Šifrování

J. Fejtek[1], M. Jelínek[2], J. Kapr[3], J. Štula[4]
[1]Gymnázium, Dukelská 1, Bruntál
[2]Gymnázium Sokolov
[3]Gymnázium Plasy
[4]Gymnázium a SOŠPg Jeronýmova, Liberec

[1]jan.fejtek@gmail.com
[2]jelinek.mi@gmail.com
[3]kapr.jiri@seznam.cz
[4]stula.jakub@seznam.cz

Abstrakt:
Většina z nás už určitě slyšela o šifrování. Může se zdát, že šifrování bylo aktuální v minulých letech a dnes už je součástí historie. Opak je pravdou. Šifry, kódy a hesla nás obklopují na každém kroku. Našim cílem bylo seznámit se s historií šifrování až po současnost. V naší práci se postupně zabýváme šiframi, jako jsou caesarova šifra, afinní šifra, jednoduchá substituční šifra, playfairova šifra, transpoziční šifra a další. Některé šifry jsou náchylné na útok hrubou silou, jiné jsou odolné vůči frekvenční analýze. S principem asymetrického šifrování se hranice této disciplíny posouvají dále k moderním technologiím a vývoj nových, odolnějších algoritmů je tak hnán kupředu. Díky znalostem základních šifer se nám podařilo vytvořit vlastní jednoduchý šifrovací a dešifrovací program v jazyce Pascal a C++. Programy šifrují pomocí caesarovy a afinní šifry.

1 Úvod

Někomu se může zdát, že se ho šifrování netýká. Stačí se ale rozhlédnout a zamyslet se. Internetová pošta, peněžní služby, vojenství. To je jen malý výčet oblastí, kde se šifry a šifrování užívají každý den. Čí zásluhou a proč šifry vůbec vznikly? Války, obchodní tajemství a tajné dopisy milenkám, to byly důvody pro utajení už před několika staletími. Historie lidstva je protkaná tajnými zprávami. My jsme se naučili, jak s těmito šiframi zacházet. Ať už se jedná o jednoduchou caesarovu šifru nebo o transpoziční šifry. Díky získaným znalostem jsme vytvořili zdařilé šifrovací a dešifrovací programy na základě caesarovy a afinní šifry.

2 Zasvěcení do kryptologie

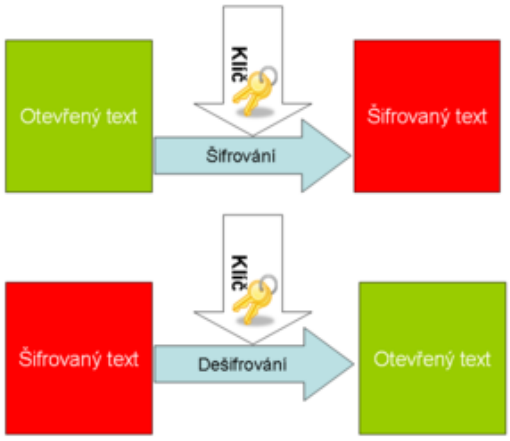
Kryptografie společně s kryptoanalýzou tvoří společnou vědu kryptologii. Kryptografie se zabývá šifrováním a dešifrováním, kdy známe klíč. Kdežto kryptoanalýza se snaží o prolomení šifry a získání otevřeného textu.

Pro začátek si vymezíme několik základních pojmů z šifrování:

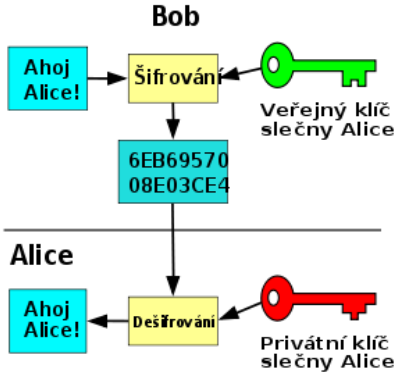
- Otevřený text (OT) – původní zpráva, kterou chceme zašifrovat
- Šifrovaný text (ŠT) – zpráva, která je zašifrovaná
- Šifrování – proces utajení zprávy
- Šifrový algoritmus (šifra) – soubor pravidel pro šifrování a dešifrování
- Šifrovací a dešifrovací klíč – slouží ke správnému užití šifry
- Prolomení šifry – zjištění šifrového algoritmu a klíče

