VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

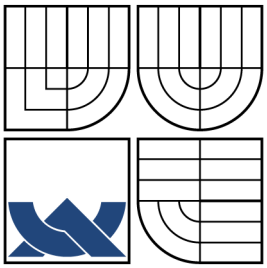
SOFTWAROVÁ PODPORA VÝUKY KLASICKÉ KRYPTOANALÝZY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

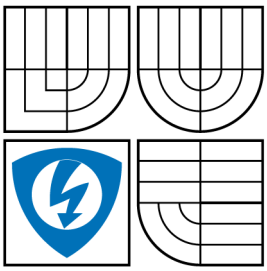
AUTOR PRÁCE
AUTHOR

BC. LUCIE FOJTOVÁ

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND
COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

SOFTWAROVÁ PODPORA VÝUKY KLASICKÉ KRYPTOANALÝZY

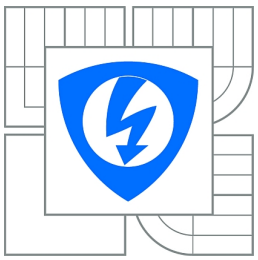
SOFTWARE SUPPORT OF EDUCATION IN CLASSICAL CRYPTOANALYSIS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — BC. LUCIE FOJTOVÁ
AUTHOR

VEDOUCÍ PRÁCE — DOC. ING. KAREL BURDA, CSC.
SUPERVISOR

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Studentka: Bc. Lucie Fojtová ***ID:*** 77707
Ročník: 2 ***Akademický rok:*** 2009/2010

NÁZEV TÉMATU:

Softwarová podpora výuky klasické kryptoanalýzy

POKYNY PRO VYPRACOVÁNÍ:

Stručně vysvětlete problematiku kryptoanalýzy vybraných klasických šifer. Na tomto základě navrhněte řešení softwarové podpory výuky kryptoanalýzy. Svůj návrh zdůvodněte, prakticky zrealizujte a ověřte. Při návrhu věnujte pozornost pedagogickým aspektům jako je interaktivita a názornost. Výukový software musí mít webové rozhraní a musí se obejít bez serveru.

DOPORUČENÁ LITERATURA:

[1] Vondruška P.: Kryptografie, šifrování a tajná písma. OKO, Praha 2006.
[2] Singh S.: Kniha kódů a šifer. Dokořán a Argo, Praha 2003.

Termín zadání: 29.1.2010 ***Termín odevzdání:*** 26.5.2010

Vedoucí práce: doc. Ing. Karel Burda, CSc.

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

ABSTRAKT

Některé z dneších moderních šifrovacích systémů obsahují ve svých základech myšlenky klasických symetrických šifer, jako je např. transpoziční princip v šifře DES. Pro úspěšnou kryptoanalýzu těchto druhů šifer je třeba znát základní krypoanalytické metody. Z toho plyne důležitost výuky klasické kryptoanalýzy - aby studenti co nejlépe pochopili danou problematiku, je třeba použít názorné pomůcky. Tato práce shrnuje poznatky teorie klasické kryptografie a krypotanalýzy vybraných druhů šifer - monoalfabetické a polyalfabetické substitiuce a dále jednoduché transpozice. Na základě této teorie je vytvořena softwarová podpora výuky klasické kryptoanalýzy - konkrétně formou webových stránek a aplikace umožňující šifrování a luštění klasických druhů šifer.

KLÍČOVÁ SLOVA

Klasická kryptoanalýza, klasická kryptografie, substituční šifra, transpoziční šifra, podpora výuky

ABSTRACT

Number of today's modern cipher systems are based on the classical symmetric cipher systems, such as the transposition principle in the DES cipher. Successful analysis and deciphering of these ciphers is therefore underlined by solid knowledge of the elementary cryptanalysis methods. This implies the importance of classical cryptanalysis education – for better a understanding of the field, using visual means is of utmost importance. The aim of the thesis is to summarize selected cipher methods of the classical cryptanalysis, namely the mono– and polyalphabetical substitution and transposition route cipher. Along with the theoretical part, ciphering/deciphering software is introduced to be used for educational purposes, particularly a website and a standalone application providing tools for ciphering, analysis and code breaking of the classical cipher based code.

KEYWORDS

Classical cryptoanalysis, classical cryptography, substitution cipher, transposition cipher, support of education

FOJTOVÁ L. *Softwarová podpora výuky klasické kryptoanalýzy*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 62 s. Vedoucí práce doc. Ing. Karel Burda, CSc.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Softwarová podpora výuky klasické kryptoanalýzy“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu diplomové práce doc.Ing. Karlovi Burdovi, CSc. z Ústavu telekomunikací FEKT VUT v Brně za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce.
Dále děkuji svému manželovi Pavlovi za naprosto nenahraditelnou podporu v průběhu tvorby této práce.

V Brně dne 18.5.2010

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

1 ÚVOD

V historii kryptologie mezi sebou odedávna soupeří dvě skupiny - šifranti a luštitelé. Šifrováním se lidstvo snaží odedávna skrýt obsah komunikace (nikoliv komunikaci samotnou). V některých obdobích dějin měla navrch kryptoanalýza (např. po objevu metody frekvenční analýzy arabskými vědci), v současné době však vítězí spíše kryptografie - existují šifrovací algoritmy, které neumíme v reálném čase prolomit.
Moderní kryptografie, tak jak ji známe dnes, se začala rozvíjet na počátku 20. století, zejména s masovým rozšířením telegrafie. Následoval velký rozmach šifrovacích systémů během 2. světové války (mimo jiné se začaly běžněji využívat mechanické stroje, např. velmi známá Enigma). Od druhé poloviny 20. století se potom začínají šifry rozšiřovat také do obchodní a finanční sféry. Kryptografie tak přestala být záležitostí téměř výhradně vojenskou.
Využití kryptoanalýzy je v dnešní době poměrně široké. Na jednu stranu se jedná o přímé luštění zachycených šifrových zpráv (ať už se jde o vojenské, diplomatické či obchodní texty), a na stranu druhou se pomocí kryptoanalýzy přímo zkoumá odolnost šifrových systémů při jejich navrhování. Moderní kryptoanalytické metody se dnes již nesnaží pouze odhalit skrytý obsah zpráv, ale také se pokouší např. prolomit integritu dat, podvrhnout autentizaci atd.
Ačkoliv se může zdát, že klasická kryptoanalýza je tedy v dnešní době prakticky již přežitá, ve skutečnosti jsou moderní metody právě na jejích základech postaveny.
Z toho plyne důležitost její výuky - aby studenti co nejlépe pochopili danou problematiku, je třeba použít názorné pomůcky. Tato práce si klade za cíl navrhnout řešení softwarové podpory výuky klasické kryptoanalýzy, mimo jiné návrh interaktivní pomůcky pro výuku, a ověřit ho v praxi.
V první části práce (kapitola 1) je shrnuta klasifikace klasických šifrovacích systému včetně stručného historického kontextu, dále metody (a konkrétní postupy) jejich luštění. Tato teorie bude použita jako součást podpory výuky. Druhá část (kapitola 3) se zabývá realizací a popisem softwaru, který by v budoucnu mohl sloužit při výuce klasické kryptoanalýzy - umožní uživateli názorně šifrovat a luštit zadaný text za pomocí vhodných kryptoanalytických nástrojů.

2 TEORIE KLASICKÉ KRYPTOLOGIE

Aby bylo možno podrobněji popsat klasické šifrové systémy a metody jejich luštění, je nutno definovat si některé pojmy.

