

Aplikace pro kryptoanalýzu substitučních šifer

Ondřej Šůstal

Bakalářská práce
2015



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2014/2015

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Ondřej ŠŮSTAL**

Osobní číslo: **A10160**

Studijní program: **B3902 Inženýrská informatika**

Studijní obor: **Informační a řídicí technologie**

Forma studia: **prezenční**

Téma práce: **Aplikace pro kryptoanalýzu substitučních šifer**

Téma anglicky: **An Application for the Crypto-analysis of Substitution Ciphers**

Zásady pro vypracování:

1. Vypracujte literární rešerši na dané téma.
2. Seznamte se s různými dostupnými metodami kryptoanalýzy substitučních šifer.
3. Vytvořte ve zvoleném prostředí (C#, JAVA, Mathematica s vlastním GUI) aplikaci pro kryptoanalýzu jednoduchých substitučních konvenčních šifer.
4. Otestujte aplikaci na zvolené sadě příkladů šifrových textů.
5. Prostudujte možnosti budoucího rozšíření, exportů a importů dat.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **ZELENKA, Josef.** Ochrana dat: kryptologie. Vyd. 1. Hradec Králové: Gaudeamus, 2003, 198 s. ISBN 80-704-1737-4.
2. **SWENSON, Christopher.** Modern cryptanalysis: techniques for advanced code breaking. Indianapolis: Wiley, c2008, xxviii, 236 s. ISBN 978-0-470-13593-8.
3. **VONDRUŠKA, Pavel.** Kryptologie, šifrování a tajná písma. 1. vyd. Praha: Albatros, 2006, 340 s. Oko. ISBN 80-000-1888-8.
4. **KATZ, Jonathan a Yehuda LINDELL.** Introduction to modern cryptography. Boca Raton: Chapman, 2008, xviii, 534 s. ISBN 978-1-58488-551-1.
5. **PIPER, F a Sean MURPHY.** Kryptografie. 1. vyd. v českém jazyce. Překlad Pavel Mondschein. Praha: Dokořán, 2006, 157 s. ISBN 80-736-3074-5.
6. **BITTO, Ondřej.** Šifrování a biometrika aneb tajemné bity a dotyky. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-866-8648-5.

Vedoucí bakalářské práce:

doc. Ing. Roman Šenkeřík, Ph.D.

Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce:

6. března 2015

Termín odevzdání bakalářské práce:

22. května 2015

Ve Zlíně dne 6. března 2015



doc. Mgr. Milan Adámek, Ph.D.
děkan

L.S.

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu


Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně


.....
podpis diplomanta

ABSTRAKT

Bakalářská práce si klade za cíl seznámit čtenáře se substitučními šiframi a s možnostmi jejich kryptoanalýzy. Úvod teoretické části je věnován vysvětlení základních pojmů a uvedení do problematiky substitučních šifer. Dále jsou charakterizovány hlavní metody kryptoanalýzy substitučních šifer a popsány možnosti využití těchto metod u jednotlivých šifer. Praktická část je věnována popisu aplikace z pohledu uživatele a nastínění postupu luštění jednotlivých šifer pomocí této aplikace.

Klíčová slova: kryptologie, kryptoanalýza, substituční šifra, frekvenční analýza

ABSTRACT

The bachelor's thesis aims to acquaint the reader with the substitution cipher and possibilities of their cryptanalysis. Introduction the theoretical part is devoted to explaining the basic concepts and introduction to the issue of substitution ciphers. Further outlines the main method of substitution cipher cryptanalysis and discussed the possibility of using these methods with different algorithms. The practical part is devoted to describing the application from the user's perspective and to outline progress deciphering the various codes using this application.

Keywords: cryptology, cryptanalysis, substitution cipher, frequency analysis

Tímto bych chtěl poděkovat svému vedoucímu doc. Ing. Romanu Šenkeříkovi Ph.D. za cenné rady a připomínky při zpracovávání bakalářské práce.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD.....	9
I TEORETICKÁ ČÁST.....	10
1 KRYPTOLOGIE.....	11
1.1 KRYPTOGRAFIE	11
1.2 STEGANOGRAFIE	11
1.3 KRYPTOANALÝZA	11
2 ZÁKLADNÍ POJMY KRYPTOGRAFIE.....	12
2.1 ŠIFROVACÍ SYSTÉM	12
2.2 ŠIFROVÁNÍ / ZAŠIFROVÁNÍ	12
2.3 DEŠIFROVÁNÍ / LUŠTĚNÍ	12
2.4 OTEVŘENÝ TEXT / ŠIFROVANÝ TEXT	12
2.5 ABECEDA OTEVŘENÉHO TEXTU	12
2.6 ŠIFROVANÁ ABECEDA.....	12
2.7 KLÍČ	13
2.8 BIGRAM, TRIGRAM, POLYGRAM.....	13
3 ROZDĚLENÍ KLASICKÝCH ŠIFROVÝCH SYSTÉMŮ	14
3.1 SUBSTITUTE	14
3.2 TRANSPOZICE	14
3.3 KÓDOVÁ KNIHA.....	14
4 SUBSTITUČNÍ ŠIFRY A JEJICH ŠIFROVANÉ SYSTÉMY.....	15
4.1 MONOALFABETICKÁ SUBSTITUTE.....	15
4.1.1 Atbash	15
4.1.2 Jednoduchý posun	15
4.1.3 Afinní šifra	16
4.1.4 Přeházená abeceda	17
4.1.5 Využití klíčového slova.....	17
4.2 POLYALFABETICKÁ SUBSTITUTE	17
4.2.1 Vigenère šifra	17
4.3 POLYGRAFICKÁ SUBSTITUTE	19
4.3.1 Playfair šifra	20
4.4 HOMOFONNÍ SUBSTITUTE	21
5 ZÁKLADNÍ METODY KRYPTOANALÝZY.....	22
5.1 FREKVENČNÍ ANALÝZA	22
5.1.1 Frekvenční analýza českého jazyka	23
5.2 INDEX KOINCIDENCE	24
5.2.1 Index koincidence náhodného textu.....	24
5.2.2 Index koincidence jazyka	25
5.2.3 Využití indexu koincidence.....	25
5.3 ÚTOK HRUBOU SILOU	26
6 KRYPTOANALÝZA SUBSTITUČNÍCH ŠIFER	27

6.1	KRYPTOANALÝZA MONOALFABETICKÉ ŠIFRY	27
6.1.1	Jednoduchý posun	27
6.1.2	Afinní šifra	28
6.2	KRYPTOANALÝZA POLYALFABETICKÉ ŠIFRY	29
6.2.1	Kasiského metoda	29
6.2.2	Index koincidence	30
II	PRAKTICKÁ ČÁST	31
7	PROGRAMOVÁ ČÁST	32
7.1	JAVA	32
7.1.1	JavaFX.....	33
7.1.2	Zdrojový kód.....	33
7.1.3	Vstupy a výstupy aplikace	33
7.1.4	Funkce aplikace.....	34
8	POPIS APLIKACE	35
8.1	HLAVNÍ PANEL	35
8.1.1	Horní menu.....	35
8.1.2	Textová pole.....	36
8.1.3	Pravé menu.....	37
8.2	OKNO FREKVENČNÍ ANALÝZY	38
8.3	OKNO INDEXU KOINCIDENCE.....	40
8.4	VIZUALIZACE KRYPTOANALÝZY	41
8.4.1	Vizualizace pro jednoduchý posun a šifru Atbash.....	41
8.4.2	Vizualizace pro Afinní šifru.....	43
8.4.3	Vizualizace kryptoanalýzy polyalfabetické substituce	44
8.4.4	Vizualizace dešifrování polygrafické substituce.....	45
8.4.5	Panel úpravy výstupu kryptoanalýzy	47
9	MOŽNOSTI EXPORTŮ A IMPORTŮ DAT.....	48
9.1	BUDOUCÍ MOŽNOSTI ROZŠÍŘENÍ IMPORTŮ A EXPORTŮ DAT.....	48
	ZÁVĚR	49
	SEZNAM POUŽITÉ LITERATURY.....	50
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	52
	SEZNAM OBRÁZKŮ	53
	SEZNAM TABULEK.....	54
	SEZNAM PŘÍLOH.....	55

ÚVOD

Kryptologie je věda, zabývající se utajením obsahu zpráv, tedy šiframi. Až donedávna byla považována spíše za vědu opředenou tajemstvím, stojící za matematikou a informatikou.

Největší pozornosti se těšila především ve dvacátém století v době první světové války, nejvíce se osvědčila i v období druhé světové války.

Kryptologie však nebyla využívána jen na šifrování válečných zpráv, ale zaměřovala se také na obchodní a diplomatické korespondence, agenturní či policejní zprávy a další podobně důležité informace.

Teoretická část bakalářské práce se zaměřuje na popis substitučních šifer od vytvoření až po jejich kryptoanalýzu. Podstatná část je zaměřena na popis metod kryptoanalýzy a jejich využití k prolomení substitučních šifer.

V praktické části je vytvořena aplikace v jazyce Java a za pomoci frameworku JavaFX pro vizualizaci kryptoanalýzy substitučních šifer. V této aplikaci jsou využity metody kryptoanalýzy substitučních šifer, popsané v teoretické části.

I. TEORETICKÁ ČÁST

1 KRYPTOLOGIE

Kryptologii můžeme zjednodušeně označit jako vědu o utajení zpráv. Mezi lidmi má stále nádech tajemna. Kryptologie se dělí na kryptografii a kryptoanalýzu a někdy se jako samostatná oblast přidává ještě steganografie. Přesné vymezení této vědní disciplíny je tedy dáno sjednocením témat, kterými se její výše uvedené části zabývají. [1]

1.1 Kryptografie

Kryptografie se zabývá matematickými metodami se vztahem k takovým prvkům informační bezpečnosti, jako je zajištění důvěrnosti zprávy, integrity dat (neporušenosti), autentizace entit (ověření subjektu) a původu dat (vlastnictví). Je to věda především o tom, jak navrhovat a používat šifrovací systémy, a tedy disciplína, která se zabývá převedením informace do podoby, v níž je tato informace skryta. Jejím úkolem je učinit výslednou zprávu nečitelnou i v situacích, kdy je zachycená třetí nepovolanou stranou. [1]

1.2 Steganografie

Steganografie je vědní disciplína, jejímž úkolem je skrýt samotnou existenci zprávy, ale zpráva samotná může být napsána nebo předána ve srozumitelné podobě. [1]

1.3 Kryptoanalýza

Kryptoanalýza je jakýsi „opak“ kryptografie. Z toho plyne, že jedním z hlavních cílů je studium metod luštění šifrovacích systémů. Obecněji se kryptoanalýza zabývá analýzou odolnosti (síly) kryptografických systémů a hledá metody vedoucí k proniknutí do těchto systémů.[1]

2 ZÁKLADNÍ POJMY KRYPTOGRAFIE

2.1 Šifrovací systém

Šifrovací systém je jakýkoliv systém, který můžeme použít pro změnu textu zprávy, tak aby byla nesrozumitelná komukoliv jinému kromě adresáta.[3]

2.2 Šifrování / Zašifrování

V případě, že použijeme šifrovací systém na nějakou zprávu, tak říkáme, že zprávu šifrujeme nebo že jsme ji zašifrovali. [1][2]

2.3 Dešifrování / luštění

Dešifrování nebo luštění je opačný proces k šifrování, tj. rekonstrukce původního otevřeného textu. Tato dvě slova neznamenaají zcela totéž. Zamýšlený příjemce zprávy tuto zprávu dešifruje, zatímco nezamýšlený příjemce, který se snaží pochopit její obsah, ji luští. [2]

2.4 Otevřený text / Šifrovaný text

Původní text zprávy, ještě před tím než byl zašifrován, se nazývá otevřený text. Poté co byl zašifrován, se nazývá šifrovaný text nebo šifrovaný zpráva. [2]

2.5 Abeceda otevřeného textu

Abecedou otevřeného textu rozumíme jakékoliv písmeno otevřeného textu, interpunkční znaménko atd., které se mohou v otevřeném textu vyskytnout.[1]

2.6 Šifrovaná abeceda

Šifrovaná abeceda může být tvořena abecedou otevřeného textu, ale i jinými obrazci viz Tab 1.[1]

Tab. 1 Ukázka šifrované abecedy

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
1	2	2	4	5	6	7	8	9	0																
#	\$	%	&	£	€	®	©	¥	@	?	>	=	<	*	+	!	¢	¶	¤	§	©	©	ζ	\]

2.7 Klíč

Klíč je nějaký kus informace, kterou si strany, které mezi sebou komunikují, vymění nějakým bezpečným kanálem. Klíč upřesňuje, jak se šifra chová.[4]

2.8 Bigram, Trigram, Polygram

Bigram je jakákoliv dvojice sousedních písmen v nějakém textu. Trigram je trojice po sobě jdoucích písmen. Polygram je tvořený blíže neurčeným počtem po sobě jdoucích písmen v textu.[1]

3 ROZDĚLENÍ KLASICKÝCH ŠIFROVÝCH SYSTÉMŮ

Klasické šifrovací systémy můžeme rozdělit na substituce, transpozice a kódovou knihu.