Druhy šifer

- Symetrické – dešifrovací klíč se dá odvodit od šifrovacího, účastníci si musí důvěřovat
- Asymetrické – odesílatel šifruje zprávu podle veřejného klíče, příjemce zprávu podle osobního tajného klíče dešifruje, nemusí si důvěřovat
- Substituční – nahrazení písmen jinými písmeny nebo znaky
- Transpoziční – zaměňuje pořadí znaků podle daného systému



Obr. 1 – Užití klíče, symetrické šifrování



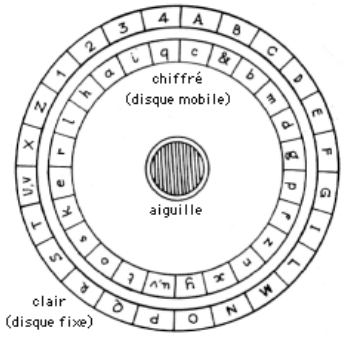
Obr. 2 – Asymetrické šifrování

Šifry napříč historií

Caesarova šifra

Je to symetrická šifra založená na substituční metodě. Každému písmenu z abecedy je podle klíče přiřazeno písmeno jiné. Klíč je celé číslo, které udává posunutí znaku v abecedě. Př. Klič = 3, pak A = D

Pomůckou k šifrování jsou dva otočné kruhy každý se stejným počtem znaků.



Obr. 3 – Pomůcka k šifrování

Afinní šifra

Pro afinní šifru platí vztah: $C_i = aT_i + b \pmod m$ pro šifrovací klíč

$T_i = (C_i - b)\, a^{-1}$ pro dešifrovací klíč

platí: $(a \cdot a^{-1}) = 1 \pmod{26}$

C_i – písmeno ŠT, T_i – písmeno OT, m – počet znaků použité abecedy, a – parametr tak, aby největší společný dělitel čísla m, a byl 1, b – libovolný parametr

Př. Písmenům abecedy přiřadíme číslice 0,1,2,3,…,25, OT – ahoj, b = 9, m = 26, a = 5, $a^{-1} = 21$. Ahoj = 0 7 14 9

$C_1 = 5 \cdot 0 + 9 = 9 \rightarrow$ J

$C_2 = 5 \cdot 7 + 9 = 44 \bmod 26 \rightarrow 1 \cdot 26 + 18 = 18 \rightarrow$ S

$C_3 = 5 \cdot 14 + 9 = 79 \bmod 26 \rightarrow 3 \cdot 26 + 1 = 1 \rightarrow$ B

$C_4 = 5 \cdot 9 + 9 = 54 \bmod 26 \rightarrow 2 \cdot 26 + 2 = 2 \rightarrow$ C

Jednoduchá substituční šifra (monoalfabetická)

K abecedě si zvolíme náhodné pořadí písmen, to nám dává 26! možností uspořádání abecedy. Pro lepší orientaci zvolíme klíčové slovo př. TYDEN VEDY NA JADERCE, žádné písmeno se nesmí opakovat → TYDENVAJRC + doplníme abecedou v normálním pořadí → TYDENVAJRCBFGHIK…Z.

Polybiův čtverec

Písmena se vypíší do tabulky 5x5 a šifra je jejich souřadnicovým zápisem. (I a J jsou v jednom políčku.

Playfairova šifra

Pracujeme se čtvercem 5x5. Písmena zapíšeme v náhodném pořadí. OT rozdělíme po dvojicích, když se nacházejí v 1 sloupci - posun o 1 dolů, když se nacházejí v 1 řádku - posun o 1 vpravo, když jsou v různých řádcích a sloupcích, doplníme na obdélník a zaměníme za rohová písmena.

Homofonní šifra

Pro písmena abecedy, která se v daném jazyce vyskytují nejčastěji (A,E,N,O,R,T), volíme dva znaky. Znaky jsou čísla.

Polyalfabetická šifra

Písmenu z OT může náležet 1, 2 i více znaků z ŠT, a naopak jednomu písmenu z ŠT můžeme najít 1, 2 i více znaků z OT.

Uvedli jsme si několik možností jednoduchého šifrování. Pro větší zabezpečení zprávy můžeme užít kombinaci různých šifer, to se nazývá superšifrování.