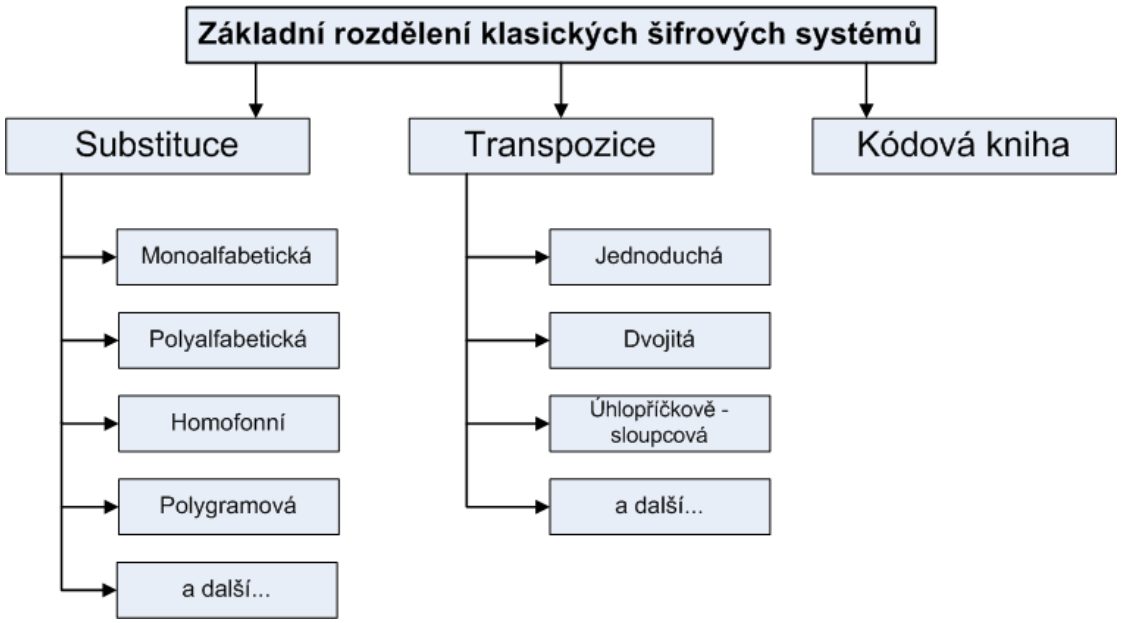
2.1 Definice pojmů

Šifrový nebo také *kryptografický systém* je jakýkoliv systém, který lze použít k pozměnění textu nějaké zprávy s cílem učinit ji nesrozumitelnou komukoliv jinému s výjimkou adresáta, kterému je určena. Původní zpráva je nazývána *otevřeným textem*, pozměněná zpráva je *šifrový text*. Proces změny zprávy za pomocí šifrového systému se nazývá *šifrování*. Je to tedy postup, pomocí kterého lze převést otevřený text na šifrový. Při tomto převodu se obvykle používá *klíč* - určitý parametr šifrového systému, který ovlivňuje podobu výsledného šifrového textu.
Šifrovací transformace je funkce, která převádí jednotku otevřeného textu (obvykle jeden znak, ale není podmínkou) zprávy na jednotku šifrového textu zprávy. Jde o zobrazení f z množiny O všech možných jednotek otevřeného textu zprávy do množiny S všech možných jednotek šifrového textu. *Dešifrovací transformace* je inverzní zobrazení f^{-1}, které převádí šifrový text na text otevřený.
Autorizovaná osoba (ta, pro kterou je zpráva určena) může provést původní rekonstrukci zprávy - její *dešifrování*, proces opačný k šifrování. Pro dešifrování zprávy je nutné znát typ šifrového systému a příslušný klíč. O původní zprávu však může mít zájem i nepovolaná osoba, bez znalosti parametrů systému i systému samotného - ta se může pokusit o *luštění*. Je to proces, jehož cílem je získat otevřený text z textu zašifrovaného bez znalosti potřebných informací (klíče).
Symetrický šifrovací systém se jinak nazývá systémem s tajným klíčem. Používá dva klíče - pro šifrování a dešifrování. Pro zajištění bezpečnosti je nutné, aby tyto klíče zůstaly utajené - jeden z druhého je totiž odvoditelný v reálném čase. Existují také *asymetrické šifrovací systémy*, jinak zvané kryptografické systémy s veřejným klíčem. Používají 2 typy klíčů: tzv. *veřejný*, který slouží pro zašifrování, a druhý tzv. *neveřejný*, který slouží pro dešifrování. Klíče jsou navzájem odlišné (ačkoliv mezi nimi existuje určitý vztah); veřejný klíč lze zveřejnit, protože jeho pomocí nelze šifrový text dešifrovat ani rozluštit.
Každá zpráva je zapsána pomocí abecedy - obvykle abecedy původního jazyka. Abeceda se skládá z jednotlivých *symbolů* - písmen, číslic, atd. Posloupnost těchto znaků se nazývá *řetězec*. Pomocí *abecedy otevřeného textu* je zapsána původní zpráva; zašifrovaná zpráva (nazývaná také *kryptogram*) je zapsána pomocí *šifrové abecedy*. Tyto dvě abecedy mohou (ale nemusí) být totožné.

Věda o šifrování se nazývá *kryptografie*. Zabývá se tvorbou šifrovacích a dešifrovacích algoritmů, jejím cílem je utajit význam zprávy. Jinými slovy, zkoumá metody utajování významu zpráv pomocí převodu do podoby, která je čitelná pouze s určitými znalostmi.
Opakem kryptografie je *kryptoanalýza*. Je to věda o metodách luštění šifrovacích systémů bez znalosti klíče. Dále se zabývá analýzou odolnosti těchto systémů. Slovo kryptoanalýza taktéž pochází z řečtiny, konkrétně ze dvou řeckých slov, a to *kryptós* - „skrytý“ a *analýein* - „uvolnit“ či „rozvázat“.
Kryptografie a kryptoanalýza tvoří společně vědní obor s názvem *kryptologie*.

2.2 Rozdělení klasických šifrových systémů

Šifrovací systémy se v základu rozdělují do dvou kategorií: **substituce** a **transpozice**.
Substituční šifra je historicky starší, její kořeny spadají až do roku 1900 př.n.l. Spočívá v nahrazení každého znaku (nebo skupin znaků) otevřeného textu jiným znakem (skupinou) textu šifrovaného. Pro tento převod lze použít jednu nebo více abeced (např. pro každý znak jinou abecedu). Substitučních metod existuje celá řada, v klasické kryptografii se nejvíce používají zejména tyto čtyři typy: *monoalfabetická substituce*, *polyalfabetická substituce*, *homofonní substituce* a *substituce polygramová*.



Obr. 2.1: Rozdělení klasických šifrovacích systémů

Při *transpozici* se jednotlivá písmena otevřeného textu nemění, ale posouvají na jiné místo v textu šifrovém podle určitých pravidel - jedná se vlastně o přesmyčku otevřeného textu. Díky tomu dojde k přerušení některých vazeb mezi znaky, což stěžuje luštění. Tato šifra nemění frekvenci výskytu původních znaků, pouze mění jejich pozici - z toho mj. vyplývá, že poměr samohlásek a souhlásek je v šifrovém textu zachován (pro český jazyk je to cca 2:3), čehož se při luštění často využívá. Nejjednodušším transpozičním systémem je jednoduchá sloupcová transpozice (někdy nazývaná zkráceně jednoduchá transpozice) dále se používají dvojitá transpozice, úhlopříčkově - sloupcová transpozice atd.
Kódová kniha je v podstatě *slovník*, který nahrazuje vybraná slova či věty otevřeného textu různě složitými kódy. Obvykle obsahuje nejčetnější výrazy (fráze), používané v daném kontextu (zřejmě bude odlišná kódová kniha vojenská a diplomatická). Každý výraz má většinou několik možností zakódování a šifrant si náhodně vybírá, kterou z nich použije. Kódová kniha se nejčastěji používá ve spojení s jinými šifrovacími metodami. Za krajní případ použití kódové knihy lze považovat překlad zprávy do jiného jazyka pomocí kódové knihy - slovníku. V některých případech se však i tato možnost využívala pro šifrování - např. během 2.světové války, kdy si americká armáda předávala některé zprávy pomocí indiánů z kmene Navajo.

