TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta přírodovědně-humanitní
a pedagogická

SBÍRKA ÚLOH K ŠIFROVÁNÍ

Diplomová práce

Studijní program: N1101 – Matematika
Studijní obory: 7504T077 – Učitelství informatiky pro střední školy
7504T089 – Učitelství matematiky pro střední školy

Autor práce: **Bc. Hana Vacatová**
Vedoucí práce: doc. RNDr. Miroslav Koucký, CSc.

Liberec 2014

TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta přírodovědně-humanitní a pedagogická
Akademický rok: **2012/2013**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Hana Říhová**
Osobní číslo:	**P12000913**
Studijní program:	**N1101 Matematika**
Studijní obory:	**Učitelství matematiky pro střední školy**
	Učitelství informatiky pro střední školy
Název tématu:	**Sbírka úloh k šifrování**
Zadávající katedra:	**Katedra aplikované matematiky**

Zásady pro vypracování:

1. Seznámit se se základy kryptografie (terminologie, klasifikace metod, specifika užití), včetně jejich historického vývoje.
2. Nastudovat teoretické základy vybraných šifrovacích metod.
3. Sestavit sbírku příkladů vybraných (po konzultaci s vedoucím DP) šifrovacích metod. Cílovou skupinu budou tvořit žáci ZŠ a SŠ (možnost zatraktivnění výuky matematiky a prezentace užitečnosti matematiky).
4. Doporučená struktura sbírky – každá kapitola bude prezentovat jednu zvolenou šifrovací metodu. Jednotlivé kapitoly budou obsahovat stručnou historickou poznámku, teoretický úvod, alespoň jeden příklad se vzorovým řešením a alespoň deset neřešených příkladů (s výsledky).

Rozsah grafických prací: **dle potřeby**

Rozsah pracovní zprávy: **cca 70 stran**

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

- **Mollin, R. An Introduction to Cryptography. Boca Raton: Chapman & Hall/CRC, 2007. ISBN 1-58488-618-8.**
- **Menezes, A., Oorschot, P., Vanstone, S. Handbook of Applied Cryptography. London: CRC Press, 2011. ISBN 0-8493-8523-7.**
- **Hankerson, D., Hoffman, D. Coding Theory and cryptography: The Essentials. New York: Marcel Dekker, 1991. ISBN 0-8247-0465-7.**
- **Singh, S. Kniha kódů a šifer. Praha: Dokořán, 2003. ISBN 80-86569-18-7.**

Vedoucí diplomové práce: **doc. RNDr. Miroslav Koucký, CSc.**
Katedra aplikované matematiky

Datum zadání diplomové práce: **15. února 2013**

Termín odevzdání diplomové práce: **20. prosince 2013**

doc. RNDr. Miroslav Brzezina, CSc.
děkan

L.S.

doc. RNDr. Miroslav Koucký, CSc.
vedoucí katedry

V Liberci dne 15. února 2013

Prohlášení

Byla jsem seznámena s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé diplomové práce pro vnitřní potřebu TUL.

Užiji-li diplomovou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědoma povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Diplomovou práci jsem vypracovala samostatně s použitím uvedené literatury a na základě konzultací s vedoucím mé diplomové práce a konzultantem.

Současně čestně prohlašuji, že tištěná verze práce se shoduje s elektronickou verzí, vloženou do IS STAG.

Datum:

Podpis:

Poděkování

Na tomto místě bych chtěla poděkovat doc. RNDr. Miroslavu Kouckému, CSc. za obrovskou trpělivost a pomoc při tvorbě této diplomové práce. Také bych chtěla poděkovat svému manželovi, který mne v průběhu psaní této práce podporoval.

Anotace

Předmětem diplomové práce je vytvoření sbírky šifrovacích úloh včetně jejich ukázkových příkladů. Práce též obsahuje objasnění základních pojmů z teorie dělitelnosti a základní pojmy z kryptografie.

Klíčová slova: teorie dělitelnosti, permutace, modulární aritmetika, kryptografie, kryptoanalýza.

Annotation

The main task of this diploma thesis is creation of set of encryption tasks, including prime examples. This work also includes explanation of essential terms in divisibility theory and essential terms in cryptography.

Key words: divisibility theory, permutation, modular arithmetic, cryptography, cryptoanalysis.

Obsah

Seznam tabulek

Seznam použitých zkratek

$\mathbb{N}$	… množina přirozených čísla
$\mathbb{Z}$	… množina celých čísla
$\mathbb{R}$	… množina reálných čísla
$\forall x$	… pro všechna x platí …
$\exists x$	… existuje x, pro které platí …
$\exists ! x$	… existuje právě jedno x, pro které platí …
$x \in A$	… x je prvkem množiny A
$x \wedge y$	... konjunkce (logická spojka „a“)
$x \rightarrow y$	… implikace („jestliže x, pak y“)
$x \mid y$	… x dělí y (beze zbytku)
$x \nmid y$	… x nedělí y
$NSD(a, b)$	... největší společný dělitel čísel a, b
$NSN(a, b)$	... nejmenší společný násobek čísel a, b
$a \equiv b \pmod{m}$	... a je kongruentní s b modulo m
$a = b \pmod{m}$	... a je zbytek po dělení modulo m
Z_m	… úplná soustava zbytků modulo m
Z_m^*	… redukovaná soustava zbytků modulo m

1. Úvod

Ve své diplomové práci se budu zabývat šifrováním, kteréžto téma mne při studiu na Technické univerzitě v Liberci zaujalo. Jelikož šifrování velmi úzce souvisí s mými aprobačními předměty – matematikou a informatikou – zaměřím se ve své práci na využitelnost šifrování v hodinách matematiky a informatiky ve smyslu zpestření a zatraktivnění výuky.

Cílem mé diplomové práce je proto vytvoření sbírky příkladů na téma šifrování. Cílovou skupinou této sbírky jsou žáci základních i středních škol, v závislosti na matematické náročnosti jednotlivých typů šifer.

V úvodu této práce bude nastíněno matematické pozadí jednotlivých šifer a budou zde vysvětleny základní pojmy v šifrování. Dále pak se v úvodu budu zabývat rozdělením typů šifer.

Jednotlivé kapitoly diplomové práce budou následně obsahovat vybrané šifry. Tyto šifry budou vysvětleny za pomocí vzorových příkladů a posléze bude přiloženo několik příkladů i s výsledky.

V závěru práce poté poukáži na využití moderních šifrovacích metod v současnosti, včetně jejich praktického využití v běžném životě.

2. Matematický úvod

Tato kapitola obsahuje základní přehled vybraných partii z diskrétní matematiky, které se využívají v kryptografii.

Základy teorie dělitelnosti

V této kapitole budeme převážně pracovat v oboru celých čísel (dále označovaných $\mathbb{Z}$), která tvoří algebraickou strukturu nazývanou eukleidovský obor integrity. Množina $\mathbb{Z}$ je uzavřená vzhledem k operaci sčítání (tj. součet celých čísel je opět celé číslo), existuje nulový prvek a ke každému prvku existuje prvek opačný (tedy je uzavřená i vzhledem k odčítání a tvoří abelovu grupu). Dále platí, že množina $\mathbb{Z}$ je uzavřená vzhledem k operaci násobení, která je asociativní, komutativní, existuje jednotkový prvek, ale není uzavřená vzhledem k inverzi (tedy vzhledem k dělení a tvoří komutativní monoid). V následující části se budeme zabývat právě vlastnostmi dělení v oboru $\mathbb{Z}$.

Definice: Buď $a \in \mathbb{Z}, b \in \mathbb{Z} - \{0\}$, řekneme, že b dělí a (píšeme $b|a$), jestliže

$$\exists q \in \mathbb{Z} \quad a = b \cdot q.$$

Poznámky

- Neexistuje-li $q \in \mathbb{Z}$ takové, že $a = b \cdot q.$ říkáme, že b nedělí $a.$ Značíme $b \nmid a$.
- Číslo q z výše uvedené definice nazýváme podílem, číslo a násobkem čísla $b.$ Číslo b dělitelem čísla $a.$ V další části textu budeme uvažovat jako dělitele vždy pouze kladná přirozená čísla.
- Každé nenulové celé číslo různé od ± 1 má alespoň dva dělitele – čísla 1 a absolutní hodnotu sama sebe. Tyto dělitele označujeme jako nevlastní dělitele, zbývající jako vlastní dělitele.

Základní vlastnosti relace „býti dělitelem“ (|) popisují následující tvrzení:

Tvrzení 2.1

1. $\forall a \in \mathbb{Z}$ platí $1|a$
2. $\forall a \in \mathbb{Z} - \{0\}$ platí $a|a$
3. $\forall a, b \in \mathbb{Z} - \{0\}, c \in \mathbb{Z}$ platí $a|b, b|c \Rightarrow a|c$
4. $\forall a \in \mathbb{Z} - \{0\}$ platí $a|0$
5. $\forall a, b, c \in \mathbb{Z}$ platí $a+b=c, d|a, d|c \Rightarrow d|b$

V obecném případě, popisuje vztah mezi čísly *a* a *b* věta o dělení se zbytkem:

Platí:

Pro každé $a \in \mathbb{Z}, b \in N^+$ existují jediná $q, r \in \mathbb{Z}$ taková, že platí

$$a = b \cdot q + r \quad \text{, kde} \quad 0 \leq r < b.$$

Poznámky

Věta o dělení se zbytkem nachází široké využití. Uplatňuje se například při převodech čísel z desítkové soustavy do soustavy o základu *b*.

V soustavě o základu *b* vyjadřujeme přirozená čísla následovně:

$$(a_n a_{n-1} \ldots a_1 a_0)_b = a_0 + a_1 \cdot b + \ldots + a_n \cdot b^n$$

kde $a_i \in \{0, \ldots b-1\}, n \in N, b \in N, b > 1$.

Při převodu z desítkové soustavy do soustavy o základu *b* získáme hledané cifry $a_0, a_1 \ldots a_n$ jako zbytky při opakovaném dělení základem *b*.

Pro názornost si uvedeme příklad převodu čísla 201 z desítkové soustavy do soustavy osmičkové:

$$\begin{aligned} 201 &= 8 \cdot 25 + 1 \\ 25 &= 8 \cdot 3 + 1 \\ 3 &= 8 \cdot 0 + 3 \end{aligned}$$

Dostáváme tak $(201)_{10} = (311)_8$.

Společný dělitel

Definice: Nenulové přirozené číslo *d* nazveme společným dělitelem nenulových celých čísel *a, b*, jestliže

$$d|a \wedge d|b, \quad \text{tj. } d \text{ dělí obě čísla.}$$

Největší společný dělitel

Definice: Největším společným dělitelem nenulových celých čísel *a*, *b.* nazveme takového jejich společného dělitele, který je ze všech společných dělitelů největší. Značíme ho $NSD(a,b)$.

Poznámky

- Označme $d_{a,b}$ množinu všech společných dělitelů nenulových čísel *a*, *b*. Zřejmě platí

$$d_{a,b} \neq \emptyset \wedge \forall d \in d_{a,b}\ 1 \leq d \leq min\{a,b\}.$$

Odtud vyplývá, že největší společný dělitel nenulových čísel existuje vždy a je určen jednoznačně (neboť množina $d_{a,b}$ je neprázdná a shora omezená).

- Největšího společného dělitele lze nalézt metodou „hrubé síly“. Postupným testováním všech čísel od minima $\{a,b\}$ k jedné. První takové číslo, které bude dělit obě čísla bezezbytku, je největší společný dělitel.
- Jestliže $NSD(a,b)=1$, potom nazýváme čísla *a*, *b* nesoudělná.

Základní vlastnosti největšího společného dělitele popisuje následující tvrzení:

Tvrzení 2.2

Nechť $a,b \in \mathbb{N}^+$ potom platí:

1. $NSD(a,b)=NSD(b,a)=NSD(\pm a,\pm b)$
2. $b|a \Rightarrow NSD(a,b)=b$
3. $k \in \mathbb{N}^+,\ NSD(k\cdot a, k\cdot b)=k\cdot NSD(a,b)$
4. $d|a,\ d|b \Rightarrow NSD\left(\frac{a}{d},\frac{b}{d}\right)=\frac{NSD(a,b)}{d}$

5. $d|a, d|b \Rightarrow d|NSD(a,b)$

6. $a = a_1 \cdot NSD(a,b); b = b_1 \cdot NSD(a,b), NSD(a_1, b_1) = 1$

Přirozenou otázkou je, jak největšího společného dělitele najít. Způsobů existuje více (již uvedená metoda hrubé síly), my si ukážeme tzv. Euklidův algoritmus, který využívá větu o dělení se zbytkem.

Euklidův algoritmus

Nechť $a, b \in \mathbb{N}^+$ potom lze Euklidův algoritmus popsat následovně:

$$a = b \cdot q_0 + r_1 \qquad 0 < r_1 < b$$

$$b = r_1 \cdot q_1 + r_2 \qquad 0 < r_2 < r_1$$

.
.
.

$$r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_n.$$

Tvrzení 2.3

Největší společný dělitel nenulových přirozených čísel *a*, *b* je roven poslednímu nenulovému zbytku v Euklidově algoritmu, tj. číslu r_n.

Důkaz

Konečnost vyplývá ze skutečnosti, že zbytky $r_1, \ldots, r_n$ tvoří klesající posloupnost přirozených čísel a tedy uvedený algoritmus skončí po provedení nejvýše *b* aplikací věty o dělení (G. Lamé dokázal, že počet dělení nepřekročí pětinásobek počtu cifer menšího z čísel *a, b*). Dále z tvrzení 2.1 část 5 vyplývá, že:

$$NSD(a,b) = NSD(b, r_1) = NSD(r_1, r_2) = \ldots = NSD(r_{n-1}, r_n) = r_n.$$

Pomocí Euklidova algoritmu určete NSD čísel 284 a 356.

$$356 = 284 \cdot 1 + 72$$

$$284 = 72 \cdot 3 + 68$$

$$72 = 68 \cdot 1 + 4$$

$$68 = 4 \cdot 17$$

Poslední nenulový zbytek: $NSD(284, 356) = 4$.

