Pedagogická fakulta
Faculty of Education
Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích
Pedagogická fakulta
Katedra matematiky

Diplomová práce

Historie šifrovacích metod a jejich aplikace

Vypracovala: Bc. Eva Milichovská
Vedoucí práce: prof. RNDr. Pavel Tlustý, CSc.

České Budějovice 2018

Poděkování

Ráda bych poděkovala prof. RNDr. Pavlu Tlustému, CSc. za odbornou pomoc a cenné rady při zpracování mé diplomové práce. Dále bych chtěla poděkovat vedení ZŠ Evžena Rošického v Jihlavě za poskytnutí pomoci při ověřování pracovních listů v rámci Matematického kroužku.

Prohlášení

Prohlašuji, že svoji diplomovou práci na téma Historie šifrovacích metod a jejich aplikace jsem vypracoval(a) samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své diplomové práce, a to v nezkrácené podobě, elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích ..... ……..……

Bc. Eva Milichovská

Anotace

Ve své diplomové práci se zabývám historickými postupy šifrování a jejich aplikací ve výuce. V následujících kapitolách předkládám stručný výčet několika šifrovacích metod, jež se využívaly od starověku až do poloviny 20. století. Následně jsou v této práci připraveny i konkrétní pracovní listy na šifrování i dešifrování. U několika šifer jsou nutné pomůcky rovněž přiložené v této práci.

Annotation

I deal with historical encryption procedures and with their application in teaching in my diploma thesis. I present a brief list of some encryption methods in following chapters which were used from antiquity to the mid-20th century. There are prepared specific worksheets for encryption and decryption in this thesis. For several ciphers, the required tools are included in this work, too.

Obsah

1. Úvod ... 7

2. Základní poznatky o šifrách ... 8

2.1. Základní klasifikace ... 8

2.2. Terminologie ... 8

2.3. Definice šifrování ... 9

2.4. Abeceda ... 10

2.5. Výběr textů ... 10

2.6. Základní typy šifer ... 11

2.6.1. Transpoziční systém ... 11

2.6.2. Substituční systém ... 12

2.6.2.1. Monoalfabetická šifra ... 13

2.6.2.2. Polygrafická šifra ... 13

2.6.2.3. Polyalfabetická šifra ... 13

2.7. Frekvenční analýza ... 13

2.8. Způsoby dešifrování ... 14

2.8.1. A Cipher - only attack ... 14

2.8.2. Known-plaintext attack ... 14

2.8.3. Brute force attack ... 14

3. Matematický základ ... 15

4. Jednotlivé šifry použité v práci ... 17

4.1. Fleissnerova mřížka ... 17

4.2. Polybiův čtverec a šifra Dellastel ... 18

4.3. Monoalfabetická šifra ... 19

4.4. Složitější substituce ... 20

4.5. Afinní šifra ... 21

4.6. Vigenèrova šifra ... 21

4.7. Playfair šifra ... 23

5. Pracovní listy ... 25

5.1. Fleissnerova mřížka ... 26

5.2. Polybiův čtverec a šifra Dellastele ... 27

5.3. Monoalfabetická Caesarova šifra ... 29

5.4. Složitější substituce ... 31

5.5. Afinní šifra ... 33

5.6. Vigenèrova šifra ... 35
5.7. Playfair šifra ... 37
5.8. Fleissnerova mřížka ... 38
5.9. Polybiův čtverec a šifra Dellastele ... 39
5.10. Monoalfabetická šifra ... 41
5.11. Anglická monoalfabetická šifra ... 44
5.12. Monoalfabetická šifra – útok hrubou silou ... 47
5.13. Šifra pozpátku ... 48
5.14. Složitější substituce ... 50
5.15. Afinní šifra ... 53
5.16. Vigenèrova šifra ... 57
5.17. Playfair šifra ... 64
5.18. Šifry na několik minut ... 65
6. Výsledky pracovních listů ... 77
7. Vyhodnocení pracovních listů ... 83
8. Závěr ... 86
9. Literatura ... 87
10. Přílohy ... 89

1. Úvod

Klasická kryptografie provází lidský rod již od samého počátku vzniku písma. Při spolehnutí se na tajnou komunikaci pouze v mluvené podobě se nevylučuje změna podstaty zprávy, způsobená špatnou pamětí poslů. Kryptografie tento aspekt vyloučí, neboť není potřeba se spoléhat na lidskou paměť.

Klasickou kryptografií jsem se zabývala již ve své bakalářské práci, ve které jsem nastínila postupný vývoj kryptografie, ale především kryptoanalýzy, a to do poloviny 20. Století. Tento mezník jsem si vytyčila záměrně, neboť do této doby byla kryptografie a i kryptoanalýza doménou lidskou a ne doménou výpočetní techniky.

Cílem této diplomové práce je navázání na mou bakalářskou práci o další možné postupy šifrování zpráv bez použití výpočetní techniky a za pomoci matematických postupů zvládnutelných pro žáky základní školy. Druhým cílem této práce je poskytnutí pracovních listů do zájmových kroužků matematiky a pro šikovné žáky posledního ročníku základní školy. Protože některé listy, především ty dešifrovací, obsahují složitější rovnice k výpočtu posunu abecedy, není vhodné využívat tyto materiály pro žáky z nižších ročníků, pokud se nejedná o nadané žáky.

Kvůli zapojení mezipředmětových vztahů do mé diplomové práce odkazují veškeré texty, které pracovní listy využívají, na známá literní díla.

2. Základní poznatky o šifrách

2.1. Základní klasifikace

Tato kapitola vás seznámí se základními pojmy kryptologie, tedy vědy zabývající se utajením komunikace, ať už se jedná o její zašifrování a nebo její důmyslné schování. Pod kryptologii patří několik věd.

Kryptografie - věda, která se zabývá skrytím pravé podstaty komunikace, tedy šifrováním. Tento pojem pochází z řeckých slov kryptós – skrytý, gráphein – psát. Jako vědní disciplína se rozvíjela již od počátků rozšíření psaného slova. V dobách, kdy písmo znala pouhá hrstka vyvolených, bylo samotné písmo dostačující ochranou před neoprávněným získáním informace.

Kryptoanalýza - věda, která se zabývá odkrytím podstaty komunikace, tedy dešifrováním, zároveň zjišťuje bezpečnost šifer před jejich prolomením.

Steganografie - věda, která se zabývá schováním zprávy. Tento způsob utajení komunikace zažil svůj vrchol ve starověku, ale s postupem vývoje matematických postupů je pouhé schování nedostatečnou ochranou dat.

2.2. Terminologie

Kryptografie, stejně jako každá věda, má svou základní terminologii.

Otevřený text – text, projde procesem šifrování. V této práci se otevřený text značí Z.

Šifrovaný text (kryptogram) – text, který prošel šifrovacím procesem. V této práci se značí C.

Šifrovací systém – způsob, jakým budeme zprávu šifrovat.

Šifrovací (dešifrovací klíč) – parametr šifrování (dešifrování). Šifrovací klíč se značí K_E a dešifrovací klíč K_D.

I. **Symetrický klíč** – dešifrovací klíč lze vypočítat z šifrovacího klíče.

II. **Asymetrický klíč** – dešifrovací klíč nelze z šifrovacího klíče odvodit. Šifrování s asymetrickým klíčem se nejčastěji používá v internetové komunikaci.

Šifrování – transformace otevřeného textu do textu šifrovaného. Značí se E.

Dešifrování – transformace kryptogramu do otevřeného textu. Značí se D.

2.3. Definice šifrování

Šifrování se dá definovat jako transformace zprávy Z na kryptogram C. Kryptogram se dá považovat za veřejný, neboť není účelem šifrování zprávu schovat, ale zamezit přístup k podstatě zprávy. Aby nedošlo k prolomení šifry, je zapotřebí parametr klíč K, který vlastní pouze odesilatel a adresát. Útočník, který chce šifru dešifrovat, by neměl být schopen šifru bez znalosti klíče dešifrovat. Pokud je šifra dešifrovatelná bez znalosti klíče, nepovažuje se za bezpečnou.

Pro správné fungování šifrování a dešifrování je zapotřebí dvou takovýchto parametrů, a to klíče šifrovacího K_E a klíče dešifrovacího K_D.

Smyslem tohoto systému jsou dvě matematické funkce (transformace), které otevřený text převedou na kryptogram a naopak.

Šifrovací funkce E je prostá funkce, která je určená klíčem K_E. Dešifrovací funkce D je určena klíčem K_D.

Matematicky jde tento proces vyjádřit následovně:

$$C = E(Z, K_E).$$

Dešifrovaní pak lze popsat následovně:

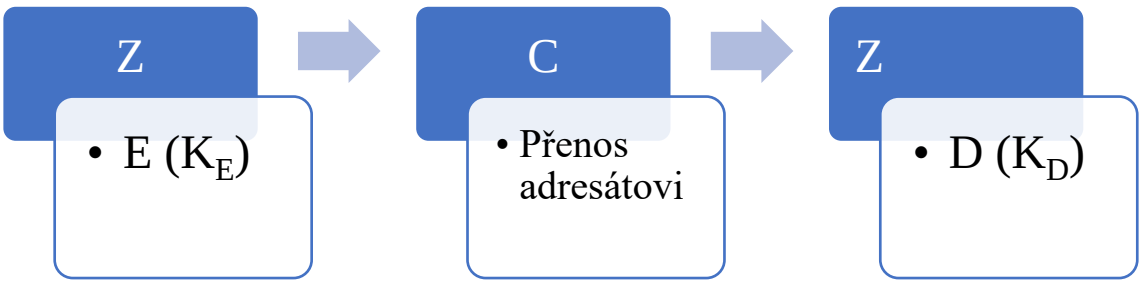
$$D(C, K_D) = Z.$$

Tento zápis dešifrování však platí pouze pro případy, kdy známe dešifrovací klíč.

Šifry, které jsou použity na pracovní listy v této práci, pracují pouze se symetrickými šifrovacími klíči, tedy takovými klíči, u nichž dokážeme poznat dešifrovací klíč z šifrovacího klíče. Proto můžeme jejich vztah vyjádřit následovně

$$K_D = f(K_E).$$

Pro šifry využívající tento způsob šifrování je nutné zachovat šifrovací klíč K_E v tajnosti.



Obrázek 1 Obecné schéma šifrovacího a dešifrovacího procesu

2.4. Abeceda

V této práci se při šifrování a dešifrování používá anglická abeceda, tedy bez háčků, a písmeno Ch se považuje za složeninu písmen C a H. Takováto abeceda obsahuje pouze 26 znaků.

U Playfair šifry a Polybiova čtverce je nutné, aby abeceda měla pouze 25 znaků, proto se zde objevuje zkrácená verze anglické abecedy, neboť se písmena I a J považují za totožné znaky.

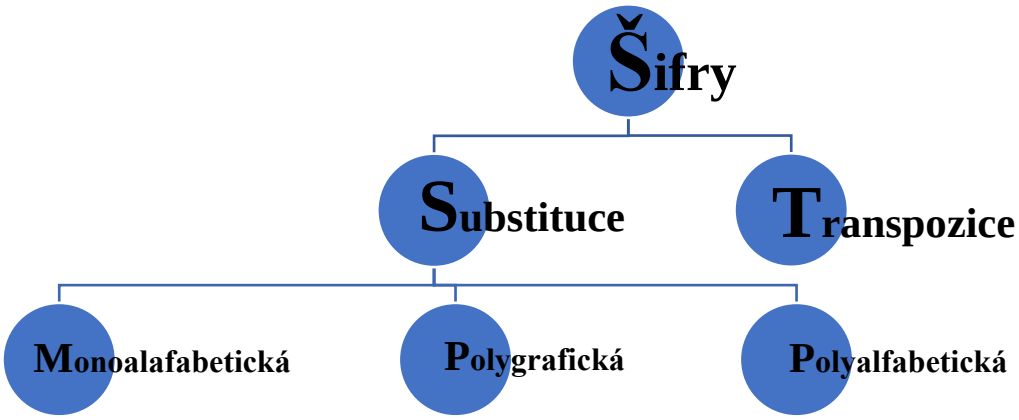
2.5. Výběr textů

Všechny texty, které jsou obsaženy v pracovních listech, poukazují na slavná literární díla, která by měli žáci na základní škole znát. Jedná se o ukázky z knihy, jméno hlavní postavy, atd.

Výběr knih i úryvků byl konzultován s vyučujícím českého jazyka a literatury na nižším gymnáziu nebo vybírán podle ŠVP základní školy Evžena Rošického v Jihlavě.

2.6. Základní typy šifer

Šifry můžeme rozdělit do dvou základních tříd, a to na šifry substituční a transpoziční.



Obrázek 2 Hierarchie šifer použitých v práci

2.6.1. Transpoziční systém

Transpoziční šifry představují určitou změnu pořadí znaků v textu. Znaky se nemění na jiné, ale pouze se v textu přeskupí podle přesně daných pravidel. Tento způsob šifrování byl populární ve starověku, ale později ztrácel svůj význam. V dnešní době je vhodný pouze pro rekreační šifrování.

Transpoziční systém můžeme popsat takto:

Budeme tvrdit, že šifra je transpoziční právě tehdy, pokud každý zašifrovaný text C je anagramem příslušného otevřeného textu Z, tj. pro každé Z, C existuje permutace $\pi(Z) = C$.

Anagramem chápeme slova, věty, které vzniknou ze skupiny písmen jejím přeskupením.

Jedna z nejznámějších transpozičních šifer se nazývá Skytale. Tento systém se používal v 7. století před naším letopočtem ve starověkém Řecku, přesněji řečeno ve Spartě. K šifrování byla využita hůl, na níž byla namotána kožená páska nebo řemínek, na tento pruh kůže se následně napsal po řádcích text. Zpráva se dešifrovala pouze za použití hole o stejném průměru, jako měla hůl šifrovací.

Obrázek 3 Transpoziční šifra Skytale

2.6.2. Substituční systém

Substituční šifry nemění pořadí znaků v textu, ale mění znaky na jiné, mohou to být jak znaky abecedy, tak zcela nové znaky, tedy byla vytvořena zcela nová šifrovací abeceda.

Substituční šifry obsažené v této práci jsou takové šifry, kdy abeceda otevřeného A_Z textu je shodná s abecedou kryptogamu A_C a kde klíč je daná permutace π této abecedy. Šifrování můžeme tady napsat jako

$$c_1, c_2, \dots, c_n = \pi(z_1), \pi(z_2), \dots, \pi(z_n).$$

Dříve však byly populární i šifry, u nichž $A_Z \neq A_C$. Marie Stuartovna[1] používala šifrovací abecedu, která nejpoužívanější písmena a slova měnila na symboly.

Existuje několik základních druhů substituce v šifrování.

[1] **Marie Stuartovna** (1542-1587) skotská královna, popravena za účast na spiknutí a svržení anglické královny Alžběty I. (1533-1603).

2.6.2.1. Monoalfabetická šifra

Při použití tohoto druhu šifrování se znaky posunují podle předem domluvené hodnoty. Rovnice takové šifry vypadá následovně

$$f(a) \equiv a + b \; mod \; 26$$

kde $f(a)$ je zašifrovaný znak, a znak, který chceme zašifrovat a b parametr, podle kterého budeme šifrovat.

Tento druh šifrování využíval například i Gaius Iulius Caesar.

2.6.2.2. Polygrafická šifra

Tento druh šifrování neprobíhá po jednotlivých znacích, ale může být prováděn i po větších skupinách znaků. Nejčastěji se provádí po skupinách o dvou znacích. Tento šifrovací systém například využívá šifra Playfair.

2.6.2.3. Polyalfabetická šifra

Tento druh šifer využívá stejně jako monoalfabetická šifra jednoduchý posun v abecedě, ale na rozdíl od monoalfabetické šifry se všechny znaky neposunují podle jednoho klíče, tedy podle jedné hodnoty, ale podle klíče s více hodnotami. Příkladem takovéto šifry je Vigenèrova šifra.