2.2.1 Substituce

Monoalfabetická šifra

Tato šifra se nazývá také *jednoduchá substituce* nebo *jednoduchá záměna*. Jedná se o jednu ze základních šifrovacích metod. Při šifrování je postupně každý znak otevřeného textu nahrazován jedním znakem z šifrové abecedy. Důležité je, že pro celou otevřenou zprávu se použije stejná šifrová abeceda - od toho název monoalfabetická. Tato abeceda může obsahovat odlišné znaky, než abeceda otevřeného textu.
Obecně není monoalfabetická substituce příliš bezpečná - díky převodu 1:1 (jeden konkrétní znak otevřeného textu odpovídá jednomu konkrétnímu znaku textu šifrového) se totiž v šifrovém textu zachovávají určité charakteristické rysy abecedy otevřeného textu, které lze s úspěchem použít při luštění pomocí frekvenční analýzy (viz kapitola 2.3.2).
Následující tabulka (2.1) ukazuje příklad otevřené a šifrové abecedy:

Otevřená 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
Šifrová abeceda	5	o	l	7	&	n	j	2	q	@	z	6	a	d	1	i	3	s	9	8	b	4	f	p	h	m

Tab. 2.1: Příklad šifrové abecedy - monoalfabetická substituce

Při znalosti šifrové abecedy je šifrování velmi jednoduché, konkrétní příklad je vidět

v tabulce 2.2. Dešifrování potom probíhá stejným - pouze inverzním - způsobem. Podle způsobu záměny se tato šifra dělí na čtyři typy (v následujícím textu je

Otevřený text	d i p l o m o v a p r a c e
Šifrový text	7 q i 6 1 a 1 4 5 i s 5 1&

Tab. 2.2: Příklad zašifrování textu monoalfabetickou substitucí

použito S(x) pro označení šifrové abecedy a O(x) pro abecedu otevřeného textu) [11]:

Jednoduchý posun V případě jednoduchého posunu vznikne šifrová abecedu tak, že abeceda otevřeného textu se posune o několik pozic (parametr k v rovnici 2.1). To znamená, že pro mezinárodní abecedu (26 znaků) existuje celkem 26 možností posunu, z čehož 25 je „použitelných“ - poslední je posun o 0 pozic, takže žádnému posunu vlastně nedojde.
Uvedený postup lze zapsat matematicky:

$$S(x) = (O(x) + k) \ mod \ 26 \tag{2.1}$$

kde k je parametr posunu; $k \in < 0; 25 >$.
Dobrým příkladem této šifry je známá Caesarova šifra, kterou používal Julius Caesar již v 1.stol. př. n. l. Tuto šifru popsal ve svých *Zápiscích o válce galské*. Jednotlivá písmena OT se zamění za písmena ležící v abecedě o tři místa dál. Jedná se o jednoduchý posun s parametrem $k = 3$. Caesarův synovec Augustus používal obdobný systém s parametrem $k = 1$ a k tomu poslední písmeno v abecedě (tehdy X) bylo nahrazeno dvojicí AA. Dešifrování probíhá zpětně, matematické vyjádření je $O(x) = (S(x) - k) \ mod \ 26$.

Afinní šifra Šifrová abeceda afinní šifry vznikne podle následujícího předpisu:

$$S(x) = a \cdot O(x) + b \ mod \ 26 \tag{2.2}$$

kde a, b jsou parametry takové, pro které platí: $a \in < 1; 25 >$ a $b \in < 0; 25 >$. V tomto případě existuje celkem 312 možností vytvoření abecedy. Vzhledem k tomu, že šifrování musí být jednoznačné (tj. jedná se o zobrazení transformace $1 \Longleftrightarrow 1$), parametr a musí splňovat ještě jednu důležitou podmínku: největší společný dělitel $nsd(a, 26) = 1$ (to mj. znamená, že a nesmí být sudé). V případě nerovnosti dojde k nejednoznačnému přiřazení (více znaků otevřeného textu bude zašifrováno stejným znakem šifrové abecedy, tzn. zpětně se šifra nebude dát dešifrovat/vyluštit). V praxi to znamená, že při otevřené abecedě o délce 26 znaků nelze použít jako parametr a sudá čísla a číslo 13 (z čehož vyplývá počet možných kombinací šifry). Speciálním případem afinní šifry je jednoduchý posun (pro $a = 1$).

Použití klíče Tabulka 2.3 demonstruje použití klíče při vytváření šifrové abecedy. Nejprve se obě strany dohodnou na klíči - v tomto případě zvoleno slovo *hotel*.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
h	**o**	**t**	**e**	**l**	a	b	c	d	f	g	i	j	k	m	n	p	q	r	s	u	v	w	x	y	z

Tab. 2.3: Vytvoření šifrové abecedy pomocí klíče

Tímto slovem bude začínat šifrová abeceda, a dále bude pokračovat abeceda stejná jako otevřená, pouze s vynecháním písmen z klíče. Pokud se v klíči vyskytují stejná písmena (např. slovo *motorka*), vynechají se písmena vyskytující se vícekrát - vyjma prvního (*motrka*).

Náhodný výběr V tomto případě se šifrová abeceda vygeneruje náhodně z abecedy otevřeného textu. Celkem existuje $26! = 403291461126605635584000000 \approx 4 \cdot 10^{26}$ možností zašifrování tímto systémem, a to znemožňuje praktické použití hrubé síly při luštění.

Aby nebylo luštění této šifry jednoduché, šifrový text se obvykle zbavuje mezer (případně se mezery nahradí některým - obvykle méně frekventovaným - znakem, či skupinou znaků) - díky tomu kryptoanalytik neví, z kolika slov se otevřený text skládá. Čísla se obvykle vypisují slovy, mohou se ale samozřejmě nahradit některými jinými znaky - stejně tak jako interpunkce.
Dešifrování jednoduché záměny není složité - obě strany potřebují znát původní abecedu a případně heslo (parametry) nebo postup, díky kterému se vytvoří abeceda šifrového textu. Za vůbec první substituční šifru je považován Hebrejci vynalezený systém *ATBAŠ* [1]. Šifrování probíhá následujícím způsobem: písmeno OT se nahradí takovým písmenem ŠT, které má stejnou vzdálenost od konce abecedy, jako původní písmeno od začátku abecedy (pro mezinárodní abecedu je to např. $d = w$, $i = r$ atd.).
Jednoduchá záměna byla použitelná do cca 17.století, od té doby byla - obzvláště pro vojenské a vládní systémy - naprosto nedostatečná a bylo nutné nahradit ji jinými systémy.

Polyalfabetická šifra

Protože monoalfabetická šifra byla poměrně dobře luštitelná již ve středověku, bylo nutné vymýšlet nové, složitější šifrovací postupy, které by odolávaly dosavadním metodám luštění. Za otce západní kryptologie je považován Leon Battista Alberti (15.stol.n.l.), který poprvé popsal *polyalfabetickou substituci*.

