Šifrování

Ondřej Maslikiewicz[1], Ondřej Hujňák[2], Jiří Stejskal[3]

[1]Střední průmyslová škola Hronov, Hostovského 910 Hronov
[2]Gymnázium Slovanské nám. 7, Brno
[3]Gymnazium Děčín, Komenského náměstí

[1]o.maslik@seznam.cz, [2]Hujnak.Ondrej@seznam.cz,
[3]Georgesamuel@seznam.cz

Abstrakt:

Jaký vliv mají šifry a šifrování na historii lidstva? Jaký vliv mají na život každého z nás? Můžeme se sami s nějakými šiframi setkat? Pro každého z nás je dobré vědět, co se jak děje a proč tomu tak je. To platí i o šifrování. V miniprojektu jsme si definovali základní matematické pojmy nezbytné pro práci s šiframi. Na několika jednoduchých historických šifrách jsme si vyzkoušeli luštění, šifrování i dešifrování textu. Dále jsme vytvořili šifrovací programy v programovacím jazyce Pascal, a to pro Caesarovu šifru a pro afinní šifru. Programy jsou odolné proti mezerám a speciálním znakům. Nakonec jsme se také dozvěděli něco málo o asymetrickém šifrování, které se dnes a denně používá.

Šifry a šifrování (neboli kryptografie) jako takové má vliv na lidské dějiny už více než 2000 let. Šifry vždy měly a budou mít velký vliv na výsledky válečných konfliktů, politická rozhodnutí a historii lidstva vůbec. Každý z nás šifry používá, aniž by si to uvědomoval. Takovým příkladem je internetové bankovnictví, elektronický podpis, internetové obchody a v neposlední řadě emailová komunikace. Smysl šifrování je v utajování informací před třetí stranou a v našich životech hraje stále větší a větší roli.

Než jsme se dostali k vlastnímu šifrování, bylo nutné vymezit si několik pojmů a definic. První z nich je kryptologie. Kryptologie je věda, zabývající se šiframi a šifrováním. Šifrování je proces zabezpečení zprávy nebo sdělení, při kterém se z otevřeného textu (nezašifrovaná informace) stává kryptogram (zašifrovaná informace). Způsob, kterým provádíme šifrování nazýváme šifrovací algoritmus (šifrovací systém) za pomocí tzv. šifrovacího klíče. Příjemce kryptogramu potom používá dešifrovací algoritmus a dešifrovací klíč. Šifrovací algoritmus je takový, že po zašifrování je možné kryptogram jednoznačně dešifrovat. Kryptologii můžeme rozdělit na dvě části. A to kryptografii, což je věda zabývající se vytvářením šifer, a kryptoanalýzu, která se zabývá prolamováním šifer (neboli zjišťováním otevřeného textu bez předchozí znalosti dešifrovacího klíče nebo algoritmu). V případě, že klíč známe, šifru neprolamujeme (neluštíme), nýbrž dešifrujeme (dešifrování patří ke kryptografii). Prolomení šifry nastane v případě, kdy je znám způsob, jak zjistit dešifrovací klíč. Jsou tři tzv. nejhorší možné podmínky , a to když kryptoanalytik

třetí strany:

1. má detailní poznatky o šifrovacím systému (zvýšené nebezpečí nalezení mezery v šifrování umožňující odhalení klíče)
2. získá velké množství kryptogramu šifrovaného jedním algoritmem a klíčem (lze uplatnit metody umožňující odhalení klíče, např. frekvenční analýzu)
3. má k dispozici části otevřeného textu a jeho kryptogramu

Rozlišujeme dva druhy šifrovacích systémů, a to symetrické, které mají šifrovací klíč ze kterého se dá odvodit klíč dešifrovací. Oproti tomu asymetrické mají dva různé klíče a klíč šifrovací neumožní zprávu dešifrovat, ani zjistit klíč dešifrovací a naopak.
Symetrické šifrování dále dělíme podle způsobu šifrování na substituční, kde dochází k záměně znaků, a transpoziční, kde dochází k záměně umístění znaků v textu. Pro bezpečnost šifry je důležité dobré utajení klíčů. Dokonalé utajení je pak takové utajení, kdy jediné možné zjištění otevřeného textu třetí stranou je prosté uhodnutí jejího obsahu. Pro dokonalé utajení je nutné, aby kryptogram nepříteli neposkytl žádnou informaci.