3.1 Substituce

Substituce neboli záměna spočívá v záměně použité abecedy otevřeného textu za znaky šifrované abecedy. Šifrák, které se tak vytváří, se říká substituční šifry. K převodu otevřeného textu na šifrovaný lze použít jednu šifrovanou abecedu pro celý text nebo může být použita pro každé písmeno otevřeného textu jiná šifrovací abeceda. Příkladem nejjednodušší záměny může být Caesarova šifra.[1]

3.2 Transpozice

Transpozice spočívá v zamíchání pořadí písmen v otevřeném textu. Jedná se o přeskupování písmen podle přesně určených pravidel, jejichž znalost umožňuje text zpětně dešifrovat. Příkladem jednoduché transpozice jsou přesmyčky nebo lištovky.[1]

3.3 Kódová kniha

Kódová kniha je slovníkem, ve kterém jsou vybraná slova nebo věty otevřeného textu nahrazována kódy. Záměrem tohoto systému je ztížit luštiteli identifikaci obsahu nejužívanějších frází.

4 SUBSTITUČNÍ ŠIFRY A JEJICH ŠIFROVANÉ SYSTÉMY

Substituční šifry popsané v této kapitole vychází ze základního šifrovaného systému substituce.

4.1 Monoalfabetická substituce

V této šifře se každý znak otevřeného textu nahradí jedním znakem šifrované abecedy. Pro celý otevřený text se použije stejná šifrovaná abeceda.

Atbash

Jde o jednoduchou substituční šifru postavenou na jediné kódovací tabulce. Principem Atbash je prohození prvního písmena abecedy s posledním, druhého písmena s předposledním atd. Při konstrukci tabulky si jednoduše do prvního řádku vypíšeme abecedu zleva doprava, do druhého pak zprava doleva viz. Tab. 2. [5]

Tab. 2 Převodová tabulka šifry Atbash

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

Příklad šifrování můžeme vidět v tabulce 3.

Tab. 3 Příklad šifrování Atbash

Zpráva	P	L	A	I	N	T	E	X	T
Šifrovaná zpráva	K	O	Z	R	M	G	V	C	G

Jednoduchý posun

Šifra jednoduchý posun spočívá v jednoduchém posouvání písmen podle abecedy v závislosti na dohodnutém číselném klíči. Obvykle používám 26 písmen. To nám dává 25 variant, jak zašifrovat otevřený text.[7][8]

Matematicky se dá tato šifra zapsat jako:

$$S_{(x)} = (O_{(x)} + k) \bmod 26 \quad (1)$$

kde k je parametr posunu $k \in \langle 0; 25 \rangle$

Dobrým příkladem této šifry je Caesarova šifra, kterou využíval Julius Caesar (100-44 př. n. l.) při korespondenci s Kleopatrou (70-30 př. n. l.). Tuto šifru popsal ve svých Zápiscích o válce galské.[6]

Caesarova šifra funguje na principu prostého posunu celé abecedy o tři písmena doprava.

Tvorba převodové tabulky šifry je tedy velmi jednoduchá. Do horní části napíšeme abecedu otevřeného textu. Do spodní řádky ji zapíšeme posunutou o 3 písmena doprava a dostaneme tak šifrovanou abecedu této šifry viz Tab. 4.[6]

Tab. 4 Převodová tabulka Caesarovi šifry

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
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

Příklad šifrování můžeme vidět na tabulce 5.

Tab. 5 Příklad šifrování Caesarovou šifrou

Zpráva	P	L	A	I	N	T	E	X	T
Šifrovaná zpráva	M	I	X	F	K	Q	B	U	Q

Afinní šifra

Afinní šifra je substituční šifra, která eliminuje zásadní nevýhodu Caesarovi šifry – málo možností transformace.[9]

Základem afinní šifry je následující transformace:

$$C_i = a * T_i + b \pmod{m} \quad (2)$$

C_i – i-té písmeno šifrovaného textu

T_i – i-té písmeno otevřeného textu

a – parametr a , $\gcd(a,m) = 1$

b – parametr b

m – modulo

Za modulo volíme prvočíslo, aby bylo předem jasné, že $\gcd(a,m) = 1$, a zároveň abychom útočníkovi nezjednodušovali práci (pokud modulo není prvočíslo, tak je méně možností, jak se dá text šifrovat a je tedy snazší šifru prolomit)[9]

■ Přeházená abeceda

Jedná se o jeden z nejstarších a v různých modifikacích i o nejpoužívanější šifrovaný systém. V této šifře se každý znak otevřeného textu nahradí jedním znakem šifrované abecedy. Šifrovaná abeceda se použije pro celý otevřený text stejná. [1]

Celkově existuje $26!$ permutací abecedy s 26 písmeny. Takto velký počet kombinací vylučuje využití útoku hrubou silou.

Jednu z možností, jak vytvořit převodovou tabulku šifry dokumentuje tabulka 6.

Tab. 6 Příklad převodové tabulky přeházené abecedy

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

■ Využití klíčového slova

Obě strany se dohodnou na klíči, který se zapíše na začátek šifrované abecedy. Dále pokračuje abeceda stejná jako otevřená, ale s vynecháním písmen z klíče. V případě, že se v klíči vyskytují stejná písmena, vynechají se písmena vyskytující se vícekrát – vyjma prvního.

Například slovo pouzdro se zapíše jako pouzdr.

Následující tabulka 7 demonstruje sestavení šifrované abecedy za pomoci klíče.

Tab. 7 Příklad převodové tabulky pro využití klíčového slova

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

4.2 Polyalfabetická substitute

Polyalfabetická substitute se skládá z několika jednoduchých substitučních šifer, které jsou podle dohodnutého systému postupně použity na jednotlivé znaky otevřeného textu. Pokud k převodu otevřeného textu napsaného v mezinárodní abecedě na šifrovaný text použijeme například 26 různých jednoduchých substitučních šifer, pak každé písmeno otevřeného textu může být zašifrováno 26 různými způsoby.[1]

■ Vigenère šifra

Vigenèrova šifra je pravděpodobně nejznámější polyalfabetickou šifrou. Své jméno nese po Blaisovi de Vigenèrere, francouzském diplomantovi z 16. století. Vigenèrova šifra byla

používaná konfederační armádou v Americké občanské válce. Ta ovšem propukla až poté, co byla tato šifra prolomena. [2]

Vigenèrova šifra používá tzv. Vigenèrův čtverec, který můžeme vidět na obrázku 1. Sloupec po levé straně (klíčový sloupec) obsahuje anglickou abecedu. Každé písmeno má svou vlastní řadu, v níž je taktéž celá abeceda, ale je posunutá v závislosti na klíčovém znaku v prvním sloupci. Každé písmeno v levém sloupci tvoří tedy Caesarovu šifru, jejíž posun je určen právě tímto písmenem. Například u písmene h je Caesarova šifra s posunem 6. [2]

	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

Obr. 1 Vigenèrův čtverec[18]

Pro zašifrování a dešifrování je zapotřebí, aby si obě strany zvolili klíč. Klíč si uživatel zapíše opakovaně nad otevřený text, aby věděl, jakou abecedu má pro zašifrování (resp. dešifrování) konkrétního písmene použít.[1]

Vyzkoušíme-li například zašifrovat zprávu PLAINTEXT klíčovým slovem fred dostaneme výsledek zachycený v tabulce 8.

Tab. 8 Příklad zápisu klíče Vigenèrovi šifry

Zpráva	P	L	A	I	N	T	E	X	T
Klíč	F	R	E	D	F	R	E	D	F

K zašifrování prvního písmene P použijeme klíčové písmeno pod ním, jímž je v tomto případě f. Takže pro zašifrování P přejdeme ve čtverci na řádek označený jako f a přečteme písmeno, které se nachází ve sloupci P. Tím je v našem případě U. Stejným způsobem pokračujeme i s ostatními písmeny a získáme zašifrovaný text UCESLIAY.[2]

Výsledek je zachycen v následující tabulce 9:

Tab. 9 Příklad šifrování pomocí Vigenèrovi šifry

Zpráva	P	L	A	I	N	T	E	X	T
Klíč	F	R	E	D	F	R	E	D	F
Šifrovaný text	U	C	E	L	S	L	I	A	D

Autoklíč

Autoklíč je modifikace Vigenèrovi šifry. Jedná se o bezpečnější variantu, než je použití periodického klíče. Osoba, která text šifrovala, se domluví s příjemcem na počátečním písmenu, které tvoří začátek autoklíče. Nad otevřený text zapíše klíč, který vytvoří z dohodnutého písmene, jež následují znaky otevřeného textu. To, co vznikne, se nazývá autoklíč otevřeného textu. Nyní zašifruje jednotlivé znaky otevřeného textu podle postupu výše.[1]

4.3 Polygrafická substituce

Polygrafická šifra používá skupinu znaků jako základní jednotku pro šifrování. To dává celkem 676 možností, jak zašifrovat každý znak. Šifra je tak více odolná proti útokům než monoalfabetická šifra.[10]

Playfair šifra

Šifru Playfair navrhl v roce 1854 britský všetranný vědec Charles Wheatstone. Jméno dostala podle propagátora této šifry, skotského barona a poslance britského parlamentu Lyona Playfaira. Šifra byla používána jako vojenská polní šifra v omezené míře dokonce ještě i za 2. Světové války.[1]

Ještě před použitím Playfair šifry je zapotřebí zprávu upravit pomocí následujících kroků.

- Celý text zbavíme háčků, čárek, interpunkce, a pokud obsahuje písmeno J, všude ho změním na I.
- Všechna písmena rozdělíme do párů.
- Dvojitá písmena, jestliže se vyskytnou v páru, musí být oddělena písmenem X nebo Z. Použitím jednou X a jednou Z se šifra vyhne přivolání pozornosti k písmenu, které by bylo použito dvakrát stejným způsobem.
- Podobně písmeno X nebo Z doplníme na konec zprávy, pokud by měl původní text lichý počet písmen.[11]

Klíčem je čtverec rozdělený na 5 x 5 polí (což omezuje počet písmen na 25, vynechává se J v anglickém jazyce a W v českém jazyce), takže máme k dispozici 25! klíčů.

Pro sestavení čtverce si musíme dohodnout heslo, které by mělo mít nejméně pět písmen, může být i delší. Nejdříve napíšeme zvolené heslo, písmena, která se opakují, vynecháváme. Potom postupně zapíšeme zbývající písmena abecedy, přičemž I a J píšeme jako I viz Tab. 10.[11]

Příklad abecedního čtverce s heslem HESLO:

Tab. 10 Příklad abecedního čtverce

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

Transformace šifrou je založena na skutečnosti, že záznam každého páru v nešifrovaném textu se může v abecedním čtverci vyskytnout pouze v jednom ze tří stavů. Pár může být

společně v jednom řádku, jednom sloupci, nebo – nejčastěji – ani v jednom. Šifrování pak probíhá takto:

1. Každé písmeno v páru písmen, která spadají do stejného řádku, je nahrazeno písmenem vpravo od něj. Písmeno napravo od posledního písmene v řádku je první písmeno téhož řádku.
2. Každé písmeno v páru písmen, která spadají do stejného sloupce, je nahrazeno písmenem pod ním. Písmeno pod posledním písmenem ve sloupci je první písmeno téhož sloupce.
3. Každé písmeno v páru písmen, která nespádají do stejného řádku ani do stejného sloupce, je nahrazeno písmenem nacházejícím se v průsečíku jeho vlastního řádku a sloupce obsahujícího druhé písmeno z páru. Musí se dodržet pořadí v páru: nejdříve určete průsečík řádku prvního písmene se sloupcem druhého písmene, potom průsečík řádku druhého písmene se sloupcem prvního písmene. [11]

Dešifrování probíhá opačným procesem k šifrování.