Polyalfabetická subtituce se skládá z několika monoalfabetických substitucí, které jsou podle určitého systému aplikovány postupně na jednotlivá písmena otevřeného textu. Zásadní výhoda této šifry spočívá v tom, že stejné písmeno lze zašifrovat více různými způsoby - obecně tolika, kolik abeced je použito pro šifrování - mohou to být i tisíce. Pro představu, německý šifrovací stroj Enigma, který byl využívaný hlavně pro vojenské účely, pracoval s 16900 abecedami [9]. Prakticky se pak konkrétní text zašifruje tolika abecedami, kolik písmen obsahuje zvolený klíč.
Následující příklad vysvětluje způsob šifrování. Jedná se o systém *Vigénere*, což byla pravděpodobně nejpoužívanější varianta polyalfabetické šifry. Tento systém byl ve své době (19.stol.) nazývan „le chiffre indéchiffrable“, tedy jako *nerozluštitelná šifra.* K šifrování je v tomto systému použito tolik abeced, kolik existuje v jazyce otevřeného textu znaků. Pro mezinárodní abecedu (tzn. 26 znaků, bez číslic, diakritických a jiných speciálních znaků) je systém abeced znázorněn v tabulce 2.4. Pro šifrování a dešifování je zapotřebí, aby si obě strany domluvily klíč - tím je nějaké slovo nebo skupina znaků (např. slovo *list*). Tento klíč se poté nadepíše nad celou délku otevřeného textu, který se bude šifrovat - v tomto případě slovo „lokomotiva“ - viz tabulka 2.5. Pokud není klíč dostatečně dlouhý (obvykle nebývá), opakuje se. Proto se tento šifrovací systém nazývá také *periodické heslo.* Čím delší je zvolený klíč, tím větší je počet možností, kterými můžeme zašifrovat jeden znak. Šifrování probíhá následujícím způsobem: první písmeno otevřeného textu (l) se zašifruje znakem z tabulky 2.4, který má tyto souřadnice:
- řádek je určen písmenem klíče umístěného nad písmenem otevřeného textu (v našem případě také l)
- sloupec je určen písmenem otevřeného textu
Na průsečíku *(l, l)* leží písmeno *w*, které tvoří první znak šifrového textu. Obdobným způsobem se postupuje dále, výsledkem je šifrový text (pro přehlednost zapsaný velkými písmeny) *WWCHX WLBGI.*
Tato metoda šifrování lze ještě mírně zjednodušit: opět se nad otevřený text napíše (opakované) heslo. První písmeno šifrového textu se získá jako součet pozic prvního písmene klíče a prvního písmene otevřeného textu, oboje ve stejné (neposunuté) abecedě. Pro určení pozice písmene v abecedě může sloužit tabulka č.2.6.
V případě šifrování slova *lokomotiva* pomocí klíče *list* vypadá postup následovně: první písmeno se získá sečtením pozic písmen l a l, tzn. 11+11=22 a tomu odpovídá dle tabulky 2.6 písmenou **w**. Druhé písmeno bude i + o = 8 + 14 = 22 a tomu odpovídá opět písmeno **w**. Pro názornost ještě třetí písmeno, kterému odpovídá s + k = 18 + 10 = 28, ale protože abeceda obsahuje pouze 26 znaků, od hodnoty větší se musí číslo 26 vždy odečíst, 28 - 26 = 2 a to odpovídá písmenu **c**. Je zřejmé, že výsledek šifrování je totožný, nebylo ale zapotřebí používat „velkou“ tabulku abeced.

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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
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	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	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	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

Tab. 2.4: Tabulka abeced pro polyalfabetickou šifru

Klíč	l	i	s	t	l	i	s	t	l	i
Otevřený text	l	o	k	o	m	o	t	i	v	a

Tab. 2.5: Šifrování slova *lokomotiva* pomocí polyalfabetické šifry

pozice	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

Tab. 2.6: Převod písmen na pozice

Dešifrování probíhá zpětně - nad šifrový text se zapíše opakovaně klíč a pomocí něj je v tabulce vyhledáván původní otevřený text: znaky šifrového textu se vyhledávají v řádku určeném písmenem hesla, které je zapsáno nad šifrovým textem. Nebo, od šifrového textu (resp. abecedních pozic jeho písmen) se odečítají abecední pozice písmen klíče (přičemž je třeba respektovat, že abeceda má pouze 26 znaků).
Šifra Vigénere je bezpečná pouze pro případ velmi krátkých textů nebo velmi dlouhých klíčů, jejichž délka se blíží délce celého otevřeného textu.
Za zmínku stojí i modifikace systému Vigénere - tzv. *autoklíč otevřeného textu* [1]. Odesílatel a příjemce se opět domluví na klíči (může to být pouze jeden znak). Ten se zapíše nad první znaky otevřeného textu, a dále se jako „klíč“ použije přímo otevřený text (dá se říct, že klíčem je původní otevřený text posunutý o tolik znaků vpravo, kolik je délka zvoleného hesla a doplněný zleva klíčem). Takto vytvořený klíč se nazývá *autoklíč*. Šifrování a dešifrování potom probíhá stejným způsobem, jako u základního systému Vigénere.
Polyalfabetická šifra byla poměrně dlouhou dobu považována za bezpečnou, protože ji nešlo snadno prolomit metodami používanými pro luštění monoalfabetické šifry. Časem se však ukázaly její jiné nevýhody - lze ji luštit na základě analýzy vzdálenosti mezi opakováními řetězců šifrových znaků (viz kapitola 2.4.3). Mezi další systémy založené na polyalfabetické subtituci např. šifry *Gronsfeld* nebo *Beaufort* [1]. Obě dvě jsou zjednodušenou variantou systému Vigénere.
Za zmínku ještě stojí Vernamova šifra. Je to Vigénerova šifra s náhodně generovaným klíčem, který je stejně dlouhý jako otevřený text. Tato šifra je jediná dokazatelně bezpečná - bez znalosti klíče ji nelze prolomit. Problémem však je v tomto případě bezpečná distribuce klíčů.

Další substituční systémy

Na *homofonní šifru* lze nahlížet jako na speciální případ šifry monoalfabetické. Substituce spočívá v postupné náhradě jednoho znaku otevřeného textu jedním z několika možných znaků textu šifrového (např. písmeno *a* otevřeného textu zašifrujeme písmenem *m*, znakem *$* nebo třeba číslicí *9*). Počet znaků zašifrovaného textu pro jeden znak otevřeného textu se může lišit - obvykle čím četnější znak, tím více možností zašifrování má (např. písmeno a, které tvoří cca 7% všech textů české abecedy, se zašifruje až sedmi možnými způsoby). Díky tomu každý z těchto symbolů tvoří po zašifrování asi 1 % šifrového textu.
Možnost zašifrování písmene různými možnostmi je podobná s polyalfabetickou šifrou - rozdíl je však v tom, že u homofonní šifry se rozhoduje šifrant o tom, který znak použije, kdežto u polyalfabetické subtituce je výběr znaku přesně dán dohodnutým systémem.

Podobnost s monoalfabetickou šifrou spočívá v tom, že jakmile je jednou ustavena šifrová abeceda, zůstává po celý proces šifrování stejná. Homofonní šifra se nedá rozluštit tak snadno jako monoalfabetická šifra, nicméně při dostatečně dlouhém textu lze i to. Název šifry je odvozen z řeckých slov *homos* (znamená „stejný“) a *phonos* (znamená „zvuk“) Každý symbol odpovídající nějakému písmenu reprezentuje vlastně „stejný zvuk“, tedy je homofonní.
Další možností subtituce je náhrada nikoliv jednotlivých znaků, ale jejich skupin (dvojic, trojic...). Taková šifra se nazývá obecně *polygramová*. V případě náhrady bigramů (dvojic) je to konkrétně bigramová, u trojic trigramová atd. Příkladem takové bigramové šifry je systém nazývaný *Playfair*. Jeho výhodou je větší odolnost vůči luštění metodami účinnými na monoalfabetickou šifru. Tato šifra byla s úspěchem používána až do období 2.světové války [1].