Nejdříve jsme se věnovali substitučním symetrickým šifrám. Jedna z nich je například šifra monoalfabetická, jejíž speciálním případem je i jedna z nejjednodušších šifer, a to je šifra Caesarova.
Caesarova šifra je založena na posunu písmen abecedy. Klíčem je číslo tři, což značí počet míst o které se otevřený text posune dopředu. Například písmeno **a** se šifruje jako písmeno **d**. Tento způsob šifrování můžeme použít pro libovolný celočíselný klíč. V případě, že posunutý text přesáhne počet písmen abecedy, odečteme celkový počet čísel abecedy od vzniklé hodnoty tolikrát, aby mělo písmeno ekvivalent ve zvolené abecedě. Tato šifra je velice náchylná na prolomení, protože může obsahovat pouze tolik klíčů, kolik je písmen v abecedě.
O něco lepší je náhodná záměna písmen. V tomto případě už ale klíč není jedno celé číslo, ale celá abeceda v náhodném pořadí.

Dalším typem je šifra afinní. Afinní šifra je založena na modulární aritmetice. Je podobná předchozímu typu šifry, ale klíčem jsou dva parametry – a, b – díky kterým je možné šifrovaný text vypočítat podle vzorce:

$$C_i = (a \cdot T_i + b) \bmod m$$

Kde „C_i“ je písmeno kryptogramu, „a“ a „b“ jsou nesoudělné parametry, „T_i“ je písmeno otevřeného textu a „m“ je počet písmen abecedy. Protože se jedná o šifru symetrickou, k jejímu dešifrování stačí vyjádřit ze vzorce „T_i“.
Můžeme šifrovat i za pomoci čísel. Příkladem je Polybiův čtverec standardně o rozměrech 5x5. Protože má anglická abeceda znaků 26, píší se I a J do jednoho políčka. Písmeno je určeno dvěma souřadnicemi, záleží na domluvě která je první.
Playfairova šifra je čtverec stejný jako v předchozím případě, ale písmena nejdou popořadě. Začínáme klíčem, který tvoří slovo dávající smysl ve kterém vynecháme duplicitní písmena a až poté doplníme zbylé znaky podle abecedy. Nešifruje se znak, ale bigram (dvojice znaků). V případě že se jedná o stejné znaky, vložíme mezi ně písmeno Z. Šifrovaný text vytváříme podle tří pravidel, kdy záleží, kde se nachází písmena bigramu ve čtverci:

1. nachází-li se v řádku, posuneme je o jedno doprava
2. nachází-li se ve sloupci, posuneme je o jedno dolů
3. pokud nesplňují ani jedno z výše uvedených pravidel, posuneme první písmeno bigramu dolů až na řádek, na kterém se nachází druhé písmeno a druhé písmeno posuneme analogicky nahoru.

Všechny výše zmíněné šifry jsou náchylné ke kryptoanalytické metodě – frekvenční analýze. Ta umožňuje podle frekvence výskytu znaků v kryptogramu a frekvence četnosti znaků v abecedě daného jazyka otevřeného textu odhadnout klíč a tím šifru prolomit.
Homofonní šifra se tento nešvar snaží ošetřit znáhodňujícími prvky. Písmenům, která se v textu vyskytují často, či těsně vedle sebe, přiřadí více hodnot. Naroste tím sice velikost klíče právě o počet znáhodňujících prvků, ale frekvenční analýza je neúčinná.