4.4 Homofonní substituce

Homofonní šifrování vylepšuje jednoduchou substituční šifru. Šifrovací abeceda je doplněna o další písmena tak, že například písmeno E z otevřeného textu je zastoupeno v šifrovaném textu více než jedním znakem. Těmto přidaným písmenům se říká znáhodňující prvky a proces rozšifrování abecedy je znám jako homofonní šifrování.[2]

5 ZÁKLADNÍ METODY KRYPTOANALÝZY

5.1 Frekvenční analýza

Jedním ze způsobů, kterak rozluštit šifrovanou zprávu, známe-li její jazyk, je nalézt odlišný otevřený text v tomtéž jazyce, dlouhý alespoň na arch papíru či podobně, a spočítat výskyty jednotlivých písmen v něm. Nejčastější písmeno nazveme pak „prvním“, druhé nejčastější „druhým“, další „třetím“ a tak dále, dokud je nepojmenujeme všechna. Pak pohlédneme na šifrovaný text, který chceme rozluštit, a rovněž sečteme výskyty symbolů. Najdeme nejčastější symbol a zaměníme jej písmenem označeným jako „první“ ze vzorku otevřeného textu. Druhý nejčastější symbol pak nahradíme písmenem „druhým“, následující „třetím“ a tak dále, dokud všechny symboly nezaměníme za písmena.[1]

Vysvětlení snáze pochopíme na běžné anglické abecedě. Nejprve musíme prostudovat delší úsek běžného anglického textu, možná několik různých textů, abychom zjistili frekvenci výskytu každé hlásky. V češtině se nejčastěji vyskytuje hláska e, následuje a, pak o - a tak dále (viz tabulka 6). V dalším kroku prozkoumáme šifrový text a stanovíme četnost výskytu jeho hlásek. Pokud se v něm jako nejčastější symbol vyskytuje například J, pak je velmi pravděpodobné, že toto písmeno nahrazuje hlásku e. Pokud je druhým nejčastějším symbolem v šifrovém textu P, pak jde pravděpodobně o náhradu za a - a tak dále. Technika popsaná al-Kindím, známá dnes jako *frekvenční analýza*, ukazuje, že není třeba zkoušet každý klíč z miliard možných. Namísto toho lze zjistit obsah zašifrovaného textu jednoduchou analýzou četnosti znaků v šifrovém textu.[1]

Frekvenční analýza českého jazyka

Následující tabulka 11 ukazuje četnost písmen v českém jazyce s diakritikou.

Tab. 11 Frekvence českých písmen[13]

znak	četnost v %	znak	četnost v %	znak	četnost v %
a	6,698	i	4,571	s	4,620
á	2,129	í	3,103	š	0,817
b	1,665	j	1,983	t	5,554
c	1,601	k	3,752	ť	0,038
č	1,017	l	4,097	u	3,131
d	3,613	m	3,262	ú	0,145
ď	0,019	n	6,676	ů	0,569
e	7,831	ň	0,073	v	4,378
é	1,178	o	8,283	w	0,072
ě	1,491	ó	0,032	x	0,092
f	0,394	p	3,454	y	1,752
g	0,343	q	0,006	ý	0,942
h	1,296	r	3,977	z	2,123
ch	1,007	ř	1,186	ž	1,022

Jelikož se obvykle luští a šifruje bez diakritických znamének, tak tabulka 12 zobrazuje četnost písmen české abecedy zbavených diakritiky.

Tab. 12 Frekvence českých písmen bez diakritiky[12]

znak	četnost v %	znak	četnost v %	znak	četnost v %
a	9,589	j	2,305	s	5,585
b	1,776	k	3,528	t	5,385
c	2,999	l	5,720	u	3,579
d	3,774	m	3,605	v	3,952
e	10,904	n	5,917	w	0,054
f	0,175	o	8,029	x	0,035
g	0,219	p	3,114	y	2,857
h	2,497	q	0,0005	z	3,302
i	6,668	r	4,396		

Následující dvě tabulky 13 a 14 ukazují 40 nejfrekventovanějších bigramů (dvojic písmen) a 40 nejfrekventovanějších trigramů (trojic písmen) v českém jazyce.

Tab. 13 Nejfrekventovanějších 40 bigramů[13]

st	74285	en	50645	le	38926	to	36355	ho	31442	al	29682	př	27885	em	26818
ní	60525	na	46737	ko	38688	ou	35191	do	30665	ed	29622	at	27603	in	26427
po	56239	je	42433	ne	38671	no	32612	os	30530	an	29326	ře	27181	sk	26085
ov	53818	pr	42099	od	38393	la	32336	se	30454	ce	28280	er	27168	lo	25981
ro	51961	te	40393	ra	37531	li	31952	ta	30177	va	27987	ti	26858	ně	25739

Tab. 14 Nejfrekventovanějších 40 trigramů[13]

pro	21322	ení	11917	ého	9475	ick	8387	edn	7429	ání	7224	pol	6704	val	6256
ost	18722	ova	11822	sti	9121	ová	8139	ské	7349	ent	7114	spo	6686	dní	6251
sta	12746	pod	10168	řed	9103	při	7878	pří	7348	str	6903	vat	6489	sto	6189
pře	12057	kte	9603	kon	9017	sou	7541	odn	7251	ové	6810	ním	6439	tak	6175
ter	11936	pra	9521	nos	8557	ist	7505	tel	7231	nov	6783	jak	6330	lov	6139

5.2 Index koincidence

Index koincidence nám udává, jak velká je pravděpodobnost, že když náhodně vybereme z textu dvě písmena, že budou stejná. Například v textu „aaaaa“ máme 100% pravděpodobnost, že zvolená dvojice bude stejná. V textu „aaaabbc“ bude pravděpodobnost $1/3$ a nejpravděpodobnější bude, že zvolíme dvě písmena „a“. [14]

Index koincidence můžeme vyjádřit jako:

$$IC = \frac{\sum_{i=1}^c n_i(n_i-1)}{N(N-1)/c} \quad (4)$$

kde N je celkový počet znaků, c označuje počet znaků abecedy a n_i je počet znaků s indexem i kde $i \in \{0,1 \dots 25\}$

Index koincidence náhodného textu

Máme-li dlouhý náhodný text s uniformním rozdělením písmen, vyskytují se v něm všechna písmena přibližně stejně často. Můžeme říci, že u nekonečně dlouhého textu s uniform-

ním rozdělením písmen budeme mít vždy pravděpodobnost $1/26$, že náhodně zvolíme dané písmeno. (Počítáme s anglickou abecedou, která má 26 písmen.) [14]

V takovém textu bychom pro každé písmeno získali pravděpodobnost $\frac{1}{26} \cdot \frac{1}{26}$, že vybereme stejnou dvojici písmen. Protože máme celkem 26 různých písmen, tak celková pravděpodobnost, že náhodně vybereme dvě stejná písmena je: [14]

$$\sum_{i=1}^{26} \frac{1}{26} \cdot \frac{1}{26} = \frac{26}{676} = \frac{1}{26} \quad (5)$$

Index koincidence jazyka

Protože text napsaný v nějakém běžném jazyku například v češtině není náhodný text, má i jiný index koincidence než náhodný text. Následující tabulka 15 zobrazuje index koincidence vybraných jazyků.

Tab. 15 Index koincidence vybraných jazyků

Jazyk	Index koincidence
čeština	0.06027
angličtina	0.06689
dánština	0.07073
finština	0.07380
francouzština	0.07460
holandština	0.07981
němčina	0.07667
italština	0.07329
ruština	0.05607
španělština	0.07661

Využití indexu koincidence

Je-li text zašifrován monoalfabetickou šifrou, měl by se jeho index koincidence blížit indexu koincidence jazyka, ve kterém byl napsán. Je-li text zašifrován polyalfabetickou šifrou, bude se jeho index koincidence blížit indexu koincidence náhodně generovaného jazyka.

5.3 Útok hrubou silou

Útok hrubou silou (anglicky brute force attack) je většinou pokus o rozluštění šifry bez znalosti jejího klíče k dešifrování. V praxi se jedná o systematické testování všech možných kombinací nebo omezené podmnožiny všech dostupných kombinací.[23]

6 KRYPTOANALÝZA SUBSTITUČNÍCH ŠIFER

Neexistuje žádná „zlatá cesta“, jak luštit substituční šifry a dosáhnout jednoznačného výsledku pro jakoukoliv substituční šifru, ale můžeme říci, že začátek by měl být pro všechny stejný. Na začátku šifrování vypočítáme index koincidence a zkusíme odhadnout, o jakou šifru se jedná, popřípadě jakým jazykem je napsána. Poté již luštíme konkrétní šifru a využijeme metody, které jsou pro ni určeny.

6.1 Kryptoanalýza monoalfabetické šifry

Jednoduchý posun

Jednoduchý posun má jednu zajímavou vlastnost vyplývající z její definice. Protože pouze posouvá písmena, vždy o stejnou vzdálenost, tak vzdálenosti písmen v otevřeném textu a šifrovém textu zůstávají stejné. [19]

Například pokud by otevřený text byl „abe“ a my bychom ho zašifrovali s klíčem „g“, získali bychom šifrový text „ghk“. Přitom vzdálenost mezi písmeny „a“, „b“, označíme $|a, b|$, je rovna jedné: $|a, b| = 1$ a pro písmena v šifrovém textu platí $|g, h| = 1$. Podobně pro dvojici $|b, e| = 3$ a $|h, k| = 3$ a nakonec pro dvojici $|a, e| = 4$ a $|g, k| = 4$.

Jediný problém nastává, pokud jdeme přes poslední písmeno, přes „z“. Pak to totiž nesedí. Pokud bychom zašifrovali „xz“ s klíčem „c“, tak bychom získali šifrový text „zb“. tom $|x, z| = 2$, ale $|z, b| = 24$. [19]

Aby to sedělo, musíme vždy počítat kratší z cest. Tzn., že z „b“ se můžeme do „z“ dostat buď směrem „bcd...xyz“, to by nám vrátilo vzdálenost 24, anebo opačným směrem „baz“, což by nám vrátilo vzdálenost 2 – to je správná vzdálenost. Vždy tak budeme brát tu kratší z obou vzdáleností. Tuto vzdálenost nazveme *minimální vzdálenost písmen*. [19]

V tabulkách najdeme tři nejčastěji používaná písmena v českém textu. To jsou „e, a, o“. Nyní v šifrovém textu najdeme šest nejčastějších písmen. V těch šesti nejčastějších písmenech nyní nalezneme takovou trojici písmen, která má mezi sebou stejné minimální vzdálenosti, jako má trojice písmen „e, a, o“. Pokud takovou trojici nalezneme, pravděpodobně jsme našli trojici písmen, na kterou se zašifrovala trojice písmen „e, a, o“. Z této informace už můžeme snadno odvodit posun šifry. [19]

Afinní šifra

Při dešifrování musíme eliminovat transformaci vzniklou šifrováním. Provedeme proto takovou transformaci:

$$T_i = (C_i - b) \cdot a^{-1} \bmod 26 \quad (6)$$

kde

C_i – i-té písmeno šifrovaného textu

T_i – i-té písmeno otevřeného textu

a – parametr a , $\gcd(a, m) = 1$

b – parametr b

a^{-1} – multiplikativní inverze a v Z_m

m – modulo

Pro prolomení šifry musíme odhadnout a^{-1} a b . Postupujeme tak, že se pokusíme napařovat alespoň 2 písmena šifrované abecedy na původní otevřenou abecedu. Poté sestavíme soustavu dvou rovnic o dvou neznámých pro šifrování:

$$C_1 = (a \cdot T_1 + b) \bmod 26 \quad (7)$$

$$C_2 = (a \cdot T_2 + b) \bmod 26 \quad (8)$$

kde T_1 a T_2 jsou písmena otevřeného textu a C_1 a C_2 jsou odpovídající písmena šifrovaného textu.

Odečteme první rovnici od druhé a vypočítáme multiplikativní inverzi pomocí rozšířeného Euklidova algoritmu a získáme proměnnou a . Dosadíme do druhé rovnice a získáme proměnnou b .

Nyní již můžeme dešifrovat dle vzorce (6).