2.7. Frekvenční analýza

Velká část šifer v této práci se dá dešifrovat pouze za pomoci tzv. frekvenční analýzy nebo frekvenční analýza významně přispívá k rozluštění.

Frekvenční analýzou chápeme výpočet četnosti jednotlivých písmen v textu. Každý jazyk má své specifické znaky a nejčastější písmena. V této práci se objevuje frekvenční analýza českého a anglického jazyka. Oba jazyky mají nejčastější písmeno E, ale dále se poměrně liší.

Frekvenční analýza se využívá nejen pro znaky, ale i pro slabiky či celá slova.

2.8. Způsoby dešifrování

Vzhledem k tomu, že se část této práce zaměřuje na dešifrování jednotlivých šifer, je nutné uvést, jakými způsoby se šifra může dešifrovat. V odborné literatuře se můžeme setkat až s osmi způsoby dešifrování, ale v této práci jsou uvedeny pouze tři z nich, které se využívají v pracovních listech a které jsou také nejčastější při běžném dešifrování.

2.8.1. A Cipher - only attack

V tomto případě máme k dispozici dostatečné množství zašifrovaných zpráv k tomu, abychom bez znalosti klíče či systému tuto šifru rozluštili. Pokud je šifra rozluštitelná tímto způsobem, považuje se za nedůvěryhodnou. Většina šifer v této práci je rozluštitelná tímto způsobem.

2.8.2. Known-plaintext attack

Zde již máme k dispozici jak zašifrované zprávy, tak i jim odpovídající zprávy dešifrované. Úkolem je poznat šifrovací systém i klíč pro další dešifrování.

2.8.3. Brute force attack

Útok hrubou silou představuje postupné zkoušení všech možných klíčů pro dešifrování. Jedná se o velmi zdlouhavou činnost, neboť i jednoduchá monoalfabetická šifra, pouze s posunem písmen o jednu konstantní hodnotu, představuje v anglické abecedě 25 možností posunu. Pokud se ovšem bude jednat o jakoukoliv permutaci abecedy, máme 26! Možností. Takový počet možností není v lidských silám vyzkoušet.

3. Matematický základ

V této kapitole jsou uvedeny základní poznatky z algebry, které se využívají při šifrování a dešifrování.

Při použití substitučního systému šifer, které pracují pouze na množině abecedy, hovoříme o permutacích.

Definice 3.1.

Nechť M je konečná množina. Permutací množiny M nazveme každé vzájemně jednoznačné zobrazení množiny M na množinu M. Značíme π.

Základy modulární algebry

Rovnice šifer, které byly v této práci použity, vycházejí z modulárních rovnic.

Definice 3.2.

Nechť $a, b \in Z$. Řekneme, že a dělí b, značíme $a \mid b$, jestliže existuje $k \in Z$ tak, že $b = a \cdot k$. V opačném případě říkáme, že a nedělí b a píšeme $a \nmid b$.

Definice 3.3.

Nechť $m \in Z$. Jestliže $m \mid (a - b)$, říkáme, že a je kongruentní s b podle modulu m a píšeme

$$a \equiv b \bmod m.$$

Věta 3.1.

Nechť $a, b, c \in Z, m \in N$. Pak platí:

1. $a \equiv a \bmod m$,
2. jestliže $a \equiv b \bmod m$, pak také $b \equiv a \bmod m$,
3. pokud $a \equiv b \bmod m$ a zároveň $b \equiv c \bmod m$, pak také $a \equiv c \bmod m$.

Věta 3.2.

Nechť $a, b, c \in Z, m \in N$. Pokud $a \equiv b \bmod m$, pak

1. $(a + c) \equiv (b + c) \bmod m$,

2. $(a - c) \equiv (b - c) \, mod \, m$,

3. $ac \equiv bc \, mod \, m$.

Věta 3.3.

Nechť $a, b, c, d \in Z, m \in N$. Pokud $a \equiv b \, mod \, m$ a $c \equiv d \, mod \, m$, pak platí:

1. $(a + c) \equiv (b + d) \, mod \, m$,

2. $(a - c) \equiv (b - d) \, mod \, m$,

3. $ac \equiv bd \, mod \, m$.

Věta 4.4.

Nechť a, $b, c \in Z, m \in N$. Nechť $D(c, m) = 1$, pokud $ac \equiv bc \, mod \, m$, pak také

$$a \equiv b \, mod \, m.$$

Protože definice modulo a její vlastnosti jsou pro cílovou skupinu složité, všechny rovnice šifrování a dešifrování byly převedeny do tvaru parametrické rovnice. A proto zápis

$$a \equiv b \, mod \, m$$

v pracovních listech nahradí zápis

$$a = b - km$$

kde k je parametr, $k \in \mathbb{N}_0$ a m je pro nás počet znaků v abecedě, tedy 26.

Výše popsané vlastnosti kongruencí platí i pro upravené rovnice šifrování.

4. Jednotlivé šifry použité v práci

4.1. Fleissnerova mřížka

Fleissnerova[2] mřížka pravděpodobně vychází z mřížky Hieronyma Cardana[3], jenž vytvořil jednoduchou transpoziční šifru. Sestrojil tabulku ve tvaru čtverce, jež měla na určených místech vyřezané otvory. Tato tabulka se pokládala na papír a do vyřezaných okének se napsal test, po odstranění tabulky se do vzniklých mezer v textu napsaly další znaky nebo symboly.

Fleissnerova mřížka využívá stejnou čtvercovou tabulku, ale v případě této šifry se tabulka při šifrování dalšího textu otáčí o 90° doleva.

Při sestavování takové šifry je nutné správně určit všechny polohy námi vybraného políčka, neboť se při otočení o 90° posune do jiného kvadrantu. Jedno políčko tedy zaujme hned 4 polohy. Pro zjednodušení lze mřížku 8×8 rozdělit na 4 kvadranty.
V těchto kvadrantech pak od počátečního krajního bodu budeme další políčka číslovat od 1 do 16.

Při šifrování pak nesmíme dané políčko využít, pokud jsme již vybrali, vyřízli políčko se stejným číslem.

Mřížka přiložená v této práci slouží i k dešifrování, neboť bez této pomůcky je dešifrování velmi dlouhavé. Nejdůležitější je najít první polohu čtverce, při které se začínalo šifrovat.

[2] **Edouard Fleissner von Wostrowitz** (1825 – 1888) – rakouský vojenský důstojník.
[3] **Hieronymus Cardanus** (1501 – 1576) – italský matematik, filosof, astronom.

1	2	3	4	13	9	5	1
5	6	7	8	14	10	6	2
9	10	11	12	15	11	7	3
13	14	15	16	16	12	8	4
4	8	12	16	16	15	14	13
3	7	11	15	12	11	10	9
2	6	10	14	8	7	6	5
1	5	9	13	4	3	2	1

Obrázek 4 Fleissnerova mřížka před vyříznutím políček

1	2	3	4	13	9	5	1
5	6	7	8	14	10	6	2
9	10	11	12	15	11	7	3
13	14	15	16	16	12	8	4
4	8	12	16	16	15	14	13
3	7	11	15	12	11	10	9
2	6	10	14	8	7	6	5
1	5	9	13	4	3	2	1

Obrázek 5 Fleissnerova mřížka po vyříznutí několika políček

4.2. Polybiův čtverec a šifra Dellastel

Polybiův[4] čtverec je substituční systém, pracující na principu udělení každému písmenu abecedy souřadnice ve čtverci 5×5. Do takového čtverce se napíší všechny znaky abecedy. Protože znaků abecedy je 26, je nutné buď nějaký znak vynechat, nebo -

[4] **Polybios** - helenistický historik, 210-120 př. n. l.

jako je tomu v této práci - ztotožnit písmena I a J. Znaku, který chceme zašifrovat, odpovídají dvě čísla, číslo řádku a číslo sloupce.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Obrázek 6 Polybiův čtverec

Systém Dellastel, v literatuře se setkáváme i s označením BIFID, je složitější než Polybios, ale vychází ze stejného principu. Do čtverce 5×5 se nejprve napíše šifrovací slovo, ve kterém se nesmí opakovat znaky, a následně zbytek znaků. Dále se otevřený text zašifruje jako při použití Polybiovy šifry, ale souřadnice se nepíší do řádku, nýbrž pod sebe, vzniknou tak dva řádky čísel. Následně se v řádku vytvářejí dvojice čísel. Tyto dvojice čísel nám v prvotním čtverci určují pozici znaku, který již považujeme za zašifrovaný.

4.3. Monoalfabetická šifra

Nejslavnější šifra tohoto typu je jistě Caesarova[5] šifra, tedy posun v abecedě o 3. V některé literatuře se ale můžeme setkat s označením Caesarovy šifry jako každé monoalfabetické šifry s libovolným posunem.

Caesar se o této šifře zmínil ve svém díle Zápisky o válce galské[6], stejně se s ní můžeme setkat v Životopisech dvanácti císařů[7].

Caesar k dešifrování využil i tzv. Caesarův kotouč, což byly dvě kruhovité desky položené přes sebe, na jejichž okrajích byly vyryty znaky abecedy. Otáčením kotouče

[5] **Gaius Julius Caesar** (100-44 B.C.) – římský diktátor.
[6] CAESAR, Gaius Julius. Zápisky o válce galské. Praha 2009.
[7] SUETONIUS TRANQUUILLIS, Gaius. Životopisy dvanácti císařů. Praha 1998.

do správné polohy tak získal na jednom kotouči šifrovanou abecedu a na druhém abecedu dešifrovanou.

Obrázek 7 Caesarův kotouč

Tato šifra je velmi jednoduchá a má pouze jedno omezení, co se týče posunu. Pokud se abeceda bude posouvat pouze o $26k$, kde $k \in N$, abeceda se v podstatě neposune.

Je vhodné ukázat, jaký je rozdíl, pokud se abeceda posune o b znaků a následně o $b + 26$ znaků.

Dešifrování probíhá pomocí frekvenční analýzy, a to poznáním posunu abecedy z grafu nebo výpočtem posunu pomocí rovnice.

4.4. Složitější substituce

Tento druh šifry je již o něco složitější, neboť k prvku otevřené abecedy se nic nepřičítá, ale násobí se číslem n. Proto se posloupnost abecedy nezachovává a pokud je například A zašifrované za N, B nemusí být O. Z tohoto důvodu je nutné vypočítat hodnotu všech znaků v abecedě podle zadané rovnice

$$f(a) = an - 26k.$$

Podmínkou pro využití této šifry je, aby prvek n byl nesoudělný s 26, tedy aby $D(n, 26) = 1$. S touto podmínkou se setkáme i u dešifrování, neboť nám mohou vyjít

dva výsledky, a to číslo soudělné a nesoudělné s 26. V pracovních listech jsou tyto podmínky uvedeny.

Zároveň n může nabývat i hodnot $n + 26k$ a šifrovací abeceda zůstává stejná.

Tuto šifru již nelze vyluštit pouze frekvenční analýzou, ale velmi nám pomůže. Stačí objevit nejfrekventovanější písmeno v zašifrovaném textu, o kterém budeme předpokládat, že je E. Následně stačí odsadit číselný ekvivalent písmene E a písmena, které mu náleží do vzorce a vypočítat prvek n.

4.5. Afinní šifra

Afinní šifra se dá považovat za kombinaci monoalfabetické šifry a šifry, jež je zde uvedená jako složitější substituce.

Rovnice takové šifry vypadá následovně

$$f(a) = an + b - 26k.$$

Podmínky této šifry jsou stejné jako u monoalfabetické šifry a u složitější substituce. Pokud bude b k-násobek čísla 26, tento posun nejde rozpoznat a tudíž se z afinní šifry stane složitější substituce. Prvek n, kterým násobíme znak otevřené abecedy, musí být nesoudělný s 26.

Dešifrování je složitější, neboť je potřeba najít dva nejvyužívanější znaky, odhadnout jejich hodnotu v otevřené abecedě a následně je dosadit do rovnic.

4.6. Vigenèrova šifra

Vigenèrova šifra je jediná polyalfabetická šifra v této práci. Jejím tvůrcem je Blaise de Vigenèr[8], který se nechal inspirovat systémem Johanna Trithemia[9] a Giovaniho Battista Bellasia[10]. Pravděpodobně ve svém díle „Traicté de Chiffres“ Vigenèr prohlásil, že „*všechno na světě je zašifrované od Boha a poznat to je možné jen tak, když to dešifrujeme*“

[8] **Blaise de Vigenèr** (1523-1596) – francouzský diplomat.
[9] **Johannes Trithemius** (1462- 1516) – německý mnich a kryptolog.
[10] **Giovani Battista Bellaso** – italský kryptolog.

Tento systém využívá posun abecedy, ale ne o jednotnou hodnotu u všech znaků. Základem šifrování je heslo, slovo nebo celá věta. První znak otevřeného textu se přičte k prvnímu znaku hesla, druhý znak z textu se přičte k druhému znaku hesla, atd.

Šifrování takovýmto způsobem je velmi dlouhavé, proto se při šifrování tímto principem využívá tzv. Vigenèrův čtverec. Tento čtverec v prvním řádku obsahuje znaky otevřené abecedy a v prvním sloupci znaky hesla, kde se protne sloupec znaku A_Z s řádkem znaku hesla, vyjde dešifrovaný znak.

Pro dešifrování se využívá tzv. Kasiského test, tento test vyhledává možné délky hesla, neboť pokud je známa délka hesla Vigenèrovy šifry, je možné šifru rozdělit do oddílů, které byly zašifrovány stejným znakem hesla. Tím nám vznikne několik monoalfabetických šifer, které jsou na luštění jednoduché. Tento test hledá v kryptogramu stejné shluky písmen. Tyto shluky pravděpodobně vznikly, když se stejné znaky zašifrovaly stejnou částí hesla. Dále se určí vzdálenost těchto shluků a dělitelé těchto vzdáleností, neboť tento dělitel nám určí délku hesla. Které číslo se nejčastěji objeví mezi děliteli, bude pravděpodobně délkou hesla.

Kvůli velké časové náročnosti byl tento test v pracovních listech již proveden.

	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	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
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	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Obrázek 8 Zašifrování písmene M podle hesla R

4.7. Playfair šifra

Šifra Playfair byla objevena Charlesem Wheatsonem v druhé polovině 19. století, ale popsal ji až Lyon Playfair[11], jehož jméno nese. Jedná se o polygrafickou substituční šifru, která byla využívaná v búrských válkách[12] a 1. světové válce.

Šifrování probíhá za pomoci čtverce 5×5, do něhož se napíše heslo, ve kterém se nesmí opakovat znaky. Do zbytku políček se popořadě napíše zbytek abecedy. Následně se zpráva rozdělí do dvojic znaků, tedy bigramů. Tyto bigramy se šifrují podle těchto pravidel.

1. Pokud se oba znaky v tabulce nacházejí na stejném řádku, každý znak se nahradí znakem ležícím o jedno políčko vpravo. Pokud je znak na konci řádku, nahradí se znakem ze začátku řádku.

[11] **Lyon Playfair** (1818-1898) skotský politik.
[12] Války osadníků jižní Afriky proti Britskému imperiu, 1899-1902.

2. Pokud se oba znaky v tabulce nacházejí ve stejném sloupci, každý znak se nahradí znakem ležícím o jedno políčko dole. Pokud je znak na konci sloupce, nahradí se znakem na začátku sloupce.
3. Pokud jsou písmena v jiném řádku i sloupci, každé se nahradí znakem ležícím ve stejném řádku jako původní písmeno, ale sloupci jako druhý znak.

5. Pracovní listy

Následující kapitola této práce obsahuje jednotlivé pracovní listy. První část se zabývá šifrováním textu, kdežto druhá část je zaměřená na dešifrování. Listy ze sebe vycházejí a princip v jednom listu se rozvíjí v dalším listě, takže je vhodné žákům listy předkládat v daném pořadí.

