Kryptografie

Michal Fuksa, Jana Zajíčková, Michal Žák

Úvod

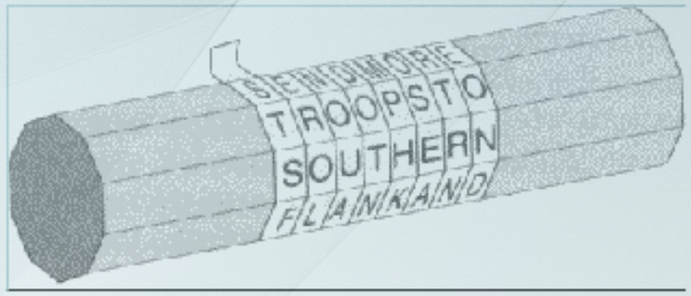
- *Kryptografie* = věda zabývající se šifrováním
- *Historie*

  - Starověký Řím, šifra posunem znaků v abecedě použitá Caesarem

  - znatelnější rozvoj zaznamenala ve 20. století během a po druhé světové válce

- *Nejznámější mechanismy:* Enigma, RSA, MD5, Vernamova šifra

Enigma



Naše výsledky

- *Teorie šifrovacích algoritmů* – lineární, afinní, maticové šifrování
- Konstrukce programu v jazyce C++ bežícího v terminálu windows

Maticové šifrování

Námi použitá šifrovací metoda

Princip

- Před šifrováním se znaky převedou na pole čísel (a => 0, ..., z => 25)
- Kódování textu po dvojicích čísel (jako vektor) za pomoci násobení maticí ***A*** o rozměrech 2x2
- Pokud nelze vytvořit inverzní matici k ***A***, uživatel je požádán o zadání jiné
- Při lichém počtu znaků je řetězec doplněn náhodným znakem kvůli nutnosti dvojic
- Zpětné dešifrování se provede násobením kódovaného textu inverzní maticí $\boldsymbol{A}^{-1}$ matice ***A***

Příklad

- Vstupní text: FEYNMANN
- Po převedení na dvojice čísel: (5 4) (24 13) (12 0) (13 13)
- Po přenásobení maticí $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$: (13 4) (23 16) (12 9) (12 10)
- Kódovaný text: NEXQMJMK
- Poznámka: všechny operace jsou prováděny modulo 27

Hlavní výhodou maticového kódování je vyšší odolnost proti frekvenční analýze četnosti znaků.

Asymetrické šifrování

Šifry s dvěma nezávislými klíči pro šifrování a dešifrování

Příklad - RSA

- Využívá dvou klíčů – veřejného a osobního. Osobní klíč se skádá z dvou velmi velkých prvočísel a veřejný klíč je jejich součinem.
- K zašifrování se využívá veřejný klíč, k rozšifrování osobní klíč.

- Zvolí se dvě různá, velká náhodná prvočísla *p* a *q*.
- Spočítá se jejich součin $n = pq$. Zpětně vypočíst prvočísla je velmi časově náročné.
- Hodnota Eulerovy funkce $\varphi(n) = (p - 1)(q - 1)$.
- Zvolí se náhodně $e < \varphi(n)$, tak aby *e* bylo s $\varphi(n)$ nesoudělné
- Vypočte se *d*: $de \equiv 1 \pmod{\varphi(n)}$.
- Pokud je *e* prvočíslo, tak $d = (1+r*\varphi(n))/e$, kde $r = (e-1)\varphi(n)^{(e-2)}$
- Šifrování pomocí rovnice $c = m^e \bmod n$
- Dešifrování zprávy podle rovnice $m = c^d \bmod n$.

Reference

[1] Rivest, R. – Shamir, A. – Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21 (1978), pp. 120–126.

[2] Extended Euclidean Algorithm http://en.wikipedia.org/wiki/Extended_Euclidean_algorithm

[3] Koblitz, N. A Course in Number Theory and Cryptography, Springer, 1994, pp.235.

Děkujeme za zhlédnutí posteru.