Výpočet lze zapsat i pomocí následujícího schématu, kde tučně psaná čísla označují zbytky r_i a kurzívou psaná čísla označují podíly q_i.

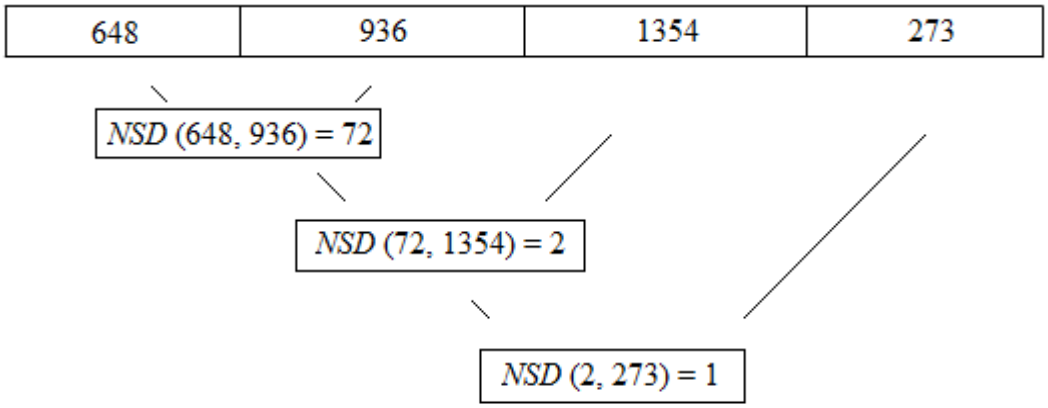
			356	284
			284	*1* …	q_0
		284	**72 …**	r_1
		216	*3* …	q_1
	72	**68 …**	r_2	
	68	*1* …	q_2	
68	**4 …**	r_3		
68	*17* …	q_3		
0 …	r_4			

Poznámka

NSD více čísel lze najít pomocí postupného hledání NSD dvou čísel, tj. následovně:

$$NSD(a_1, a_2, \ldots, a_n) = NSD \ldots (NSD(NSD(a_1, a_2), a_3) \ldots, a_n)$$

viz následující příklad:



Společný násobek

Definice: Společným násobkem nenulových celých čísel a, b nazveme nenulové přirozené číslo *D*, které je dělitelné čísly *a* i *b* tj.

$$a|D \wedge b|D.$$

Nejmenší společný násobek

Definice: Nejmenším společným násobkem nenulových celých čísel *a*,*b* nazveme takový jejich společný násobek, který je ze všech společných násobků nejmenší a značíme ho *NSN* (*a*, *b*).

Poznámky

- Označme $D_{a,b}$ množinu všech společných násobků nenulových čísel *a*,*b*. Zřejmě platí:

  $$|a \cdot b| \in D_{a,b} \subseteq \mathbb{N}$$

  a tedy $D_{a,b}$ má nejmenší prvek. Odtud vyplývá, že $NSN(a,b)$ existuje vždy a je určen jednoznačné.

- K výpočtu se užívá vztah

  $$NSN(a,b) = \frac{a \cdot b}{NSD(a,b)}.$$

Kongruence

Z věty o dělení se zbytkem vyplývá, že při dělení celých čísel kladným číslem *m*, dostáváme vždy zbytky pouze z množiny $\{0,1,...m-1\}$. Čísla, která dávající stejný zbytek budeme z pohledu dělitelnosti považovat za „totožná“.

Definice: Nechť $a, b \in \mathbb{Z}; m \in \mathbb{N} - \{0,1\}$, řekneme, že čísla *a*, *b* jsou kongruentní modulo *m*, píšeme $a \equiv b(mod\ m)$, jestliže obě čísla dávají při dělení číslem *m* stejný zbytek.

Poznámky

- Číslo *m* nazýváme modul.
- Běžně se používá i zápis $a = b \pmod m$, kde *a* je přímo zbytek po dělení čísla *b* modulem *m*.

Základní vlastnosti relace „býti kongruentní modulo *m*“ popisuje následující tvrzení:

Relace „býti kongruentní modulo *m*“ je relace ekvivalence na $\mathbb{Z}$, tj. platí

Tvrzení 2.4

1. $\forall a \in \mathbb{Z}$ platí $a \equiv a \pmod m$ … reflexivita
2. $\forall a, b \in \mathbb{Z}$ platí $a \equiv b \pmod m \Leftrightarrow b \equiv a \pmod m$ … symetrie
3. $\forall a, b, c \in \mathbb{Z}$ platí $a \equiv b \pmod m, b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$ … tranzitivita

Početní pravidla

Nechť $a, b \in \mathbb{Z}, m \in \mathbb{N} - \{0,1\}$ potom platí:

1. $a_1 \equiv b_1 \pmod m, a_2 \equiv b_2 \pmod m \Rightarrow (a_1 + a_2 \equiv b_1 + b_2 \pmod m, a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod m)$
2. $k \in \mathbb{N}, a \equiv b \pmod m \Rightarrow k \cdot a \equiv k \cdot b \pmod m$
3. $d \in \mathbb{N}, a \equiv b \pmod m, d \mid m \Rightarrow a \equiv b \pmod d$
4. $d \in \mathbb{N}, d \mid a, d \mid b, NSD(d, m) = 1 \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod m$

Tvrzení 2.5

Nechť $a, b \in \mathbb{Z}, m \in \mathbb{N} - \{0,1\}$ potom platí:

1. $a \equiv b \pmod m, d \mid NSD(a, b, m) \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \left(\mathrm{mod} \frac{m}{d} \right)$
2. $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2} \Rightarrow a \equiv b \pmod{NSN(m_1, m_2)}$

Definice – úplná a redukovaná soustava zbytků:

Úplnou soustavou zbytků modulo *m* nazveme každou množinu, která obsahuje *m* modulo *m* nekongruentních celých čísel. Značíme Z_m.

Redukovanou soustavou zbytků modulo *m* nazveme takovou podmnožinu zbytků modulo *m*, která obsahuje právě všechny zbytky s modulem *m* nesoudělné. Značíme Z_m^*.

Poznámky

- Nejčastěji se využívá tzv. soustava nejmenších nezáporných zbytků modulo *m*, značí se $Z_m=\{[0],[1],...,[m-1]\}$, kde $[0],[1],...[m-1]$ jsou jednotlivé zbytkové třídy. Běžně se užívá zjednodušený zápis *a* místo $[a]$. Zbytková třída $[i]$ obsahuje všechna celá čísla, která jsou kongruentní s *i* modulo *m*, tj. dávají při dělení číslem *m* zbytek *i*.
- Na Z_m lze definovat algebraické operace sčítání a násobení modulo *m*:
  - $[a]+[b]=[a+b]$, součet zbytkových tříd je zbytková třída s reprezentantem rovným součtu reprezentantů jednotlivých členů.
  - $[a]\cdot[b]=[a\cdot b]$, součin zbytkových tříd je zbytková třída s reprezentantem rovným součinu reprezentantů jednotlivých činitelů.
- Inverzní prvek $[a]^{-1}$ existuje právě tehdy, je-li *a* nesoudělné s modulem *m* a platí-li, že $[a]\cdot[a]^{-1}=[1]$
- Množina Z_m tvoří spolu s operací sčítání a násobení modulo *m* komutativní okruh a v případě, kdy *m* je prvočíslo tvoří konečné těleso.
- Naleznout inverzní prvek lze například metodou hrubé síly, tedy systematickým násobení všech prvků v dané modulární aritmetice s prvkem, ke kterému hledáme prvek inverzní. Jestliže výsledkem daného násobení je 1, jedná se o inverzní prvek.
  - Příklad: Uvažujeme-li modulo 5 a hledáme inverzní prvek k číslu 3. Vynásobíme číslo 3 postupně čísly 1, 2, 3, 4. Zjistíme, že inverzním prvkem je číslo 2, protože je jediné, u kterého při vynásobení vyjde 1.

Permutace

Důležitým pojmem v oblasti diskrétní matematiky (i šifrování – transpoziční šifry) jsou permutace.

Definice: Permutace na množině $X=\{1,2,\dots,n\}$ je vzájemně jednoznačné zobrazení *X* na *X*.

Poznámky

- Permutace budeme značit malými řeckými písmeny a zapisovat ve tvaru tabulky

  $\pi=\begin{pmatrix}1 & 2 & \dots n\\ \pi(1) & \pi(2) & \dots \pi(n)\end{pmatrix}$, kde v horním řádku se nachází vzor a v dolním obraz příslušný danému vzoru.

- Množinu všech permutací na *n*-prvkové množině značíme S_n a platí

$$|S_n|=n!$$

Na množině S_n lze definovat operaci násobení permutací (skládání zobrazení). Je-li $\pi,\rho\in S_n$, potom

$$\pi\cdot\rho=\begin{pmatrix}1 & 2 & 3 & \dots n\\ \rho(\pi(1)) & \rho(\pi(2)) & \rho(\pi(3)) & \dots \rho(\pi(n))\end{pmatrix}.$$

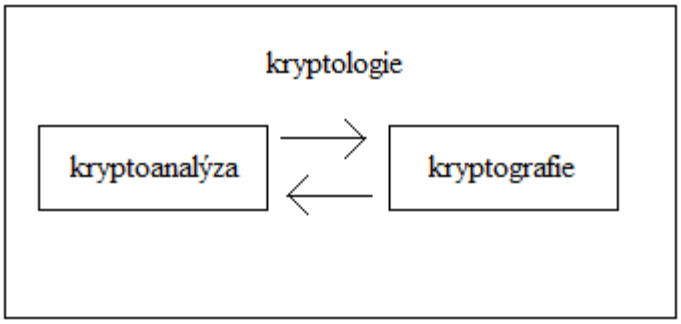
Zřejmě platí:

1. $\forall \pi,\rho,\varphi\in S_n \quad (\pi\cdot\rho)\cdot\varphi=\pi\cdot(\rho\cdot\varphi)$ … asociativita
2. $\forall n\geq 3\ \exists \pi,\rho\in S_n \quad \pi\cdot\rho\neq\rho\cdot\pi$ … není komutativní
3. $\exists id=\begin{pmatrix}1 & 2 & 3\dots n\\ 1 & 2 & 3\dots n\end{pmatrix}\forall \pi\in S_n$ platí $\pi\cdot id=id\cdot\pi=\pi$, … *id* je jednotkový prvek
4. $\forall \pi\in S_n\ \exists \pi^{-1}$ tak, že $\pi\cdot\pi^{-1}=\pi^{-1}\cdot\pi=id$ … π^{-1} je inverzní prvek

Inverzní permutaci vytvoříme formálním přehozením řádků. Permutace poté vypadá následovně: $\pi^{-1}=\begin{pmatrix}\pi(1) & \pi(2)\dots\pi(n)\\ 1 & 2\dots n\end{pmatrix}$.

Množina všech permutací S_n s operací násobení tvoří pro $n \geq 3$ nekomutativní grupu , kterou nazýváme symetrickou grupou.

3. Úvod do šifrování



Kryptologie se rozděluje na

- kryptografii → věda zabývající se ochranou dat před neautorizovaným přístupem,
- kryptoanalýzu → věda zabývající se metodami prolomení kryptografické ochrany,
- steganografii → utajování existence zprávy.

Otevřená abeceda

Konečná množina znaků, jež využíváme k zápisu nezašifrovaných zpráv.

Jedná se převážně o českou abecedu, ale v této práci se omezíme na abecedu anglickou.

Otevřený text

Konečný řetězec *m* znaků otevřené abecedy, který je určen k zašifrování. *M* je prostor otevřených textů.

Šifrová abeceda

Abeceda zašifrovaných textů, dříve stejná jako otevřená abeceda, ale v dnešní době se užívá spíše $\{0,1\}$ (binární šifrování).

Zašifrovaný text

Konečný řetězec *c* znaků šifrové abecedy, jež vznikl zašifrováním otevřeného textu. *C* je prostor zašifrovaných textů.

Prostor klíčů, klíč

Klíč je parametr šifrovací a dešifrovací metody, dělí se na šifrovací e a dešifrovací d, společně tvoří uspořádanou dvojici.

Prostor klíčů K je množina všech potenciálně použitelných klíčů $k \in K, k = (e, d)$.

Šifrování

Proces transformace otevřeného textu na zašifrovaný text.

Zobrazení $E_e : M \to C$, které je prosté, $m \to c = E_e(m)$.

Dešifrování

Proces transformace zašifrovaného textu na otevřený text.

Zobrazení $D_d : C \to M$, které je prosté, $c \to m = D_d(c)$.

