Šifrování tajných zpráv

P. Pompe, Gymnázium Jeseník, patrik.pompe@gmail.com
J. Veselý, Gymnázium Nad Kavalírkou Praha
M. Macko, Gymnázium Vídeňská Brno
O. Perutka, SPŠ Uherské Hradiště

Abstrakt:

Kryptografie jako věda zabývající se šifrováním a následným dešifrováním zpráv využívá různé matematické postupy. Uvádíme příklady funkcí jednotlivých metod a podrobně jsme zkoumali šifrování pomocí matic. Součástí naší práce je i jednoduchý program využívající této metody.

1 Úvod

Šifrování tajných zpráv – kryptografie, slouží ke změně zprávy tak, aby ji nepovolaná osoba nemohla přečíst. Historie šifrovaní je snad stejně stará jako historie posílání vojenských a milostných zpráv. Na jedné straně ji využíval Caesar při komunikaci se svými jednotkami a na straně druhé se zmínky o šifrování objevují i v kamasutře [2]. V dnešní době neustále vzrůstají požadavky na bezpečný přenos dat, především v oblasti internetu, bankovnictví a v armádě.

Cílem naší práce bylo vyzkoušet si některé základní metody kryptografie a využít je při tvorbě programu na šifrování a dešifrování zpráv.

2 Metody kryptografie

Prvním krokem většiny kryptografických metod je převedení zprávy do podoby posloupnosti čísel. Např. máme-li zprávu zapsanou velkými písmeny a bez mezer, můžeme použít následující mapování znaků: A → 0, B → 1, …, Z → 25**.**

Číselnou reprezentaci zprávy dále modifikujeme pomocí matematické funkce, která je závislá na tzv. klíči (parametr funkce). Podle klíče lze kryptografii rozdělit na:

- **Symetrickou**
- **Asymetrickou**

U symetrické kryptografie je využíván stejný klíč pro zakódovaní i dekódování zprávy, je tedy nutné, aby ho znal příjemce i odesilatel zprávy. Před odesláním zprávy si jej musí nějak bezpečně předat. Její výhodou je nižší výpočetní náročnost, a proto je využívána zejména při šifrování velkého objemu dat. Příkladem symetrické kryptografie je metoda posuvné a afinní transformace. Při afinní metodě je číselná reprezentace zprávy modifikována pomocí funkce:

$$f(x) = ax + b \bmod N,$$

kde a, b jsou celočíselné parametry transformace (klíč), N počet znaků abecedy a funkce mod (modulo) zabraňuje přetečení mimo obor hodnot. Posuvná metoda je zvláštní variantou metody afinní, kdy $a = 1$.

V současnosti jsou při menším objemu dat používány metody asymetrické, které využívají dvou odlišných klíčů. Příjemce bez obav sdělí svůj veřejný klíč odesilateli, který pomocí něj zprávu zašifruje. Příjemce je schopen zprávu rozluštit jen pomocí klíče soukromého, který drží v tajnosti. Základem těchto metod jsou tzv. trapdoor funkce. To jsou algoritmicky rychle vyčíslitelné funkce, u kterých navíc požadujeme, aby nalezení inverzního zobrazení (které se používá při dekódování) bylo – bez nějaké dodatečné informace (soukromý klíč) – co nejsložitější. Trapdoor funkce využívají např. jednoduchého součinu velkých prvočísel a jeho následného složitého rozkladu, bodů na eliptických křivkách, či násobení v konečných (velkých) Abelovských grupách.

3 Použití kódovacích matic

My jsme při tvorbě kryptografického programu použili metodu kódovacích matic. Zprávu jsme rozdělili na dvojice znaků, které představují dvojrozměrné vektory. Následně jsme tyto vektory násobili kódovací maticí $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix} \bmod N\,.$$

Aby byla zachována bijektivnost (jednoznačnost) transformace, musí být největší společný dělitel determinantu matice $\det A = ad - bc$ a N roven jedné [2, Tvrzení III.2.1].

Dekódování probíhá pomocí inverzní matice

$$\begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix},$$

kde $D = \det A$ a D^{-1} je inverzní prvek k D mod N, tzn. $DD^{-1} = 1 \bmod N$. Inverzní prvek D^{-1} se hledá pomocí rozšířeného Euklidova algoritmu [3].

Vstupem našeho programu je řetězec obsahující malá písmena a mezery, šifrovací matice. Výstupem je zašifrovaný řetězec. Náš program umožňuje samozřejmě i převod opačným směrem.

4 Závěr

```
l lg ghpeqmynskxgrcvzjleg yp hivnuz
nhvuvcypnahetkehjuuyqieghejgvyukxs bc
rcuytvhvrxnpfbyprctktqdig lkxzjtkvcoedpmxfbardpnssknhnsyp
hl kxaoxugeukdxhdbwtkvciszcpgzcjfpzl
fveqlrpztkgitsvydpnslkjcbhohg gyqmmf
```

$$\begin{pmatrix} 5 & 7 \\ 2 & 17 \end{pmatrix}$$

Poděkování

Děkujeme FJFI ČVUT za organizaci fyzikálního týdne, jmenovitě našemu supervizorovi Ing. Petrovi Ambrožovi, PhD za uvedení do problematiky a ochotnou pomoc při vypracování projektu a Ing. Vojtěchu Svobodovi, CSc. za obětavou organizaci

Reference:

[1] HTTP://CS.WIKIPEDIA.ORG/WIKI/KRYPTOGRAFIE, 19.6.2007

[2] KOBLITZ, N.: *A Course in Number Theory and Cryptography,* Springer, 1994

[3] HTTP://EN.WIKIPEDIA.ORG/WIKI/EXTENDED_EUCLIDEAN_ALGORITHM, 19.6.2007