uvod/bulletin1.pdf>

PINKAVA, Jaroslav. Základy kryptografie II. [online]. [cit. 2013-02-03]. Dostupné z: <http://crypto-world.info/pinkava/uvod/bulletin2.pdf>