Šifrovací systém

Uspořádaná trojice (E, D, K) kde

K je prostor klíčů (parametrů šifrovacích, resp. dešifrovacích funkcí),

$E = \{E_e | (e, d) \in K\}$ je množina šifrovacích funkcí,

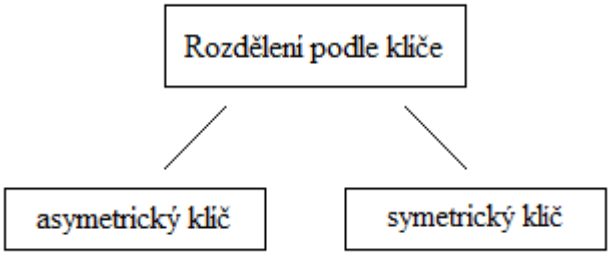
$D = \{D_d | (e, d) \in K\}$ je množina dešifrovacích funkcí,

tvoří šifrovací systém, jestliže

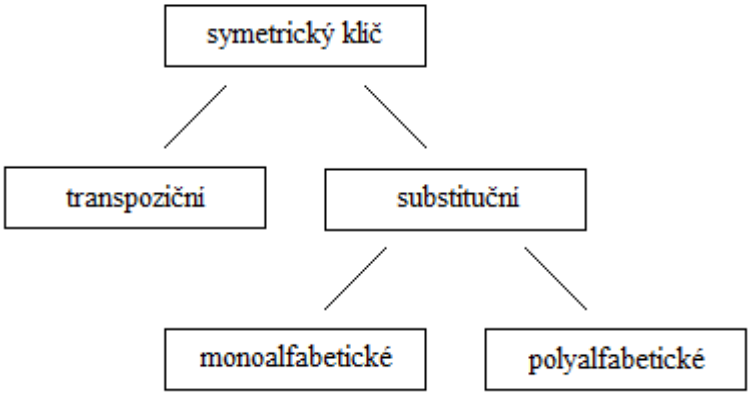
$$\forall k = (e, d) \in K, \forall m \in M, D_d(E_e(m)) = m.$$

Metody šifrování

Metody šifrování lze schematicky rozdělit:



Šifry využívající symetrický klíč se dále rozděluji:



Poznámky

Asymetrické šifrovací metody jsou metody, které využívají veřejný a soukromý klíč. Jsou založeny na tom, že z veřejného (šifrovacího) klíče nelze dostatečně efektivně odvodit soukromý (dešifrovací) klíč. Tuto metodu například využívá metoda RSA, jejíž bezpečnost je založena na neexistenci efektivního algoritmu pro nalezení kanonického rozkladu velkých čísel.

Symetrické šifrovací metody, jsou metody klasické, kde z šifrovacího klíče lze výpočetně efektivně odvodit klíč dešifrovací. Tato diplomová práce se zabývá převážně těmito metodami. Symetrické metody se dále dělí na *transpoziční*, kde si znaky uchovávají identitu, ale mění svoji pozici a na *substituční*, kde si znaky uchovávají pozici, ale mění svoji identitu.

Substituční metody se dále dělí na *monoalfabetické*, které využívají pouze jednu šifrovací abecedu a *polyalfabetické* šifry, které využívají více šifrovacích abeced, které se mění v závislosti na klíči.

Kerckhoffův princip

Auguste Kerckhoff formulovat v roce 1883 základní princip pro šifrovací metody: „Utajení a bezpečnost zašifrovaných dat nesmí záležet na utajení postupu, kterým se šifrují, ale musí spočívat na klíči, který nikdo jiný nezná.“

Poznámka - terminologická

Také je důležité rozlišovat pojmy šifrování a kódování:

- Šifrování se zabývá bezpečností dat, neboli ochranou dat před neautorizovaným přístupem.
- Hlavním principem kódování je převod mezi dvěma způsoby zápisu zprávy. Přičemž hlavní význam je umožnit tento přenos zpráv pomocí specifických médií bez ztráty dat.

Historické poznámky

Šifrování se využívalo k posílání tajných zpráv například v armádách nebo diplomacii už od nejstarších civilizací. Celé období kryptografie lze rozdělit na klasickou kryptografii, která trvala až do první poloviny 20. století. Druhou část lze nazvat jako moderní kryptografie.

Klasická kryptografie na rozdíl od moderní kryptografie nepotřebuje k šifrování výpočetní techniku. K šifrování i dešifrování stačí znalost metody a klíče.

Různé státy užívaly specifické šifrovací metody a některé z nich se dodnes ve školách vyučují. Ve starém Římě se kupříkladu užívala Caesarova šifra a různé její obměny. Hebrejci používali velice jednoduchou substituční šifru Atbash. Velkým pokrokem u substitučních metod pak byla Vigenèrova šifra.

3.1 Transpoziční šifry

Transpoziční šifry lze zjednodušeně charakterizovat jako šifry, kde znaky otevřeného textu si zachovávají svou identitu, ale předepsaným způsobem mění svoji pozici. Způsob, jakým mění svoji pozici je obvykle definován pomocí permutací. Zjednodušeně řečeno u transpozičních šifer se mění pouze pořadí znaků, nikoliv jejich identita.

Jednoduchá transpoziční šifra (permutační šifra)

Šifrovací klíč: $\pi \in S_d$, kde $d \in \mathbb{N} - \{0,1\}$

Šifrovací transformace: $E_\pi(m_1 \dots m_n) = C_1 \dots C_n$ kde

$C_i = m_{a+\pi(i-a)}$,

$a = i - (i \bmod d)$, přičemž v tomto případě použijeme jako úplnou soustavu zbytků modulo *n* množinu $\{1, \dots, n\}$.

Dešifrovací klíč: $\pi^{-1} \in S_d$, kde π^{-1} označuje inverzní permutaci k π

Dešifrovací transformace: $D_{\pi^{-1}}(C_1 \dots C_n) = m_1 \dots m_n$ kde

$m_i = C_{a+\pi^{-1}(i-a)}$,

$a = i - (i \bmod d)$, přičemž v tomto případě použijeme i zde jako úplnou soustavu zbytků modulo *n* množinu $\{1, \dots, n\}$.

Poznámky

- Postup šifrování: Nejprve text rozdělíme na podřetězce délky *d*. A každý tento podřetězec $s_1 \dots s_d$ zašifrujeme pomocí permutace π na řetězce $S_{\pi(1)} \dots s_{\pi(d)}$. Analogicky postupujeme i při dešifrování, kde používáme inverzní permutaci π^{-1}
- Pokud délka otevřeného textu není násobkem čísla *d*, doplníme text libovolnými znaky na délku rovnou násobku čísla *d*.

Příklad

Uvažujte jednoduchou transpozici s klíčem $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}$

Zašifrujte slovo *šifrování.*

Text rozdělíme do bloků po pěti znacích. A postupně zašifrujeme:

$$C_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ s & i & f & r & o \end{pmatrix}$$

$$C_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ v & a & n & i & x \end{pmatrix}$$

Zadaná permutace nám říká, který znak bude na kterém místě. Zašifrovaný text by v tomto případě byl: *OSRFIXVINA.*

Dešifrujte text *UPMREXTECA,* jestliže šifrovací permutace je stejná jako v předchozím příkladě. Nejprve musíme z šifrovací permutace vytvořit permutaci inverzní. Poté text rozdělíme do bloků a postupně dešifrujeme.

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$$

Vyjde nám otevřený text: *permutace.*

Jednoduché transpoziční systémy

V některých případech se šifruje pomocí tabulky. Tato metoda by pro žáky základních škol mohla být lépe pochopitelná, než šifrování pomocí permutace, i když je to založeno na stejném principu.

Příklad 1

Máme otevřený text *„kdo jinemu jamu kopa sam do ni pada“,* zašifrujte tento text pomocí způsobu zápisu do tabulky (7x4), kde text vypíšeme po sloupcích:

K	I	U	U	A	D	P
D	N	J	K	S	O	A
O	E	A	O	A	N	D
J	M	M	P	M	I	A

Zašifrovaný text poté vypíšeme po řádcích je

KIUUADPDNJKSOAOEAOANDJMMPMIA.

Příklad 2

Případně je možné stejný otevřený text začít psát v prvním sloupci na posledním řádku a text zapisovat směrem nahoru do tvaru spirály.

J	I	N	E	M	U	J
O	M	D	O	N	I	A
D	A	A	D	A	P	M
K	S	A	P	O	K	U

Zašifrovaný text po řádcích je *JINEMUJOMDONIADAADAPMKSAPOKU.*

Příklad 3

Další systém by mohl vypadat následovně:

První písmeno napíšeme do prvního řádku, prvního sloupce a následně pokračujeme

šikmým směrem zezdola nahoru, přičemž skončíme v posledním řádku posledního sloupce.

K	O	N	J	K	S	O
D	I	U	U	A	D	P
J	M	M	P	M	I	D
E	A	O	A	N	A	A

Zašifrovaný text po řádcích je *KONJKSODIUUADPJMMPMIDEAOANAA*.

Transpozice dle klíče a mřížky

U transpozic podobných jako v předchozí podkapitole lze použít i klíčové slovo.

Jedním ze způsobů využití klíče je zvolit si klíčové slovo a poté text zapsat do záhlaví sloupců, přičemž sloupců bude stejný počet, jako počet písmen v klíčovém slově. Zašifrování potom probíhá pomocí uspořádání klíčového slova dle abecedy. V případě opakování jednoho písmene v klíči, dodržujeme pořadí písmen ve slově.

Zašifrovaný text lze zapsat po řádcích i po sloupcích.

Dešifrujeme obráceným postupem. Seřadíme klíčové slovo dle abecedy a zapíšeme do záhlaví. Následně seřadíme sloupce dle správného tvaru klíčového slova.

Příklad

Zašifrujte pomocí klíče „krizovka“ a mřížky otevřený text *kolik reci umis, tolikrat jsi clovekem:*

k	**r**	**i**	**z**	**o**	**v**	**k**	**a**
K	O	L	I	K	R	E	C
I	U	M	I	S	T	O	L
I	K	R	A	T	J	S	I
C	L	O	V	E	K	E	M

Seřadíme sloupce dle záhlaví podle abecedy:

a	**i**	**k**	**k**	**o**	**r**	**v**	**z**
C	L	K	E	K	O	R	I
L	M	I	O	S	U	T	I
I	R	I	S	T	K	J	A
M	O	C	E	E	L	K	V

Zašifrovaný text vypíšeme dle řádků: *CLKEKORILMIOSUTIIRISTKJAMOCE ELKV*

Příklad

Dešifrujte pomocí klíče „tabulky“ a mřížky zašifrovaný text *ECAVNHLNEERDPDECERVEM*:

a	**b**	**k**	**l**	**t**	**u**	**y**
E	C	A	V	N	H	L
N	E	E	R	D	P	D
E	C	E	R	V	E	M

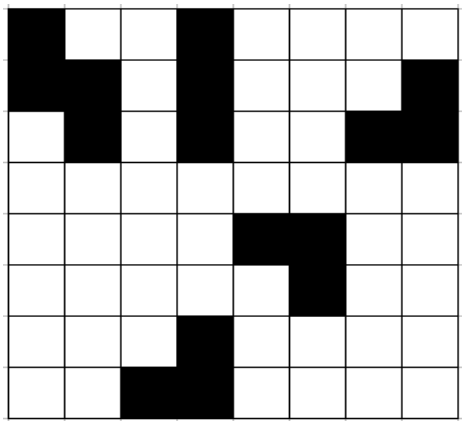
Úprava pořadí sloupců:

t	**a**	**b**	**u**	**l**	**k**	**y**
N	E	C	H	V	A	L
D	N	E	P	R	E	D
V	E	C	E	R	E	M

Otevřený text je *Nechval dne pred vecerem.*

Cardanova mřížka

Cardanova mřížka je druhem transpoziční šifry, u které je utajena mřížka, která generuje výsledný zašifrovaný text. Tato mřížka tedy funguje jako klíč.



Subjekt, který chce dešifrovat zprávu, musí disponovat stejnou mřížkou, jako subjekt, který zprávu šifroval. Příkladem takové mřížky může být mřížka na obrázku.

Černá políčka v tomto případě znázorňují umístění textu, který se čte po řádcích. Po přečtení se mřížka otočí, nejčastěji o 90° ve směru hodinových ručiček. Možnou alternací je jiné pořadí otočení mřížky.

Otevřený text postupně zapisujeme do jednotlivých polí a tím ho zašifrujeme.

Ideálními texty pro šifrování jsou texty, které plně zaplní tabulku. V případě kratšího textu se využívají pomocné znaky.

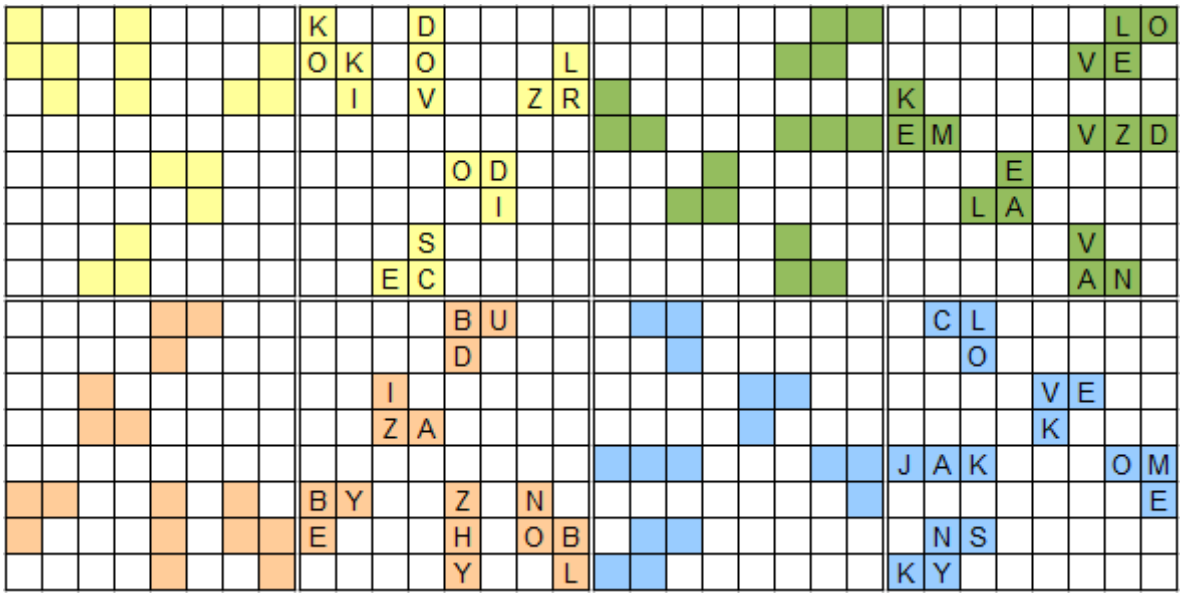
Při tvorbě mřížky je nezbytné, aby každé políčko bylo zobrazeno právě jednou.

