Teorie čísel a šifrování

J. Zajíčková, M. Žák, M. Fuksa
Gymn. Fr. Palackého, Gymn. L. Pika, Gymn. Litoměřická,
janaave@centrum.cz, mick321@gmail.com, michal.fuksa@gmail.com

Abstrakt

Cílem našeho projektu bylo seznámení se s vědou, která se zabývá různými metodami šifrování a dešifrování zpráv za využití různých matematických postupů – kryptologií. Součástí projektu je i program, který jsme vytvořili pro demonstraci vybrané metody – kódování pomocí matic.

1 Úvod

Kryptologii lze rozdělit na dvě složky: Kryptografii, jejímž cílem je změnit zprávu před odesláním do takové míry, aby ji dokázal rozluštit pouze příjemce, a ne žádná nepovolaná osoba, které by se mohla dostat do rukou. Druhou složkou je kryptoanalýza. Cílem kryptoanalýzy je dešifrování zakódovaných zpráv.

V průběhu dějin došlo k podstatnému zdokonalení kryptografických metod. Od Caesarovy šifry (ta v sobě zkombinovala substituční šifru a lineární transformaci), k asymetrickým šifrám (například algoritmu RSA) vedla dlouhá cesta.

2 Typy šifer

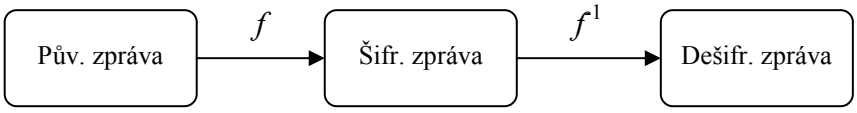
K úspěšnému zašifrování a předání zprávy od odesilatele k adresátovi je zapotřebí dvou klíčů. Prvním z nich je klíč šifrovací, který slouží odesilateli k převodu původní zprávy na zprávu zakódovanou a druhým z nich je dešifrovací klíč, který slouží adresátovi k převodu zakódované zprávy na původní. Na základě „vztahu“ těchto dvou klíčů se dělí kryptografické metody na symetrické a asymetrické. U symetrické šifry jsme ze znalosti šifrovacího klíče schopni zjistit klíč dešifrovací a naopak. U asymetrické šifry tomu tak není. Oba dva klíče jsou na sobě nezávislé a ze znalosti šifrovacího klíče je velmi obtížné a velmi časově náročné zjištění klíče dešifrovacího.

Asymetrické šifry

Nejznámější asymetrickou šifrou je tzv. RSA algoritmus [1]. U tohoto jde v zásadě o to, že ke zjištění součinu dvou (prvo)čísel je zapotřebí nepoměrně kratší doby, než k rozkladu jednoho čísla na součin prvočísel. Uživatel využívající tohoto algoritmu si tedy zvolí dvě prvočísla, která mezi sebou vynásobí. K zašifrování zprávy stačí znalost součinu, zatímco k jejímu dešifrování je potřebná znalost jednotlivých prvočísel. Šifrovací klíč tedy může být veřejně přístupný a díky tomuto se řadí algoritmus RSA mezi tzv. šifry s veřejným klíčem.

Symetrické šifry

Výhodou symetrických šifer oproti asymetrickým je jejich nižší výpočetní náročnost, a proto se nyní budeme věnovat právě jim.



Obr. 1: Šifrovací schéma

Jak už bylo řečeno v úvodu, k šifrování i dešifrování zpráv se využívá matematických postupů (funkce f a f^{-1}, viz obr. 1). Pokud tedy chceme nějaké kódování používat, musíme jednotky (typicky písmena, nebo dvojice písmen) původní i zakódované zprávy zapsat pomocí nějakých matematických objektů.

Nejsnazší, a pro naše potřeby zcela dostačující, je použít množinu celých čísel. Za předpokladu, že původní i kódovaná zpráva je tvořena znaky A–Z a že zvolenou jednotkou je jeden znak, můžeme písmenu A přiřadit číslo 0, písmenu B číslo 1, …, písmenu Z číslo 25. Teprve v tomto okamžiku můžeme začít kódovat.