Poslední část se zaměřuje na úlohy pouze na několik minut. Předpokládá se znalost principů v této práci již popsaných.

V předposlední části této práci se nacházejí výsledky všech úloh, které jsou až na šifrování Fleissnerovou mřížkou jednoznačné. Pro šifrování mřížkou jsou uvedeny čtyři možnosti šifrování.

Časová náročnost se u listů liší. Listy se se složitější substitucí, afinní šifrou a Vigenèrovou šifrou vyžadují celou vyučovací hodinu, tedy 45 minut. Zbylé listy žáci zvládají vyřešit průměrně dva za vyučovací hodinu.

5.1. Fleissnerova mřížka

Tento list tě seznámí s jednoduchým způsobem šifrování, tzv. transpozicí. V tomto případě nebudeš měnit písmena ve zprávě na jiná písmena nebo znaky, ale pouze je jinak přeskupíš. Pro naši Fleissnerovu šifru budeš potřebovat pomůcku, tedy speciální mřížku, která ti umožní napsat písmena do předem připravených okének. Na připravenou tabulku polož mřížku a po sloupcích začni psát znaky zprávy, poté tuto mřížku otoč o 90° doleva a začni znovu psát, tak pokračuj, dokud mřížku 4krát neotočíš. Pokud je zpráva příliš dlouhá, vytvoř druhou tabulku a pokud je zpráva moc krátká, do zbylých okének napiš znaky X. Mřížka může mít různé rozměry, ale musí se jednat o čtverec.

Zkus tedy zašifrovat tento text.

Text: Gilgameš se stal králem Uruku z vůle a milosti bohů, a to jako pátý vladař.

Do této tabulky můžeš šifru zašifrovat.

Je možné, aby tvému kamarádovi vznikla úplně jiná šifra? Proč je tomu tak?

5.2. Polybiův čtverec a šifra Dellastele

Teď tě již čekají šifry substituční, tedy šifry, kde se písmena neboli znaky mění na jiné znaky. Tento list tě seznámí s Polybiovým čtvercem, což je šifra stará více než 2000 let. Na zašifrování zprávy se používá čtverec, který má 5×5 políček, do těchto políček se vepíše celá abeceda, protože v abecedě je 26 znaků, bude pro tebe písmeno I stejné jako J. Ve zprávě jsou háčky i čárky, ale ty při šifrování zanedbej. A teď už budeš pouze ke každému znaku zprávy hledat jeho souřadnice, tedy číslo řádku a sloupce. Mezi každé dvojčíslí, tedy mezi souřadnice každého písmena, dej pomlčku, celá šifra bude srozumitelnější.

Zpráva: Hrdliččin zval ku lásce hlas, kde borový zaváněl háj.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Jak zní tento literární úryvek zašifrovaný?

……

……

……

Jak se jmenuje kniha, ze které je tento úryvek, a kdo je jejím autorem?

…….

Protože se jedná o jednoduchou šifru, zkusíme složitější verzi, a to šifru Dellastele. Tato šifra používá podobný princip jako Polybios, ale písmena v tabulce nemusejí být seřazená podle abecedy. Následně se do druhé připravené tabulky píší číselné souřadnice znaků, ale do řádku, co jedna buňka, to jedna číslice. Po zaplnění prvního řádku se další souřadnice napíší do řádku pod ním. Tak nám vzniknou dva

řádky souřadnic, ze kterých vytvoříme šifru. Číslo z prvního řádku označuje číslo řádku tabulky a číslo pod ním určuje číslo sloupce.

	1	2	3	4	5
1	M	H	E	I	C
2	G	B	V	L	S
3	R	X	T	W	F
4	Z	U	K	A	P
5	Q	D	O	Y	N

Do připravené tabulky zašifruj následující zprávu. Do prvního, tučně vyznačeného řádku napiš až konečné znění šifry.

Text: Vita Caroli

O kterém českém panovníkovi daná kniha pojednává?

.....

5.3. Monoalfabetická Caesarova šifra

Tento pracovní list tě seznámí pravděpodobně s nejznámější starověkou šifrou, jedná se o tzv. Caesarovu šifru. Tato šifra funguje na principu posunu písmen v abecedě. Každému písmenu přiřadíš jeho číselný ekvivalent A=0, B=1, ….. Z=25. K tomuto číslu nyní připočteme námi zvolené číslo, které jsme si domluvili s adresátem, toto číslo se značí b. V některých případech dostaneš číslo větší než 25, v těchto případech od takového čísla odečti 26, tedy jeden cyklus celé abecedy. Rovnice takovéto šifry pak vypadá následovně

$$f(a) = a + b - 26k$$

kde $f(a)$ je číselný ekvivalent zašifrovaného znaku, a je ekvivalent znaku, který chceme zašifrovat, b je hodnota posunu v abecedě a k mohou být všechna přirozená čísla včetně nuly, tedy $\mathbb{N}_0$.

Abys dokázal, že jsi zadání pochopil, zašifruj daný text, když $b = 3$, stejně tak, jak to Gaius Julius Caesar ve skutečnosti dělal.

Text: Orfeus, Midas, Iásón a Médea, Theseus, Prometheus, O zlatém rounu, Daidalos a Ikaros.

Zde máš prostor pro nezbytné výpočty.

Do následující tabulky napiš, jak se které písmenko zašifruje.

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 teď celou zprávu můžeš zašifrovat.

……

……

……

Poznal jsi, z jaké knížky pocházejí tyto kapitoly a kdo je jejich autor?

……

5.4. Složitější substituce

Nyní tě čeká šifra, která je mezistupněm mezi Caesarovou šifrou a šifrou afinní, která tě čeká později. V této šifře nebudeš k číselným ekvivalentům písmen přičítat žádná čísla, ale budeš násobit číslem, které budeme nazývat n. Jedinou podmínkou je násobit číslem nesoudělným s číslem 26, tedy s počtem znaků abecedy.

Rovnice dané šifry vypadá následovně

$$f(a) = an - 26k$$

kde $f(a)$ je zašifrovaný znak, a znak, který chceme zašifrovat a k mohou být všechna přirozená čísla včetně nuly, tedy $\mathbb{N}_0$.

Zašifruj tedy daný text, pokud jsme zvolili $n = 11$.

Nejdříve si připrav tabulku, která ti ukáže, jak se konkrétní znaky šifrují. V daném rámečku proveď konkrétní výpočty a následně doplň do tabulky výsledky.

Do tabulky doplň, jak se které písmeno zašifruje.

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 nyní zašifruj tento úryvek z knihy.

Text: Robinson, spatřiv Pátka, pokývl, aby vstoupil k němu do stáje.

Šifra:

……

……

……

Poznáš, z jakého literárního díla je tato věta?

……

5.5. Afinní šifra

Tento pracovní list tě seznámí s tzv. afinní šifrou. Nejprve si musíš rozmyslet dva parametry, podle kterých se bude šifrovat, budeme jim říkat n, b. Poté, co opět převedeš abecedu na číselné ekvivalenty, číslem n tento ekvivalent vynásobíš a ještě k tomu přičteš druhý parametr b. Podmínkou pro tento druh šifry je, aby n bylo nesoudělné s 26.

Rovnice takové šifry vypadá následovně

$$f(a) = an + b - 26k$$

kde $f(a)$ je zašifrovaný znak a k mohou být všechna přirozená čísla včetně nuly, tedy $\mathbb{N}_0$.

Tento rámeček máš připravený pro výpočty. Připrav si šifrovací abecedu, pokud naše parametry pro šifrování budou $n = 5, b = 2$.

Do následující tabulky napiš šifrovací abecedu.

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

Nyní, když již máš přichystanou abecedu, zkus zašifrovat danou ukázku z knihy a opět zkus přijít na autora a knihu, ze které daná ukázka pochází.

Text: Copak je po jméně. Co růži zvou, i zváno jinak vonělo by stejně.

Jak tedy zní zašifrovaná zpráva?

……

……

……

A kdo je jejím autorem a ze kterého jeho díla úryvek pochází?

……

5.6. Vigenèrova šifra

Nyní tě čeká tzv, Vigenèrova šifra, jež byla po dobu 300 let považována za nerozluštitelnou. Jejím autorem je francouzský diplomat ze 16. století Blaise de Vigenèr. V této šifře budeš stejně jako u Caesarovy šifry posouvat písmena v abecedě. Pro tento posun si odesílatel a příjemce domluví heslo, tedy slovo nebo i celou větu, podle které se budou jejich zprávy šifrovat. Text zprávy stejně jako heslo se převede na číselné ekvivalenty a následně se sečte první písmeno zprávy s prvním písmenem hesla, druhé s druhým atd. Heslo se dále bude opakovat, dokud tímto stylem nezašifruješ celou zprávu.

Zpráva: Zemřela matka a do hrobu dána, siroty po ní zůstaly; i přicházely každého rána a matičku svou hledaly.

Heslo: Erben

Aby se ti lépe šifrovalo, jako pomůcku využij tzv. Vigenèrův čtverec. V prvním řádku vyhledej písmeno ze zprávy a v prvním sloupci zase odpovídající písmeno z hesla. Tam, kde se řádek a sloupec protnou, máš zašifrované písmeno podle hesla.

	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	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
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	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Zašifrovaná zpráva:

……

……

……

Dokážeš určit, z jaké knihy je daný úryvek?

.....

5.7. Playfair šifra

Tento list tě seznámí se šifrou, která byla používána za 1. světové války. Tato šifra bude pracovat stejně jako Polybios se čtvercem 5×5, do kterého se napíše abeceda, i v tomto případě budou znaky I a J totožné. Nejprve se do této tabulky napíše heslo, tedy slovo, které jsme si spolu s příjemcem předem domluvili. V tomto hesle se nesmí opakovat písmena. Následně se do tabulky postupně napíší po řadě zbylé znaky abecedy. Podle takto připravené tabulky se následně bude šifrovat.

Naši zprávu, kterou chceme odeslat, si rozdělíme na skupinky po dvou znacích, pokud je ve zprávě lichý počet znaků, přidáme na konec zprávy znak X. Šifrování probíhá podle těchto tří pravidel.

1. Pokud jsou oba znaky ve stejném řádku, zamění se za znaky ležící o jedno místo napravo. Pokud je znak na konci řádku, zamění se za znak na začátku stejného řádku.
2. Pokud jsou oba znaky ve stejném sloupci, zamění se za znak ležící o jedno místo dole. Pokud je znak na konci sloupce, zamění se za znak na začátku stejného sloupce.
3. Pokud jsou znaky v různých řádcích a sloupcích, nahradí se za znak ve stejném řádku, ale ve sloupci, jako je druhý znak.

Nyní se pokusíš zašifrovat text podle hesla: NEMCOVA.

Text: Babicka

Sestav tedy šifrovací tabulku a podle ní šifruj.

Jak zní šifra?.....

5.8. Fleissnerova mřížka

S Fleissnerovou mřížkou ses už setkal, nyní ale nebudeš šifrovat, ale dešifrovat. V tabulce je zašifrovaná fráze z velmi populární knihy, přilož na tabulku mřížku a zkus zjistit, která kniha se v šifře ukrývá. Opět budeš daný text číst po sloupcích a nezapomínej danou mřížku 4krát otočit doleva.

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

Dešifrovaná zpráva zní: …….

……

……

Ze které knihy pochází tato ukázka a kdo je jejím autorem?

.....

5.9. Polybiův čtverec a šifra Dellastele

Šifrování pomocí Polybiova čtverce je velmi jednoduché a stejně tak i dešifrování. V předkládaném čtverci máš všechna písmena abecedy kromě J, místo tohoto písmene budeš používat písmeno I. Každé políčko ve čtverci má své souřadnice, číslo řádku a číslo sloupce. Tato dvojice čísel je pro nás šifrou.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Následující šifra označuje jméno hlavní postavy známé knihy.

Šifra: 25-11-44-33-24-43-43-15-51-15-42-14-15-15-33

O jakou postavu se jedná a z jaké je knihy?

…….

Šifra Dellastele

Předcházející šifra byla velmi snadná, proto se teď pokusíš dešifrovat složitější šifru Dellastele. Tato šifra taky využívá čtverec s písmeny, ale oproti Polybiovi zde nemusejí být písmena poskládána podle abecedy, ale tak, jak si odesílatel a příjemce zprávy domluvili. Tvým prvním úkolem je přiřadit písmenům číslo řádku a sloupce a doplnit je po řádcích do dané tabulky. První řádek si ponechej volný, do něj napíšeš písmeno, které odpovídá souřadnicím pod ním. První souřadnice je číslo řádku, číslo pod ním je číslo sloupce.

Šifra: AVAKGRDHMQOK

	1	2	3	4	5
1	N	D	L	G	I
2	H	X	Q	U	R
3	T	C	W	B	O
4	P	Z	F	S	A
5	K	E	V	M	Y

Tuto tabulku použij pro zápis souřadnic znaků.

Která postava se skrývá v dané šifře?.....

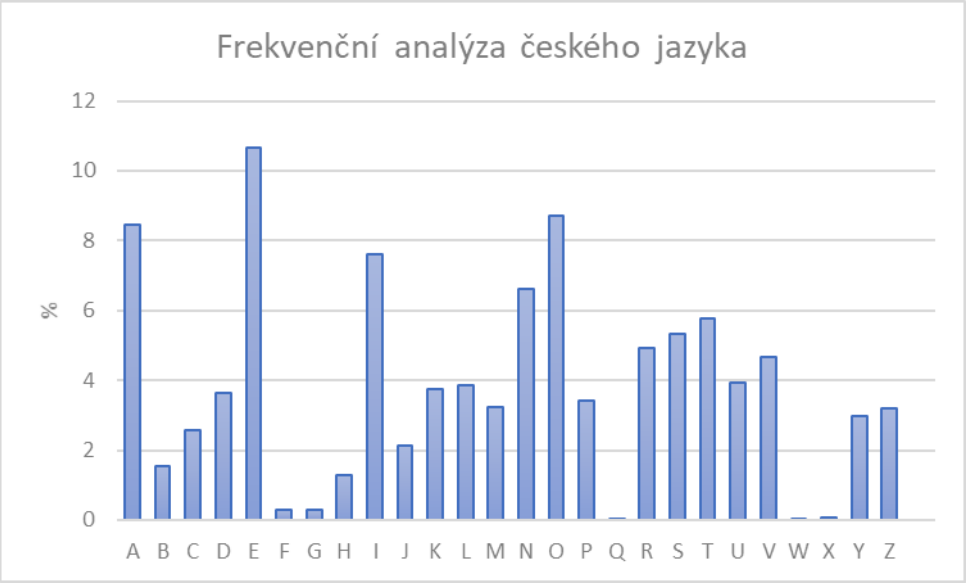
5.10. Monoalfabetická šifra

Tento list je zaměřen na dešifrování jednoduché monoalfabetické šifry. K jejímu prolomení nám postačí jednoduchá frekvenční analýza, tedy počet znaků jednoho druhu (např. A) v dané šifře porovnaný s počtem stejného znaku v průměrném textu. Daný zašifrovaný úsek opět poukazuje na slavnou knihu. Dokážeš poznat, o jakou knihu se jedná?