Nejčastěji se při šifrování užívá mřížka 8x8, nicméně lze použít libovolnou sudou čtvercovou mřížku (4x4, 6x6, ...), která splňuje pravidlo zobrazení každého políčka právě jednou. Mřížky lichého řádu by tomuto pravidlu odporovaly, protože například střed by se zobrazoval v každém otočení.

Příklad:

Chceme zašifrovat text: *Kdokoliv zrodi se clovekem vzdelavan budiz aby z neho byl clovek. J A Komensky*

Použijeme mřížku z ukázky, kterou budeme postupně otáčet o 90° ve směru hodinových ručiček.



Výsledek:

K	C	L	D	B	U	L	O
O	K	O	O	D	V	E	L
K	I	I	V	V	E	Z	R
E	M	Z	A	K	V	Z	D
J	A	K	E	O	D	O	M
B	Y	L	A	Z	I	N	E
E	N	S	S	H	V	O	B
K	Y	E	C	Y	A	N	L

K	C	L	D	B	U	L	O
O	K	O	O	D	V	E	L
K	I	I	V	V	E	Z	R
E	M	Z	A	K	V	Z	D
J	A	K	E	O	D	O	M
B	Y	L	A	Z	I	N	E
E	N	S	S	H	V	O	B
K	Y	E	C	Y	A	N	L

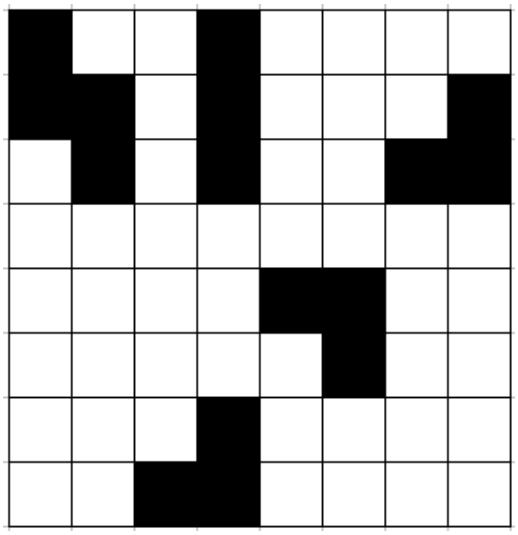
Subjekt, který chce šifru odeslat, pošle pouze tabulku bez barev, aby nebyla čitelná pro neoprávněné osoby. Případně pošle pouze text:

KOKEJBEKYKYMAYNYLOIZKLSEDOVAEASCBDVKOZHYUVEVDIVALOZ ZONONOLRDMEBL.

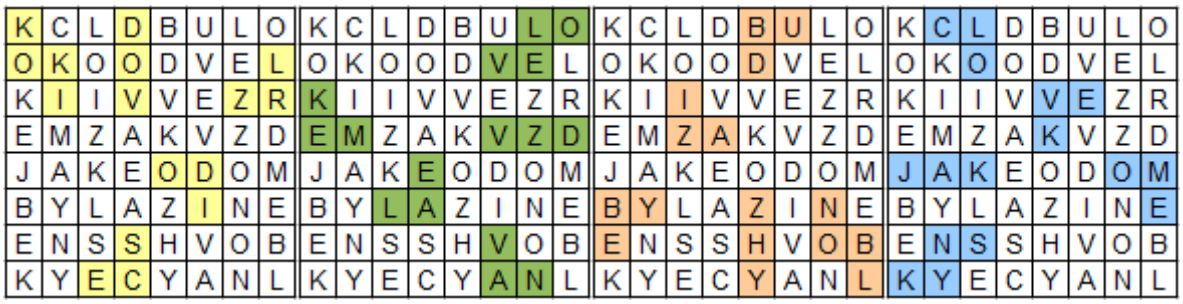
Dešifrování:

Máme k dispozici pouze tabulku a mřížku.

K	C	L	D	B	U	L	O
O	K	O	O	D	V	E	L
K	I	I	V	V	E	Z	R
E	M	Z	A	K	V	Z	D
J	A	K	E	O	D	O	M
B	Y	L	A	Z	I	N	E
E	N	S	S	H	V	O	B
K	Y	E	C	Y	A	N	L



Budeme postupovat analogicky jako při zašifrování, akorát nyní budeme tabulku „vybarvovat“ a až poté z ní vyčteme text. Zachováme stejné pořadí barev: žlutá, zelená, oranžová a modrá.



Vyjde text:

- žlutá: kdokolivzrodisec
- zelená: lovekemvzdelavan
- oranžová: budizabyznehobyl
- modrá: clovekjakomensky

Výsledek:

„*kdokoliv zrodi se clovekem vzdelavan budiz aby z neho byl clovek j a komensky*“

Poznámka

- Ve škole lze tuto šifru využít i v návaznosti jiných předmětů, například v informatice je možno nechat žáky, aby vytvořili vlastní mřížku v tabulkovém editoru a poté je v hodinách výtvarné výchovy vytvořili z papíru. V hodinách českého jazyka mohou žáci formulovat vlastní citáty tak, aby dosáhli přesně 64 (případně 100, 144, ...) znaků. Následně si žáci vyberou jeden z jimi vytvořených citátů a každý jej zašifruje za pomocí své mřížky. Další poté může zkusit tuto šifru dešifrovat.

3.2 Substituční šifry

Substituční šifry lze charakterizovat jako šifry, kde znaky otevřeného textu si zachovávají svoji pozici, ale předepsaným způsobem mění svoji identitu.

Monoalfabetické šifry

Šifrovací metody, využívající pouze jednu šifrovací abecedu.

Jednoduchá substituce

Šifrovací klíč: $\pi \in S_{26}$

Šifrovací funkce: $E_\pi(m_1 \dots m_n) = \pi(m_1) \dots \pi(m_n)$

Dešifrovací klíč: $\pi^{-1} \in S_{26}$, kde π^{-1} značí inverzní permutaci k π

Dešifrovací funkce: $D_{\pi^{-1}}(C_1 \dots C_n) = \pi^{-1}(C_1) \dots \pi^{-1}(C_n)$

Příklad

Je zadán otevřený text *informatika,* zašifrujte pomocí jednoduché substituce. Jako šifrovací klíč použijte:

$$\pi = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ Q & W & V & R & T & Z & U & Y & J & P & A & S & D & F & G & H & O & E & L & I & X & C & K & B & N & M \end{pmatrix}$$

Schematický zápis šifrování můžeme zapsat do tabulky následovně:

Otevřený text	*i*	*n*	*f*	*o*	*r*	*m*	*a*	*t*	*i*	*k*	*a*
Zašifrovaný text	J	F	Z	G	E	D	Q	I	J	A	Q

V případě dešifrování se postupuje analogicky.

Dešifrujte text *LJZEGCQFJ:*

Zašifrovaný text	L	J	Z	E	G	C	Q	F	J
Otevřený text	*s*	*i*	*f*	*r*	*o*	*v*	*a*	*n*	*i*

Poznámka:

- U této šifry můžeme žáky nechat, aby si sami vymysleli permutaci. Přičemž

musí myslet na to, že každý znak se zobrazí právě jednou, jinak by šifra nebyla dešifrovatelná.

Substituce s klíčovým slovem

Substituce s klíčovým slovem je alternativní způsob zadání jednoduché substituce. V tomto případě tvoří šifrovací klíč textový řetězec, který je umístěn na začátku permutace. Dále pak doplníme ostatní znaky dle abecedy. Šifrování i dešifrování je analogické jako u předchozí šifry.

Příklad

Pomocí substituce s klíčovým slovem „sifrovani“ zašifrujte text *vajicko*.

Nejprve se vytvoří permutace:

$$\pi = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ S & I & F & R & O & V & A & N & B & C & D & E & G & H & J & K & L & M & P & Q & T & U & W & X & Y & Z \end{pmatrix}$$

Zašifrujte:

v	*a*	*j*	*i*	*c*	*k*	*o*
U	S	C	B	F	D	J

Dešifrujte text MJNEBD pomocí permutace z předchozího příkladu:

M	J	N	E	B	D
r	*o*	*h*	*l*	*i*	*k*

Afinní šifrování

Šifrovací klíč: (a, b), kde $a, b \in \mathbb{Z}_{26,}\ NSD(a, 26) = 1$

Šifrovací funkce: $E_{(a,b)}(m_1 \ldots m_n) = C_1 \ldots C_n$, kde $C_i = ((a \cdot m_i + b) \bmod 26)$

m_i je číselná reprezentace *i*-tého znaku otevřeného textu.

Poznámka:

- Nejprve je nutné převést textový řetězec na číselný řetězec viz tabulka 1.

Dešifrovací klíč: $(a^{-1,}, b)$, kde a^{-1} je inverzní prvek k a mod 26

Dešifrovací funkce: $D(a^{-1,}, b)(C_1 \ldots C_n) = m_1 \ldots m_n$

kde $m_i = (a^{-1} \cdot (C_i - b) \bmod 26)$

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Tabulka 1: Pořadí znaků (mod 26)

Příklad:

Zašifrujte pomocí afinní šifry slovo *kniha*, jestliže klíčem je $e = (a, b)$, kde $(a = 21, b = 8)$

Vznikne funkce $Y = 21x + 8 (mod\ 26)$. Postupně zašifrujte jednotlivá písmena tak, že je budete dosazovat za proměnnou *x*:

Otevřený text	k	n	i	h	a
Pořadí znaku	10	13	8	7	0
$Y = 21 \cdot x + 8 (mod\ 26)$	10	21	20	25	8
Zašifrovaný text	*K*	*V*	*U*	*Z*	*I*

Zašifrovaný text je *KVUZI.*

Dešifrujte v afinní šifře slovo *ENTSC* pomocí klíče $e=(a,b)$ kde $(a=15, b=4)$.

Vznikne dešifrovací funkce: $x \equiv 15^{-1} \cdot (Y-4) (\mathrm{mod}\, 26)$, přičemž inverzní prvek naleznete v přiložené tabulce inverzních prvků.

Tabulka 2: Inverzní prvek modulo 26

Prvek	1	3	5	7	9	11	15	17	19	21	23	25
Inverzní prvek	1	9	21	15	3	19	7	23	11	5	17	25

Zašifrovaný text	*E*	*N*	*T*	*S*	*C*
Pořadí znaku	4	13	19	18	2
$Y=7\cdot(x-4)(mod\ 26)$	0	11	1	20	12
Otevřený text	*a*	*l*	*b*	*u*	*m*

Otevřený text je *album*.

Caesarova šifra

Caesarova šifra je speciálním typem afinní šifry. Je založena na posunu písmen o tři znaky. Takže místo písmene A zapisujeme písmeno o tři znaky dále tedy písmeno D. Vzniklé substituční schéma vypadá následovně:

$$\pi = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z & A & B & C \end{pmatrix}$$

Při dešifrování použijeme inverzní permutaci.

Příklad

Zašifrujte otevřený text *Nazdar Pepo* pomocí Caesarovy šifry.

Otevřený text	*n*	*a*	*z*	*d*	*a*	*r*	*p*	*e*	*p*	*o*
Zašifrovaný text	Q	D	C	G	D	U	S	H	S	R

Výsledný zašifrovaný text je *QDCGDU SHSR*.

Dešifrujte pomocí Caesarovy šifry text *MDNV HPDV:*

Zašifrovaný text	M	D	N	V	H	P	D	V
Otevřený text	*j*	*a*	*k*	*s*	*e*	*m*	*a*	*s*

Výsledný otevřený text je *jak se mas*.

Další typy šifer podobné Caesarově šifře

Caesarova šifra je založena na posunu o tři písmena. Další alternativou je šifra, kde je posun udán pomocí klíče.

Příklad

Zašifrujte otevřený text: *posun je o sedm* jestliže víte, že posun bude o sedm písmen.

$$\pi = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z & A & B & C & D & E & F & G \end{pmatrix}$$

Otevřený text	*p*	*o*	*s*	*u*	*n*	*j*	*e*	*o*	*s*	*e*	*d*	*m*
Zašifrovaný text	W	V	Z	B	U	Q	L	V	Z	L	K	T

Zašifrovaný text: *WVZB UQLV ZLKT*

Dešifrujte zašifrovaný text *KULZ QLB ALYF* pomocí permutace z předchozího příkladu*:*

Zašifrovaný text	K	U	L	Z	Q	L	B	A	L	Y	F
Otevřený text	*d*	*n*	*e*	*s*	*j*	*e*	*u*	*t*	*e*	*r*	*y*

Otevřený text: *dnes je utery*

Atbash

Atbash je velice jednoduchá monoalfabetická substituční šifra využívající permutaci: $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(n) & \pi(n-1) & \dots & \pi(1) \end{pmatrix}$.

$$\pi = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ Z & Y & X & W & V & U & T & S & R & Q & P & O & N & M & L & K & J & I & H & G & F & E & D & C & B & A \end{pmatrix}$$

Příklad:

Zašifrujte pomocí metody Atbash otevřený text *abeceda:*

Otevřený text	*a*	*b*	*e*	*c*	*e*	*d*	*a*
Zašifrovaný text	Z	Y	V	X	V	W	Z

Zašifrovaný text je *ZYVXVWZ.*

V případě dešifrování, se postupuje analogicky.

Dešifrujte pomocí metody Atbash text *PLNVQZ:*

Zašifrovaný text	P	L	N	V	G	Z
Otevřený text	*k*	*o*	*m*	*e*	*t*	*a*

Otevřený text je *kometa*.