Rozšířený Euklidův algoritmus

Euklidův algoritmus, který byl uveřejněn řeckým matematikem Euklidem v knize cca 300 let př.n.l., slouží k nalezení nejvyššího společného dělitele dvou čísel (značíme gcd - greatest common divisor), jeho rozšířená verze pak i k nalezení multiplikativní inverze čísla $x \bmod (m)$. [20]

Rozšířená verze Euklidova algoritmu umožňuje nalézt multiplikativní inverzi na tělese Z_p , kde p je prvočíslo. Není nezbytně nutné, aby se jednalo o těleso, ale v takovém případě nemáme zaručeno, že inverze bude existovat. [20]

Nalezněte multiplikativní inverzi čísla 15 v Z_{133} . Předpokládejme, že $\gcd(133,15)$ je 1, protože jinak by multiplikativní inverze neexistovala. Vždy se nyní rozepsat zbytky tak, aby byly vyjádřeny jako součet násobků čísel 133 a 15. Proto očekáváme, že v posledním korku vyjde rovnost tvaru $x \cdot 133 + y \cdot 15 = 1$, kde 1 je nejvyšší společný dělitel těchto čísel. Protože jsme v Z_{133} tak víme, že $x \cdot 133$ je kongruentní s 0 a tedy y je multiplikativní inverzí čísla 15 v Z_{133} . [20]

6.2 Kryptoanalýza polyalfabetické šifry

Základem pro prolomení této šifry je určení délky klíče. Pro určení délky klíče je možné využít hned několik metod.

Kasiského metoda

Existuje postup, kterým lze alespoň přibližně odhadnout délku použitého klíče, případně snížit počet možných klíčů na nějakou rozumně malou množinu. Tuto slabinu objevili nezávisle na sobě dva lidé: Charles Babbage a Friedrich Kasiski. Prvním byl sice Babbage, ale prvním publikujícím byl Kasiski, takže se metoda jmenuje po něm – Kasiského metoda nebo Kasiského test.[17]

V šifrovaném textu hledáme opakující se polygramy, stejné kombinace aspoň dvou po sobě jdoucích písmen. Pokud tyto kombinace opravdu odpovídají stejným slovům nebo částem slov v otevřeném textu, pak jejich vzdálenost v šifrovém textu musí být násobkem délky klíče. Tímto způsobem najdeme délku klíče, případně ji redukuje na několik málo možností. Čím delší je opakovaný polygram, který v šifrovém textu najdeme, tím lépe. Ale i opakované bigramy mohou být k užitku.[16]

Index coincidence

Index coincidence použijeme pro testování, zda daná délka je délkou původního šifrového klíče Vigenèrovy šifry.

Odhadneme, že by klíč mohl být v rozmezí 2 až 15 (proč zrovna 15? Je to jedno.) Označme: $K_o = \{2, \dots, 15\}$. Pomocí kasiského metody zjistíme další množinu pravděpodobných klíčů, označme ji K_k . [14]

Obě množiny sjednotíme $K = K_o \cup K_k$. Získáme tím všechny pravděpodobné délky Vigenèrovy šifry. Jinými slovy – budeme zkoušet všechny délky mezi 2 a 15 plus ty délky, které vrátí Kasiského test. [14]

Pro každou délku klíče, tj. pro každé $k \in K$: rozdělíme šifrový text do k bloků, v prvním bloku bude vždy 1. písmeno šifrového textu, $(1 + k)$ -té písmeno, $(1 + 2k)$ -té písmeno, atd. Ve druhém bloku bude vždy 2. písmeno šifrového textu, $(2 + k)$ -té písmeno, $(2 + 2k)$ -té písmeno, atd. Bloky si označíme B_i . [14]

Pro každý blok B_i spočítáme index coincidence IC_i . A následně spočítáme průměrný index coincidence všech bloků. Nalezneme délku klíče, která má odpovídající index coincidence nejmenší. Tuto délku má pravděpodobně i originální klíč. [14]

Ve chvíli, kdy známe délku klíče, můžeme rozdělit šifrový text na jednotlivé bloky textu, které jsou vždy zašifrovány jednoduchým posunem o stejném klíči. Pokud například zjistíme, že klíč má délku 3, rozdělíme šifrový text na 3 bloky textu. V prvním bloku bude 1., 4., 7., ... písmeno otevřeného textu, ve druhém bloku 2., 5., 8., ... písmeno atd. Každý blok prolomíme jako jednoduchý posun a nakonec všechny tyto klíče spojíme do jednoho slova, čímž získáme hledaný klíč Vigenèrovy šifry. [18]

II. PRAKTICKÁ ČÁST

7 PROGRAMOVÁ ČÁST

Cílem praktické části je vytvořit program v prostředí Java, který implementuje dostupné metody kryptoanalýzy substitučních šifer a dává možnost nahlédnout pod proces kryptoanalýzy. S využitím Frameworku JavaFX je vytvořeno uživatelské prostředí, které poskytuje možnost provést snadněji kryptoanalýzu substitučních šifer popsanych v teoretické části.

7.1 Java

Historie programovacího jazyka Java se začala psát na počátku 90. let, kdy ve společnosti Sun Microsystems vznikla v týmu Jamese Goslinga iniciativa pro vytvoření jednoduchého, ale efektivního jazyka určeného pro spotřební elektroniku. Výsledný jazyk se jmenoval Oak.[21]

V roce 1995, kdy internet začal masivně pronikat do každodenního života, si lidé ze Sun Microsystems uvědomili, že mají v ruce jazyk, který je velmi dobře použitelný na webu. Oak byl přejmenován na Java a byla vydána její první veřejná verze 1.0, která se stala populární zejména díky Java Appletům.[21]

V roce 1997, byla Java 1.1 stažena více než 220 tisíckrát během prvních třech týdnů po uvedení. Za rok 1998 toto číslo vzrostlo již na 2 miliony. V roce 1998 došlo v rámci verze 1.2 k rozdělení Javy do třech částí dle uplatnění (Micro Edition, Standard Edition, Enterprise Edition). V roce 2005 již Javu používalo přes 4,5 milionu vývojářů a podporovalo ji více než 2,5 miliardy zařízení. V současné době (srpen 2010) je Java (nyní verze 1.6) jedním z nepoužívanějších imperativních programovacích jazyků na světě.[21]

Program v jazyce Java je interpretován prostřednictvím virtuálního počítače (Java Virtual Machine, JVM), díky čemuž je nezávislý na konkrétním hardwaru či operačním systému. Původně se jednalo o čistě interpretovaný jazyk, ale dnes z důvodu rychlosti převažuje JIT kompilace. Nejfrekventovanější části kódu (cykly) jsou za běhu (Just-In-Time) překládány do nativního kódu. Rychlost vykonávaného mezikódu (bytecode) ovšem nemůže dosahovat rychlosti nativního kódu.[20]

Společnost Sun definuje programovací jazyk Java jako jednoduchý, objektově orientovaný, distribuovaný, robustní, bezpečný, nezávislý na architektuře, portabilní, interpretovaný, vysoce výkonný a vícevláknový.[20]

JavaFX

JavaFX je moderní framework pro tvorbu bohatých okenních aplikací. Bohatých je zde myšleno vizuálně. JavaFX přináší podporu obrázků, videa, hudby, grafů, CSS stylů a dalších technologií, které zajistí, že výsledná aplikace je opravdu líbivá. Zároveň je kladen důraz na jednoduchost tvorby, všechny zmiňované věci jsou v JavěFX v základu. JavaFX se hodí jak pro desktopové aplikace, tak pro webové applety nebo mobilní aplikace.

V JavaFX je možné vyvíjet podobně jako ve starším Swingu, tedy tak, že tvoříte instance jednotlivých formulářových prvků (tlačítko, textové pole). Ty poté vkládáte do tzv. layoutů, což jsou vlastně kontejnery na formulářové komponenty.[21]

Druhým způsobem, je FXML. FXML je jazyk pro návrh formulářů. Asi vás podle názvu nepřekvapí, že je to další jazyk odvozený z XML. Použití XML pro návrh prezentační části aplikace (to je ta část, se kterou komunikuje uživatel) není nic nového, naopak se jedná o osvědčený princip z webových aplikací. Java se zde stejně jako C# inspiruje a přenáší principy HTML a CSS do desktopových aplikací.[21]

Zdrojový kód

Zdrojový kód byl sepsán v IDE Eclipse a je součástí přiloženého CD. Je členěn do balíků sdružující třídy, které k sobě logicky svým obsahem patří.

GUI hlavního panelu bylo vytvořeno pomocí JavaFX Scene Builderu 2.0 s použitím FXML kódu. Ostatní okna jsou vytvořena klasickou metodou tvoření instancí jednotlivých formulářových prvků a vkládáním těchto prvků do layoutů. Toto grafické rozhraní je odděleno od tříd, obsahujících jednotlivé šifrovací mechanismy a funkce.

V budoucnu je případně možné doplnit projekt o další šifry nebo jiné funkce.

Vstupy a výstupy aplikace

Program pracuje s textovými vstupy a výstupy. Vstupem je textový soubor, který se dá otevřít pomocí horního menu Soubor → Otevřít. Textový vstup musí mít minimální délku sto znaků.

Výstupem je opět textový soubor, ve kterém je zapsán obsah textového pole dešifrovaný text. Takovýto textový soubor lze vytvořit pomocí horního menu Soubor → Uložit jako.

Funkce aplikace

Aplikace obsahuje následující funkce:

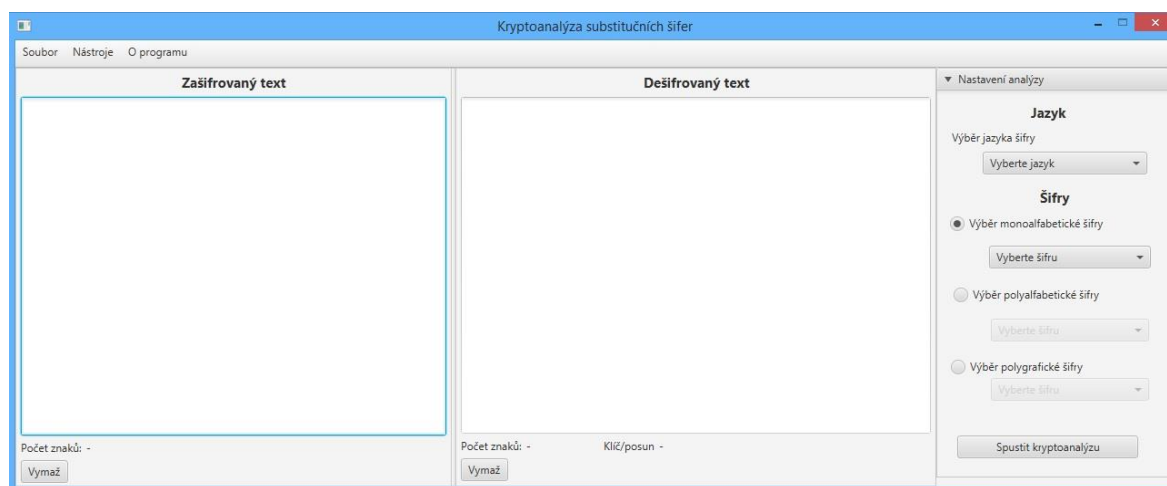
- Možnost otevřít textový dokument se zašifrovaným textem
- Možnost uložení dešifrovaného textu do textového dokumentu
- Frekvenční analýzu šifrovaného textu s grafickým a tabulkovým porovnáním frekvenční analýzy českého nebo anglického jazyka
- Uložení grafu frekvenční analýzy do obrázku formátu jpg.
- Porovnání nejčastějších trigramů a bigramů šifrovaného textu s nejčastějšími trigramy a bigramy českého nebo anglického jazyka
- Výpočet indexu koincidence šifrovaného a náhodného textu
- Kryptoanalýzu monoalfabetické substituce, konkrétně šifry Jednoduchá záměna, Atbash a Afinní, v českém a anglickém jazyce s možností zobrazení mezivýsledků.
- Kryptoanalýza polyalfabetické substituce, konkrétně Vigenèrovi šifry v českém a anglickém jazyce s možností zobrazení mezivýsledků
- Dešifrování polygrafické substituce, konkrétně Playfair šifry
- Úpravu výstupu pomocí výměny jednotlivých písmen

8 POPIS APLIKACE

Aplikaci můžeme rozdělit na několik částí, jejichž základním společným prvkem je hlavní panel aplikace. Každá substituční šifra má své vlastní okno, ve kterém se zobrazují výsledky a průběh kryptoanalýzy. V následujících kapitolách jsou popsány všechny prvky aplikace včetně jejich použití.

8.1 Hlavní panel

Po spuštění aplikace se zobrazí hlavní okno aplikace, které je znázorněno na obrázku 2. Obsahuje 2 textová pole pro šifrovaný text a dešifrovaný text, horní menu a pravé menu.