2.2.2 Transpozice

Transpozice je obecně přeuspořádání pořadí písmen otevřeného textu podle vybraných pravidel, výsledkem čehož je šifrový text. V současné době se používá mj. jako součást moderních algoritmů (DES, AES). Protože jednotlivé znaky otevřeného textu se ničím nenahrazují, zůstává při této šifrovací metodě zachována četnost hlásek. Naopak nezachovávají se vazby mezi hláskami (bigramy - dvojhlásky a trigramy - trojhlásky).

Jednoduchá transpozice

Nejjednodušším transpozičním systémem je *jednoduchá sloupcová transpozice* (někdy nazývaná krátce *jednoduchá transpozice*). Pochází z 16.stol., byla vytvořena kardinálem Richelieu, prvním ministrem francouzského krále Ludvíka XIII. Richelieu dokonce údajně založil šifrovací oddělení, které se zabývalo šifrováním předávaných informací.
Vlastní šifrování spočívá ve výběru klíče a následně vytvoření transpoziční tabulky, do které se vepíše po řádcích otevřený text. Poté se zamění pořadí sloupců tabulky, podle zvoleného klíče.
Klíčem je v případě této šifry skupina čísel, která znamenají pořadí sloupců. Je možné zvolit si přímo řadu čísel jako klíč (např. 6 4 1 3 2 5), nicméně pro snazší zapamatovatelnost je lépe zvolit si nějakou frázi. Může to být například slovo *luštění*, které je třeba zbavit diakritických znamének - *LUSTENI*. Jednotlivá písmena klíče se očíslují tak, jak odpovídá pořadí písmen pořadí jejich výskytu v abecedě.
V tomto případě je písmenu *E* přiřazeno číslo 1, písmenu *I* přiřazeno číslo 2, písmenu *L* číslo 3 atd. Výsledkem je klíč *3756142*. Tomuto způsobu získání klíče se říká tzv. *permutační vyčíslení*. Pokud se některá písmena ve frázi opakují, přiřazují

se jim čísla vzestupně dle pořadí ve frázi. Pokud se opakují přímo dvě písmena za sebou, druhé se obvykle vynechává - nicméně tyto konvence lze po dohodě s druhou stranou samozřejmě změnit. V praxi je vhodné volit klíč alespoň o délce 20 [1].
Z délky klíče vyplývá počet sloupců, které bude mít šifrovací tabulka - v případě klíče *LUSTENI* je to 7 sloupců. Následující příklad (tab.2.7) demonstruje zašifrování otevřeného textu „diplomová práce“. Text se vepíše po řádcích do tabulky o sedmi sloupcích, nad níž je zapsán permutační klíč.

3	7	5	6	1	4	2
D	I	P	L	O	M	O
V	A	P	R	A	C	E

Tab. 2.7: Otevřený text před zašifrováním jednoduchou transpozicí

V dalším kroku se vymění pořadí sloupců tak, aby odpovídalo pořadí čísel klíče (tab.2.8). Výsledný šifrový text se získá čtením znaků tabulky po sloupcích a v tomto případě je to *OAOEDVMCPPLRIA*. Při šifrování lze samozřejmě vynechat krok výměny pořadí sloupců v tabulce a šifrový text rovnou zapisovat dle pořadí klíče. Šifrový text se ještě obvykle dělí na menší skupiny znaků, např. po pěti (pozůstatek telegrafické konvence), takže výsledek by potom vypadal *OAOED VMCPP LRIA*.
V případě, že se otevřený text nedá rozdělit přesně podle počtu sloupců, nabízí se dvě možnosti. V prvním případě se doplní potřebný počet míst v tabulce o různé - předem domluvené - znaky. Jedná se o tzv. *jednoduchou transpozici s úplnou tabulkou*. Naopak, pokud tabulka na konci šifrování těmito znaky doplněna není, jedná se o *jednoduchou transpozici s neúplnou tabulkou*. Pro šifrování a dešifrování se při systému s neúplnou tabulkou nic nemění, ovšem pro luštění je náročnější druhá varianta. Důvodem je obtížnější určení rozměrů tabulky, což je prvním krokem při luštění této šifry.
Jednoduchou transpozici lze dále modifikovat, aby byla vůči luštění odolnější - například je možné použít ji dvakrát za sebou: otevřený text se zapíše do úplné tabulky a je přeuspořádán dle permutačního klíče. Výsledek je potom znovu zapsán do - tentokrát již neúplné - tabulky, a opět dojde k přeházení sloupců dle jiného domluveného klíče. Tento systém se nazývá *dvojitá neúplná transpozice* a její prolomení

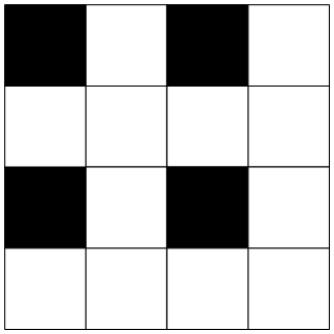
1	2	3	4	5	6	7
O	O	D	M	P	L	I
A	E	V	C	P	R	A

Tab. 2.8: Výměna sloupců při transpozici dle zvoleného klíče

je velmi nesnadné (nikoliv však nemožné).
Pro dešifrování jednoduché transpozice musí druhá strana znát klíč. Ten určuje počet sloupců tabulky a zároveň jejich pořadí. Pokud se počet znaků šifrového textu vydělí počtem sloupců (odvozených z klíče), dešifrant získá informaci o počtu řádků - a tím pádem zná rozměr transpoziční tabulky. Do ní se pak po sloupcích zapíše šifrový text, který se po přeuspořádání podle klíče čte po řádcích.

Další transpoziční systémy

Úhlopříčkově - sloupcová transpozice byla používána nejvíce během 1.světové války a to po dobu tří let - na jeden šifrový systém nevídaná doba. Otevřený text se - stejně jako u jednoduché transpozice - vepíše po řádcích do transpoziční tabulky, vytvořené podle klíče. Rozdíl však spočívá v tom, že šifrový text se z tabulky nevyčítá po sloupcích, ale nejprve po vybraných úhlopříčkách a až poté po sloupcích.
Fleissnerova otočná mřížka je pojmenovaná po svém autorovi, Fleissnerovi von Wostrovitz, který ji vytvořil r.1881. Pro šifrování touto metodou je zapotřebí pomůcka - velký čtverec s vyznačenou sítí malých čtverců (viz obrázek 2.2). Některé malé čtverce se označí - tak, aby při postupném otáčení velkého čtverce o 90° malé označené čtverce postupně pokryly celý velký čtverec). Tímto způsobem získáme otočnou mřížku. Šifrování je pak poměrně jednoduchá záležitost - text postupně



Obr. 2.2: Fleissnerova otočná mřížka

vepisujeme do označených čtverečků; ve chvíli, kdy je zaplníme, otočíme velký čtverec o 90° a pokračujeme tímto způsobem dále. Pro dešifrování je zapotřebí vlastnit stejnou šablonu, která postupně odhaluje otevřený text.
Transpozice plukovníka Roche spočívá v rozdělení textu do nestejně dlouhých bloků. Nejprve je třeba zvolit klíč - pro jednoduchost číselný, např. *53124*. Tento klíč určuje velikost bloků, do kterých bude původní text rozdělen. Pro tento konkrétní příklad budou vypadat následujícím způsobem:
Otevřený text (pro příklad zvolena fráze *diplomová práce*) se vpisuje do těchto bloků - postupně každé písmeno do jednoho bloku. Jakmile dojdeme k poslednímu bloku,

```
  5      3    1   2      4
XXXXX  XXX   X   XX   XXXX
```

posunujeme se opět na začátek k prvnímu (ale na druhou pozici) a postup opakujeme, dokud nezašifrujeme celý otevřený text: *DMPCX IOR P LV OAAE*. Ten se přeskupí do skupin po pěti znacích, výsledný šifrovaný text bude vypadat *DMPCX IORPL VOAAE*. Dešifrování probíhá následovně: ze znalosti klíče se určí počet a délka jednotlivých bloků, do kterých se rozdělí šifrový text. Ten potom lze postupně číst - první pozice bloků, druhé pozice a tak dále.