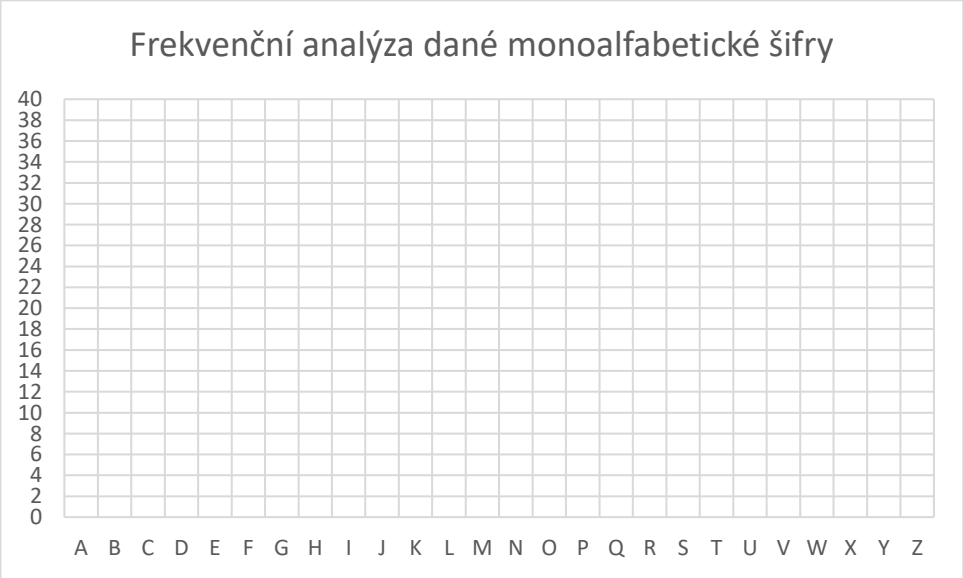
JWFLT SEFPQ JPQIT ZIZXF SJMTY WFASN PZFEP ZXJSD RTPJR UWJQJ YQXYT UDUTI QJTYN XPZGD QFEAJ WSFQT ZHJXT YAFUW JIUZQ MTINS TZGWE DXJZQ TENPJ XUFSP ZOJMT PTWNX YRFQF XWSFP YJWFA DWFES JPZQM FQFSF QJATZ UWJIS NSTMZ GDQFX YFQJX JXYFI JRUWJ PAFUT AFQTM TEJON OJXYJ SJEFM ZGNQA QPSJG TRJIA JISJG JGDQT HNXYJ FUTYJ RSJQJ KTZPF QRNWS DANYW PTQJR JWFLT SFXJY DHNQD MTWDF SFISN RNXJS JXQXY WNGWS DRWFP OJMTT PWFOJ UQFQD HJWAJ SDRXA JYQJR OFPOJ TXAJH TAFQR JXNHA ZUQSP ZXYTO NHNSF TGQTE JRJEN IAJRF EFXSJ EJSDR NAWHM TQPD

A	B	C	D	E	F	G	H	I	J	K	L	M
17	0	0	16	12	37	9	8	11	54	1	2	10
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
20	8	20	31	16	27	34	12	0	22	23	17	17

Tato tabulka ukazuje četnost jednotlivých písmen v šifře, v této podobě se však s obtížemi dá poznat, o kolik písmen se šifrovací abeceda posunula. Abys to poznal, zadej hodnoty do grafu, bude to přehlednější. Následně porovnej s frekvenční analýzou českého jazyka. Najdi v grafu nejčastější písmena, najdi mezi nimi stejné rozestupy.



Do dané tabulky nakresli graf četnosti znaků šifry a porovnej je s horním grafem.



Jinou metodou, jak zjistit posun abecedy, je její výpočet. Najdi nejpoužívanější písmeno v šifře, můžeš předpokládat, že se jedná o písmeno E. Nyní číselný ekvivalent tohoto písmena použij v následující rovnici pro dešifrování monoalfabetické šifry. Jedná se o parametrickou rovnici, kdy pro nás bude b neznámá a k parametr.

$$a = f(a) - b + 26k$$

$f(a)$ je číselný ekvivalent zašifrovaného znaku, a je ekvivalent znaku, který v dané šifře odpovídá $f(a)$, b je hodnota posunu v abecedě a k mohou být všechna přirozená čísla včetně nuly, tedy $\mathbb{N}_0$.

Doplň následující tabulku, která ti ukáže, jaké písmeno se zašifrovalo na jaké, a pomocí této tabulky dešifruj zprávu.

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

Abys poznal knihu, dešifruj následující část šifry, pro lepší přehlednost písmeno, které jsi již dešifroval, zaškrtni, bude to přehlednější.

JWFLT SEFPQ JPQIT ZIZXF SJMTY WFASN PZFEP ZXJSD RTPJR UWJQJ YQXYT

Dešifrovaný text: ……

…….

O jakou knihu se tedy jedná a kdo je jejím autorem?

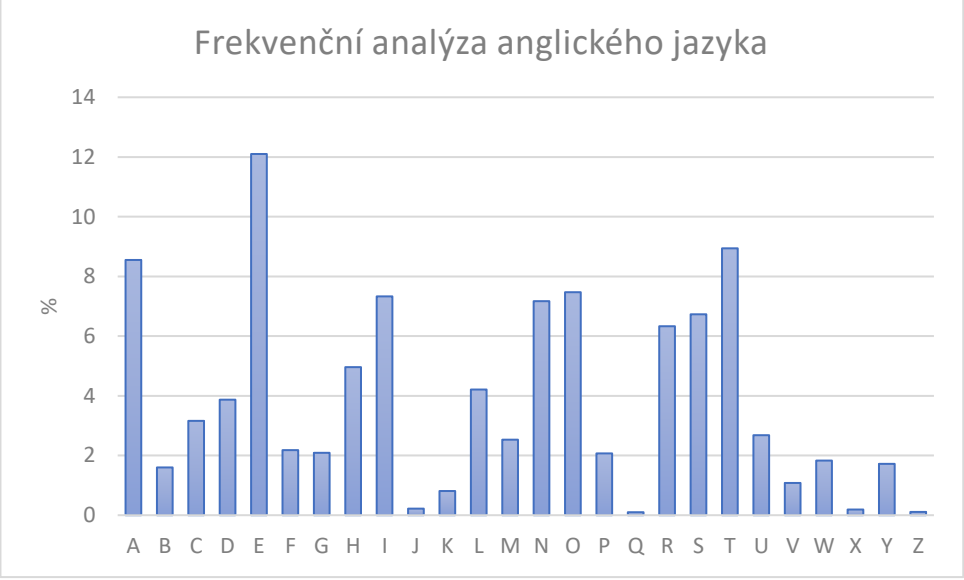
……

5.11. Anglická monoalfabetická šifra

Při řešení tohoto listu si ukážeme, jak je nutné znát nebo alespoň předpokládat, v jakém jazyce je daný text napsán, neboť frekvenční analýza se u různých jazyků liší. Daný text je anglicky, pochází z velmi známé dětské knihy. Tučně zvýrazněný text poukazuje na hlavní postavu. Dokážeš vyluštit, o jakou knihu se jedná?

Šifrovaný text:
DOHAZ FVBYU HTLOL HZRLK DLUKF TVPYH HUNLS HKHYS PUNZO LYLWS PLKDP AOZVT LZHAP ZMHJA PVUDO HAPZF VBYUH TL**WLA LYWHU** ZOLDH ZHSYL HKFZB YLAOH AOLTB ZAILW LALYI BAPAK PKZLL THJVT WHYHA PCLSF ZOVYA UHTLP ZAOHA HSSFL ZOLZH PKYHA OLYZO HYWSF OLMLS AMVYA OLMPY ZAAPT LAOHA PADHZ HZOVY APZOU HTL

Daný graf nám ukazuje frekvenční analýzu anglického jazyka. Je vidět, že se od českého jazyka částečně liší.



Tabulka četností písmen v naší šifře vypadá následovně.

A	B	C	D	E	F	G	H	I	J	K	L	M
25	5	1	6	0	7	0	29	2	2	8	31	4
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	18	16	0	1	9	10	9	9	6	0	17	21

Doplň následné hodnoty do tabulky a zjisti, podle kterého písmene se šifrovalo. Najdi nejčastější písmena, najdi mezi nimi stejné rozestupy, jako jsou v grafu frekvenční analýzy anglického jazyka.

Podle kterého písmena se šifrovalo? ……..

Pokud ti graf nepomohl s nalezením posunu abecedy, zkus ho vypočítat podle této rovnice

$$a = f(a) - b + 26k$$

$f(a)$ je číselný ekvivalent zašifrovaného znaku, a je ekvivalent znaku, který v dané šifře odpovídá $f(a)$, b je hodnota posunu v abecedě a k mohou být všechna přirozená čísla včetně nuly, tedy $\mathbb{N}_0$.

Zde máš prostor pro nezbytné výpočty.

Doplň následující tabulku, která ti ukáže, jaké písmeno se zašifrovalo na jaké.

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

Dokážeš rozluštit danou část šifry, ve které se skrývá hlavní postava známého literárního díla?

WLALY WHU

Pokud si poznal posun abecedy, které vlastní jméno je v šifře tučně zvýrazněno?

……..

5.12. Monoalfabetická šifra – útok hrubou silou

Tento list ti ukáže, jak je frekvenční analýza textu důležitá. Dešifruj zprávu, u které je tato analýza zbytečná, neboť má málo znaků na to, aby se zde projevily specifické znaky jednotlivých písmen.

Znění šifry

PIVAK PZQAB QIVIV LMZAM V

Text byl zašifrován jednoduchou substitucí, ale posun abecedy je neznámý, toto číslo však není větší než 9, neboť zkoumat všechny možné posuny je velmi časově náročné.

V prvním řádku připravené tabulky je napsaná šifra, v prvním sloupci posuny abecedy, které musíš vyzkoušet. U jednoduché monoalfabetické šifry je těchto posunů dohromady 25, ale v tomto případě víme, že maximální posun je 9. Do připravených políček tedy začni vypisovat, jak by vypadala dešifrovaná zpráva, pokud předpokládáš, že se zpráva šifrovala s posunem 1, 2, atd.

	P	**I**	**V**	**A**	**K**	**P**	**Z**	**Q**	**A**	**B**	**Q**	**I**	**V**	**I**	**V**	**L**	**M**	**Z**	**A**	**M**	**V**
-1																					
-2																					
-3																					
-4																					
-5																					
-6																					
-7																					
-8																					
-9																					

Dešifrovaný text:……..

5.13. Šifra pozpátku

Šifra pozpátku není nic složitého a sama o sobě nemůže být využita k ochraně dat ani při rekreačním šifrování. Velmi jednoduše se však dá využít jako klamač při použití s dalším druhem šifrování. Tím se zvyšuje účinnost celého šifrovacího systému. Stačí již zašifrovanou zprávu napsat pozpátku.

Šifra v tomto listě byla zašifrovaná jednoduchou substitucí, poznej posun i to, ze které knihy je daný text. Pro poznání knihy nemusíš dešifrovat text celý, ale pouze takovou část, která ti pomůže s poznáním knihy.

Text:

GSXIZ LPKQV IVIGS ZIBAT WXMTI UMDWS IBUWV MRSMD WTKIU WSIRG BAZXQ RIUMV PKISK QXITB PKMBI VIGSK QXITB MVDWS QAMVI MTIUQ RIUMH WBWZX QTMUC MVSIB GSKGL HDWBQ VWMTI MLQTQ KTMDQ RITML WBSIR SIBBI TMLWV PKMAD QTMBP KIQTM TLGJC TWXAU IBISM KMUWL RCDAI AMTCQ TMUQT QZILX AWPCT WXAMB AMRIS KQKWS IUMSA RMXGL SBIZS VMBWT GJWB

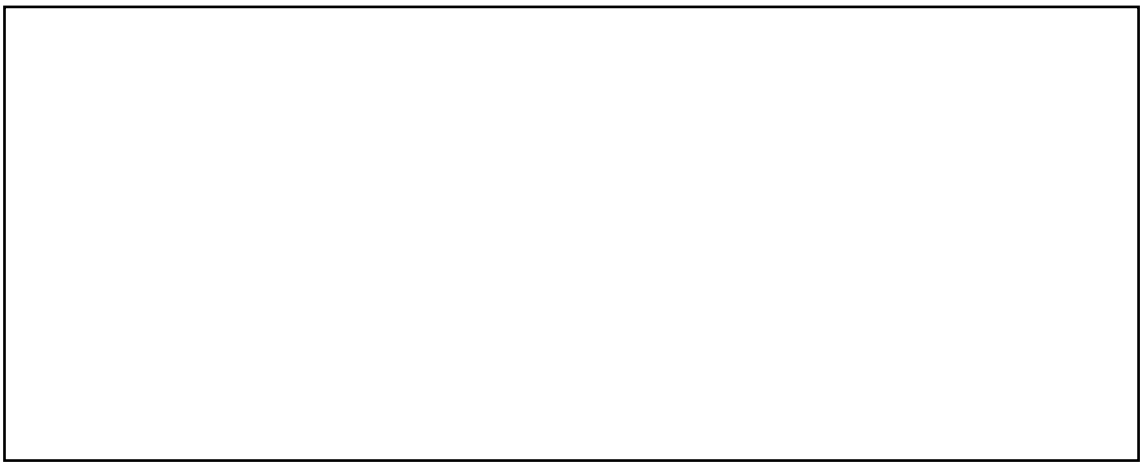
Frekvenční analýza textu vypadá následovně

A	B	C	D	E	F	G	H	I	J	K	L	M
11	18	5	7	0	0	9	3	31	2	13	0	29
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	0	6	17	9	18	21	11	11	20	10	0	6

Opět využij rovnici pro výpočet posunu abecedy.

$$a = f(a) - b + 26k$$

$f(a)$ je číselný ekvivalent zašifrovaného znaku, a je ekvivalent znaku, který v dané šifře odpovídá $f(a)$, b je hodnota posunu v abecedě a k mohou být všechna přirozená čísla včetně nuly, tedy $\mathbb{N}_0$.



O jaký se jedná posun v abecedě?.....

Doplň dešifrovací tabulky a dešifruj zprávu, ale odzadu, neboť tam se nachází začátek otevřeného textu.

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

Dešifrovaný text:

…….

……

……

Autor knihy:……

5.14. Složitější substituce

Následující šifra bude o poznání složitější než předchozí, neboť ti samotná frekvenční analýza nebude stačit k jejímu rozluštění. Tato šifra se totiž šifrovala tak, že každé písmeno abecedy, tedy jeho číselný ekvivalent, se násobil neznámým číslem n. Tvým úkolem bude vypočítat hodnotu n.

Znění šifry:

DPEBP WDCNM BPUSP AZCCZ JKBUV NCHCG WCVGR ZAVOK GDPBA WZESK RWENE OXTSA GCNCV CRCDG KTKGS ATVML CSWGP DEUVW UKTCN LCVCN BPUDC GNCXU BANAL CNTVZ ENADP KNCRT CGEGU PVUPS VCWCW NUKHE WCPUW WCPCG **LCVCN BPWDC NRZAV NCRWC G**LCVC NLEGR WCGSA TCLCV CNRWC OXNMB PERCV CVUDC GNUDM WRATC RTCGE GUPVU PSVCW CWNUK HEWCP UWWCP CG

Frekvenční analýza pro daný text vypadá následovně.

A	B	C	D	E	F	G	H	I	J	K	L	M
11	8	46	10	12	0	18	3	0	1	9	7	4
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
20	3	18	0	11	8	9	16	18	21	3	0	6

Vytvoření grafu frekvenční analýzy textu a jeho porovnání s frekvenční analýzou českého jazyka nám v tomto případě nepomůže, neboť se písmena zašifrovala pomocí algoritmu, jenž nezachoval jejich pořadí, například pokud se písmeno A zašifrovalo na písmeno M, neznamená to, že písmeno B bude N. Ale přesto nám tabulka může napovědět, které písmeno v šifře bude pravděpodobně písmeno E v dešifrované zprávě.

Které písmeno to bude a jaké číslo se mu přiřazuje? ……=-……..

Nyní použij následující parametrickou rovnici dešifrování, kde pro nás bude n neznámá a k je parametr. Podmínkou je, aby n bylo nesoudělné s 26.