Obr. 2 Hlavní okno aplikace

Horní menu

Horní menu obsahuje položky Soubor, Nástroje a O programu.

Soubor

Menu soubor obsahuje položky Otevřít, Uložit jako, Zavřít.

1. *Otevřít* - pomocí této položky lze vybrat textový soubor uložený na disku, který slouží jako vstup do textového pole Zašifrovaný text. Program dovoluje otevřít pouze textové soubory, ostatní soubory nejsou implementovány.
2. *Uložit jako* - pomocí položky uložit jako lze uložit obsah textového pole Dešifrovaný text do textového souboru kdekoliv na disk.
3. *Zavřít* - ukončí program

Nástroje

Menu Nástroje obsahuje položky Frekvenční analýzy a Index koincidence.

1. Frekvenční analýza - tato položka umožňuje zobrazit grafické a tabulkové porovnání frekvenční analýzy šifrovaného textu a uživatelem zvoleného jazyka. Detailněji je popsána v kapitole 8.2.
2. Index koincidence – položka zobrazí nové okno s tabulkou indexu koincidence pro anglický a český jazyk a vypočítanou hodnotu indexu koincidence šifrovaného textu. Detailněji popsán v kapitole 8.3.

O programu

Zobrazuje krátké informace o programu a autorovi.

Textová pole

Textová pole slouží k zobrazení vstupu a finálního výstupu programu.

Textové pole – Šifrovaný text

Textové pole - šifrovaný text představuje vstup pro jednotlivé metody kryptoanalýzy. Vstup je před zobrazením v textovém poli upraven tak, že je zbaven diakritiky, převeden na velká písmena a rozdělen do pětic. Již upravený text lze vidět na obrázku 3.

Textové pole – Dešifrovaný text

Textové pole dešifrovaný text představuje výstup jednotlivých metod kryptoanalýzy. Stejně jako v textovém poli pro vstup i zde je text upraven do tvaru, který je vidět na obrázku 5. Pomocí volby Uložit jako v horním menu, lze jeho obsah uložit do textového souboru na disk.

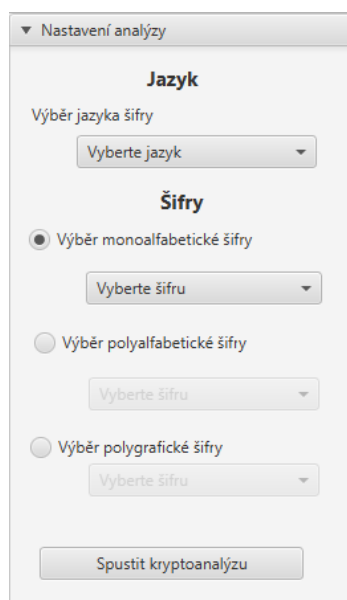


Obr. 3 Ukázka úpravy textu v textovém poli

Obě textová pole jsou needitovatelná. V případě potřeby smazání vstupního nebo výstupního textového pole, lze využít tlačítka Vymaž, která jsou umístěna pod těmito textovými poli.

Pravé menu

Pravé menu obsahuje základní nastavení nezbytné pro spuštění kryptoanalýzy. A to výběr jazyka šifry a výběr samotné šifry. Jeho detail je zobrazen na obrázku 4.



Obr. 4 Detail levého menu

Výběr jazyka

Pomocí výběru jazyka lze zvolit mezi anglickým a českým jazykem šifry. V případě, že jazyk šifry nevíme, využijeme nástroj index koincidence, popsáný výše, který nám může pomoci jazyk šifry určit.

Výběr šifry

Pomocí radio tlačítka můžeme volit mezi monoalfabetickou, polyalfabetickou nebo polygrafickou substitucí.

Monoalfabetická substituce obsahuje jednoduchý posun, Atbash šifru a Afinní šifru. Polyalfabetická substituce je zaměřena na Vigenèrovu šifru a polygrafická substituce obsahuje šifru Playfair.

Tlačítko spustit kryptoanalýzu

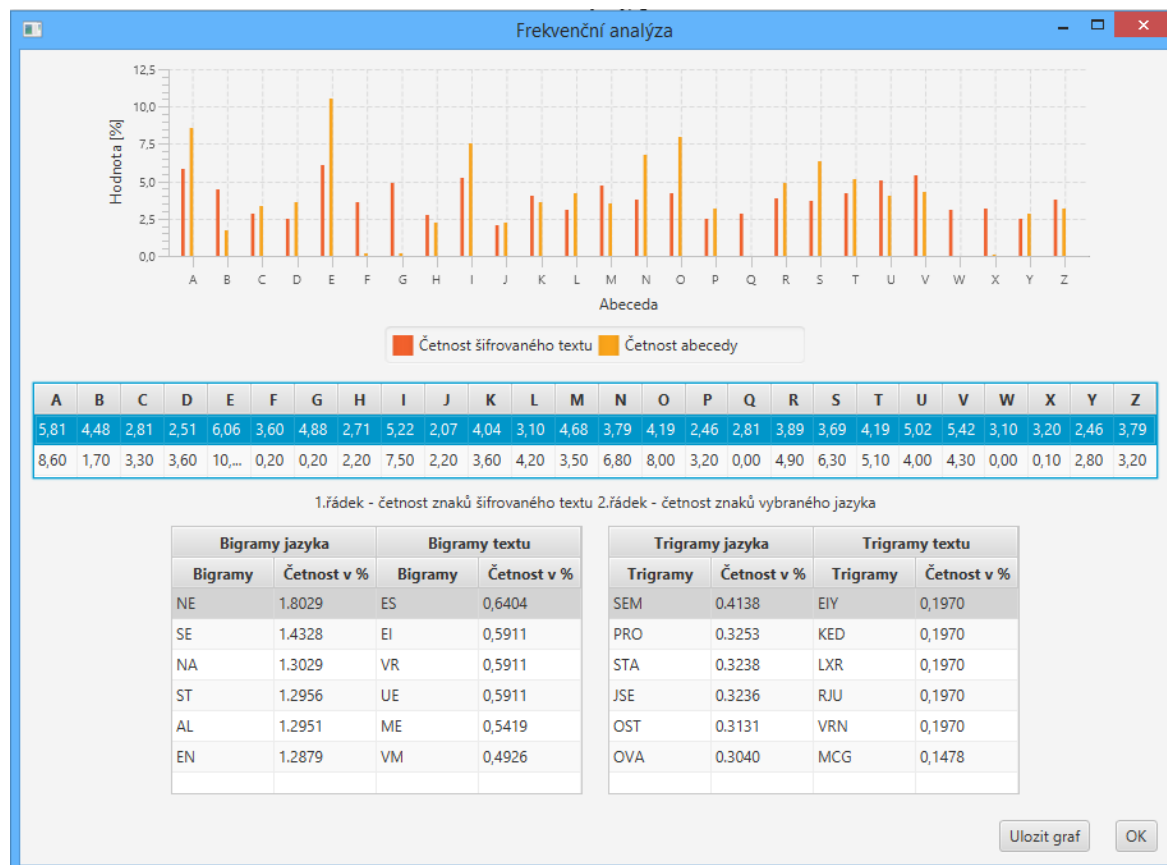
Spustí kryptoanalýzu substituční šifry dle vybraných parametrů.

8.2 Okno frekvenční analýzy

Pokud chceme zobrazit frekvenční analýzu šifrovaného textu, musíme nejdříve nastavit všechny její parametry.

Frekvenční analýza přebírá 2 parametry na vstupu – jazyk šifry, který vybereme v levém panelu, a šifrovaný text, který vložíme do textového pole Zašifrovaný text pomocí menu Soubor – Otevřít.

Pokud budou všechny parametry správně nastaveny, zobrazí se okno frekvenční analýzy, které je zobrazeno na obrázku 5. V opačném případě program vyzve k zadání všech parametrů.



Obr. 5 Okno frekvenční analýzy šifrovaného textu

Okno frekvenční analýzy obsahuje některé statistické údaje o zadaném textu. Jedná se o sloupcový graf, který zobrazuje četnost písmen ve vybraném jazyce (oranžová barva) a zároveň četnost písmen v šifrovaném textu (červená barva).

Stejnou statistiku zobrazuje první tabulka pod grafem. Tedy četnost písmen v šifrovaném textu (1. řádek) a četnost písmen ve vybraném jazyce (2. řádek).

Další dvě tabulky zobrazují četnosti 6 nejčastějších bigramů a trigramů v šifrovaném textu a ve vybraném jazyce.

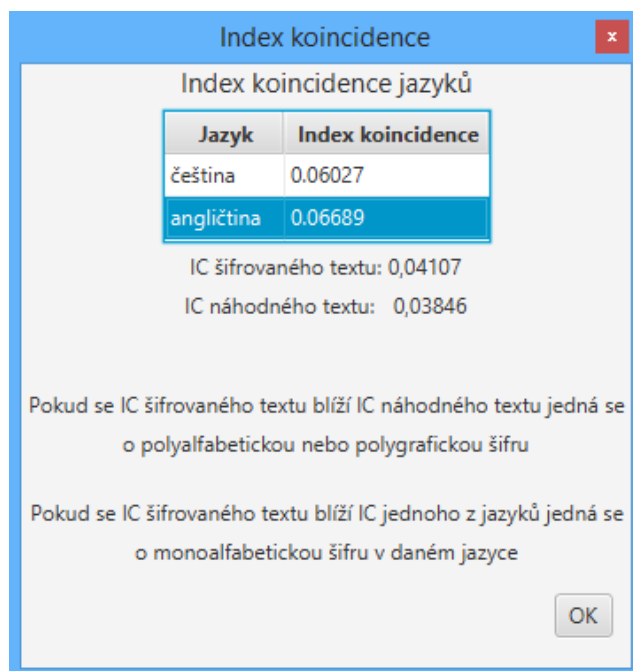
Všechny četnosti jsou uvedeny v procentech.

Graf frekvenční analýzy je možné uložit jako obrázek a to tlačítkem Uložit graf. Po kliknutí na tlačítko se graf uloží jako obrázek ve formátu jpg a to do souboru na disk, ve kterém je uložen spouštěcí soubor BakalarskaPrace.jar.

Kliknutím na tlačítko OK, okno frekvenční analýzy ukončíme.

8.3 Okno indexu koincidence

Po zavolání indexu koincidence v horním menu se zobrazí okno indexu koincidence, které můžeme vidět na obrázku 6.



Obr. 6 Okno indexu koincidence

Okno indexu koincidence zobrazuje tabulku, která udává index koincidence českého a anglického jazyka.

Pod touto tabulkou jsou vypočítány indexy koincidence šifrovaného textu a náhodného textu. Postup výpočtu byl popsán v kapitole 5.2.

Kliknutím na tlačítko OK, okno indexu koincidence ukončíme.

8.4 Vizualizace kryptoanalýzy

Abychom mohli zobrazit panely jakékoliv kryptoanalýzy, musíme nejdříve pomocí hlavního okna programu nastavit jejich parametry. Všechny kryptoanalýzy uvedené v programu přebírají tři parametry:

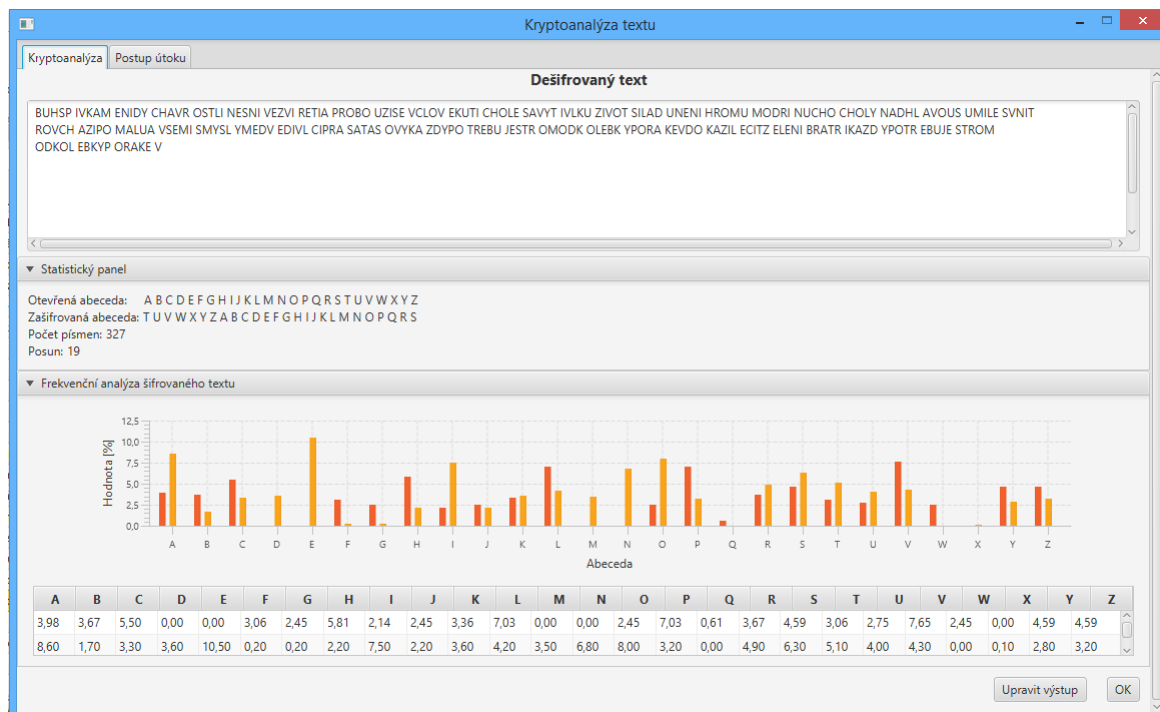
- Obsah textového pole zašifrovaný text, které můžeme naplnit pomocí horního menu Soubor → Otevřít.
- Jazyk, který vybereme pomocí pravého menu.
- Substituční šifru, kterou také vybereme pomocí pravého menu.