Nejjednodušší formou šifrování pomocí symetrických šifer je tzv. **lineární transformace**. V tomto případě ke každému z čísel, které jsme přiradili jednotlivým písmenům, přičteme nějakou konstantu. Jediná komplikace nastává, pokud výsledné číslo přesáhne počet jednotek dané abecedy. Toto řešíme pomocí operace 'modulo N', tj. funkce, která danému číslu přiřadí zbytek po celočíselném dělení číslem N.

Tento algoritmus poté zapisujeme funkcí:

$$f(d)=d+a \mod N,$$

kde d je číslo, které reprezentuje jednotku původní zprávy, N je počet jednotek zprávy a a je konstanta, kterou přičítáme.

Ovšem dešifrování této šifry je poměrně jednoduché. Pokud jsou ve zprávě použita pouze písmena A–Z, máme vlastně pouze 26 možných šifer, k dešifrování tedy stačí vyzkoušet 26 posunů a vybrat ten, jehož výsledkem je smysluplné sdělení. Možná ještě rychlejší metodou dešifrování (obzvláště v případě dlouhých textů) je využití tzv. frekvenční analýzy. U této dešifrovací metody jde o to, že některá písmena se v daném jazyce používají častěji než jiná. Pokud tedy zjistíme, jaké číslo se v kódované zprávě vyskytuje nejčastěji, jsme mu s velkou pravděpodobností schopni správně přiřadit písmeno. Po dosazení do rovnice funkce jsme schopni vypočítat parametr a.

Jisté ztížení pro kryptoanalytika představuje **transformace afinní**. Jde vlastně o přidání jednoho parametru do algoritmu funkce. Výsledný algoritmus pak vypadá nějak takto:

$$f(d) = a \cdot d + b \mod N^2,$$

kde d je číslo, které nám označuje jednotku původní zprávy, N je počet jednotek zprávy a a, b jsou konstanty.

Ovšem i toto je velmi snadno dešifrovatelné pomocí frekvenční analýzy. Jediný rozdíl oproti předchozímu případu je ten, že potřebujeme přiřadit písmena dvěma číslům s nejčastějším výskytem a parametry a a b pak zjistíme vyřešením soustavy dvou rovnic o dvou neznámých.

Další možností je použít **jiné kódování písmen**. Jako jednotky původní zprávy si nezvolíme jednotlivá písmena, ale třeba dvojice písmen. Každé dvojici přiřadíme číslo podle vztahu

$$(X,Y) \rightarrow N \cdot x + y \mod N^2$$

kde X,Y jsou jednotlivá písmena, x, y jsou hodnoty přiřazené jednotlivým písmenům a N je počet znaků v abecedě.

Pro dvojice je i tato metoda celkem snadno dešifrovatelná pomocí frekvenční analýzy.

3 Kódování využité v našem programu

Asi nejspolehlivější metodou je **kódování pomocí matic**. Předpokládejme, že máme *N* písmennou abecedu a jako jednotky chceme použít dvojice znaků. Jednotku budeme reprezentovat celočíselným vektorem $\vec{d} = \begin{pmatrix} x \\ y \end{pmatrix}$, kde *x* je číselná hodnota jednoho znaku a *y* druhého znaku.

Nyní si musíme zvolit kódovací matici

$$\mathrm{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{kde } a,b,c,d \in {}^{Z}\!/_{N \cdot Z}$$

Pozn.: ${}^{Z}\!/_{N \cdot Z}$ je množina všech možných zbytků při dělení celých čísel číslem *N*.

Algoritmus pro zakódování vypadá takto:

$$\mathrm{f(d)} = \mathrm{A} \cdot \mathrm{d} = \begin{pmatrix} \mathrm{a} \cdot \mathrm{x} + b \cdot y \\ c \cdot x + d \cdot y \end{pmatrix}.$$

K zakódování zprávy tímto způsobem využíváme 4 parametry a případnému kryptoanalytikovi značně ztížíme použití frekvenční analýzy.