3.3 Polyalfabetické šifry

Polyalfabetické šifry jsou šifrovací metody využívající více šifrovacích abeced, které se systematicky dle zadaných pravidel střídají.

Vigenèrova šifra

Šifrovací klíč: $(\pi_{1,}\dots\pi_d)\in S_{26}$

Šifrovací funkce: $E_{\pi_1\dots\pi_d}(m_1\dots m_n)=C_1\dots C_n$ kde $C_i=\pi_i \bmod d\,(m_i)$

(využíváme úplnou soustavu zbytků $\{1,\dots,d\}$)

Dešifrovací klíč: $(\pi_1^{-1}\dots\pi_d^{-1})\in S_{26}$,

kde π_i^{-1} označuje inverzní permutaci k π_i

Dešifrovací funkce: $D_{(\pi_1^{-1}\dots\pi_d^{-1})}(C_1\dots C_n)=m_1\dots m_n$ kde $m_i=\pi_i^{-1} \bmod d\,(C_i)$

Poznámky

- Vigenèrova šifra je polyalfabetická šifra, jejíž klíč tvoří *d* cyklicky se střídajících substitučních abeced.
- Speciálním případem je šifrování pomocí tzv. Vigenèrova čtverce (viz následující tabulka), jehož první řádek tvoří otevřená abeceda a následující řádky reprezentují substituční abecedy vzniklé pouhým posunutím. Šifrovací klíč tvoří textový řetězec, který určuje řádky, používané k zašifrování daného znaku otevřeného textu.

Tabulka 3: Vigenèrův čtverec

	a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
c	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
d	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
e	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
f	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
g	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

h	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
i	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
j	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
k	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
l	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
m	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
p	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
q	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
r	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
s	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
t	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
u	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
v	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
w	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
x	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
y	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
z	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Příklad

Zašifrujte pomocí Vigenèrovy šifry otevřený text *sifrovani ,* jeli zadán klíč „klic“.

Otevřený text	*s*	*i*	*f*	*r*	*o*	*v*	*a*	*n*	*i*
klíč	k	l	i	c	k	l	i	c	k
Zašifrovaný text	C	T	N	T	Y	G	I	P	S

Zašifrovaný text je CTNTYGIPS.

Dešifrujte pomocí Vigenèrovy šifry zašifrovaný text *AVKFFHAGQ,* máte-li klíč „informatika“.

Zašifrovaný text	A	V	K	F	F	H	A	G	Q
Klíč	i	n	f	o	r	m	a	t	i
Otevřený text	*s*	*i*	*f*	*r*	*o*	*v*	*a*	*n*	*i*

Otevřený text je *sifrovani*

Poznámky:

- Ve škole lze žákům zadat například i úkoly typu zašifrujte své oblíbené zvíře s klíčem zvíře. Poté si to vyměňte se sousedem a dešifrujte ho. Podobně lze zašifrovat oblíbený předmět, herce, ovoce, …

3.4 Moderní šifry

V současné době se užívají šifrovací metody, které používají binární abecedy , což znamená, že $A = B = \{0,1\}$ a tedy šifrují binární řetězec reprezentující otevřený text opět na binární řetězec tvořící šifrový text.

Poznámky

- Bitové logické operace
  - $\neg 0 = 1, \neg 1 = 0$ (negace)
  - $1 \cdot 1 = 1$; $1 \cdot 0 = 0 \cdot 1 = 0$; $0 \cdot 0 = 0$ (and - „logické násobení“)
  - $1 + 1 = 1 + 0 = 1 + 0 = 1$; $0 + 0 = 0$ (or - „logické sčítání“)
  - $1 \oplus 0 = 0 \oplus 1 = 1$; $1 \oplus 1 = 0 \oplus 0 = 0$ (xor - „vylučovací nebo“)
- Pro převod otevřeného textu na binární řetězec budeme využívat ASCII tabulku:

Tabulka 4: ASCII kód malých písmen

Znak	a	b	c	d	e	f	g
ASCII	01100001	01100010	01100011	01100100	01100101	01100110	01100111
Znak	h	i	j	k	l	m	n
ASCII	01101000	01101001	01101010	01101011	01101100	01101101	01101110
Znak	o	p	q	r	s	t	u
ASCII	01101111	01110000	01110001	01110010	01110011	01110100	01110101
Znak	v	w	x	y	z		
ASCII	01110110	01110111	01111000	01111001	01111010		

Tabulka 5: ASCII kód velkých písmen

Znak	A	B	C	D	E	F	G
ASCII	01000001	01000010	01000011	01000100	01000101	01000110	01000111
Znak	H	I	J	K	L	M	N
ASCII	01001000	01001001	01001010	01001011	01001100	01001101	01001110
Znak	O	P	Q	R	S	T	U
ASCII	01001111	01010000	01010001	01010010	01010011	01010100	01010101
Znak	V	W	X	Y	Z		
ASCII	01010110	01010111	01011000	01011001	01011010		

Vernamova šifra

Šifrovací klíč: $k=(b_1 b_2 \ldots b_d)$

Šifrovací funkce: $C=m \oplus k$,

kde $m=(m_1 \ldots m_d)$ je binární reprezentace části otevřeného textu

$C=(C_1 \ldots C_d)$ je binární reprezentace části zašifrovaného textu

$\oplus$ je symbol pro operaci xor („vylučovací nebo“)

Dešifrovací klíč: $k=(b_{1,} b_{2,} \ldots b_d)$, kde $b_i \in \{0,1\}$

Dešifrovací funkce: $m=C \oplus k$

Poznámky:

- Dešifrování má stejný klíč jako šifrovaní, neboť platí:

$$C \oplus k=(m \oplus k) \oplus k=m \oplus (k \oplus k)=m \oplus 0=m.$$

- Postup šifrování: Nejprve otevřený text převedeme na bitový řetězec, který rozdělíme na po sobě jdoucí bitové řetězce délky klíče (tj. *d*). Tyto řetězce pak zašifrujeme pomocí uvedené šifrovací funkce.
- Šifrovací klíč lze zadat pomocí klíčového slova, jehož binární reprezentace tvoří skutečný klíč.

Příklad

Zašifrujte otevřený text: *ahoj* , znáte-li klíčové slovo: klic.

ahoj = 0110 0001 0110 1000 0110 1111 0110 1010

klic = 0110 1011 0110 1100 0110 1001 0110 0011

otevřený text	*a*	*h*	*o*	*j*
binární reprezentace	01100001	01101000	01101111	01101010
klíč	01101011	01101100	01101001	01100011
zašifrovaný text	00001010	00000100	00000110	00001001

Dešifrujte zadanou posloupnost bitů: 0000 0001 0001 1111 0000 0100 0000 1111 0001 1111 0000 1101 0000 0000 jestliže víte, že klíčem je slovo: rovnice.

ZT	00000001	00011111	00000100	00001111	00011111	00001101	00000000
klíč	01110010	01101111	01110110	01101110	01101001	01100011	01100101
BR	01110011	01110000	01110010	01100001	01110110	01101110	01100101
OT	*s*	*p*	*r*	*a*	*v*	*n*	*e*

Otevřený text je *spravne.*

Poznámky:

- V případě, že bychom tuto šifru vyučovali na střední škole, můžeme žákům dát za úkol, aby napsali program, který by byl schopen takto šifrovat. V rámci předmětu alternativní metody programování jsem si také zkusila vytvořit program na Vernamovu šifru a to v programovacím jazyku Scheme (viz příloha)
- Během své pedagogické praxe jsem žáky prvního ročníku čtyřletého gymnázia učila počítání v dvojkové soustavě a jelikož jsem žákům chtěla ukázat nějaké využití dvojkové soustavy, bylo mi cvičným vyučujícím povoleno ukázat jim tuto šifru.

  Většinu žáků to bavilo a přišlo jim to jako dobré oživení informatiky a i když jsem neměla dostatek prostoru jim říct nějaký úvod do šifrování, tak látce porozuměli. Navíc jsem inspirovala i svého cvičeného vyučujícího, kterému tato šifra přišla jako dobrý příklad na procvičování programování ve vyšších ročnících.

Feistelova šifra

Feistelova šifra patří mezi blokové šifry. Je to nejrozšířenější třída šifer. Její princip je využíván i v dnešní době (DES, AES).

Šifrovací klíč: $(f_{1,}\dots f_r)$, kde $f_i:\{0,1\}^n \rightarrow \{0,1\}^n$

Šifrovací proces probíhá následovně, v (r + 1) na sebe navazujících cyklech:

1. cyklus: $m=(m_{0,}m_1) \overset{f_1}{\rightarrow} (m_{1,}m_2); m_2=m_0 \oplus f_1(m_1)$

2. cyklus: $(m_{1,}m_2) \overset{f_2}{\rightarrow} (m_{2,}m_3); m_3=m_1 \oplus f_2(m_2)$

…

r-tý cyklus: $(m_{r-1}, m_r) \overset{f_r}{\rightarrow} (m_r, m_{r+1}); m_{r+1}=m_{r-1} \oplus f_r(m_r)$

(r + 1) cyklus: $C=(m_{r+1}, m_r)$

kde $m=(m_{0,}m_1)$ je bitový řetězec délky 2n reprezentující část otevřeného textu, kde m_0 reprezentuje prvních n bitů, m_1 reprezentuje následujících n bitů.

C je bitový řetězec délky 2n reprezentující zašifrovaný text příslušný m.

Dešifrovací klíč: $(f_r, \dots f_1)$, kde f_i odpovídá šifrovacímu klíči

Dešifrovací proces probíhá následovně, v (r + 1) na sebe navazujících cyklech:

1. cyklus: $C=(C_{0,}C_1) \overset{f_r}{\rightarrow} (C_{1,}C_2); C_2=C_0 \oplus f_r(C_1)$

2. cyklus: $(C_{1,}C_2) \overset{f_{r-1}}{\rightarrow} (C_{2,}C_3); C_3=C_1 \oplus f_{r-1}(C_2)$

…

r-tý cyklus: $(C_{r-1}, C_r) \overset{f_1}{\rightarrow} (C_r, C_{r+1}); C_{r+1}=C_{r-1} \oplus f_1(C_r)$

(r + 1) cyklus: $m=(C_{r+1}, C_r)$

Příklad

Zašifrujte slovo *KUN* pomocí dvoustupňové Feistelovy šifrovací metody, kde máme zadané funkce:

$$f_1(x_1, x_2, x_3, x_4)=(x_1 \cdot x_4, x_2, 0, x_3) \quad , \quad f_2(x_1, x_2, x_3, x_4)=(x_2 \oplus x_4, x_1, x_2 \oplus x_1, x_3)$$

Nejprve si slovo *kun* převedeme na bitové řetězce 01001011, 01010101, 01001110. Zašifrujeme nejprve první písmeno *K*:

1. cyklus:
$$(0100, 1011) \overset{f_1}{\rightarrow} (1011, m_2);$$
$$m_2=0100 \oplus f_1(m_1);$$
$$m_2=0100 \oplus 1001$$
$$m_2=1101$$

2. cyklus:
$$(1011, 1101) \overset{f_2}{\rightarrow} (1101, m_3);$$
$$m_3=1011 \oplus f_2(m_2);$$
$$m_3=1011 \oplus 0100$$
$$m_3=1111$$

Zašifrovaný řetězec pro první písmeno (*K*) je $c=(m_3, m_2); c=(1111,1101)$.

Nyní zašifrujeme stejným postupem písmeno *U*:

1. cyklus
$$(0101, 0101) \overset{f_1}{\rightarrow} (0101, m_2);$$
$$m_2=0101 \oplus f_1(m_1);$$
$$m_2=0101 \oplus 0100$$
$$m_2=0001$$

2. cyklus
$$(0101, 0001) \overset{f_2}{\rightarrow} (0001, m_3);$$
$$m_3=0101 \oplus f_2(m_2);$$
$$m_3=0101 \oplus 1000$$
$$m_3=1101$$

Zašifrovaný řetězec pro druhé písmeno (*U*) je $c=(m_3, m_2); c=(1101,0001)$.

Písmeno *N*:

2. cyklus
$$(0100, 1110) \overset{f_1}{\rightarrow} (1110, m_2);$$
$$m_2=0100 \oplus f_1(m_1);$$
$$m_2=0100 \oplus 0101$$
$$m_2=0001$$

2. cyklus
$$(1110, 0001) \overset{f_2}{\rightarrow} (0001, m_3);$$
$$m_3=1110 \oplus f_2(m_2);$$
$$m_3=1110 \oplus 1000$$
$$m_3=0110$$

Poslední zašifrovaný řetězec je $c=(m_3, m_2); c=(0110,0001)$.

Celkový zašifrovaný řetězec: $11111101, 11010001, 01100001$

Příklad

Dešifrujte tento řetězec 11110001, 00001110, 00110000, jestliže funkce f_1 a f_2 jsou definovány následovně:

$$f_1(x_1, x_2, x_3, x_4) = (x_1 \cdot x_2, x_3, x_4 \oplus 1, 0) \qquad f_2(x_1, x_2, x_3, x_4) = (1, x_2, x_1 \oplus x_3, x_4)$$

První řetězec 11110001:

1. cyklus

$$(1111, 0001) \overset{f_2}{\rightarrow} (0001, m_1);$$
$$m_1 = 1111 \oplus f_2(m_2);$$
$$m_1 = 1111 \oplus 1001$$
$$m_1 = 0110$$

2. cyklus

$$(0001, 0110) \overset{f_1}{\rightarrow} (0110, m_0);$$
$$m_0 = 0001 \oplus f_1(m_1);$$
$$m_0 = 0001 \oplus 0110$$
$$m_0 = 0101$$

První dešifrovaný znak má posloupnost 01010110 což odpovídá písmenu *V*.