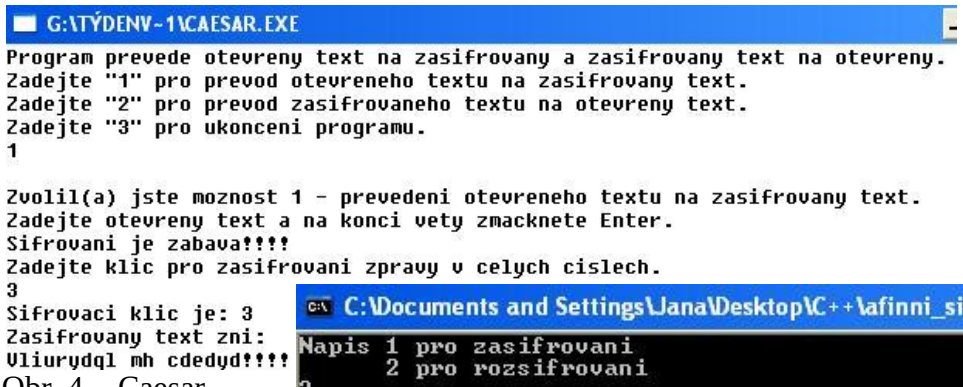
Jedna z metod prolomování šifer se nazývá frekvenční metoda. Využívá četnosti znaků v jazyce. Z výše uvedených šifer jsou proti této metodě odolné homofonní a polyalfabetická šifra.

Moderní kryptografie

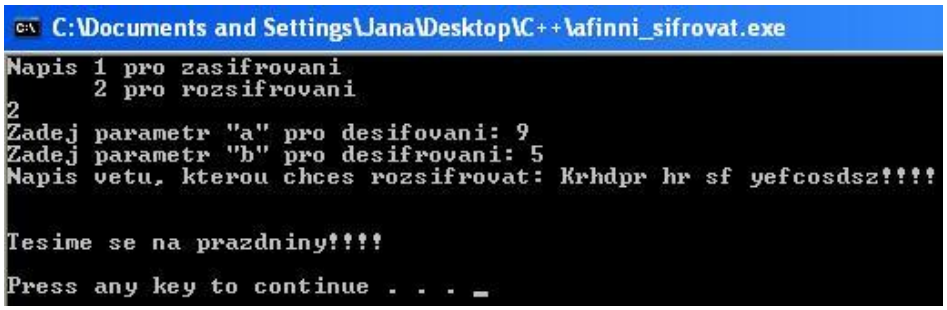
Používá se především v elektronice při přenosu a zabezpečení dat. Je postavena na binárním zápisu čísel a využívá asymetrického šifrování. Nejznámějším užitím asymetrického šifrování je RSA algoritmus, který využívá obrovská prvočísla.

Šifrovací programy

Cílem naší práce bylo vytvořit šifrovací a dešifrovací program v programovacím jazyce Pascal a C++. V jazyce Pascal jsme vytvořili program Caesar, který je založený na principu caesarovy šifry. V jazyce C++ jsme vytvořili program, který využívá principu afinní šifry.



Obr. 4. - Caesar



Obr. 5 – Afinní_šifrování

3 Shrnutí

V dnešní době plné elektrotechnických vymožeností jsou šifry a šifrování nepostradatelnou součástí systému. Napříč staletími byly klíčem k úspěchu a i dnes a v budoucnu se bez nich moderní člověk neobejde. Na vlastní kůži jsme poznali složitou práci šifrantů a luštitelů, kde i malá chyba hraje velkou roli. Výsledkem naší práce jsou správně fungující šifrovací a dešifrovací programy.

Poděkování

Velké poděkování patří Bc. Janě Hradilové za zasvěcení do problematiky kryptologie a za pomoc při Týdnu vědy 2011. Dále chceme poděkovat FJFI a celému realizačnímu týmu za velice povedenou akci, zvláště pak Ing. V. Svobodovi, Csc.

Reference:

[1] PŘIBIL, J. – KODL, J.: *Ochrana dat v informatice*, Vydavatelství ČVUT, 1997

[2] PIPER, F. – MURPHY, S.: *Kryptografie*, Dokořán, s. r. o., 2006

[3] JANEČEK, J.: *Rozluštěná tajemství*, Nakladatelství XYZ, 2008

http://friedo.szm.com/hist1.html, [cit. 15. 6. 2010]

http://cs.wikipedia.org/wiki/Symetrick%C3%A1_kryptografie, [cit. 15. 6. 2010]

http://cs.wikipedia.org/wiki/Asymetrick%C3%A1_kryptografie, [cit. 15. 6. 2010]