Pro zpětné dešifrování potřebujeme znát *inverzní matici* A^{-1}. Tj. matici, pro kterou platí:

$$A^{-1} \cdot A = I ,$$

kde $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ je tzv. jednotková matice.

Vynásobením zakódovaného vektoru $\begin{pmatrix} x' \\ y' \end{pmatrix}$ inverzní maticí získáme původní vektor a tím i původní zprávu:

$$A \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix} \quad \Rightarrow \quad \begin{pmatrix} x \\ y \end{pmatrix} = I \cdot \begin{pmatrix} x \\ y \end{pmatrix} = A^{-1} \cdot A \cdot \begin{pmatrix} x \\ y \end{pmatrix} = A^{-1} \cdot \begin{pmatrix} x' \\ y' \end{pmatrix}$$

Inverzní matice ale neexistuje ke každé matici. Podmínkou pro existenci inverzní matice je, že determinant matice $D = a \cdot d - b \cdot c$ a počet znaků abecedy *N* jsou nesoudělná čísla. Za splnění této podmínky pak pro inverzní matici platí

$$A^{-1} = \begin{pmatrix} D^{-1} \cdot d & -D^{-1} \cdot b \\ -D^{-1} \cdot c & D^{-1} \cdot a \end{pmatrix}.$$

Ověření nesoudělnosti čísel *D* a *N* provádíme pomocí Euklidova algoritmu [2]. Euklidův algoritmus se uplatňuje hlavně u zjišťování největšího společného dělitele velkých čísel, protože jeho použití je rychlejší než použití prvočíselného rozkladu.

Postupem opačným k Euklidovu algoritmu získáme vyjádření největšího společného dělitele pomocí celočíselné kombinace původních čísel *D* a *N*:

$$nsd(D,N) = r \cdot D + s \cdot N , \quad \text{kde } r,s \in Z .$$

Jak najít D^{-1}: D^{-1} je prvek množiny ${}^{Z}\!/_{N \cdot Z}$, který splňuje podmínku

$$D^{-1} \cdot D = 1 \mod N \qquad (1)$$

Z Euklidova algoritmu máme

$$nsd(D,N) = 1 = r \cdot D + s \cdot N \quad / \mod N$$

$$1 \mod N = r \cdot D \mod N + s \cdot N \mod N$$

$$1 = r \cdot D \mod N + 0 \qquad (2)$$

Porovnáním vztahů (1) a (2) zjišťujeme, že platí:

$$D^{-1} = r\,.$$

Za znalosti tohoto jsme již schopni získat původní zprávu:

1. Dosadíme za D^{-1} do inverzní matice A^{-1}.
2. Vynásobíme zakódovaný vektor inverzní maticí, čímž získáme původní vektor a tím i původní zprávu.

4 Náš program

V našem programu jsme použili metodu šifrování pomocí čtyřprvkové matice. Nejprve je uživatel požádán o zadání libovolného textu skládajícího se z písmen anglické abecedy a mezer, který je následně kryptován čtyřprvkovým klíčem, který si uživatel sám zvolí. Řetězec je poté zašifrován a uložen do souboru. Dešifrovací program funguje opačnou cestou. Zašifrovaný text je načten, dešifrován a zobrazen. Program běží v konsolovém prostředí systému Windows.

Vstup: „TOTO BUDE ZASIFROVANO“ [1 2 3 4] „UFUFBB SCIZVHFMCCS ZEW“

Poděkování

Zde bychom chtěli poděkovat předně ČVUT a Fakultě jaderné a fyzikálně inženýrské za to, že umožnili a finančně podpořili Fyzikální týden, díky němuž tento článek vůbec mohl vniknout. Dále bychom chtěli poděkovat Ing. Svobodovi, CSc. za organizaci této akce, ale především našemu supervizorovi Ing. Petru Ambrožovi, Ph.D., bez jehož pomoci by tato práce určitě nevznikla.

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.