Druhý řetězec 00001110:

1. cyklus

$$(0000, 1110) \overset{f_2}{\rightarrow} (1110, m_1);$$
$$m_1 = 0000 \oplus f_2(m_2);$$
$$m_1 = 0000 \oplus 1100$$
$$m_1 = 1100$$

2. cyklus

$$(1110, 1100) \overset{f_1}{\rightarrow} (1100, m_0);$$
$$m_0 = 1110 \oplus f_1(m_1);$$
$$m_0 = 1110 \oplus 1010$$
$$m_0 = 0100$$

Druhý dešifrovaný znak má posloupnost 01001100, odpovídající písmenu *L*.

Třetí řetězec 00110000:

1. cyklus

$$(0011, 0000) \overset{f_2}{\rightarrow} (0000, m_1);$$
$$m_1 = 0011 \oplus f_2(m_2);$$
$$m_1 = 0011 \oplus 1000$$
$$m_1 = 1011$$

2. cyklus

$$(0000, 1011) \overset{f_1}{\rightarrow} (1011, m_0);$$
$$m_0 = 0000 \oplus f_1(m_1);$$
$$m_0 = 0000 \oplus 0100$$
$$m_0 = 0100$$

Třetí dešifrovaný posloupnost je 01001011, což odpovídá znaku *K*.

Získali jsme otevřený text *VLK*.

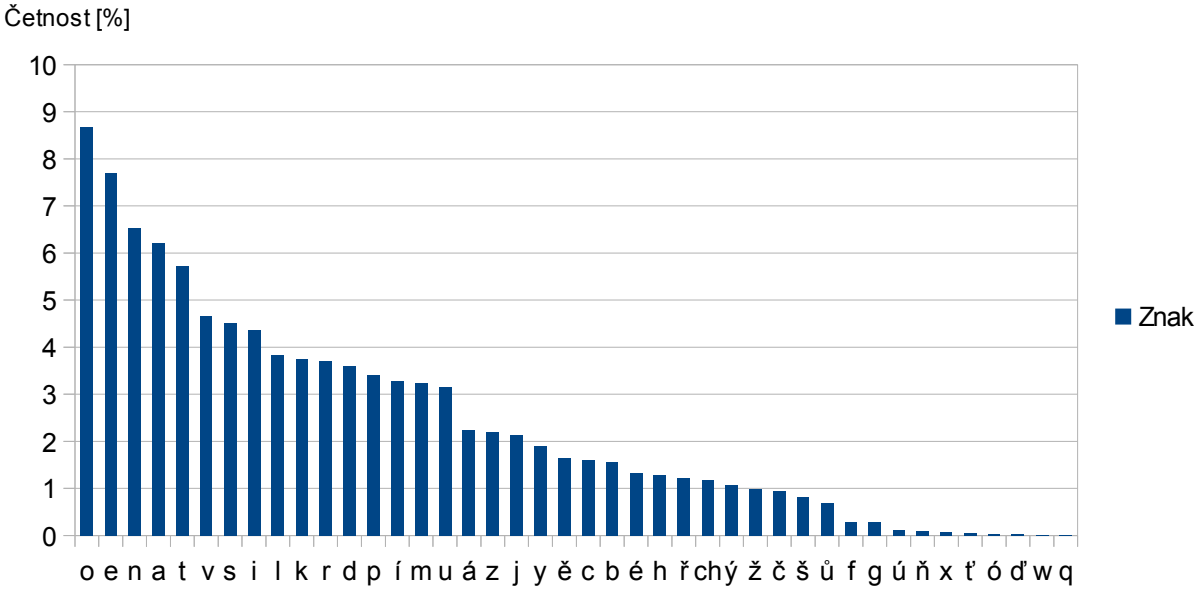
3.5 Kryptoanalýza

Kryptoanalýza, jak je již v úvodu psáno, je věda, která se zabývá prolomením šifer. U monoalfabetických substitučních šifer je založena na porovnání četností výskytu znaků v textu a obecně platné četnosti znaků. V českém jazyce je četnost písmen následující:

Tabulka 6: Četnost znaků v českém jazyce

Znak	Četnost (%)	Znak	Četnost (%)
a	6,2193	ň	0,0814
á	2,2355	o	8,6664
b	1,5582	ó	0,0313
c	1,6067	p	3,412
č	0,9490	q	0,0013
d	3,6019	r	3,6970
ď	0,0222	ř	1,2166
e	7,6952	s	4,5160
é	1,3346	š	0,8052
ě	1,6453	t	5,7268
f	0,2732	ť	0,0426
g	0,2729	u	3,1443
h	1,2712	ú	0,1031
ch	1,1709	ů	0,6948
i	4,3528	v	4,6616
í	3,2699	w	0,0088
j	2,1194	x	0,0755
k	3,7367	y	1,9093
l	3,8424	ý	1,0721
m	3,2267	z	2,1987
n	6,5353	ž	0,9952

Seřazené dle četnosti:



Při dešifrování se nejprve vytváří tabulka četnosti znaků zašifrovaného textu, a poté se porovnává s četností znaků abecedy. Dále se hledají možné substituce pomocí jednotlivých pravděpodobných slov. Názorněji si to ukážeme následujícím příkladu.

Příklad

Zašifrujeme text: „*Ačkoliv nemám rád všechna ta přirovnání a podobenství, kterými doktor Vlach propletá své temperamentní řeči, uznávám, že na tom názorném příkladu s kavárnou, člověkem a mísou koblih něco je. Lze na něm aspoň přibližně ukázat, jakým člověkem je Saturnin. Doktor Vlach si totiž rozdělil lidi podle toho, jak se chovají v poloprázdné kavárně, mají-li před sebou mísu koblih.*[1]“ pomocí následující substituční tabulky:

Otevřený text	a	á	b	c	č	d	ď	e	é	ě	f	g	h	ch	i	í	j	k	l	m	n
Zašifrovaný text	Q	W	Ě	E	R	Š	T	Z	Č	U	I	Ř	O	P	Ž	Ú	A	Ý	S	D	Á

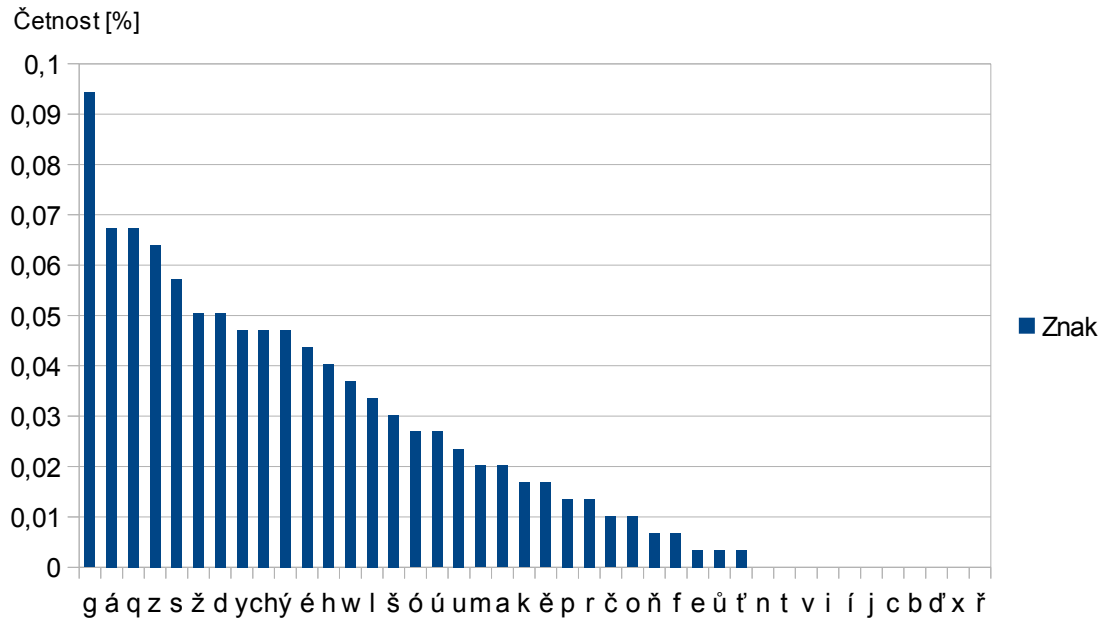
Otevřený text	ň	o	ó	p	q	r	ř	s	š	t	ť	u	ů	ú	v	w	x	y	ý	z	ž
Zašifrovaný text	Ť	G	Í	H	J	É	K	L	Ů	Y	X	Ó	V	C	CH	B	N	Ď	F	M	Ň

1 Citováno z knihy Saturnin od Zdeňka Jirotky, strana 9.

Zašifrovaný text: „QRÝGSŽCH ÁZDWD ÉWŠ CHŮZPÁQ YQ HKŽÉGCHÁWÁÚ Q HGŠGĚZÁLYCHÚ, ÝYZÉFDŽ ŠGÝYGÉ CHSQP HÉGHSZYW LCHČ YZDHZÉQDZÁYÁÚ KZRŽ, ÓMÁWCHWD, ŇZ ÁQ YGD ÁWMGÉÁČD HKÚÝSQŠÓ L ÝQCHWÉÁGÓ, RSGCHUÝZD Q DÚLGÓ ÝGĚSŽO ÁUEG AZ. SMZ ÁQ ÁUD QLHGŤ HKŽĚSŽŇÁU ÓÝWMQY, AQÝFD RSGCHUÝZD AZ LQYÓÉÁŽÁ. ŠGÝYGÉ CHSQP LŽ YGYŽŇ ÉGMŠUSŽS SŽŠŽ HGŠSZ YGOG, AQÝ LZ PGCHQAÚ CH HGSGHÉWMŠÁČ ÝQCHWÉÁU, DQAÚ-SŽ HKZŠ LZĚGÓ DÚLÓ ÝGĚSŽO.“

Nyní provede frekvenční analýzu četnosti znaků:

Znak	Četnost (%)	Znak	Četnost (%)
a	0,0202	ň	0,0067
á	0673	o	0,0101
b	0	ó	0,0269
c	0	p	0,0135
č	0,0101	q	0,0673
d	0,0505	r	0,0135
ď	0	ř	0
e	0,0033	s	0,0572
é	0,0438	š	0,0303
ě	0,0168	t	0
f	0,0067	ť	0,0033
g	0,0942	u	0,0236
h	0,0404	ú	0,0269
ch	0,0471	ů	0,0033
i	0	v	0
í	0	w	0,0370
j	0	x	0
k	0,0168	y	0,0471
l	0,0337	ý	0,0471
m	0,0202	z	0,0640
n	0	ž	0,0505



Dle analýzy budeme předpokládat, že G = *o*. Dále máme v textu slovo: *dqaú-sž*, kde za pomlčkou s největší pravděpodobností bude „li“, tudíž S = *l*, Ž = *i*.

Nyní si vybereme dvě taková slova, která budou obsahovat co nejvíce nám již známých písmen.

H	G	Š	G	Ě	Z	Á	L	Y	CH	Ú
d p í	o	í m u	o	á z j	e n a t	e n	p í m	t v s	i l k	m u á z

Š	G	Ý	Y	G	É
í m u	o	k r	t v s	o	r d p

Z druhé tabulky bychom se mohli domnívat, že vyjde slovo *doktor*, přiřadíme tedy tato písmena do naší hypotézy: Š = *d*, Ý = *k*, Y = *t*, É = *r*.

Doplníme tato písmena do našeho prvního vybraného slova a vyjde nám:

H	G	Š	G	Ě	Z	Á	L	Y	CH	Ú
d p í	o	d	o	á z j	e n a t	e n	p í m	t	i l k	m u á z

Zde by se dalo odvodit, že H = p, protože ostatní písmena nedávají smysl, ale jinak tento postup nebyl přínosem.

Další slovo, které si vybereme, bude slovo poslední, protože obsahuje 4 z našich zvolených písmen:

ý	g	ě	s	ž	o
k	o	á z j	l	i	h ř ch

V tomto případě bychom mohli Ě považovat za *b* a O za *h*, vzniklo by nám tím slovo *koblih*.

Nyní máme již několik písmen rozluštěných, doplníme je do textu a uvidíme, zda se nám něco potvrdí, že vyvrátí.

Již známe: G = o, S = l, Ž = i, Š = d, Ý = k, Y = t, É = r, H = p, Ě =b, O = h.

„QRkoliCH ÁZDWD rWd CHŮZPÁQ YQ pKiroCHÁWÁÚ Q podobZÁLtCHÚ, ktZrFDi doktor CHlQP proplZtW LCHČ tZDpZrQDZÁtÁÚ KZRi, ÓMÁWCHWD, ŇZ ÁQ toD ÁWMorÁČD pKÚklQdÓ L kQCHWrÁoÓ, RloCHUkZD Q DÚLoÓ koblih ÁUEo AZ. lMZ ÁQ ÁUD QLpoŤ pKibliŇÁU ÓkWMQt, AQkFD RloCHUkZD AZ LQtÓrÁiÁ. doktor CHlQP Li totiŇ roMdUlil lidi poŠlZ toho, AQk LZ PoCHQAÚ CH poloprWMdÁČ kQCHWrÁU, DQAÚ-li pKZd LZboÓ DÚLÓ koblih.“

Vzniklo nám několik slov, které se dají odvodit. Například první slovo bude *ačkoliv*. Tím získáváme další tři písmena, Q = *a*, R = *č*, CH = *v*. Dalším vybraným slovem je *ktZrFDi,* což pravděpodobně bude slovo *kterými*, Z = e, F = ý, D = m. Také by se část: „*totiŇ roMdUlil lidi podlZ toho“,* dala rozluštit jako: „*totiž rozdělil lidi podle toho*“. Ň = ž, M = z, U = ě.