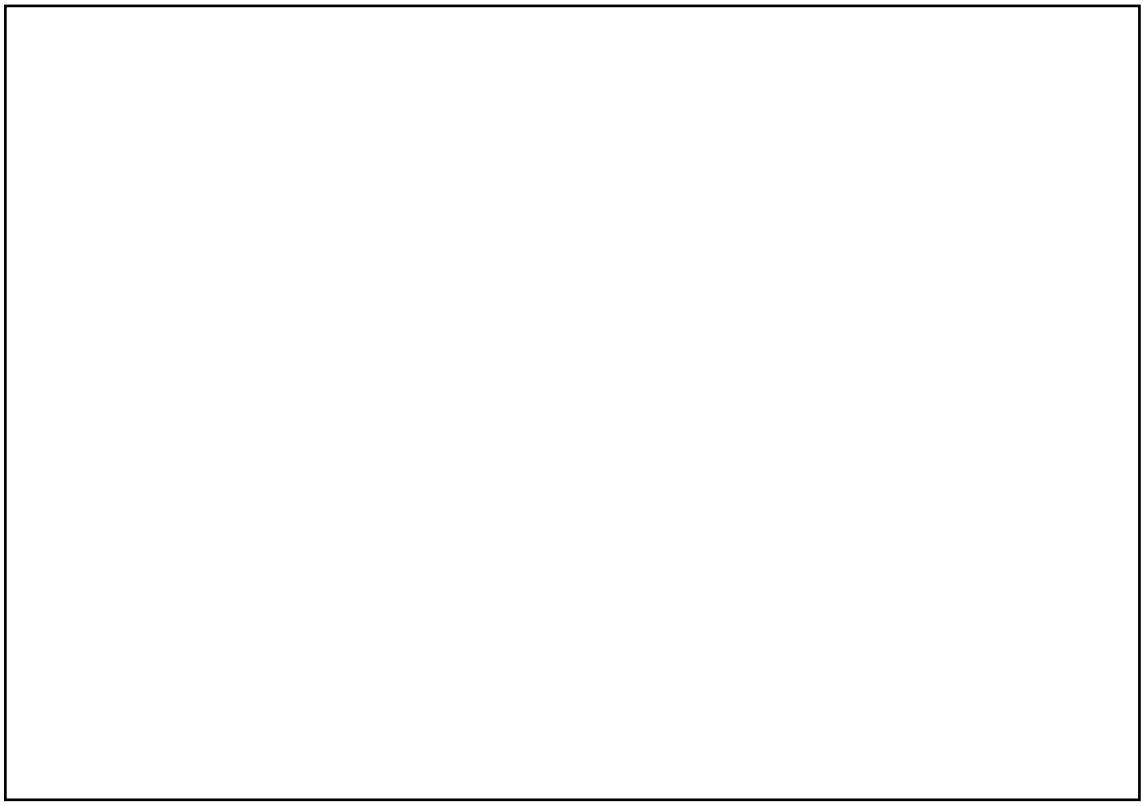
$$an = 26k + f(a)$$

$f(a)$ je číselný ekvivalent zašifrovaného znaku, a je ekvivalent znaku, který v dané šifře odpovídá $f(a)$ a k mohou být všechna přirozená čísla včetně nuly, tedy $\mathbb{N}_0$.

Zde máš prostor pro vykonání všech výpočtů.

Jaký parametr byl tedy při šifrování použit? $n =$……..

Když znáš parametr, můžeš vypočítat, jak vypadá celá šifrovací abeceda.



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

Pokud jsi našel šifrovací abecedu, která byla použita k zašifrování literárního úryvku, poznáš, z jaké knihy je tato ukázka?

LCVCNBPWDCNRZAVNCRWCG

Znění úryvku:

……

Ze které knihy je daný úryvek a kdo je jeho autorem?

……

5.15. Afinní šifra

Nyní tě čeká dešifrování afinní šifry. Následující text je úryvek ze slavné knihy. Dokážeš rozluštit jaké? Podle jakého klíče je text zašifrován? Afinní šifra se vyznačuje dvojící klíčů, a to prvkem n, kterým se znak vynásobí, a následně prvkem b, který se k výsledku přičte.

Znění šifry:

EFGSX QHNZZ FESXK NYHCZ GFWHU EXCFY QFDOD VXXKP RFOQF UFCJH NQDUF QURFS DKPCQ DAXZG HQFNQ FSXQD ESXGD ACDZF EXWYF YXQXR HUEXZ CFYQH YXKFE SFZGD UDCXE FGSYQ HXUHQ FODVZ CXNWH GWYSD UHZDJ XZXKF SHVDU DCWFZ FSDQX ESXKX NWHOD VXKPW YSFUF QFCPD QFZRA XEFQZ XNZTS FYHGJ PZCFQ VP

Takto vypadá frekvenční analýza šifrovaného textu.

A	B	C	D	E	F	G	H	I	J	K	L	M
3	0	11	18	10	29	8	14	0	3	7	0	0
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7	4	6	18	4	13	1	10	5	7	24	10	15

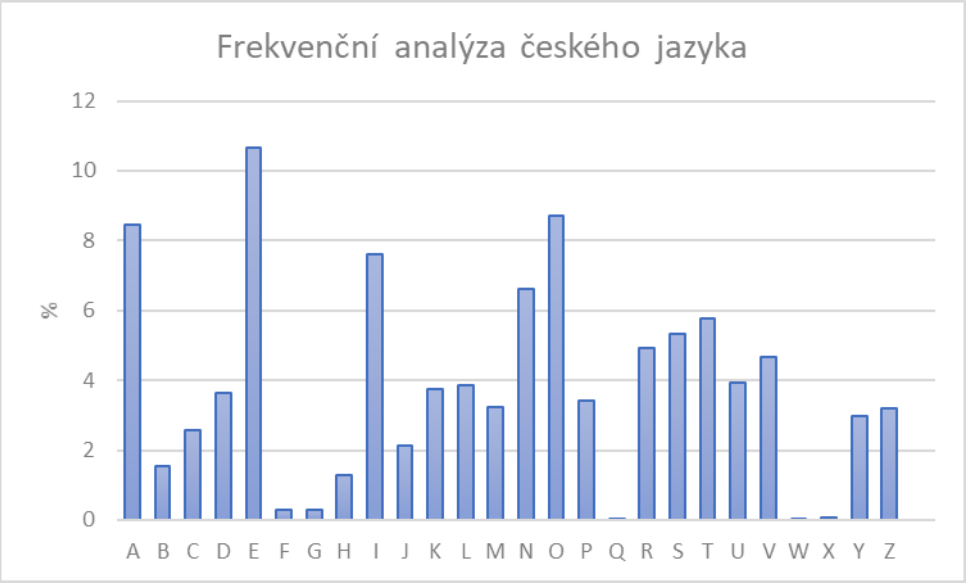
Při dešifrování afinní šifry nám bohužel samotná frekvenční analýza nepomůže. Jedinou možností, jak zjistit, jakým způsobem jsme zprávu zašifrovali, je výpočet parametrů, podle kterých jsme tak učinili.

Parametrická rovnice dešifrování má následující tvar

$$an + b = 26k + f(a)$$

Pro dešifrování této šifry potřebuješ sestavit dvě rovnice, proto vybereš dvě nejčastější písmena v šifře, jejichž číselné ekvivalenty budeme značit $f(a)$. Přiřadíš k nim dvě nejčastější písmena v českém jazyce, jejichž ekvivalenty nazveme a. Následně vytvoříš dvě rovnice, ve kterých budou n, b neznámé a k je parametr.

Nezapomeň na podmínky, neboť $n \in \mathbb{N} - \{1\}$ a $D(n, 26) = 1, b \in \mathbb{N}$.



Která dvě písmena jsou nejčastěji používaná písmena české abecedy a jaký mají číselný ekvivalent?

I. ……. = …..

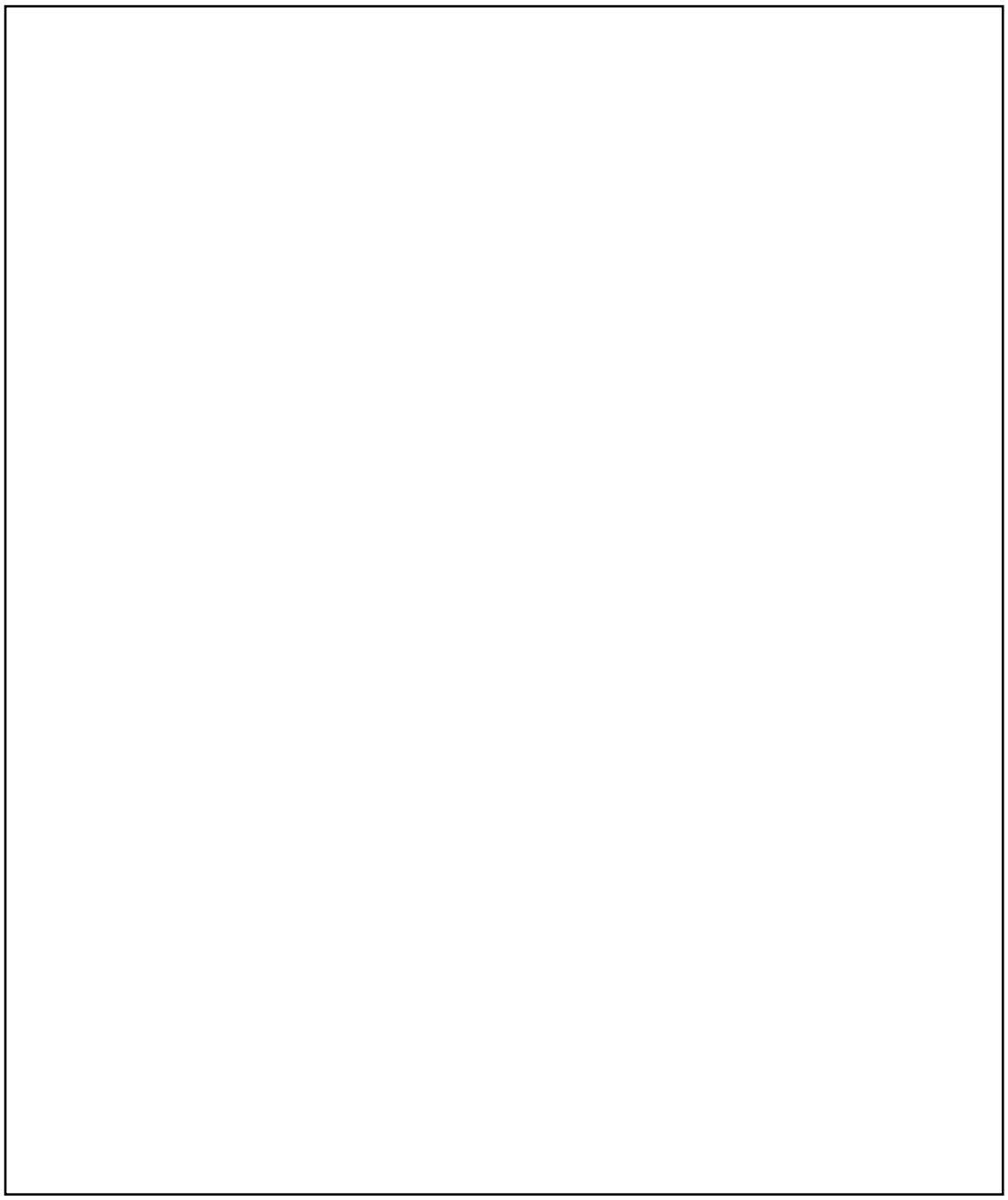
II. ……. = ……

Sestav tedy rovnice dešifrování. Po sestavení rovnic použij sčítací metodu pro jejich řešení, ale pozor, protože v každé rovnici může k být jiné číslo, nemůže se ti pravá strana rovnice vyrušit, ale zůstane ti tam stále $26k$.

Do následujícího rámečku proveď všechny výpočty.

Jaký ti vyšel výsledek? n =…….. , b =……..

Dokážeš teď sestavit šifrovanou abecedu, pokud znáš parametry, které jsme použili?



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

Dešifruj tuto část šifry, která ti napoví, o jakou knihu se jedná.

EFGSX QHNZZ FESXK NYHCZ GFWHU EXCFY QFDOD VXXKP RFOQF
UFCJH NQDUF QURFS DKPCQ DAXZG HQFNQ FSXQD

Dešifrovaná zpráva:

……

……

……

O jakou knihu a od koho se jedná?

……

5.16. Vigenèrova šifra

V tomto pracovním listě se pokusíš dešifrovat Vigenèrovu šifru. Po dlouhá léta byla šifra považována za nerozluštitelnou, a to až do poloviny 19. století. Nyní si ukážeme, jak ji dokážeš sám rozluštit. Jedná se o složitou polyalfabetickou šifru, která používá opakující se heslo, podle kterého se zpráva šifruje.

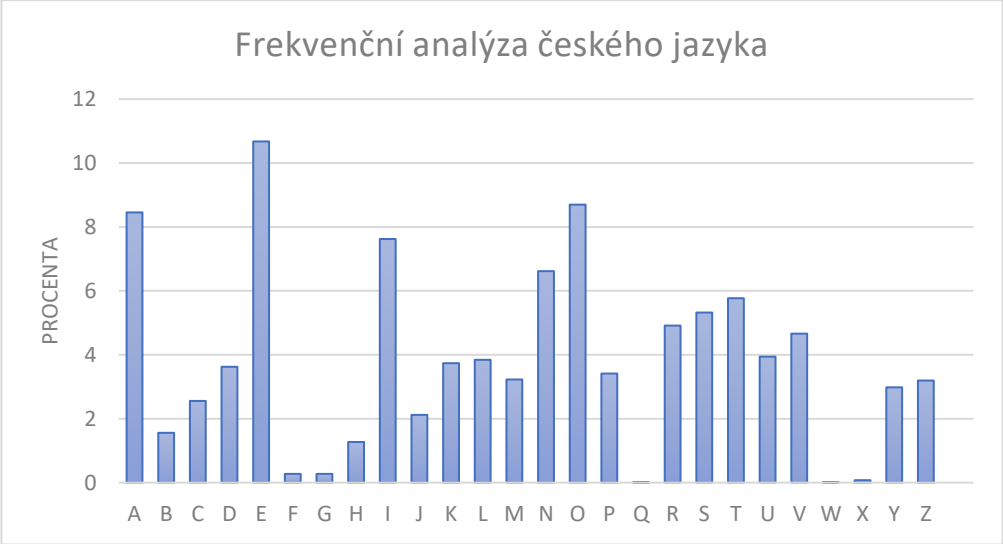
Znění šifrované zprávy:

BATIT MNOLY DSRMC AVOHH AMAKM ELUKX KRODD ABOCP UCODD
PYISC TRJMT DONTE EOBIP UZKRW AUTIT DOYBS ZOXUE XNOIR ADKSY
VESMD MOVBE ZIHGP UOVZE HDAXS ELKLR UOJSS TOHGW FEIMO MLOHI
EEFIT XEZMH ANKKI TOVWH UVTML ANKJS LANIH ZENWT ANKDE PZZIO
AVKVI EMEAP KZQZE FKGIH ABXMR QUFVE HARQT MNJCV ELKGF
KLXMH UTKTI YFOZQ KJSMR QMMZY ZNOVK EKZMV MVEZE
NERIZDTGKOKBETXAVEASWYZMPZAZGGTLGXMWKZMVKNKUIXMGTIY
ZGLRK KXSDM TUUIX VKTMO EJTSG HESRU RVIRU DAZWX EEWZM
BETET UHMRM BRWRP YTIEW RQUIX AYSSD OJDEW RGBHQ LYQRQ
ZPQRU LOLIO OFAIV IBMPU CKPSP IRWTA NKDEP ZNWGQ LKPSP ITGRM
TGPSH ARITD EYXPA TGAPU DOTEO OYMHQ JKCWA UYMHG DAZWX
EEWZU MKTMY ARMLA SEVOM KZMVK SKRQQ NUDEX DALPQ YGXSP
LKRIV IIPRM ZUZYF OHGPF ETVIV UFIWZ EPAMO HRITQ CTIWH EZMM

Prvním krokem při luštění této šifry je tzv. Kasiského test. Kvůli jeho časové náročnosti se v tomto listě již nebudeš tímto testem zabývat. Test se opírá o výpočet délky hesla. V textu se hledají podobné shluky písmem, které pravděpodobně vznikly tak, že se stejná písmena ve zprávě zašifrovala stejnou částí hesla. U těchto shluků písmen se následně určí jejich vzdálenost. V tomto textu bylo vybráno 20 shluků. Dále byly určeny všechny dělitele těchto vzdáleností, které nám určí délku klíče. Jednička se jako dělitel nebude brát v potaz, neboť by to ukazovalo na monalfabetickou šifru. Kvůli množství dělitelů vybereš čísla, která se objevují alespoň dvakrát. Nejčastěji se objevilo 5, a proto ho budeš považovat za délku našeho klíče.