2.3 Základní metody luštění šifer

Aby byl luštitel schopný šifru rozluštit, musí s šifrovým textem obvykle provést několik základních kroků. Pomocí *indexu koincidence* se pokusí zjistit, zda jde o šifru polyalfabetickou (která je charakteristická vyrovnáním rozdílu četnosti jednotlivých znaků v textu) nebo jednoduchou substituci či záměnu. V případě jednoduché substituce a transpozice se zároveň pokusí určit, v jakém jazyce byl psán otevřený text. Pro další luštění se používá metoda *frekvenční analýzy*, která si všímá znakových vazeb charakteristických pro daný jazyk.
Následující metody vycházejí z předpokladu, že otevřený text je psán mezinárodní abecedou.

2.3.1 Index koincidence

Luštitel obvykle na začátku stojí před úkolem zjistit, jakým způsobem je šifrový text zašifrován (odhalit použitý šifrový systém). V případě klasických šifer lze úspěch obvykle znásobit použitím některého ze statických testů, které pomáhají učit typ luštěné šifry. Prvotní analýza textu může často ušetřit spoustu marných pokusů. Významnou metodou pro rozhodování je tzv. index koincidence (IC). Autorem této techniky je William Frederick Friedman (1891 - 1969), který působil jako kryptolog u americké armády. Index koincidence se poprvé objevil v jeho publikaci The Index of Coincidence and Its Applications to Cryptography a zcela pozměnil tehdejší možnosti kryptoanalýzy šifer. Svého času byla tato kniha dokonce označována jako nejvýznamnější počin v oblasti kryptografie a přinášela do tohoto odvětví vyšší matematiku, statistiku a pravděpodobnost.
Index koincidence (dále jen IC) je míra relativní četnosti písmen v (šifrovém) textu. Tento statistický test může výrazně usnadnit kryptoanalýzu klasických šifer - zejména pak polyalfabetické. Pro určení délky klíče této šifry se dá použít Kasiského metoda

nebo jako alternativa právě odhad pomocí IC (více viz 2.4.3). IC je tedy definován jako pravděpodobnost, že dva znaky náhodně vybrané z šifrového textu budou stejné. Tato pravděpodobnost se vyjádří následujícím vztahem:

$$IC = \sum_{i=1}^{c} \frac{n_i \cdot (n_i - 1)}{N \cdot (N - 1)} \tag{2.3}$$

V tomto vzorci N znamená celkový počet znaků textu, ze kterého je IC počítán, c označuje počet znaků abecedy a n_i je počet znaku s indexem i, kde $i \in \{0, 1..25\}$ - pro mezinárodní abecedu n_1 je počet všech znaků **a** v celém textu, n_2 počet všech znaků **b** atd.). Čitatel zlomku vyjadřuje počet dvojic obsahujících dvě stejná písmena, jmenovatel vyjadřuje počet všech dvojic písmen v analyzovaném textu [4].
Z uvedeného vzorce vyplývá, že čím větší jsou rozdíly v četnosti výskytu jednotlivých písmen u daného jazyka, tím větší je jeho index koincidence a naopak - v případě analýzy náhodně vygenerovaného sledu znaků je obvykle IC znatelně menší (blíží se hodnotě 0,0385).
Každý jazyk je charakteristický svým indexem koincidence, který hodnotí kolísání četností znaků textu. Pro náhodný text je IC vypočítán jako hodnota 1/26 - což vyplývá z následujícího:
uvažujeme-li mezinárodní abecedu (26 znaků), pravděpodobnost náhodného výběru jednoho z nich je $P(znak) = 1/26 = 0,0385$. Tato hodnota zároveň vyjadřuje velikost pravděpodobnosti (označovaná jako κ_r), že bude náhodně vybrán identický pár:

$$\kappa_r = \frac{1}{26} \cdot \frac{1}{26} + \frac{1}{26} \cdot \frac{1}{26} + \ldots + \frac{1}{26} \cdot \frac{1}{26} = 26 \cdot \frac{1}{26^2} = \frac{1}{26} = 0,0385 \tag{2.4}$$

Jinými slovy, na každých 100 dvojic písmen připadají necelé čtyři shody znaků. Tato hodnota pravděpodobnosti však platí pouze v případě, kdy písmena jsou rozložena naprosto nahodile, tj. žádné z nich nemá vyšší četnost výskytu než ostatní. Pokud však vezmeme v úvahu charakteristické rysy konkrétního jazyka - např. rozložení hlásek (mezinárodní abeceda) v českém jazyce (viz tabulka 2.11), pravděpodobnost se změní následujícím způsobem:

$$\begin{aligned}
\kappa_p &= \sum_{i=1}^{26} p_i^2 = (0,0865)^2 + (0,0163)^2 + (0,0355)^2 + (0,0356)^2 + (0,1029)^2 + \\
&+ (0,0038)^2 + (0,0034)^2 + (0,0226)^2 + (0,0752)^2 + (0,0194)^2 + \\
&+ (0,0368)^2 + (0,0402)^2 + (0,032)^2 + (0,0662)^2 + (0,0815)^2 + \\
&+ (0,0339)^2 + (0,00)^2 + (0,0051)^2 + (0,00)^2 + (0,0506)^2 \\
&+ (0,0533)^2 + (0,0548)^2 + (0,0377)^2 + (0,043)^2 + (0,0007)^2 + \\
&+ (0,0009)^2 + (0,0344)^2
\end{aligned} \tag{2.5}$$

kde p_i je pravděpodobnost výskytu i-tého znaku v abecedě, tj. na každých 100 dvojic znaků českého textu připadá něco mezi pěti a šesti shodami. Tato hodnota je charakteristická pro každý jazyk.
Známe-li četnost rozložení písmen v daném jazyce, můžeme pomocí zobecněné rovnice