Zašifrovaný text	A	Á	B	C	Č	D	Ď	E	É	Ě	F	G	H	CH	I	Í	J	K	L	M	N
Otevřený text			-	-		m	-		r	b	ý	o	p	v	-	-	-			z	-

Zašifrovaný text	Ň	O	Ó	P	Q	R	Ř	S	Š	T	Ť	U	Ů	Ú	V	W	X	Y	Ý	Z	Ž
Otevřený text	ž	h			a	č	-	l	d	-		ě			-		-	t	k	e	i

Nyní již zbývá rozluštit zbytek písmen. Použijeme některá z delších slov, kde je pravděpodobnost správného odhadu větší.

t	Z	D	p	Z	r	Q	D	Z	Á	t	Á	Ú
t	e	m	p	e	r	a	m	e		t		

Z tohoto slova lze odvodit, že Á = n, Ú = í

Ze slova ÁZDWD získáme W = á (slovo *nemám*).

Opět text přepíšeme a doplníme již dešifrovaná písmena: „ačkoliv nemám rád vŮechna ta pKirovnání a podobenLtví, kterými doktor vlaP propletá LvČ temperamentní Keči, Óznávám, že na tom názornČm pKíkladÓ L kavárnoÓ, člověkem a míLoÓ koblih něEo Ae. lze na něm aLpoŤ pKibližně Ókázat, Aakým člověkem Ae LatÓrnin. doktor vlaP Li totiž rozdělil lidi podle toho, Aak Le PovaAí v poloprázdnČ kavárně, maAí-li pKed LeboÓ míLÓ koblih.“

Nyní lze jednoduše doplnit zbývající písmena:

Zašifrovaný text	A	Á	B	C	Č	D	Ď	E	É	Ě	F	G	H	CH	I	Í	J	K	L	M	N
Otevřený text	j	n	-	-	é	m	-	c	r	b	ý	o	p	v	-	-	-	ř	s	z	-

Zašifrovaný text	Ň	O	Ó	P	Q	R	Ř	S	Š	T	Ť	U	Ů	Ú	V	W	X	Y	Ý	Z	Ž
Otevřený text	ž	h	u	ch	a	č	-	l	d	-	ň	ě	š	í	-	á	-	t	k	e	i

Výsledný text: „ *Ačkoliv nemám rád všechna ta přirovnání a podobenství, kterými doktor Vlach propletá své temperamentní řeči, uznávám, že na tom názorném příkladu s kavárnou, člověkem a mísou koblih něco je. Lze na něm aspoň přibližně ukázat, jakým člověkem je Saturnin. Doktor Vlach si totiž rozdělil lidi podle toho, jak se chovají v poloprázdné kavárně, mají-li před sebou mísu koblih.“*

Poznámky

- Čím je text delší, tím více odpovídá četnosti znaků.
- Je samozřejmé, že ne vždy se úspěch hned dostaví. Některé hypotézy mohou být špatné a je tedy dobré jednotlivé hypotézy ověřovat dalšími slovy.

4. Sbírka úloh

Permutační šifra

Zašifrujte pomocí klíče zadaného permutací:

1. *Hrnecek* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$

2. *Internet* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 2 & 3 & 5 & 4 & 1 & 8 \end{pmatrix}$

3. *Algoritmus* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$

4. *Skupina* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 2 & 1 & 7 & 4 \end{pmatrix}$

5. *Instalace* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$

Dešifrujte pomocí šifrovací klíče π

6. *TVRINAI* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 4 & 2 & 1 & 6 \end{pmatrix}$

7. *KYKODRLO* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 7 & 1 & 3 & 6 & 2 & 8 & 5 \end{pmatrix}$

8. *POLODNEXED* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$

9. *AIUMMMX* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 5 & 7 & 1 & 3 \end{pmatrix}$

10. *TKREACKA* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 3 & 7 & 2 & 6 & 1 & 5 \end{pmatrix}$

Výsledky:

1. KEHCREN, 2. NENTREIT, 3. GRALOMSITU, 4. NUIKSAP, 5. ATSNIXEVAL

6. *antivir, 7. krokodyl, 8. odpoledne, 9. maximum, 10. kartacek*

Jednoduché transpoziční systémy

Zašifrujte pomocí spirály začínající v prvním sloupci a posledním řádku a pokračující směrem nahoru. Mřížka má čtyři řádky a osm sloupců:

1. *spatnostem se lze naucit i bez ucitele*
2. *hladovi nechteji vladnout, nybrz jist* (ch zapisujte jako dva znaky)

Dešifrujte pomocí spirály začínající v prvním sloupci a posledním řádku a pokračující směrem nahoru. Mřížka má šest sloupců a pět řádků:

3. AVITEZ KESE BISJS IEAAH TEVTL CARTS
4. EZITO SLOPRE TIHU XVIR OKELMP NMIJA

Výsledky:

1. TNOS TEM SAI BEZU CEPTE LETIL SICU ANEZ,
2. DOVI NECH AUTN YBRT LOTS IJZE HNDA LVIJ
3. *laska vitezi at strach je sebevetsi*
4. *prilezitosti mají mnoho prevleku x*

Transpozice dle mřížky s klíčovým slovem

Zašifrujte pomocí klíčových slov uvedených v závorkách, přičemž klíčová slova vám napoví velikost mřížky:

1. *Doma je tam kde si povesim klobouk (lampion)*
2. *Nevim co delam ale zatím to vychazi (sporty)*
3. *Pomoc rodicu lze jinak nazvat uplatek (kulecnik)*
4. *Kazde zbozi vypada na fotografii lepe (sardinky)*
5. *Energie je to co vse uvadi do pohybu x (talent)*

Dešifrujte pomocí klíčového slova uvedeného v závorce, přičemž klíčové slovo nám napoví velikost mřížky:

6. MNTAU ILELC EEENG IEIN PJSEL ZENOE ZRV BTX OASBL (nevolnik)
7. JDZK DEYH OUDE HTDK ZOYSA AVPE RIY (lepidlo)
8. TUSE DNNE TPOI UJSC EVCI IISJ NZEARK (jablko)
9. IYDKN EAPON USUJ KEYN SPOSUKP (valec)
10. ESDV EAIL MNEY TJDN EESA EESM YTATFK (stovka)

Výsledky

1. OJDM TEA MEA KISD OSPV MIE LOKO KUB
2. VEINM CEDL OAME LZAAT TMOI VYAH ZCIX
3. COOP DMRO ZLJI IUEC ANVN AKZA ALET KPTU
4. ADEB ZZKO IYPD AVZA AOTG OFNR FILP EIAE
5. NREGE IJTEO ECVES UOVD DIOA PHBY UOX
6. *Umela inteligence je lepsi nez vrozena blbost*
7. *Kdyz jde do tuheho kazdy se vypari*
8. *Student neopisuje cvici si jen zrak*
9. *Nikdy neopakuj uspesny pokus*
10. *Veda se nemyli nedejte se mast fakty*

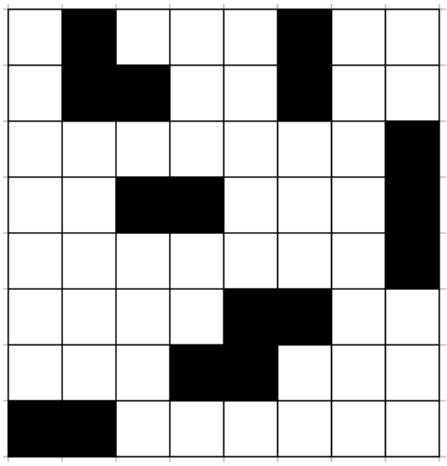
Cardanova mřížka

Zašifrujte následující texty pomocí zadané příslušné mřížky:

Příklad 1:

Text: „*Prvotni lidskou slabosti je, ze clovek nepredvida bouri, kdyz je pekne pocasi.*“

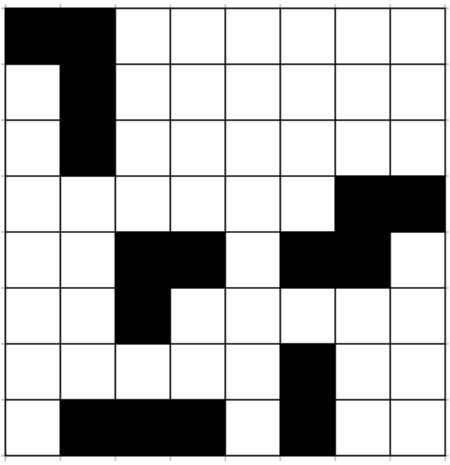
Mřížka:



Příklad 2:

Text: „*Internet se zasekne prave ve chvili, kdy najdete co jste dlouhou dobu hledali.*“

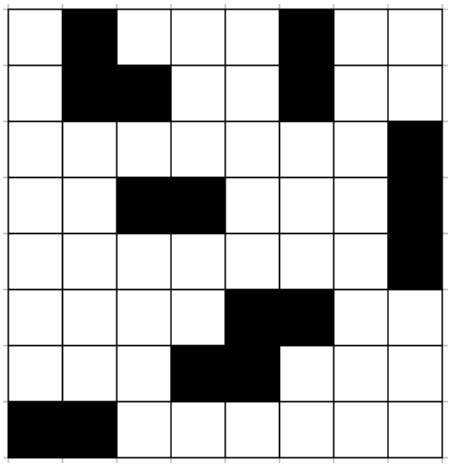
Mřížka:



Dešifrujte, co se skrývá v jednotlivých tabulkách, jestliže máte k dispozici příslušné mřížky. Přičemž víte, že mřížka je v základní poloze.

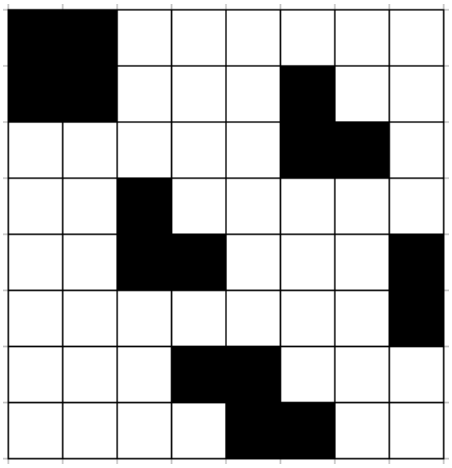
Příklad 3:

C	N	E	T	O	I	J	D
O	K	D	E	N	Y	N	E
N	E	E	K	J	J	D	N
D	E	E	R	N	D	E	I
O	E	B	A	K	D	U	K
O	D	O	E	E	J	T	S
L	A	N	Z	E	E	V	T
N	E	I	E	N	A	Z	O



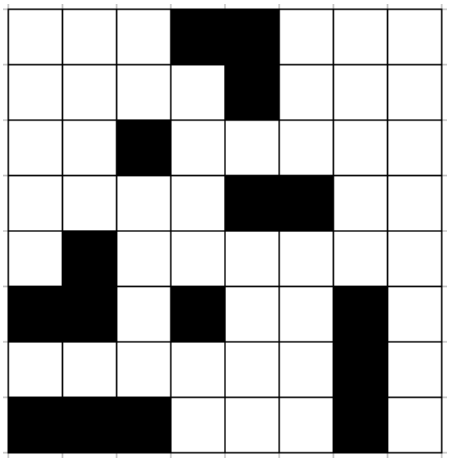
Příklad 4:

D	O	T	O	B	Y	E	N
T	E	L	J	E	T	A	P
N	Y	P	S	A	A	B	O
N	T	U	C	A	V	U	Z
O	K	L	K	E	A	P	Y
O	S	C	R	I	L	I	M
K	L	I	U	Z	V	T	A
A	D	J	E	E	T	T	Y



Příklad 5:

I	K	J	K	D	D	O	S
E	I	V	L	O	I	Z	A
A	M	S	C	Y	S	S	L
I	N	T	A	I	M	I	I
B	Y	Z	E	C	Y	H	L
S	L	T	I	O	U	Z	T
U	B	A	Z	R	O	E	U
S	E	U	U	M	B	C	A



Výsledky:

1. APDYZ RNEB VOPR TOSJ EEDT PINV JILE EKII ZENDA EDBP COSK LOCA OOUU RSSL
2. INYO NAJE PTDU HRAV EEVE OEUD CTEHC ORNJ SETO SEB VIZLU HTLE DAIK AEL ISEK DNDL
3. *„nikdy nerikej ze neco nejde nebot se najde nekdo kdo nevi ze to nejde a udela to“*
4. *„do te tabulky muzete napsat cokoliv je to jen na vas citaty byly pouze priklad“*
5. *„kdo si mysli ze se uci je vlasti chlouba kdo si mysli ze uz umi zacina byt trouba“*

Jednoduchá substituce

Zašifrujte pomocí tabulky u vzorového příkladu:

1. *anglictina*
2. *kapesnik*
3. *skolnik*
4. *tabule*
5. *zvoneni*
6. *student*
7. *orangutan*

Dešifrujte pomocí tabulky u vzorového příkladu:

8. XVJITSAQ
9. SQCJVT
10. HQHEJAQ
11. MJEQZAQ
12. HGSJVJLIQ
13. AFJYGCFQ
14. HETLIQCAQ

Výsledky šifrování

1. QFUSJVIJFQ, 2. AQHTLFJA, 3. LAGSFJA, 4. IQWXST, 5. MCGFTFJ,

6. LIXRTFI, 7. GEQFUXIQF**,**

8. *ucitelka,* 9. *lavice,* 10. *paprika,* 11. *zirafka,* 12. *policista,* 13. *knihovna,*

14. *prestavka*

Substituce s klíčovým slovem

Zašifrujte slova dle klíčových slov uvedených v závorkách:

1. *kralik* (*zviratko*)
2. *predmet* (*nemecky jazyk*)
3. *tajenka* (*kryptografie*)
4. *priklad* (*matematika*)
5. *chleba* (*pecivo*)
6. *monitor* (*pocitac*)