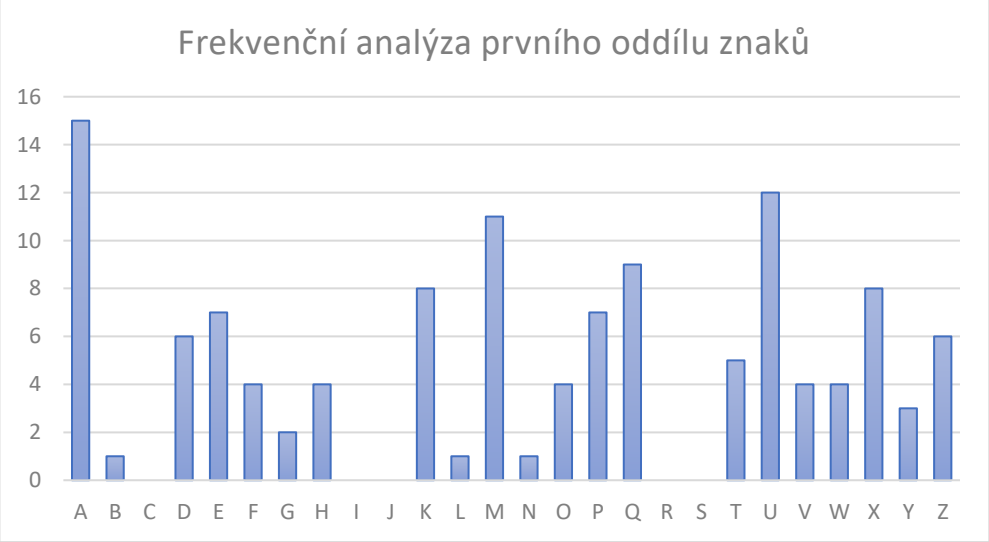
Dalším krokem je rozdělení zprávy do úseků po 5 tak, aby daný úsek písmen byl zašifrován podle stejného písmene. Vybereš tedy první, šesté, jedenácté atd. písmeno do prvního oddílu.

Nyní nás bude čekat frekvenční analýza daných úseků. Frekvenční analýza českého jazyka vypadá následovně.



Oddíl 1.

Pro první úsek písmen vypadá graf četnosti takto.

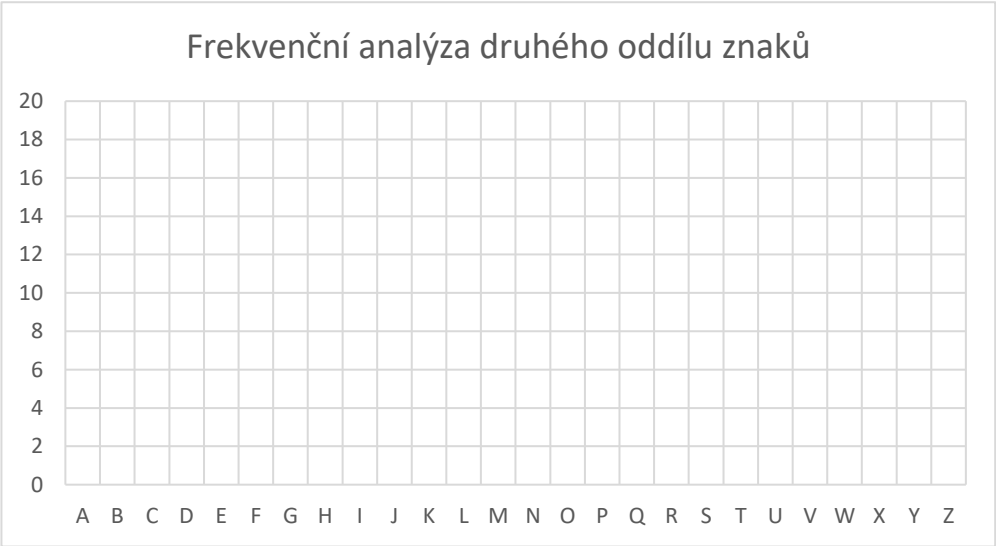


Podle tohoto grafu jsme zjistili, že první klíčové písmeno bude pravděpodobně M.

Pro další dešifrování tu máš tabulky s četností znaků v oddílu, ale graf si již vytvoříš sám.

Oddíl 2.

A	B	C	D	E	F	G	H	I	J	K	L	M
7	5	3	6	13	1	0	2	5	2	5	10	5
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
10	13	0	0	5	3	5	5	6	0	0	4	7



Výsledným písmenem hesla z druhého oddílu je písmeno …… .

Oddíl 3.

A	B	C	D	E	F	G	H	I	J	K	L	M
5	2	0	0	8	4	9	4	3	5	18	0	1
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4	11	2	2	8	2	8	4	4	0	4	6	8

Výsledným písmenem hesla z třetího oddílu je písmeno …… .

Oddíl 4.

A	B	C	D	E	F	G	H	I	J	K	L	M
5	3	3	6	1	0	6	2	15	1	4	5	19
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	0	4	3	3	6	8	4	5	7	4	0	8

Pro poslední dva oddíly nebudeš sestavovat grafy, ale posun abecedy budeš počítat.

Použij nejčetnější písmeno v šifře, pravděpodobně se bude jednat o písmeno E. Nyní tyto údaje použij do dané rovnice.

$$a = f(a) - b + 26k$$

Kde $f(a)$ je číselný ekvivalent zašifrovaného znaku, a je ekvivalent znaku, který v dané šifře odpovídá $f(a)$, b je hodnota posunu v abecedě a k mohou být všechna přirozená čísla včetně nuly, tedy $\mathbb{N}_0$.

Výsledným písmenem hesla z čtvrtého oddílu je písmeno …… .

Oddíl 5.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	0	2	4	13	1	2	8	12	0	1	2	7
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	4	11	2	13	11	9	0	4	7	2	4	3

Zde opět použij rovnici.

$$a = f(a) - b + 26k$$

Výsledným písmenem hesla z pátého oddílu je písmeno …… .

Nyní sestav popořadě písmena ze všech oddílů a tak vytvoříš heslo, podle kterého se šifrovalo: …….

Dalším úkolem bude dešifrovat prvních 43 písmen šifry, která ti prozradí, jaká kniha je zde zašifrovaná. Jako pomůcka ti poslouží daná tabulka. První znak z klíče najdi v prvním tučném sloupci, následně hledej v daném řádku písmeno šifry. Až ho najdeš, písmeno v prvním řádku, které je ve stejném sloupci jako tvoje nalezené písmeno, je písmeno dešifrované zprávy. Takto pokračuj i u dalších písmen a dešifruj celou zprávu.

BATIT MNOLY DSRMC AVOHH AMAKM ELUKX KRODD ABOCP UCO

	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	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
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	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

Dešifrovaná zpráva zní

……

……

…….

O jakou knihu se tedy jedná? ……

5.17. Playfair šifra

S Playfair šifrou ses již setkal, nyní se ji pokusíš dešifrovat. Protože bez hesla je to velmi složité, heslo pro tebe bude známé. Abys dokázal šifru dešifrovat, rozděl ji na skupinky po dvou znacích. Tyto znaky poté vyhledej v tabulce a dešifruj podle daných pravidel.

1. Pokud jsou oba znaky ve stejném řádku, zamění se za znaky ležící o jedno místo nalevo. Pokud je znak na začátku řádku, zamění se za znak na konci stejného řádku.
2. Pokud jsou oba znaky ve stejném sloupci, zamění se za znaky ležící o jedno místo nahoře. Pokud je znak na začátku sloupce, zamění se za znak na konci stejného sloupce.
3. Pokud jsou znaky v různých řádcích a sloupcích, nahradí se za znak ve stejném řádku, ale ve sloupci, jako je druhý znak.

Šifra: QPWHR MZLFH PTQDH AQLRW

Pomocí této tabulky zprávu dešifruj

N	E	R	U	D
A	B	C	F	G
H	I	K	L	M
O	P	Q	S	T
V	W	X	Y	Z

Jak zní zpráva?.....

5.18. Šifry na několik minut

V této části jsou krátké šifry, které zaberou pouze několik minut. Jejich dešifrování je závislé na povědomí o klasických šifrách, které se objevují v předcházející části práce.

1. Zašifruj text MARCO POLO. Pokud se každé písmeno v abecedě má posunout o tolik, kolik je zbytek čísla jeho pozice po dělení čtyřmi.

Zašifrovaný text zní:…….

2. Dešifruj text LQPINTMB. Pokud víš, že každé písmeno se posunulo v abecedě o tolik, kolik je zbytek čísla jeho pozice po dělení pěti.

Dešifrovaný text: ……

3. Zašifruj text ILIAS, pokud víš, že každé písmeno se posunulo v abecedě o tolik, kolik je výsledek dané slovní úlohy.

    A. Na jaké největší množství skupinek lze rozdělit 90 dětí a 24 učitelů, pokud má být v každé skupince stejný počet dětí a stejný počet učitelů?

Zašifrovaný text:……..

4. Dešifruj text WLGAAMI, pokud víš, že každé písmeno se posunulo v abecedě o tolik, kolik je výsledek dané slovní úlohy.

    A. Jaký nejmenší počet žáků by musel být ve třídě, aby za sebou dokázali beze zbytku nastoupit v trojstupu, čtyřstupu, pětistupu i šestistupu.

Dešifrovaný text:……

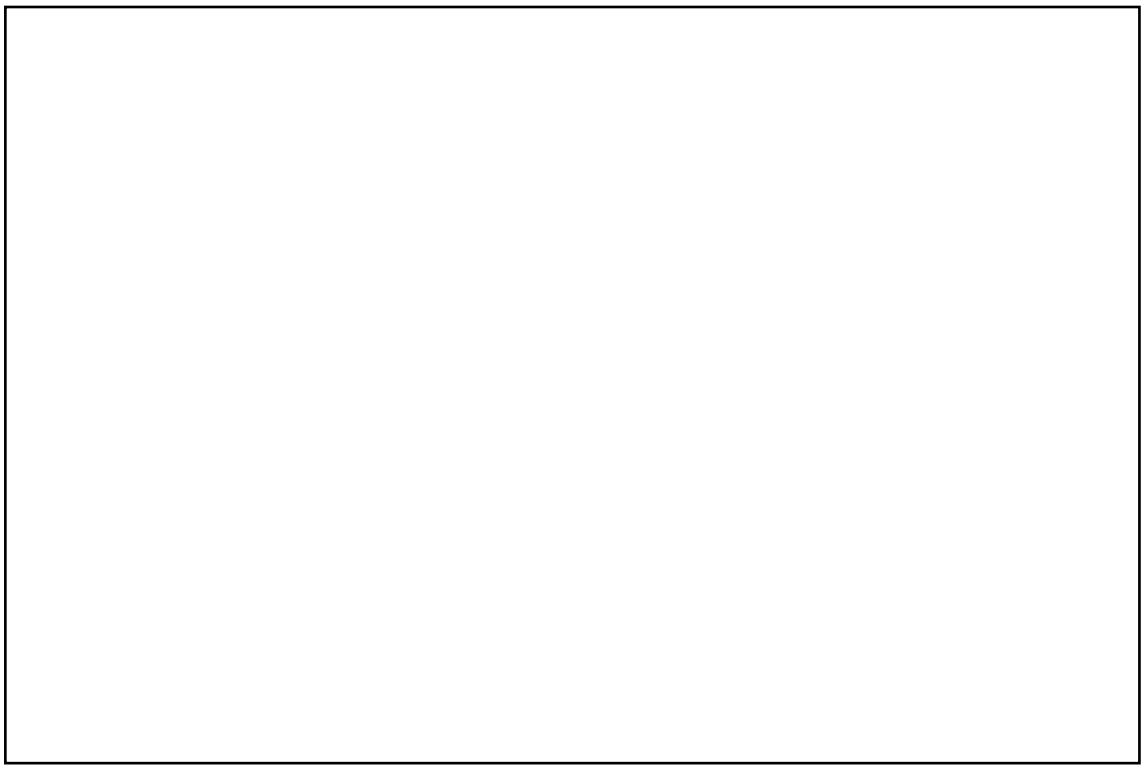
5. Dešifruj text OCNZ RTKPE, pokud víš, že se abeceda posunula o číslo p, kde p je prvočíslo.
   Která čísla to mohou být, pokud předpokládáme, že $p < 10$.

Dešifrovaný text zní:…….

6. Zašifruj text EVANGELIUM, pokud písmena na pozici se sudým číslem posuneš o 7 a písmena na pozici s lichým číslem zašifruješ o 5.

Zašifrovaný text zní:……..

7. Zašifruj text ZIVOT KONSTANTINUV, pokud znaky, jejichž číslo pozice je násobkem některého z dělitelů čísla 6, kromě čísla 1, posuneš v abecedě o 2 a zbytek znaků posuneš o 3.



Zašifrovaný text zní:……

8. Dešifruj šifru, která se skrývá v řešení následujících příkladů. Výsledky použij jako souřadnice v Polybiově čtverci.

A – B – C – D – E – F – B – G – D – A

A. V obchodě se prodával tentýž model hračky v barvě bílé, modré, červené a zelené. Z celkového počtu 80 kusů této hračky bylo během dne prodáno 8 bílých, 3 modré, 5 červených a 4 zelené modely. Určete, kolik procent z celkového počtu této hračky bylo prodáno.

B. Rozdíl nadmořských výšek míst P, Q na železniční trati je 38,5 m, jejich vodorovná vzdálenost je 3,5 km. Určete v promile stoupání trati.

C. Na úseku nové budované silnice pokládají stroje různé výkonosti asfaltový koberec. Položení asfaltového koberce jedním strojem by trvalo 78 hodin, druhým 91. Jak dlouho bude trvat práce při současném nasazení obou strojů.