Pokud jsou všechny parametry správně nastaveny, program zobrazí okno kryptoanalýzy dle nastavení. V opačném případě program vyzve k zadání všech parametrů.

V následujících kapitolách jsou popsány panely, které vizualizují výsledky a postup kryptoanalýzy pro jednotlivé šifry.

Vizualizace pro jednoduchý posun a šifru Atbash

Vzhled panelu výsledku kryptoanalýzy je zobrazen na obrázku 7.



Obr. 7 První panel kryptoanalýzy pro jednoduchý posun a šifru Atbash

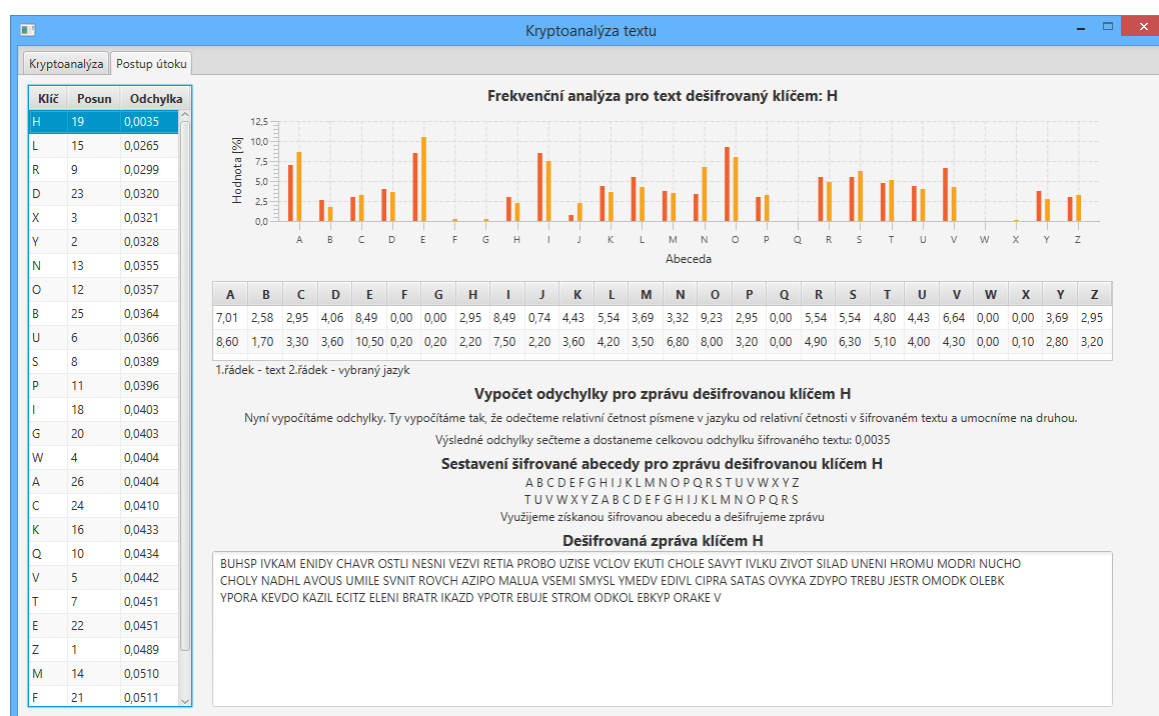
Druhý panel je zobrazen níže na obrázku 8. Panel je vertikálně rozdělen na 2 části. V levé části panelu je tabulka všech možných klíčů, které jsou seřazeny vzestupně podle velikosti

vypočítané odchylky (čím menší odchylka, tím větší pravděpodobnost, že právě tento klíč byl použit pro zašifrování textu).

V pravé části je zobrazen graf, který zobrazuje četnost písmen ve vybraném jazyce (oranžová barva) a zároveň četnost písmen v dešifrovaném textu (červená barva).

Stejnou statistiku zobrazuje tabulka pod grafem. Tedy četnost písmen v šifrovaném textu (1. řádek) a četnost písmen ve vybraném jazyce (2. řádek).

Pod údaji frekvenční analýzy je nastíněn postup kryptoanalýzy šifrovaného textu a vytvoření šifrované abecedy. Nakonec je zobrazen dešifrovaný text vybraným klíčem.



Obr. 8 Druhý panel kryptoanalýzy pro jednoduchý posun a šifru Atbash

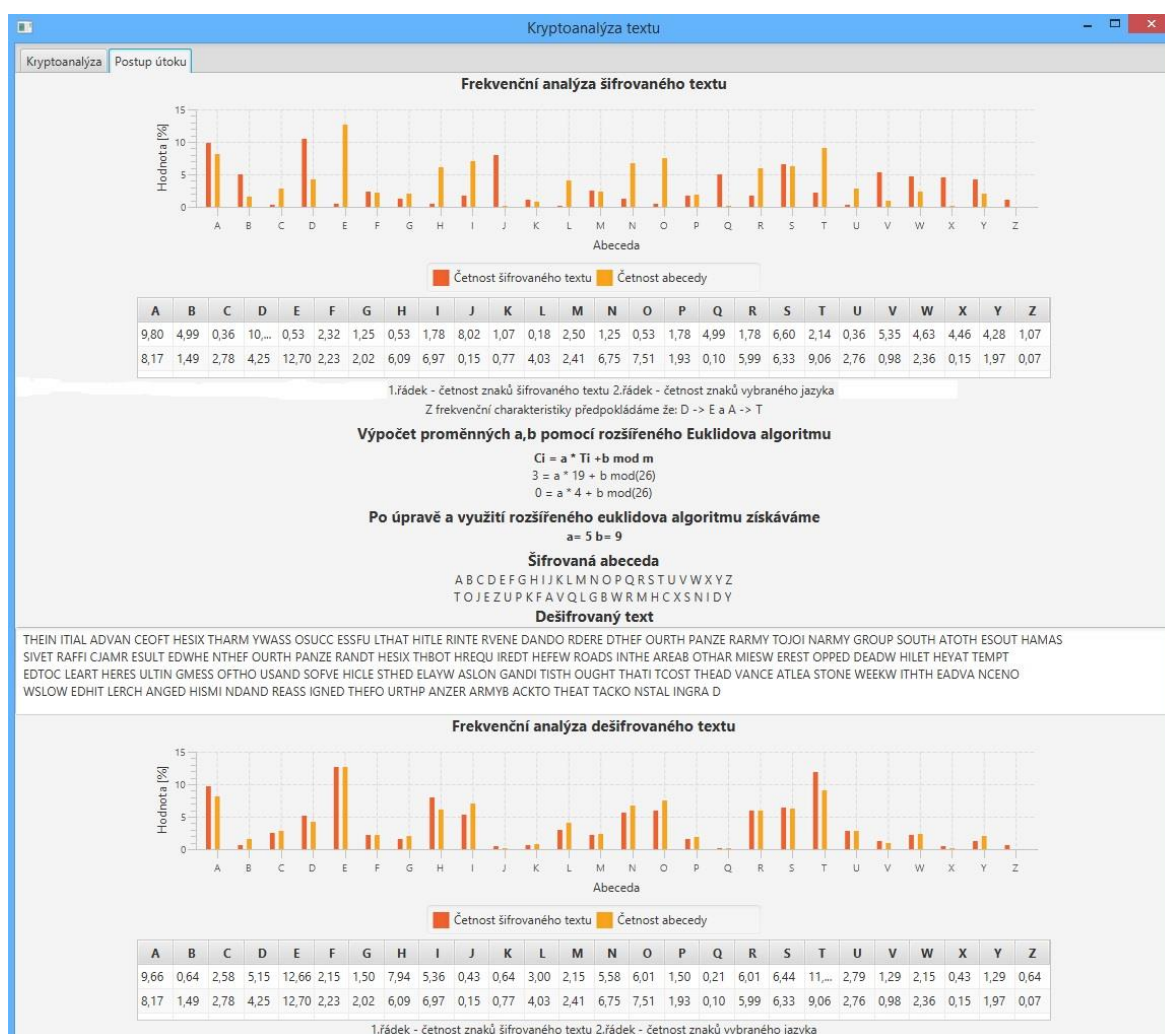
V případě, že nejsme spokojeni s dešifrovaným textem, můžeme z tabulky v levé části panelu vybrat jiný klíč a pravá strana panelu se automaticky přepočítá. Můžeme si tak vyzkoušet jednotlivé klíče a porovnávat výsledky mezi nimi.

Vizualizace pro Afinity šifru

V případě afinní šifry je první část panelu stejná jako na obrázku 8 a změna je až v případě druhé části panelu.

Druhá část panelu je zobrazena níže na obrázku 9. Panel obsahuje graf, který zobrazuje četnost písmen ve vybraném jazyce (oranžová barva) a zároveň četnost písmen v šifrovaném textu (červená barva).

Stejnou statistiku zobrazuje tabulka pod grafem. Tedy četnost písmen v šifrovaném textu (1. řádek) a četnost písmen ve vybraném jazyce (2. řádek). Dále je opět nastíněn postup kryptoanalýzy afinní šifry. Následně je zobrazen dešifrovaný text a frekvenční analýza dešifrovaného textu.



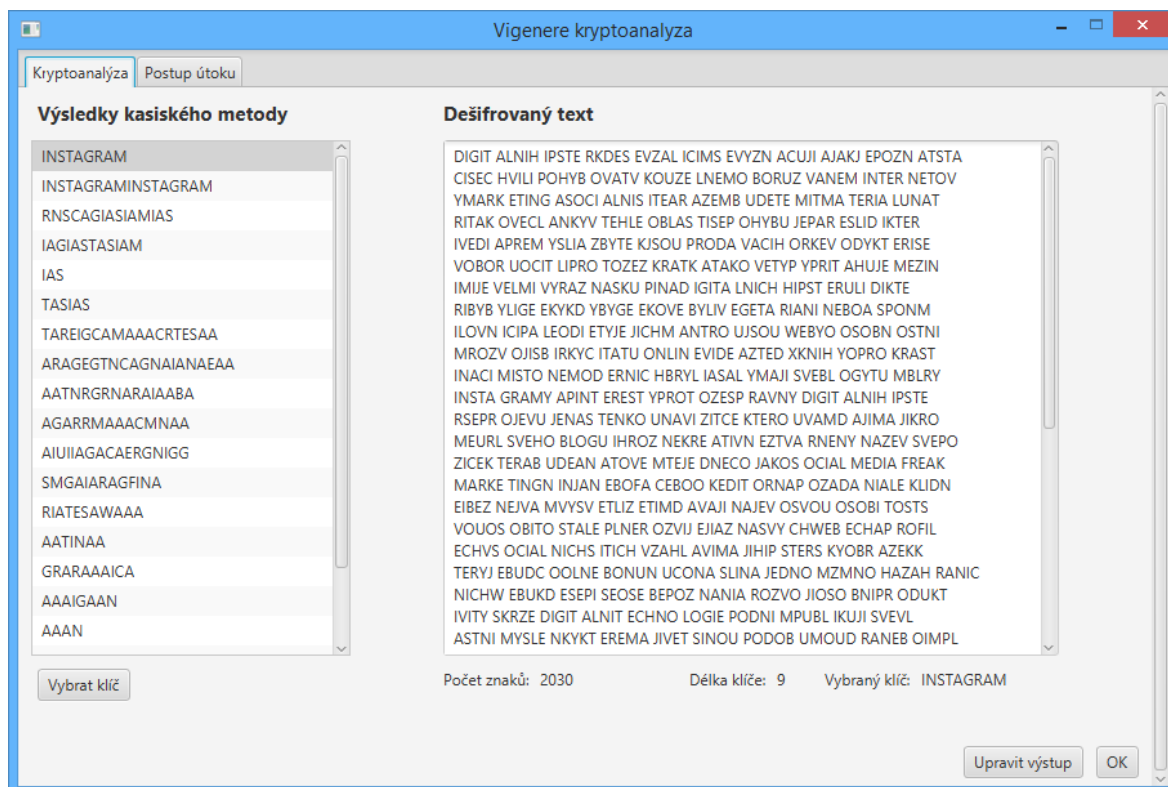
Obr. 9 Druhý panel kryptoanalýzy pro afinní šifru

Vizualizace kryptoanalýzy polyalfabetické substituce

Okno kryptoanalýzy polyalfabetické substituce konkrétně Vigenèrovi šifry je opět rozděleno na dva panely. První panel, který zobrazuje výsledky kryptoanalýzy je zobrazen na obrázku 10.