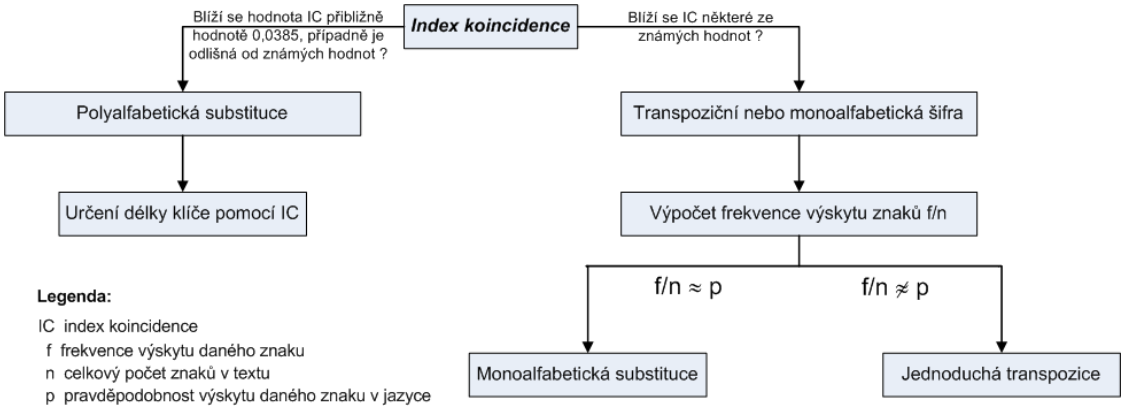
$$\kappa_p = \sum_{i=1}^{N} p_i^2 \tag{2.6}$$

kde N je počet znaků abecedy, určit očekávaný index koincidence příslušného jazyka. Hodnota pro náhodný text je označována jako κ_r. Jedná se o tzv. kappa - test, který vyjadřuje index koincidence daného jazyka [15].
Jednotlivé hodnoty κ_p pro různé jazyky uvádí tabulka 2.9. (vždy počítáno z mezinárodní abecedy, pouze u ruštiny se jedná o 32 znaků).

jazyk	hodnota IC (κ_p)
Němčina	0,0824
Francouzština	0,0801
Španělština	0,0769
Italština	0,0754
Angličtina	0,0676
Slovenština	0,0581
Čeština	0,0577
Ruština	0,0470
Náhodný text (κ_r)	0,0385

Tab. 2.9: Index koincidence pro vybrané druhy jazyků

Obrázek 2.3 znázorňuje využití IC pro určení typu šifry. Jak již bylo řečeno v před-



Obr. 2.3: Využití indexu koincidence

chozích kapitolách (2.2.1 a 2.2.2), monoalfabetická šifra a jednoduchá transpozice zachovávají rozložení četnosti znaků. V případě, že se vypočítaný IC šifrového textu blíží některé z hodnot v tabulce 2.9, je na základě výše uvedených poznatků pravděpodobné, že se bude jednat právě o jednoduchou substituci nebo transpozici s otevřeným textem v příslušném jazyce.
Pro rozlišení, zda se jedná o substituci nebo transpozici, pak stačí spočítat pravděpodobnost výskytu jednotlivých znaků v šifrovém textu: pokud jsou pravděpodobnosti shodné s pravděpodobností výskytu znaků v jazyce určeném pomocí IC, jedná se zřejmě o transpozici, naopak pokud jsou pravděpodobnosti pro totožné znaky odlišné, jde o substituci.
Polyalfabetická substituce vyhlazuje rozdíly mezi četností znaků v dané abecedě, to znamená že IC pro takový šifrový text bude nižší než příklady uvedené v tabulce 2.9, pravděpodobněji se bude blížit hodnotě IC pro náhodný text (tj. 0,0385).
Čím delší šifrový text je k dispozici, tím lépe bude IC fungovat - samozřejmě jen v případě, že nepůjde o otevřený text záměrně napsaný tak, aby nesplňoval základní statistické charakteristiky příslušné danému jazyku.

2.3.2 Frekvenční analýza

Základ frekvenční analýze položili kolem r.750 n.l. arabští učenci a úředníci, kteří pro své účely potřebovali bezpečný komunikační systém - nejlépe šifrovaný. Obvykle používali šifrovou abecedu, která vznikla pouhým přeuspořádáním otevřené abecedy. Byl tak položen základ *monoalfabetické substituční šifře* (viz kapitola 2.1). Kromě šifrování a dešifrování však tito učenci dokázali tyto šifry také luštit - dá se na ně pohlížet jako na zakladatele kryptoanalýzy. Ta však nemohla vzniknout dříve, než se v dostatečné míře rozvinuly některé další vědní disciplíny - matematika, statistika nebo lingvistika [1].
Základ pro luštění šifer metodou frekvenční analýzy byl položen v teologických školách, které zkoumaly zjevení proroka Muhammada sepsaná v Koránu. Teologové se snažili jednotlivá zjevení chronologicky uspořádat, a použili k tomu velmi důmyslnou metodu: všímali si četnosti slov v textech jednotlivých zjevení. Vycházeli přitom z předpokladu, že některá slova se vyvinula poměrně nedávno na rozdíl od jiných - takže pokud daný text taková slova obsahoval, zřejmě byl novější než ostatní. Arabští učenci však při analýze textů zašli ještě dál, a to až na úroveň jednotlivých hlásek - všímali si jejich četnosti v textu. Od tohoto byl už jen malý krok k luštění šifer: první známý popis frekvenční analýzy v souvislosti s luštěním šifry pochází od arabského učence, v Evropě známého pod jménem Alkindus, z 9.století n.l. V době rozmachu arabského umění šifrování a luštění prožívala Evropa v tomto směru zcela dobu temna. Jediné výjimky představovaly kláštery, ve kterých mniši studovali Bibli

a snažili se odkrýt utajené významy v jejím textu.
Metoda frekvenční analýzy spočívá v aplikaci statistiky na šifrový text. Každý jazyk (anglický, český..) je charakteristický některými významnými rysy, jako jsou například průměrná četnost jednotlivých hlásek (případně skupin hlásek) nebo vazby mezi samohláskami atd. Z toho důvodu je při luštění výhodné znát jazyk otevřeného textu (k tomu může být nápomocný index koincidence, viz 2.3.1). Tabulka 2.10 zobrazuje první z důležitých vlastností - četnost jednotlivých hlásek v českém jazyce.

znak	počet[1]	% četnost	**znak**	počet[1]	% četnost	**znak**	počet[1]	% četnost
a	357907	6,698%	**i**	244242	4,571%	**s**	246867	4,62%
á	113756	2,129%	**í**	165786	3,103%	**š**	43636	0,817%
b	88974	1,665%	**j**	105955	1,983%	**t**	296779	5,554%
c	85538	1,601%	**k**	200479	3,752%	**ť**	2057	0,038%
č	54341	1,017%	**l**	218906	4,097%	**u**	167322	3,131%
d	193038	3,613%	**m**	174323	3,262%	**ú**	7736	0,145%
ď	1040	0,019%	**n**	356743	6,676%	**ů**	30430	0,569%
e	418434	7,831%	**ň**	3926	0,073%	**v**	233960	4,378%
é	62945	1,178%	**o**	442617	8,283%	**w**	3843	0,072%
ě	79674	1,491%	**ó**	1704	0,032%	**x**	4942	0,092%
f	21055	0,394%	**p**	184548	3,454%	**y**	93620	1,752%
g	18319	0,343%	**q**	308	0,006%	**ý**	50312	0,942%
h	69236	1,296%	**r**	212533	3,977%	**z**	113450	2,123%
ch	53802	1,007%	**ř**	63395	1,186%	**ž**	54602	1,022%

Tab. 2.10: Frekvence písmen české abecedy

Protože se však obvykle šifruje (a luští) text zbavený diakritických znamének, tabulka 2.11 zobrazuje četnost hlásek české abecedy, zbavené diakritiky (četnost výskytu písmene i je rovna součtu četnosti výskytu písmen ***i*** a ***í***) [2] [5] . Následuje výčet některých statistických údajů českého jazyka, které mohou být při luštění monoalfabetické šifry velmi užitečné [1].

- frekvence znaků - vybereme ty nejčetnější znaky vyskytující se v šifrovém textu a přeložíme je dle tabulky 2.11
- ve slovech se samohlásky se souhláskami téměř pravidelně střídají
- poměr souhlásek a samohlásek v českém textu je přibližně 60:40 (přesněji 58,56:41,44).