D. Vyřeš rovnici

$$\frac{1}{3}u + \frac{1}{4}u - \frac{3}{5}u = \frac{1}{2}\left(\frac{u}{6} - 3\right)$$

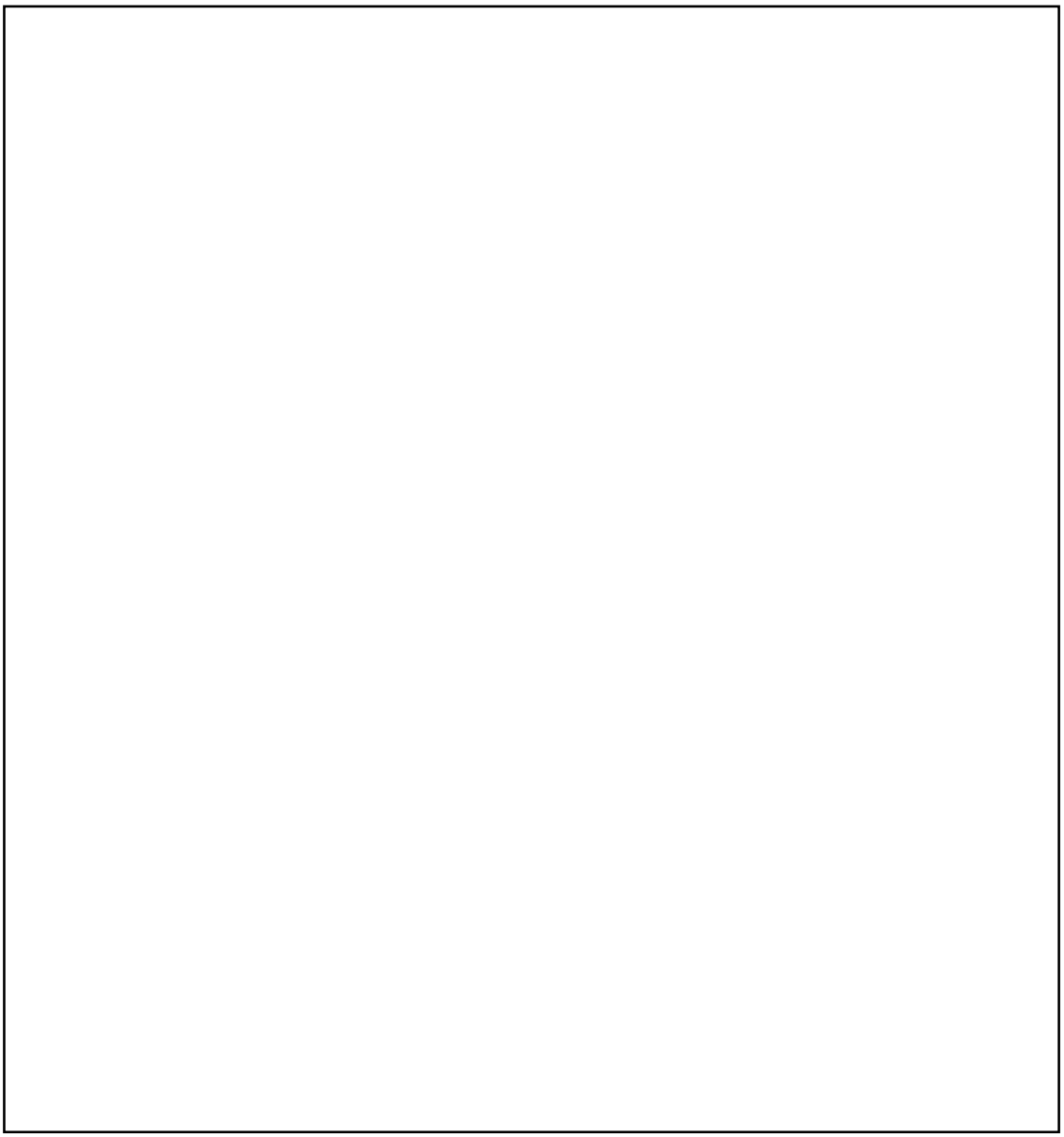
E. Vypočítej

$$\sqrt[3]{25} \cdot \sqrt[3]{5} + \sqrt{16} + \sqrt[3]{50} \cdot \sqrt[3]{20} + \sqrt{121} + \sqrt{1} =$$

F. Vyřeš rovnici

$$1 - \frac{3 - x}{4} = \frac{2x - 5}{6}$$

G. Ve školní jídelně připravují na oběd 490 porcí po 50 g vařeného masa. Vařením ztrácí maso asi 30 % své hmotnosti. Kolik kilogramů syrového masa musí školní jídelna připravit k vaření oběda?



Dešifrovaný text:

……..……

…….

Znáš nějaké knihy od tohoto člověka?

…….....

.....

9. Zašifruj KRAL LAVRA, pokud ke každému písmu připočteš výsledek rovnice, kde je šifrované písmeno neznámou.
   A. $3 - k + 5k/6 = 1/2 - k/(8\ )$
   B. $5/3\ (r - 6) = r/7 + 22$
   C. $7 + a/3 = 8 + a/4$
   D. $3/8\ [10(l - 5) + l] = 4l - 25/4$
   E. $-17/19\ v + 51 = 0$

Šifrovaný text:…….

10. Zašifruj text QUIJOTE podle Dellastele šifry. Do čtverce napiš znaky od těch nejpoužívanějších v českém jazyce po ty nejméně používané. Nejpoužívanější znak bude mít tedy souřadnice 11 a nejméně používaný znak souřadnice 55. Pokud znakům odpovídá stejná hodnota, seřaď je podle abecedy. Písmena I a J jsou totožná a tak jsou jejich hodnoty sečteny.

A	B	C	D	E	F	G	H	I + J	K	L	M	N
8,46	1,56	2,56	3,63	10,68	0,27	0,27	1,27	9,74	3,74	3,84	3,23	6,62
O	P	Q	R	S	T	U	V	W	X	Y	Z	
8,7	3,41	0	4,91	5,32	5,77	3,94	4,66	0,01	0,08	2,98	3,19	

Tabulku na pro šifrování a druhou tabulku na sestavení šifry máš připravenou.

	1	2	3	4	5
1					
2					
3					
4					
5					

Šifrovaný text:……

11. Zašifruj text ALMANACH afinní šifrou, pokud parametry získáš jako řešení rovnic.

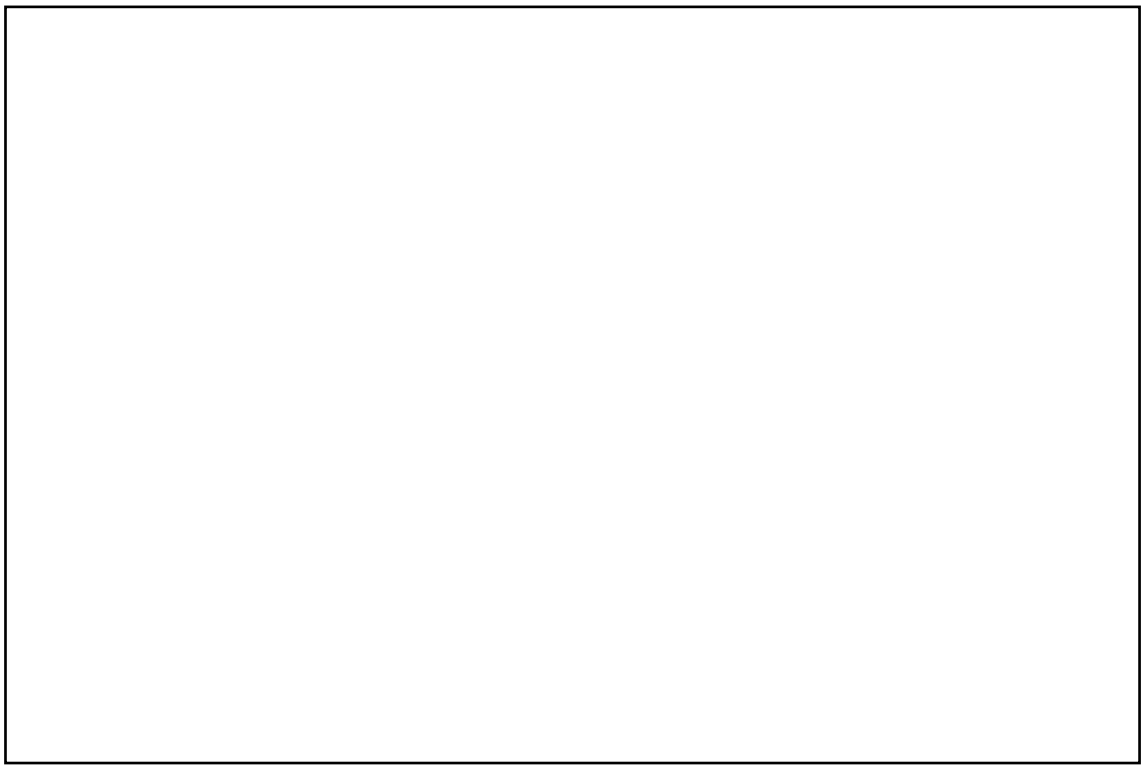
A. $(4n + 1)/3 - (3n - 1)/5 = 15 - (25 - n)/4$

B. $(b - 3)(b + 4) - 2(3b - 2) = (b - 4)^2$

Zašifrovaný text:……..

12. Dešifruj text LYGFQZ VISQ, pokud víš, že je tato šifra zašifrovaná podle složitější substituce, tedy že se každý znak v otevřené abecedě vynásobil číslem, které odpovídá výsledku slovní úlohy.

    A. Třída s 25 žáky si naplánovala výlet. Cena rozpočítaná na jednoho žáka činila 550 Kč. Výletu se nakonec někteří žáci nezúčastnili, takže každý účastník musel zaplatit 625 Kč. Kolik žáků se nezúčastnilo výletu?



Dešifrovaný text:……..

13. Slovo ZOLA bylo zašifrováno na MOYA pomocí Vigenèrovy šifry. Poznej heslo a podle něj zašifruj ZABIJAK.

14. Pokud budeme používat transpoziční šifru, tedy budeme pouze přehazovat písmena ve slově podle daného klíče, kolika způsoby můžeme zašifrovat slovo DEKAMERON?

K zašifrování toho slova máme možností: ……..

15. Pokud budeme používat Caesarovu šifru, kolik šifrovacích abeced máme k dispozici, tedy kolika způsoby můžeme zašifrovat jeden vybraný znak?

Celkový počet šifrovacích abeced pro Caesarovu šifru je: ……

6. Výsledky pracovních listů

Šifrování

Fleissnerova mřížka

A.

O	L	Y	R	S	U	X	J
G	L	A	B	D	V	A	E
P	O	U	L	U	S	X	A
A	G	T	S	A	A	L	R
I	T	M	U	H	T	O	X
I	E	I	A	Z	X	L	A
A	S	V	K	E	T	X	K
L	M	E	O	R	U	K	M

B.

I	L	T	M	D	Z	O	E
O	I	Y	U	H	S	X	L
L	E	A	B	S	R	J	A
G	T	U	A	U	V	A	X
A	S	V	E	U	X	L	K
P	L	R	O	E	T	X	K
O	M	I	S	A	U	A	M
A	G	L	K	A	T	X	R

C.

A	I	U	V	H	E	L	L
I	P	T	E	U	R	O	X
L	L	Y	U	D	A	E	K
O	S	A	O	Z	S	X	K
G	M	I	L	S	T	A	M
L	A	M	K	A	U	J	X
E	G	R	A	U	T	A	R
O	T	B	S	V	X	A	X

D.

G	P	A	I	U	A	A	X
A	L	U	L	S	A	L	J
I	A	T	E	H	V	L	X
I	M	Y	K	E	R	O	M
O	G	R	B	D	U	X	R
L	O	V	S	U	T	E	A
L	T	M	O	Z	X	K	X
E	S	U	A	S	T	A	K

(Vojtěch Zamarovský – Epos o Gilgamešovi)

Polybiova mřížka

23-42-14-31-24-13-13-24-33 55-51-11-31 25-45 31-11-43-13-15 23-31-11-43 25-14-15 12-34-42-34-51-54 55-11-51-11-33-15-31 23-11-24

(Karel Hynek Mácha - Máj)

Dellastele šifra

LWEZ FTUAMY

(Karel IV.)

Monoalfabetická Caesarova šifra

RUIHXV, PLGDV, LDVRQ D PHGHD, WKHVHXV, SURPHWKHXV, R CODWHP URXQX, GDLGDORV D LNDURV.

(Eduard Petiška – Staré řecké báje a pověsti)

Složitější substituce

FYLKNQYN QJABFKX JAB GA JYGEXR ALE XQBYMJKR G NSCM HY QBAVS

(Daniel Defoe – Robinson Crusoe)

Afinní šifra

MUZCA VW ZU VKWPW MU JYXQ XDUY Q XDCPU VQPCA DUPWFU HS OTWVPW
(William Shakespeare – Romeo a Julie)

Vigenèrova šifra

DVNVRPR NEGOR B HB LIPFH HROE FMIPXL TF OM MYJUEYC
Z QVVGYBDRPP LEMHVISEEE BEZE K JGXYJWS HLCF HNPPCIM
(Karel Jaromír Erben – Kytice)

Playfair šifra

DBIRDSBW

Dešifrování

Fleissnerova mřížka

Když hraješ hru o trůny, buď zemřeš, nebo zvítězíš. Střední cesta neexistuje.
(George R.R. Martin – Píseň ohně a ledu (Hra o trůny))

Polybiova šifra

Katniss Everdeen
(Suzanne Collins – Hunger games)

Dellastelova šifra

Peeta Mellark
(Suzanne Collins – Hunger games)

Monoalfabetická Caesarova šifra

$b = 5 + 26k$

Eragon zaklekl do udusaného trávníku a zkušeným okem přelétl stopy. Podle otisků byla zvěř na louce sotva před půlhodinou. Brzy se uloží ke spánku. Jeho kořist, malá srna, která výrazně kulhala na levou přední nohu, byla stále se stádem. Překvapovalo ho, že ji ještě nezahubil vlk nebo medvěd. Nebe bylo čisté a potemnělé. Foukal mírný

vítr. Kolem Eragona se tyčily hory a nad nimi se nesl stříbřitý mrak. Jeho okraje plály červeným světlem, jak je osvěcoval měsíc v úplňku, stojící na obloze mezi dvěma zasněženými vrcholky.
(Christopher Paolini – Eragon)

Monoalfabetická šifra anglicky

$b = 7 + 26k$

„What's your name?" he asked. „ Wendy Moira Angela Darling" she replied with some satisfaction. „What is your name?" „**Peter Pan**." She was already sure that he must be Peter, but it did seem a copaparatively short name. „Is that all?" „Yes" He said rather sharply. He felt for the first time that it is a shortish name.
(J. M. Barrie – Peter Pan)

Monoalfabetická šifra – útok hrubou silou

Hans Christian Andersen

Šifra pozpátku

To bylo tenkrát, když pejsek a kočička ještě spolu hospodařili, měli u lesa svůj domeček a tam spolu bydleli a chtěli všechno dělat tak, jak to dělají velcí lidé. Ale oni to vždycky tak neuměli, protože mají malé a nešikovné tlapičky a na těch tlapičkách nemají prsty, jako má člověk, jenom takové malé polštářky a na nich drápky.
(Josef Čapek – Povídání o pejskovi a kočičce)

Složitější substituce

$n = 7 + 26k$

Tři prsteny pro krále elfů pod nebem, sedm vládcům trpaslíků v síních z kamene, devět mužům, každý je k smrti odsouzen, jeden pro temného pána, jenž dlí na trůně v zemi Mordor, kde se snoubí šero s šerem. Jeden prsten vládne všem, jeden jim všem káže, jeden všechny přivede, do temnoty sváže, v zemi Mordor, kde se snoubí šero s šerem.
(J. R. R. Tolkien – Pán prstenů)

Afinní šifra

$n = 7 + 26k, b = 3 + 26k$

Petronius se probudil stěží v poledne a jako obyčejně velmi unaven. Včera byl na hostině u Nerona. Protáhla se pozdě do noci. V poslední době přestávalo Petroniovi nějak sloužit zdraví. Sám o sobě říkával, že se ráno probouzí jakoby zdřevěnělý a neschopen soustředit myšlenky.
(Henryk Sienkiewicz – Quo vadis)

Vigenèrova šifra

Heslo: MAGIE

Pan a paní Dursleyovi z domu číslo čtyři v Zobí ulici vždycky hrdě prohlašovali, že jsou naprosto normální, ano, děkujeme za optání. Byli opravdu poslední, od koho byste čekali, že se zaplete do něčeho podivného nebo záhadného, poněvadž takové nesmysly zkrátka a dobře neuznávali. Pan Dursley byl ředitelem firmy jménem Grunnings, která vyráběla vrtačky. Byl to vysoký, tělnatý chlapík, který neměl málem žádný krk, zato měl velice dlouhý knír. Paní Dursleyová byla hubená blondýna a krk měla skoro dvakrát delší než jiní lidé, což se jí velice hodilo, poněvadž ho celé hodiny natahovala přes plot a slídila, co se děje u sousedů. Dursleyovi měli malého synka, který se jmenoval Dudley, a podle jejich názoru to byl ten nejúžasnější chlapec na světě.
(J. K. Rowling – Harry Potter)