Panel je rozdělen vertikálně na 2 části. V levé části jsou zobrazeny všechny klíče, které jsme získali pomocí Kasiského metody. V pravé části je zobrazen dešifrovaný text, který je dešifrován právě vybraným klíčem z levé části panelu.

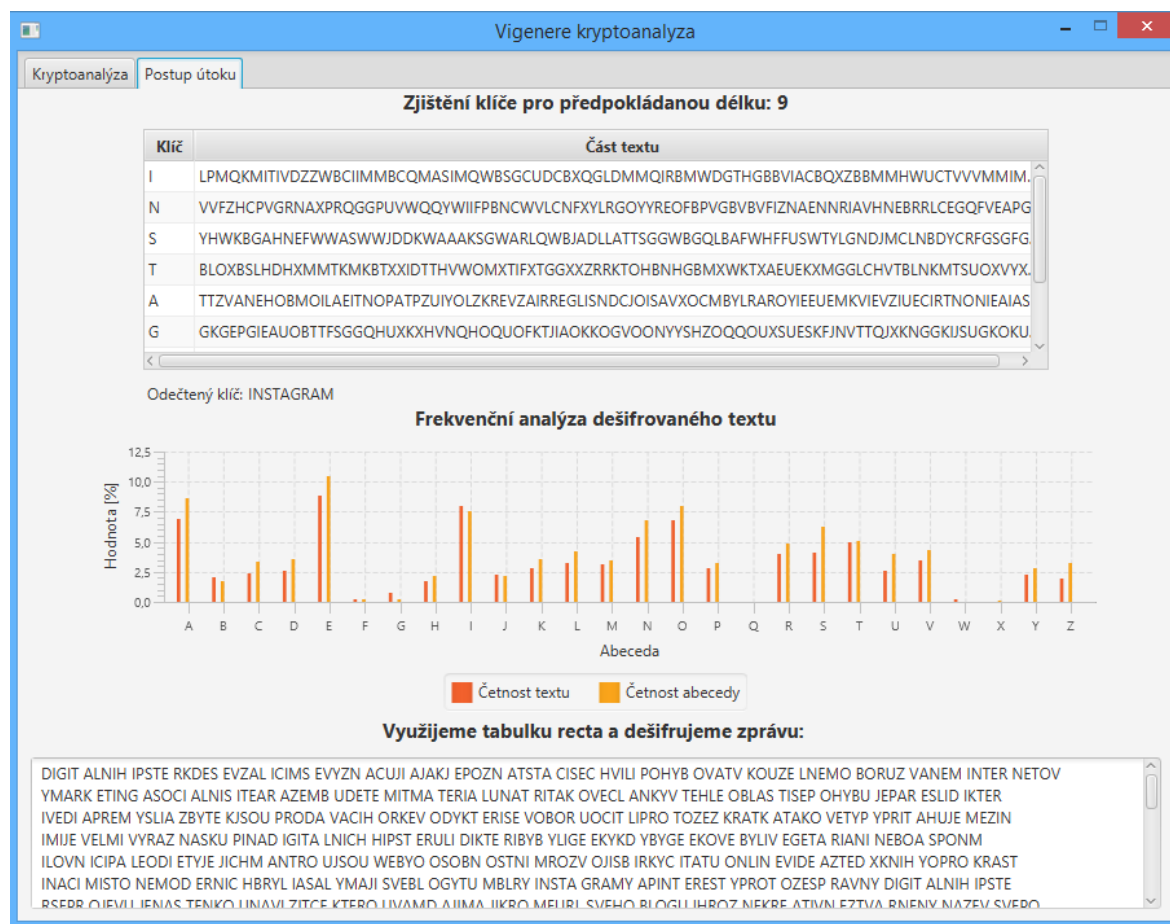
V případě, že chceme vybrat jiný klíč, stačí jej označit a kliknout na tlačítko Vybrat klíč. Poté se provede znovu algoritmus dešifrování vybraným klíčem.



Obr. 10 První panel kryptoanalýzy Vigenèrovi šifry

Druhý panel zobrazuje postup útoku na Vigenèrovu šifru. Jeho vizualizaci můžeme vidět na obrázku 11.

Panel zobrazuje postup zjištění klíče, který byl vybrán pomocí prvního panelu kryptoanalýzy. Na začátku je sestavena tabulka, obsahující rozdělené bloky textu podle délky klíče a klíč každého bloku. Následuje frekvenční analýza dešifrovaného textu, která se porovnává s frekvenční analýzou vybraného jazyka. Jako poslední je uveden dešifrovaný text.



Obr. 11 Druhý panel kryptoanalýzy Vigenèrovi šifry

Vizualizace dešifrování polygrafické substitute

Před spuštěním samotného okna polygrafické substitute, se spustí dialogové okno pro zadání klíče (viz. Obr. 12).

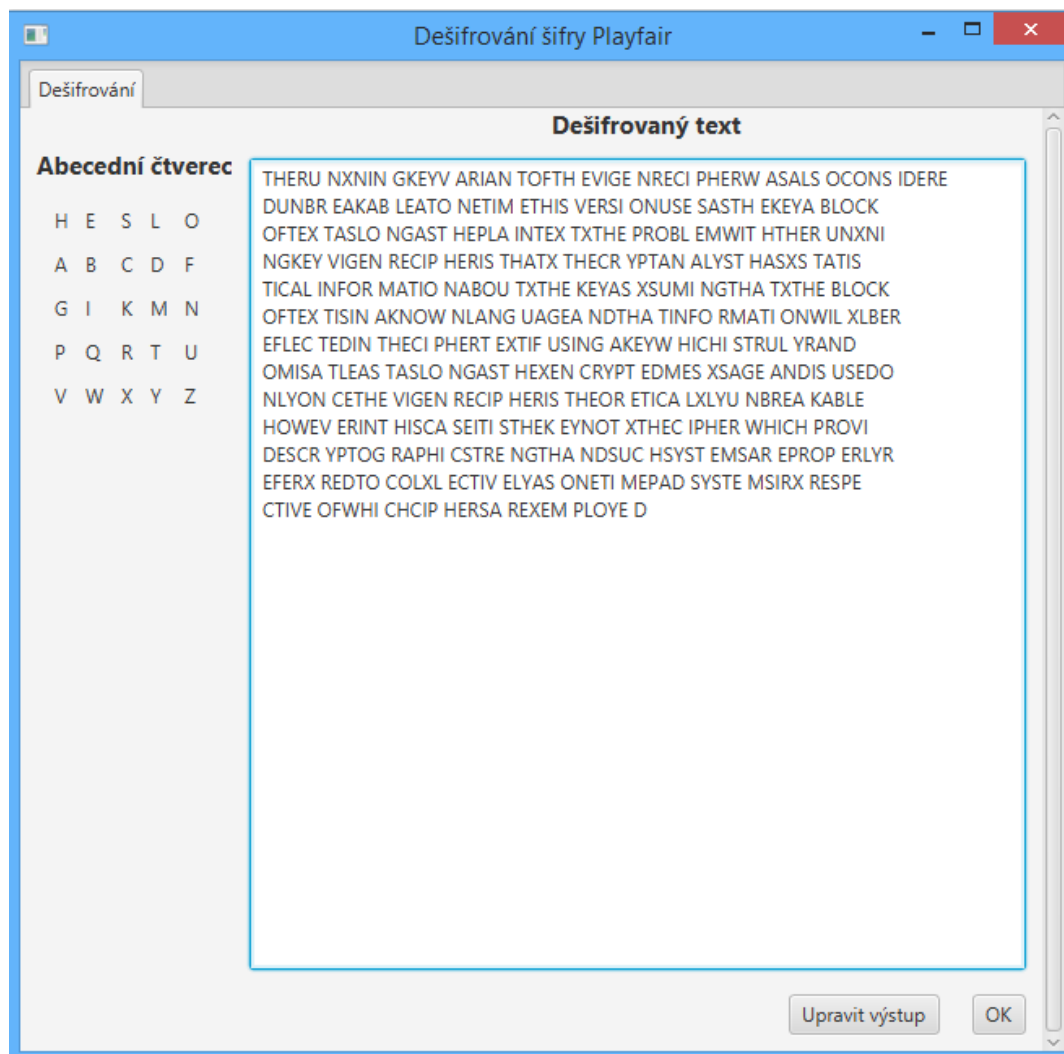
Klíč

Zadejte prosím klíč šifry

Klíč: OK

Obr. 12 Dialogové okno pro zadání klíče

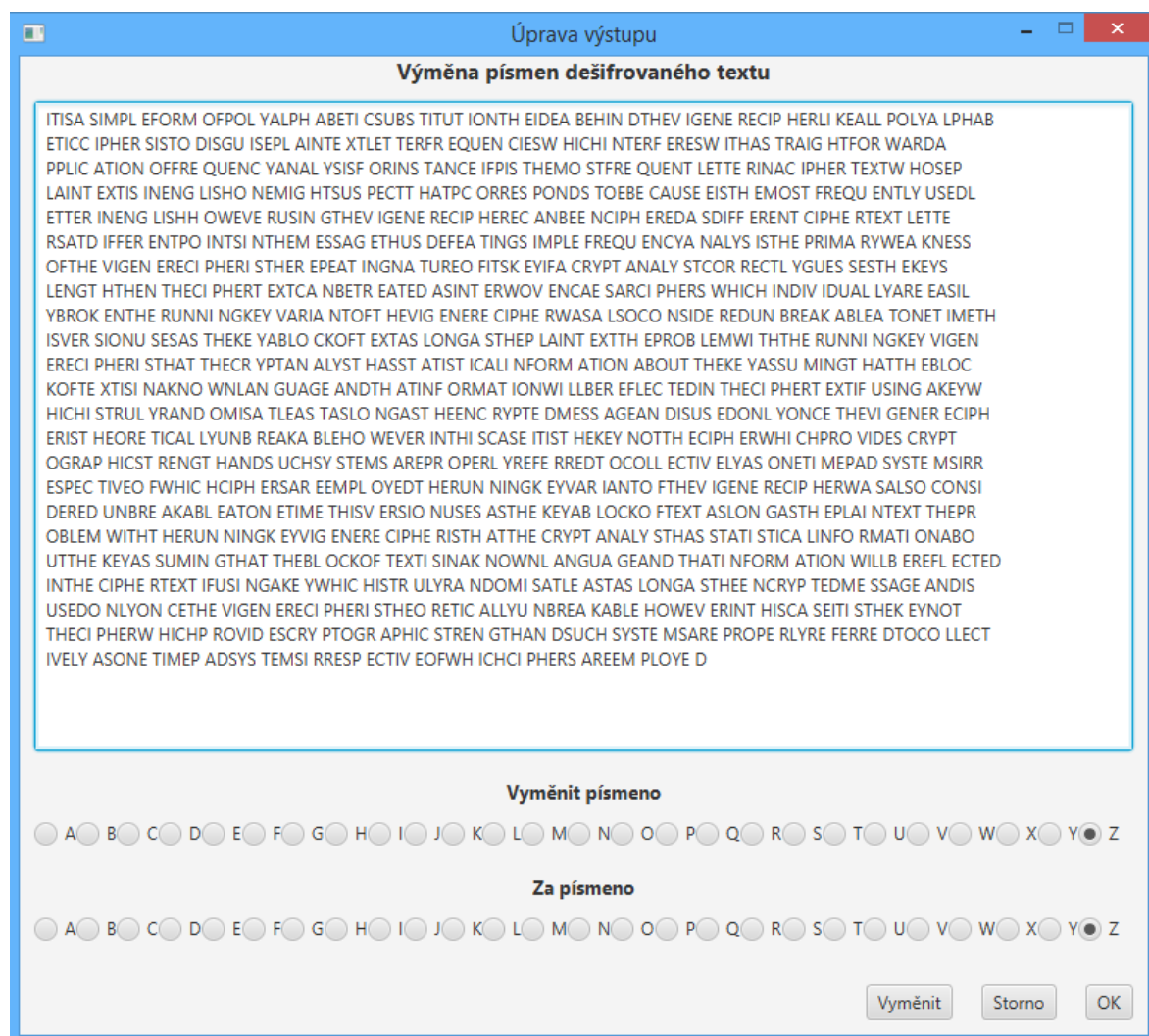
Po zadání klíče a potvrzení tlačítkem OK, program zobrazí okno, které obsahuje vygenerovaný abecední čtverec a dešifrovanou zprávu. Vizualizace okna je zobrazena na následujícím obrázku 13.