Kromě monoalfabetických šifer, můžeme použít také šifry polyalfabetické. Tyto šifry se snaží o vyhlazený histogram použitých znaků a tím znemožnění frekvenční analýzy. Písmeno kryptogramu neodpovídá vždy právě jednomu písmenu otevřeného textu a zároveň dva stejné znaky otevřeného textu neodpovídají vždy jednomu znaku kryptogramu. Z tohoto typu šifer jmenujme Vigenèrovu šifru, která používá tzv. Vinegèrův čtverec. Vinegérův čtverec má rozměry počtu písmen abecedy a vyrobíme ho tak, že zapíšeme abecedu do prvního sloupce i řádku a doplníme do čtverce posunutím abecedy podle prvního řádku. Klíčem je libovolné slovo, ve kterém se neopakují písmena (nebo opakující se písmena vynecháme). Šifrujeme tak, že napíšeme zprávu na řádek a na řádek pod ni opakovaně zapisujeme klíč tak dlouho, dokud zpráva neskončí. Šifrujeme vždy dvojice písmen ve sloupci (zpráva, klíč). Ve Vinegèrově čtverci vyhledáme znak zprávy v prvním řádku a odpovídající znak klíče v prvním sloupci. Šifrované písmeno je to, u kterého se protne řádek a sloupec, který začíná písmenem ze zprávy.
Druhou skupinou jsou šifry transpoziční. U těchto šifer písmena nenahrazujeme, nýbrž přemisťujeme. Pro transpoziční šifry je klíčem celé číslo **k**, které udává počet sloupců tabulky, do kterých otevřený text naskládáme a to tak, že prvních **k** znaků tvoří první řádek tabulky, druhých **k** znaků tvoří druhý řádek, atd. Když délka otevřeného textu není dělitelná **k**, doplníme volná místa v tabulce písmenem z. Výslednou šifru pak zapisujeme po sloupcích místo po řádcích.
Aby se snížila pravděpodobnost prolomení šifry, používá se superšifrování. Superšifrování je zřeťezení alespoň dvou šifrovacích algoritmů.

Hlavní bod našeho miniprojektu je vytvoření šifrovacího a dešifrovacího programu. Jako šifrovací systém jsme si vybrali Caesarovu šifru a Afinní šifru. Program jsme napsali v programovacím jazyce Pascal.

Dále jsme krátce zabrousili do asymetrického šifrování. Vzhledem k vyšší složitosti těchto šifer je nutné znovu ujasnit si pár pojmů. U asymetrických klíčů se používají vysoká prvočísla a modulární aritmetika. Další častý prvek je tzv. jepičí klíč, jenž je použit jen a pouze jedenkrát a poté je zničen. Mezi nejpoužívanější algoritmy patří RSA a El-Gamal algoritmus s veřejným klíčem, kde se počítá s diskrétním logaritmem. Výhodou asymetrického šifrování je, že není nezbytně nutná důvěra mezi komunikujícími stranami, což posunulo kryptografii dále ve vývoji kupředu.

Shrnutí

Šifry a šifrování mají velký vliv na historii celého lidstva a na život každého z nás. Se šiframi se setkáváme každý den, aniž bychom o tom věděli. V miniprojektu jsme se dozvěděli mnohé o jednoduchých historických šifrách. Na několika příkladech jsme si vyzkoušeli jak asi kryptoanalytikové přemýšlejí, jaké chyby dělají a jaké náhody mohou vést k úspěšnému vyluštění. Dále jsme si zkusili šifrovat a dešifrovat známé historické šifry a naprogramovat šifrovací a dešifrovací program k některým z nich, konkrétně pro Caesarovu a afinní šifru.

Poděkování

Děkujeme Bc. Janě Hradilové za přiblížení problematiky kryptologie a cennou pomoc při porozumění šifrám a zpracování tohoto výstupního příspěvku. Dále děkujeme Ing. Svobodovi, CSc. za organizaci akce Týden vědy.

Reference:

[1] Piper, F. - Murphy, S.: *Kryptografie* Dokořán, 2006, 7-87.

[2] Janeček, J.: *Rozluštěná tajemství* XYZ, 2008