Dešifrujte pomocí klíčových slov uvedených v závorkách:

7. HJBIDZ (*zviratko*)
8. RKXDIQR (*nemecky jazyk*)
9. ABKUHBKC (*kryptografie*)
10. QNVLDTI (*matematika*)
11. QLBHDG (*pecivo*)
12. GHPVTRKECT (*pocitac*)

Výsledky

1. DMZEBD, 2. LPKCGKR, 3. QKITDEK, 4. OQDGHME, 5. CBHVEP,

6. JLKESLQ

7. *opicka,* 8. *tezkost,* 9. *hlavolam,* 10. *rovnice,* 11. *rohlik,* 12. *klavesnice,* 13. *Atbash*

Afinní šifra

Zašifrujte pomocí klíče uvedeného v závorce:

1. *Chemie* (11, 3)
2. *sifra* (17, 7)
3. *zeli* (9, 4)
4. *obdobi* (19, 12)
5. *tuzka* (25, 18)

Dešifrujte pomocí klíče uvedeného v závorce:

6. ZWDEN (21, 3)
7. ZSHSZ (5, 18)
8. GABA (7, 0)
9. GLCPQ (23, 10)
10. IRIHM (15, 17)

Výsledky:

1. ZCVFN, 2. BNOKH, 3. VOZY, 4. SFRSFI, 5. ZYTIS**,** 6. *grafy,* 7. *radar,* 8. *mapa,* 9. *kruhy,* 10. *papir*

Caesarova šifra

Zašifrujte:

1. *Liberec*
2. *technika*
3. *kolecko*
4. *notebook*
5. *derivace*
6. *hodinky*
7. *padouch*

Dešifrujte:

8. YHYHUND
9. SRGPDVOL
10. FBNOLVWD
11. EHCSHFQRVW
12. PHGYLGHN
13. WUHVQLFNB
14. VWXGQD

Výsledky

1. OLEHUHF
2. WHFKQLND
3. NROHFNR
4. QRWHERRN
5. GHULYDFH
6. KRGLQNB
7. SDGRXFK
8. *veverka*
9. *podmasli*
10. *cyklista*
11. *bezpecnost*
12. *medvidek*
13. *tresnicky*
14. *studna*

Další typy Caesarovi šifry

Zašifrujte (pomocí posunu uvedeného v závorce)

1. *tramvaj* (7)
2. *nadrazi* (13)
3. *pizzerie* (21)
4. *okenko* (19)
5. *cepice* (8)
6. *sloucenina* (24)

Dešifrujte:

7. VISVOH (7)
8. YRQAVPR (13)
9. NZYVXFV (21)
10. DTEAHMR (19)
11. UZIDMVMK (8)
12. TCIRMP (24)

Výsledky:

1. AYHTCHQ
2. ANQENMV
3. KDUUZMDZ
4. HDXGDH
5. KMXQKM
6. QJMSACLGLY
7. *obloha*
8. *lednice*
9. *sedacka*
10. *kalhoty*
11. *mravenec*
12. *vektor*

Atbash

Zašifrujte:

1. Mam rad informatiku
2. Me oblibene zviratko je kocicka
3. Prosim jedno jablicko
4. Venku sviti slunicko
5. Zasifrovava se pomoci obracene abecedy

Dešifrujte:

6. EVMPF KIHR
7. KLNVIZMX QV LIZMALEB
8. XSXR MLEV ZFGL
9. KIZO YBXS HR KLXRGZX
10. GL QV EHV KIZGVOV

Výsledky

1. NZN IZW RMULINZGRPF
2. NV LYORYVMV AERIZGPL QV PLXRXPZ
3. KILHRN QVWML QZYORXPL
4. EVMPF HERGR HOFMRXPL
5. AZHRUILEZEZ HV KLNLXR LYIZXVMV ZYVXVWB
6. Venku prsi
7. Pomeranc je oranzovy
8. Chci nove auto
9. Pral bych si pocitac
10. To je vse pratele

Vigenerova šifra

Zašifrujte pomocí klíče uvedeného v závorce:

1. *sifrovani* (sifrovani)
2. *zelvicka* (zvire)
3. *informatika* (klic)
4. *pocitac* (klic)
5. *ctverec,* (matematika)
6. *monitor* (pocitac)
7. *prezentace* (klic)

Dešifrujte pomocí klíče uvedeného v závorce:

8. FTOGXPZ (klic)
9. JBZAVBP (znameni)
10. RSMKSSRAV (heslo)
11. ZZCDXSPXQG (pocitac)
12. OMIJESFW (zvire)
13. SYNQBXIVSVI (klic)
14. ULTMEWIEUL (klic)

Výsledky

1. KQKICQAAQ, 2.YZTMMBFI, 3. SYNQBXIVSVI, 4.ZZKKDLK, 5. OTOIDEV, 6.BCPQMOT, 7. ZCMBOYBCMP, 8. *vigener*, 9. *kozoroh*, 10. *kouzelnik*, 11. *klavesnice*, 12. *prasatko*, 13. *informatika,* 14. *kalkulacka*

Vernamova šifra

Zašifrujte pomocí klíčů uvedených v závorce:

1. *klokan* (zvire)
2. *funkce* (pohyb)
3. *testoviny* (priloha)
4. *Karolina* (spoluzacka)
5. *zaclona* (okno)
6. *cervena* (barva)
7. *pondeli* (den)

Dešifrujte pomocí klíče uvedeného vzorce:

8. QPDVJKYE (00000001 00011111 00001001 00010011 00011000 00001010 00010111 00000110)
9. TDVJIMLASO (00000111 00001000 00000011 00000100 00001100 00001110 00000010 00001000 00010000 00001010)
10. QDBPJC (00000111 00000001 00010001 00011101 00000011 00010001)
11. GHFJDK (00001000 00000000 00011111 00000100 00000001 00000000)
12. ECUMXRN (00001110 00000010 00000101 00011000 00001011 00000110 00001111
13. JCEYSOTA (00011010 00010001 00001010 00011101 00010010 00011001 00010101 00000010
14. ABCDEFGH (00011011 00000111 00001111 00000001 00001011 00001111 00001001 00001001

Výsledky

1. 00010001 00011010 00000110 00011001 00000100 00010100
2. 00010110 00011010 00000110 00010010 00000001 00010101
3. 00000100 00010111 00011010 00011000 00000000 00011110 00001000 00011110 00001011
4. 00011000 00010001 00011101 00000011 00011001 00010011 00001111 00000010
5. 00010101 00001010 00001101 00000011 00000000 0000101 00001111
6. 0000001 00000100 00000000 00000000 00000100 00001100 00000000
7. 00010100 00001010 00000000 00000000 00000000 00000010 00001101

8. *POMERANC*
9. *SLUNECNICE*
10. *VESMIR*
11. *OHYNEK*
12. *KAPUSTA*
13. *PRODAVAC*
14. *ZELENINA*

Feistelova šifra

Zašifrujte pomocí zadaných funkcí:

1. *LUCIE*
$$f_1(x_1, x_2, x_3, x_4) = (x_1 \cdot x_2, x_3, 0, x_4 \oplus 1)$$
$$f_2(x_1, x_2, x_3, x_4) = (x_4, x_3, x_2, x_1)$$

2. *METR*
$$f_1(x_1, x_2, x_3, x_4) = (x_2 \cdot x_4, x_1, x_3, 0)$$
$$f_2(x_1, x_2, x_3, x_4) = (x_3 \oplus 0, x_1, x_4 \oplus x_2, 1)$$

3. *BRYLE*
$$f_1(x_1, x_2, x_3, x_4) = (x_2, x_4, x_1 \oplus x_3, x_1 \cdot x_3)$$
$$f_2(x_1, x_2, x_3, x_4) = (x_4 \oplus x_1, x_3, 1, x_2)$$

4. *POCIT*
$$f_1(x_1, x_2, x_3, x_4) = (x_2, x_1 \oplus x_4, x_3, 0)$$
$$f_2(x_1, x_2, x_3, x_4) = (x_4, x_2, x_3, x_1 \oplus 1)$$

5. *BANKA*
$$f_1(x_1, x_2, x_3, x_4) = (1 \oplus x_1, x_2 \cdot x_3, x_4, 0)$$
$$f_2(x_1, x_2, x_3, x_4) = (x_2, x_1 \oplus x_3, 1, x_4)$$
$$f_3(x_1, x_2, x_3, x_4) = (1, x_2, x_1 \cdot x_3, x_4)$$

Dešifrujte pomocí zadaných funkcí:

6. 11111001 10111101 11101100 00011001

$$f_1(x_1, x_2, x_3, x_4) = (1, x_1 \oplus x_3, 0, x_2 \cdot x_4)$$
$$f_2(x_1, x_2, x_3, x_4) = (x_1, x_4, x_2 \oplus x_3, 0)$$

7. 00111010 10000110 10010110 10100000

$$f_1(x_1, x_2, x_3, x_4) = (x_1, x_3, x_2, x_4 \oplus 1)$$
$$f_2(x_1, x_2, x_3, x_4) = (1, x_1 \oplus x_2, x_4, x_3 \oplus 1)$$

8. 00011100 10001001 10100100 1000101 01110000

$$f_1(x_1, x_2, x_3, x_4) = (x_1, x_2 \cdot x_3, 0, x_4)$$
$$f_2(x_1, x_2, x_3, x_4) = (x_2 \oplus x_3, x_4, x_1, 1)$$

9. 11101000 10110100 01111001 00110000 01110100

$$f_1(x_1, x_2, x_3, x_4) = (x_1 \cdot x_2, x_3, 0, x_4 \oplus 1)$$
$$f_2(x_1, x_2, x_3, x_4) = (x_4, x_3, x_2, x_1)$$

10. 01101011 01011011 01111000 10110101 01011011

$$f_1(x_1, x_2, x_3, x_4) = (1 \oplus x_1, x_2 \cdot x_3, x_4, 0)$$
$$f_2(x_1, x_2, x_3, x_4) = (x_2, x_1 \oplus x_3, 1, x_4)$$
$$f_3(x_1, x_2, x_3, x_4) = (1, x_2, x_1 \cdot x_3, x_4)$$

Výsledky:

1. 01111101 11110101 00110000 10110100 01110100
2. 10001000 00101100 01010101 10110111
3. 01010110 11010111 01110011 00111110 11111000
4. 11010101 10011110 00000010 11000100 10001101
5. 00001100 01011011 11001100 10110101 01011011
6. *SEDM*
7. *OTEC*
8. *JOSEF*
9. *MINCE*
10. *TASKA*

5. Závěr

Cílem této diplomové práce primárně bylo vytvoření sbírky příkladů na téma šifrování, a proto poslední část je věnována právě sbírce, kde jsou jednoduché příklady využitelné jak na základních tak na středních školách.

V první části diplomové práce je pak věnován prostor matematické teorii, která je nezbytná k pochopení principu uvedených šifer. Tato část je psána převážně na středoškolské úrovni, jelikož tato práce má být využitelná zejména na základních a středních školách.

Po matematické teorii následuje úvodní kapitola k šifrování, kde jsou vysvětleny základní pojmy potřebné k jednotlivým šifrám.

V další části jsou představeny jednotlivé šifry se vzorovými příklady. U vybraných šifer je popsána i možnost využití a propojení s jinými vyučovacími předměty.

Tato práce by mohla být rozšířená větším množství teorie a to jak po stránce matematické, tak po stránce informatické.

Po matematické stránce by se jednalo o odbornější metody, například při hledání inverzních prvků v modulární aritmetice, případně o důkazy jednotlivých matematických vět.

Po informatické stránce by bylo možné zapojit programování a vytvářet programy na jednotlivé šifry.

Dále by také bylo možné práci rozšířit o komplexnější a složitější příklady, ale to už by se jednalo spíše o vysokoškolskou úroveň, která není těžištěm této práce.

6. Zdroje

[1] KOUCKÝ, Miroslav. *Matematika pro informatiky,* (přednášky) FP TUL, Liberec, 2010/2011.

[2] KOUCKÝ, Miroslav. *Šifrování, kódování a jejich aplikace,* (přednášky) FP TUL, Liberec, 2012/2013.

[3] KOUCKÝ, Miroslav. *Diskrétní matematika II,* Skripta TUL, Liberec, 2004.

[4] MLÝNEK, Jaroslav. *Kryptografie a bezpečnost informací,* (přednášky) FP TUL, Liberec, 2012/2013.

[5] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací,* vydání první, Brno: Computer Press, 2007. ISBN 978-80-251-1511-4.

[6] SINGH, Simon. *Kniha kódů a šifer. Tajná komunikace od starého Egypta po kvantovou kryptografii,* Praha: Dokořán a Argo, 2003. ISBN 80-86569-18-7.

[7] MENEZES, A., OORSCHOT, P., VANSTONE, S. *Handbook of Applied Cryptography*, London: CRC Press, 2011. ISBN 0-8493-8523-7.

[8] HANKERSON, Darrel R. et al. *Coding Theory and Cryptography. Second Edition,* New York: Marcel Dekker, 2000. ISBN 0-8247-0465-7.

[9] HANŽL, Tomáš. *Šifry a hry s nimi: kolektivní outdoorové hry se šiframi,* vydání první, Praha: Portál, 2007. ISBN 978-80-7367-196-9.

[10] POSKITT, Kjartan. *Šifry: od Caesara ke kreditním kartám,* vydání první, Praha: Egmont, 2009. ISBN 978-80-252-1213-4.

[11] *Algoritmy.net* [online]. [cit. 2014-07-28]. Dostupné z: http://www.algoritmy.net/article/40/Cetnost-znaku-CJ

7. Přílohy

Vernamova šifra ve Scheme

viz CD