Obr. 13 Panel dešifrování Playfair šifry

Panel úpravy výstupu kryptoanalýzy

Všechna výše popsaná okna kryptoanalýz mají společný panel pro úpravu výstupu. Tento panel lze zavolat tlačítkem Upravit výstup, které je umístěno na každém jednotlivém panelu kryptoanalýzy dole vpravo. Po kliknutí na tlačítko, program vyvolá okno pro úpravu textu, jehož vizualizaci lze vidět na obrázku 14.



Obr. 14 Okno úpravy výstupu

9 MOŽNOSTI EXPORTŮ A IMPORTŮ DAT

Aplikace povoluje import a export šifrovaného a dešifrovaného textu v textovém souboru. Jednotlivé funkce programu pracují pouze se znaky mezinárodní abecedy, tzn. má smysl pracovat pouze s textovými soubory (*.txt).

Další možnost exportu dat, které program umožňuje, je exportovat graf frekvenční analýzy do obrázku formátu jpg. A to pomocí okna frekvenční analýzy.

9.1 Budoucí možnosti rozšíření importů a exportů dat

Java podporuje mnoho dalších formátů pro import a export dat (csv, doc, xlsx a jiné). V případě, že by mělo smysl rozšiřovat možnosti importů dat (aplikace by byla rozšířena o další ukázky šifer, které nepracují pouze s mezinárodní abecedou), lze toto rozšíření provést úpravou a přidáním funkcí do třídy FileBrowser, která je umístěna v balíčku mainAppWindow.

Další možností rozšíření exportů dat může být ukládání dat tabulek do Excelu. Změna by se provedla opět rozšířením třídy FileBrowser o novou funkci.

ZÁVĚR

Cílem práce bylo vysvětlení základních principů kryptoanalýzy monoalfabetických substitučních šifer a stručných principů šifer samotných.

Úvod teoretické části je věnován objasnění oborů Kryptologie, Kryptografie, Steganografie, Kryptoanalýzy a také základních pojmů, které s těmito obory souvisí a jsou využity v této práci.

Druhá část teorie se zabývá popisem substitučních šifer a jejich šifrovaných systémů. Substituční šifry můžeme rozdělit na monoalfabetickou, polyalfabetickou, polygrafickou a homogonní substituci. Každá z těchto substitucí má své šifrované systémy, jejichž principy jsou v této části detailně popsány.

Dále jsou popsány základní metody kryptoanalýzy substitučních šifer, frekvenční analýza, index koincidence a útok hrubou silou.

Poslední část teorie je věnována samotné kryptoanalýze vybraných substitučních šifer a jejich šifrovacích systémů. Je zde kladen důraz na vysvětlení postupů a metod, které jsou poté využity v praktické části této práce, jako je využití frekvenční analýzy k získání posunu šifrované abecedy u šifry jednoduchý posun, využití Euklidova rozšířeného algoritmu k získání multiplikativní inverze u Afinní šifry a využití Kasiského metody a indexu koincidence k získání délky hesla u Vigenèrovi šifry.

Praktická část spočívala v naprogramování výše popsaných metod kryptoanalýzy substitučních šifer v jazyce Java. Pro grafické prostředí byl využit framework JavaFX. Při návrhu programu byl kladen důraz na jednoduchost ovládání a celkovou přehlednost. Funkce programu jsou detailně popsány a je vysvětleno, jak se dají využít pro spuštění jednotlivých kryptoanalýz. Samostatná okna kryptoanalýz zobrazují její výsledek (dešifrovaný text), a také nastiňují postup algoritmem dané kryptoanalýzy. Výsledný dešifrovaný text program umožňuje uložit do textového souboru na disk.

SEZNAM POUŽITÉ LITERATURY

- [1] SINGH, Simon. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii*. 2. vyd. v českém jazyce. Překlad Dita Eckhardtová, Petr Koubský. Praha: Dokořán, 2009, 382 s. Aliter (Argo: Dokořán). ISBN 978-80-7363-268 7.
- [2] TŮMA, J. Kapitola 1: základní pojmy [online]. [cit. 18. 5. 2015]. Dostupné z: <http://www.karlin.mff.cuni.cz/~tuma/nciphers/nciphers1.pdf>
- [3] PIPER, F a Sean MURPHY. *Kryptografie*. 1. vyd. v českém jazyce. Praha: Dokořán, 2006, 157 s. Průvodce pro každého. ISBN 80-7363-074-5.
- [4] Kryptografie & šifrování. *Matematika.cz* [online]. [cit. 2015-05-18]. Dostupné z: <http://www.matematika.cz/kryptografie>
- [5] Hebrejský Atbash. *Shaman.cz* [online]. [cit. 2015-05-18]. Dostupné z: <http://www.shaman.cz/sifrovani/hebrejsky-atbash.htm>
- [6] Cesarova šifra. *Shaman.cz* [online]. [cit. 2015-05-18]. Dostupné z: <http://www.shaman.cz/sifrovani/cesarova-sifra.htm>
- [7] TŮMA, J. Kapitola 2: jednoduchá záměna [online]. [cit. 18. 5. 2015]. Dostupné z: <http://www.karlin.mff.cuni.cz/~tuma/nciphers/nciphers2.pdf>
- [8] Šifra posun písmen. *Shaman.cz* [online]. [cit. 2015-05-18]. Dostupné z: <http://www.shaman.cz/sifrovani/sifra-posun-pismen.htm>
- [9] Afinní šifra. *Algoritmy.net* [online]. [cit. 2015-05-18]. Dostupné z: <http://www.algoritmy.net/article/49/Afinni-sifra>
- [10] Lekcia 07 - Kryptografia (Ako na mysterky?). *Geocaching.com* [online]. [cit. 2015-05-18]. Dostupné z: http://www.geocaching.com/geocache/GC2R042_lekcia-07-kryptografia-ako-na-mysterky?guid=b62ab997-7d37-40df-bee9-589d2f10b6d3
- [11] Šifra Playfair. *Shaman.cz* [online]. [cit. 2015-05-18]. Dostupné z: <http://www.shaman.cz/sifrovani/sifra-playfair.htm>
- [12] Frekvenční analýza. *Matematika.cz* [online]. [cit. 2015-05-18]. Dostupné z: <http://www.matematika.cz/frekvencni-analyza>
- [13] Frekvence písmen, bigramů, trigramů, délka slov. *Centrum NLP* [online]. [cit. 2015-05-18]. Dostupné z: <https://nlp.fi.muni.cz/web3/cs/FrekvencePismenBigramu>
- [14] Friedmanuv test. *Matematika.cz* [online]. [cit. 2015-05-18]. Dostupné z: <http://www.matematika.cz/friedmanuv-test>

- [15] Třetí přednáška z Kódování a šifrování. *cvut.cz* [online]. [cit. 2015-05-18]. Dostupné z: http://kix.fsv.cvut.cz/~vanicek/vyuka_l01/kos3.htm
- [16] TŮMA, J. Kapitola 3: Periodický klíč [online]. [cit. 18. 5. 2015]. Dostupné z: <http://www.karlin.mff.cuni.cz/~tuma/nciphers/nciphers3.pdf>
- [17] Kasiskeho test. *Matematika.cz* [online]. [cit. 2015-05-18]. Dostupné z: <http://www.matematika.cz/kasiskeho-test>
- [18] Kryptoanalýza Vigenèrovy šifry. *Matematika.cz* [online]. [cit. 2015-05-18]. Dostupné z: <http://www.matematika.cz/kryptoanaliza-vigenerovy-sifry>
- [19] Kryptoanalýza Caesarovy šifry 2. *Matematika.cz* [online]. [cit. 2015-05-18]. Dostupné z: <http://www.matematika.cz/kryptoanaliza-caesarovy-sifry-2>
- [20] Historie a vývoj jazyka Java. *Fi.muni.cz* [online]. [cit. 2015-05-18]. Dostupné z: <http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xnovotn8.htm>
- [21] Java pro začátečníky (1) - Úvod. *Algoritmy.cz* [online]. [cit. 2015-05-18]. Dostupné z: <http://www.algoritmy.net/article/21340/Uvod-1>
- [22] Java tutoriál úvod do JavaFX. *Itnetwork.cz* [online]. [cit. 2015-05-18]. Dostupné z: <http://www.itnetwork.cz/java-tutorial-uvod-do-javafx>
- [23] Útok hrubou silou. *Wikipedia.org* [online]. [cit. 2015-05-18]. Dostupné z: http://cs.wikipedia.org/wiki/Útok_hrubou_silou

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IC	Index coincidence.
JPG	grafický rastrový formát.
GUI	Graphical User Interface
IDE	Integrated Development Environment
CSV	Comma Separated Values
DOC	Document
XLSX	formát souboru pro ukládání dat z tabulkového editoru
TXT	Textový soubor

SEZNAM OBRÁZKŮ

Obr. 1	Vigenèrův čtverec[18].....	18
Obr. 2	Hlavní okno aplikace.....	35
Obr. 3	Ukázka úpravy textu v textovém poli	37
Obr. 4	Detail levého menu.....	37
Obr. 5	Okno frekvenční analýzy šifrovaného textu.....	39
Obr. 6	Okno indexu koincidence.....	40
Obr. 7	První panel kryptoanalýzy pro jednoduchý posun a šifru Atbash.....	41
Obr. 8	Druhý panel kryptoanalýzy pro jednoduchý posun a šifru Atbash	42
Obr. 9	Druhý panel kryptoanalýzy pro afinní šifru	43
Obr. 10	První panel kryptoanalýzy Vigenèrovi šifry	44
Obr. 11	Druhý panel kryptoanalýzy Vigenèrovi šifry.....	45
Obr. 12	Dialogové okno pro zadání klíče.....	45
Obr. 13	Panel dešifrování Playfair šifry	46
Obr. 14	Okno úpravy výstupu	47

SEZNAM TABULEK

Tab. 1	Ukázka šifrované abecedy.....	12
Tab. 2	Převodová tabulka šifry Atbash	15
Tab. 3	Příklad šifrování Atbash.....	15
Tab. 4	Převodová tabulka Caesarovi šifry.....	16
Tab. 5	Příklad šifrování Caesarovou šifrou.....	16
Tab. 6	Příklad převodové tabulky přeházené abecedy	17
Tab. 7	Příklad převodové tabulky pro využití klíčového slova.....	17
Tab. 8	Příklad zápisu klíče Vigenèrovi šifry	19
Tab. 9	Příklad šifrování pomocí Vigenèrovi šifry.....	19
Tab. 10	Příklad abecedního čtverce.....	20
Tab. 11	Frekvence českých písmen[13]	23
Tab. 12	Frekvence českých písmen bez diakritiky[12]	23
Tab. 13	Nejfrekventovanějších 40 bigramů[13].....	24
Tab. 14	Nejfrekventovanějších 40 trigramů[13]	24
Tab. 15	Index koincidence vybraných jazyků.....	25

SEZNAM PŘÍLOH

K bakalářské práci je přiloženo CD s prací v elektronické podobě zdrojový kód vytvořený v Javě a samostatně spustitelný soubor programu BakalarskaPrace.jar.