Playfair šifra

Povídky malostranské

Hry na pár minut

1. NCUCP RRLP
2. Komenský
3. OROHY
4. ODYSSEA
5. Malý princ
6. JCFULLQPZT

7. CKXQW MRPUVDPWKPWY
8. A = 25, B = 11, C = 42, D = 15, E = 31, F = 13, G = 35, Karel Čapek
9. *k* = 18, *r* = 21, *a* = 12, *l* = 100, *v* = 57, SMMH HMAMM
10. GFRGETE
11. INEIVIQX
12. Nezúčastnili se 3 žáci. Viktor Hugo
13. Heslo: NANA, MAOIWAX
14. 362 880 možností
15. 25 šifrovacích abeced

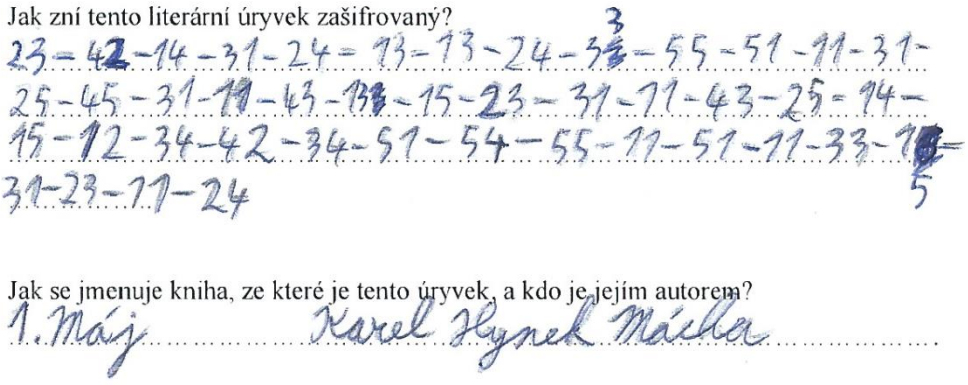
7. Vyhodnocení pracovních listů

Pro vyhodnocení pracovních listů jsem využila Matematický kroužek na Základní škole Evžena Rošického v Jihlavě a několik dobrovolníků. Protože je podobných kroužků na škole několik, v mém konkrétním byli pouze žáci devátých tříd. Na vyzkoušení listů jsem získala několik vyučovacích hodin tohoto předmětu. Za jednu vyučovací hodinu, tedy 45 minut času, byli žáci schopni vyplnit průměrně jeden složitější list, např. dešifrování Vigenèrovy šifry, afinní šifry, atd., nebo dva jednodušší listy, např. šifrování i dešifrování monoalfabetické šifry, Playfair atd. Pro složitější výpočty složitějších rovnic měli žáci k dispozici kalkulačky.

Při zadávání listů jsem několikrát musela žákům pomoci s postupem, vysvětlením principu nebo opravou nevhodně sestavené rovnice. Výsledky žáků byly ve většině případů správné. Nejčastější chyby byly spojené se špatným dosazením do rovnice, špatným přiřazením číselného ekvivalentu znaku. V minimu případů se jednalo o naprosté nepochopení zadání. Žáci měli ovšem velké problémy poznat posun abecedy pouze z grafu, rovnice pro ně byla srozumitelnější.

Rozpoznání literárních děl v pracovních listech bylo složitější u klasických děl než u těch populárních. Většina dětí, pokud si vzpomněla na jméno knihy, potřebovala ke jménu autora buď mou nápovědu a nebo rady celé třídy. U několika děl nedokázali jméno autora ani název knihy vymyslet.

Polybiova šifra nedělala žákům problém ani při šifrování, ani při dešifrování. Občasné chyby byly pravděpodobně způsobené přehlednutím v tabulce.


Jak zní tento literární úryvek zašifrovaný?

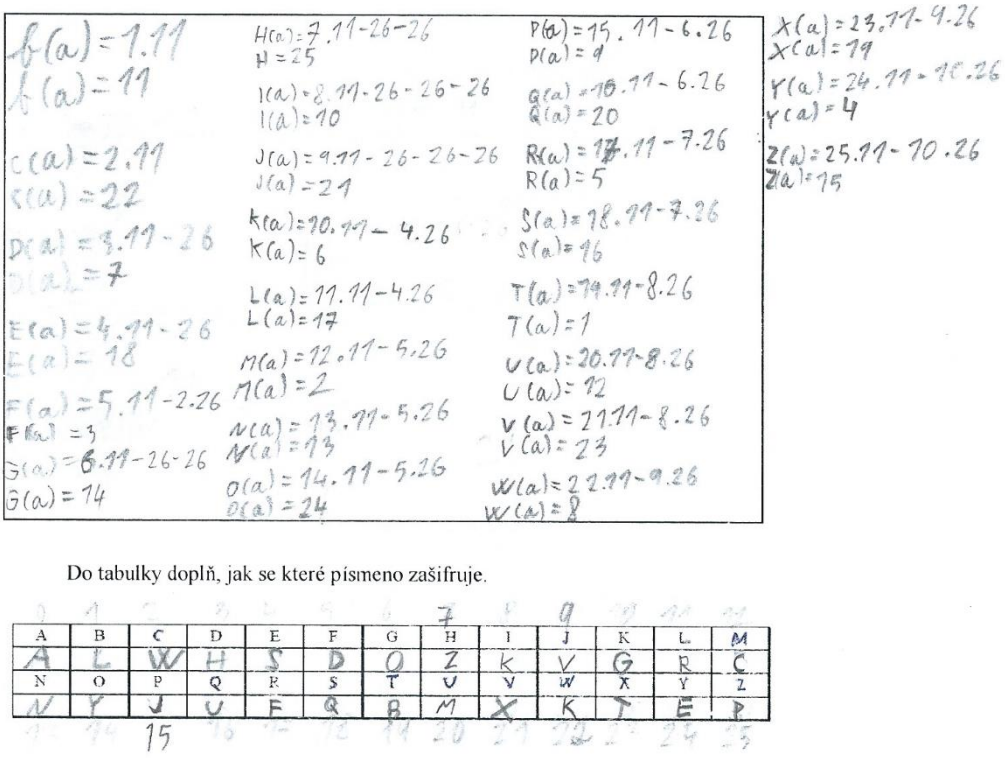
23-42-14-31-24-13-13-24-33-55-51-11-31-
25-45-31-11-43-13-15-23-31-11-43-25-14-
15-12-34-42-34-51-54-55-11-51-11-33-11-
31-23-11-24

Jak se jmenuje kniha, ze které je tento úryvek, a kdo je jejím autorem?

1. Máj Karel Hynek Mácha

Obrázek 9 - Polybiova šifra

V tomto pracovním listu žák velmi zdařile pracuje s šifrováním podle složitější substituce. Výpočet je přesný a velmi zjednodušený. Žádný žák ovšem nepracoval s možností, že pokud je $f(a)$ již zašifrovaný znak, další v abecedě bude písmeno $f(a) + 11 - 26k$. Tedy že již k zašifrovanému znaku stačí přičíst 11.



Do tabulky doplň, jak se které písmeno zašifruje.

A	B	C	D	E	F	G	H	I	J	K	L	M
A	L	W	H	S	D	O	Z	K	V	G	R	C
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	Y	J	U	F	Q	B	M	X	K	T	E	P

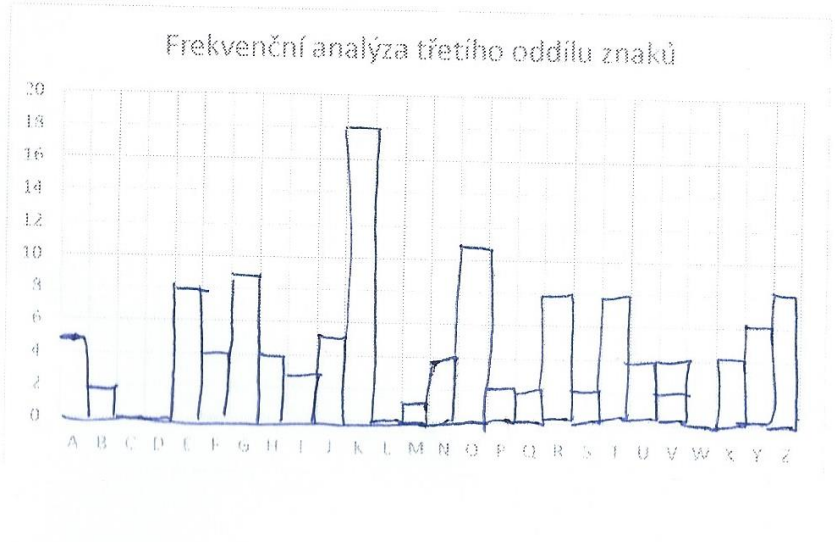
15

Obrázek 10 - Složitější substituce

Sestrojit graf pro posun abecedy nebyl pro žáky problém, ovšem poznat z grafu posun abecedy se jim nedařilo.

Oddíl 3.

A	B	C	D	E	F	G	H	I	J	K	L	M
5	2	0	0	8	4	9	4	3	5	18	0	1
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4	11	2	2	8	2	8	4	4	0	4	6	8



Obrázek 11 - Graf posunu abecedy

8. Závěr

Cílem mé práce je jak navázat na mou bakalářskou práci, tedy podat základní výčet šifer, jež byly využívány v průběhu staletí od starověku až po studenou válku a nástup počítačů jako prostředku k dorozumívání.

Tato práce rovněž obsahuje pracovní listy, jenž samy o sobě jsou jak výukovým materiálem, tak pracovním listem, neboť k těmto listům není potřeba v podstatě žádný úvod, všechny potřebné informace o šifrování a zároveň o původu šifry tyto listy již obsahují.

Listy jsem vyzkoušela v hodinách matematického kroužku, kvůli nedostatečné časové dotaci část žáků vypracovala listy s šifrováním a část žáků vypracovala listy s dešifrováním.

Dle mého názoru žáky tyto hodiny poměrně bavily, neboť se jednalo pro žáky o zcela nové poznatky.

9. Literatura

1. BURDA, Karel. *Úvod do kryptografie*. Brno: Akademické nakladatelství CERM, 2015.
2. FARANA, Radim. *Šifrování pro radost a poučení*. Brno: Mravenec, 2006.
3. GROŠEK, Otokar , PORUBSKÝ, Štefan. *Šifrovanie - algoritmy, metódy, prax*. Praha: Grada, 1992.
4. GROŠEK, Otokar, VOJVODA, Milan, ZAJAC, Pavol. *Klasické šifry.* Slovenská technická univerzita v Bratislave, 2007.
5. KAHN, David. *The Codebreakers: The Story of Secret Writing*. New York: Macmillan, 1968.
6. HANŽL, Tomáš, PELÁNEK, Radek, VÝBORNÝ, Ondřej. *Šifry a hry s nimi: kolektivní outdoorové hry se šiframi*. Praha: Portál, 2007.
7. KRÁLÍK, Jan. *Statistika českých grafémů s vyuţitím moderní výpočetní techniky*. Slovo a slovesnost XLIV, 1983, s. 295-304.
8. KOBLITZ, Neal. *A Course in Number Theory and Cryptography.* Springer-Verlag New York, 1994.
9. LUNDE, Paul, ed. *Tajemství kódů.* Praha: Svojtka & Co., 2013.
10. PIPER, Frederic, Charles, MURPHY, Sean. *Kryptografie*. Praha: Dokořán, 2006.
11. *Praktické základy Kryptologie a Steganografie* [online]. [cit. 2018-04-12]. Dostupné z: http://www.security-portal.cz/clanky/praktick%C3%A9-z%C3%A1klady-kryptologie-steganografie
12. SCHNEIER, Bruce. *Applied cryptography*. New York: Wiley, 1996.
13. SINGH, Simon. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii*. Praha: Dokořán, 2009.
14. *Šifrování a biometrie pod drobnohledem* [online]. [cit. 2018-04-12]. Dostupné z: https://www.svethardware.cz/sifrovani-a-biometrie-pod-drobnohledem/25723.
15. TILBORG, Henk. *Fundamentals of cryptology*. Boston: Kluwer Academic Publishers, 2000.
16. *Tajemství šifer - po stopách kryptografie a steganografie V: Jeroným Cardan - Otočná mřížka* [online]. [cit. 2018-04-12]. Dostupné z:

http://www.epochtimes.cz/200807295638/Tajemstvi-sifer-po-stopach-kryptografie-a-steganografie-V.html

17. TLUSTÝ, Pavel. *Obecná algebra pro učitele*. České Budějovice: Jihočeská univerzita, 2006.
18. WILLERS, Michael. *Algebra bez (m)učení: od arabských matematiků k tajným šifrám.* Praha: Grada, 2012.

Literatura použitá v pracovních listech

1. BARRIE, J.M. *Peter Pan*. Ware: Wordsworth Classics, 1993.
2. ČAPEK, Josef. *Povídání o pejskovi a kočičce: jak spolu hospodařili a ještě o všelijakých jiných věcech*. Ostrava: Librex, 1999.
3. ERBEN, Karel Jaromír. *Kytice*. Říčany: Sun, 2015.
4. MÁCHA, Karel Hynek. *Máj: báseň od Karla Hynka Máchy*. V České Lípě: Vlastivědné muzeum a galerie, 2016.
5. MARTIN, George R. R. *Píseň ledu a ohně. Kniha první, Hra o trůny*. Praha: Talpress, 2013.
6. NOVOTNÝ, František. *Robinson Crusoe*. Praha: Albatros, 2005.
7. PAOLINI, Christopher. *Odkaz Dračích jezdců. Eragon*. Praha: Fragment, 2009.
8. PETIŠKA, Eduard. *Staré řecké báje a pověsti*. Praha: Ottovo nakladatelství, 2011.
9. ROWLING, J. K. *Harry Potter a kámen mudrců.* V Praze: Albatros, 2010.
10. SHAKESPEARE, William. *Dvanáct nejlepších her*. Praha: Romeo, 2011.
11. SIENKIEWICZ, Henryk. *Quo vadis*. Praha: Český klub, 2003.
12. TOLKIEN, J. R. R. *Pán prstenů. Společenstvo prstenu*. Praha: Argo, 2006.

ZAMAROVSKÝ, Vojtěch. *Gilgameš*. Praha: Albatros, 1976.

10. Přílohy

Obrázek 12 - Šifra Marie Stuartovny

	P	I	V	A	K	P	Z	Q	A	B	Q	I	V	I	V	L	M	Z	A	M	V
-1	O	H	U	Z	J	O	Y	D	E	A	P	H	V	H	U	K	L	Y	E	L	U
-2	N	G	T																		
-3	M	F	S																		
-4	L	E	R	W	G																
-5	K	D	Q																		
-6	J	C	P																		
-7	I	B	O	T	D	I	S	J													
-8	H	A	N	S	C	H	R	I	S	T	I	A	N	A	N	D	E	R	S	E	N
-9																					

Dešifrovaný text: Hans Christian Andersen

Obrázek 13 - Šifra pozpátku

V této části jsou krátké šifry, které zaberou pouze několik minut. Jejich dešifrování je závislé na povědomí o klasických šifrách, které se objevují v předcházející části práce.

1. Zašifruj text MARCO POLO. Pokud se každé písmeno v abecedě má posunout o tolik, kolik je zbytek čísla jeho pozice po dělení čtyřmi.

Zašifrovaný text zní: ncucp rrlp

Obrázek 14 - Šifra na pár minut

Nyní se pokusíš zašifrovat text podle hesla: NEMCOVA.

Text: Babicka

Sestav tedy šifrovací tabulku a podle ní šifruj.

N	E	M	C	O
V	A	B	D	F
G	H	I	K	L
P	Q	R	S	T
U	W	X	Y	Z

Jak zní šifra? BDIRDSBV

Obrázek 15 - Šifra Playfair