[1] Jedná se o celkový výskyt znaku v českých slovech
[2] Různé zdroje se v těchto statistických údajích mohou mírně lišit

znak	počet[1]	% četnost	**znak**	počet[1]	% četnost	**znak**	počet[1]	% četnost
a	471663	8,740%	**j**	105955	1,963%	**s**	290503	5,383%
b	88974	1,649%	**k**	200479	3,715%	**t**	298836	5,537%
c	143722	3,589%	**l**	218906	4,056%	**u**	205488	3,808%
d	194078	3,596%	**m**	174323	3,230%	**v**	233960	4,335%
e	561053	10,396%	**n**	360669	6,683%	**w**	3843	0,071%
f	21055	0,390%	**o**	444321	8,233%	**x**	4942	0,092%
g	18319	0,340%	**p**	184548	3,420%	**y**	143932	2,667%
h	73079	2,280%	**q**	308	0,006%	**z**	168052	3,114%
i	410028	7,580%	**r**	275928	5,113%			

Tab. 2.11: Frekvence písmen základní abecedy (26 znaků)

- 2 samohlásky uprostřed slova se vedle sebe téměř nevyskytují
- v souhláskových vazbách se písmeno R chová jak samohláska
- nejčastěji vyskytující se písmena na začátku (českých) slov jsou: p (12,50%), s (9,72%), v (9,19%), z (8,95%), n (7,64%), o (5,56%); obecně samohlásky tvoří počátek slov pouze z 15,49%, zbytek tvoří souhlásky
- nejčastěji vyskytující se písmena na konci (českých) slov jsou: e (16,67%), i (13,96%), a (10,94%), o (8,93%), u (7,94%), y (7,03%); obecně souhlásky tvoří počátek slov pouze z 34,53%, zbytek tvoří samohlásky
- důležitými bigramy jsou ST, PR, SK, CH, DN, TR (frekvence výskytu v českém jazyce viz tabulka 2.12)
- bigram CH: písmeno H má (dle tabulky) jen o něco nižší frekvenci než C; CH se často vyskytuje na konci slov a předchází ho samohláska; naopak, pokud ho předchází souhláska, samohláska obvykle následuje (schod)
- bigram PR: často stojí na začátku slov; R má přibližně dvojnásobnou frekvenci výskytu oproti P; obrácený bigram RP se téměř nevyskytuje;
- bigram ST: obvykle se vyskytuje na konci i uprostřed slova; písmena S a T mají přibližně stejnou četnost výskytu;
- existují také často se vyskytující trigramy (viz tabulka 2.13): STR (nejčastější trigram), PRO, UNI, OST, STA, ANI, OVA, YCH, STI, PRI, PRE, OJE, REN, IST, EHO, TER, RED, ICH
- průměrná délka slova v textu činí 5,54 písmene

pořadí	bigram	počet[3]	pořadí	bigram	počet[3]	pořadí	bigram	počet[3]
1.	st	74285	15.	ra	37531	29.	ce	28280
2.	ní	60525	16.	to	36355	30.	va	27987
3.	po	56239	17.	ou	35191	31.	př	27885
4.	ov	53818	18.	no	32612	32.	at	27603
5.	ro	51961	19.	la	32336	33.	ře	27181
6.	en	50645	20.	li	31952	34.	er	27168
7.	na	46737	21.	ho	31442	35.	ti	26858
8.	je	42433	22.	do	30665	36.	em	26818
9.	pr	42099	23.	os	30530	37.	in	26427
10.	te	40393	24.	se	30454	38.	sk	26085
11.	le	38926	25.	ta	30177	39.	lo	25981
12.	ko	38688	26.	al	29682	40.	ně	25739
13.	ne	38671	27.	ed	29622			
14.	od	38393	28.	an	29326			

Tab. 2.12: Nejčastější bigramy českého jazyka

pořadí	trigram	počet[4]	pořadí	trigram	počet[4]	pořadí	trigram	počet[4]
1.	pro	21322	15.	nos	8557	29.	ové	6810
2.	ost	18722	16.	ick	8387	30.	nov	6783
3.	sta	12746	17.	ová	8139	31.	pol	6704
4.	pře	12057	18.	při	7878	32.	spo	6686
5.	ter	11936	19.	sou	7541	33.	vat	6489
6.	ení	11917	20.	ist	7505	34.	ním	6439
7.	ova	11822	21.	edn	7429	35.	jak	6330
8.	pod	10168	22.	ské	7349	36.	val	6256
9.	kte	9603	23.	pří	7348	37.	dní	6251
10.	pra	9521	24.	odn	7251	38.	sto	6189
11.	ého	9475	25.	tel	7231	39.	tak	6175
12.	sti	9121	26.	ání	7224	40.	lov	6139
13.	řed	9103	27.	ent	7114			
14.	kon	9017	28.	str	6903			

Tab. 2.13: Nejčastější trigramy českého jazyka

Je důležité uvědomit si, že frekvenční analýzu nelze používat zcela mechanicky. Tabulka četnosti výskytu hlásek v abecedě představuje pouze průměr a nemusí zcela přesně odpovídat poměru výskytu v konkrétním zašifrovaném textu. Zcela záměrně lze totiž vytvořit takový otevřený text, který nebude splňovat průměrné charakteristiky daného jazyka. Obecně čím delší šifrový text je analyzován, tím lépe, protože s největší pravděpodobností bude lépe fungovat statistika a výše popsané poznatky se dají spolehlivěji využít. Naopak čím kratší šifrový text, tím je pravděpodobnější, že výskyt hlásek nebude odpovídat tabulce četnosti. Za hranici použitelnosti je považován text o délce minimálně 100 znaků [1].

2.4 Luštění

Kryptoanalytik se vždy na počátku snaží odhalit, jaký šifrovací sytém byl použit. Tato fáze se nazývá *identifikace*. Použije k tomu nejen nástroje jako je třeba *index koincidence*, ale také veškeré dostupné informace o autorovi šifry (jaké šifry používal v minulosti atd.). V případě, že je zachycená zpráva příliš krátká, těžko se na ni uplatní statistické testy - je třeba získat nějakou další.
Nejobtížnější fází luštění je *prolomení*. Jednoduché šifrovací systémy, kterými se zabývá tato práce, se obvykle dají prolomit *ručně*. Moderní šifrovací metody jsou dnes již natolik výpočetně složité, že se luštitel neobejde bez výpočetní techniky. I tak může prolomení trvat týdny, měsíce a nebo k němu nemusí vůbec dojít.
Pro luštění šifrového textu lze využít několika různých metod, v závislosti na možnostech, kterými kryptoanalytik disponuje [1].

Luštění na základě znalosti šifrového textu Pokud má kryptoanalytik k dispozici více šifrových textů zašifrovaných stejným systémem, může se pokusit odvodit na základě luštění klíč, nebo přímo rozluštit tyto zprávy. Tato situace nastává nejčastěji, ale je také nejobtížnější.

Luštění na základě znalosti otevřeného textu V případě, že má kryptoanalytik k dispozici jak šifrový text, tak jeho otevřenou předlohu, může se pokusit o odhalení klíče, případně šifrovacího algoritmu.

Útok hrubou silou V tomto případě přichází obvykle na řadu výpočetní technika. Kryptoanalytik zkoumá všechny možnosti šifrování textu a vyhodnocuje, jestli byl nalezen ten správný. Ne vždy se však všechny možnosti dají otestovat v reálném čase, takže tento postup zůstává sice teoreticky, nikoliv však vždy prakticky možný.

[3] Jedná se o celkový výskyt bigramu v českých slovech
[4] Jedná se o celkový výskyt trigramu v českých slovech

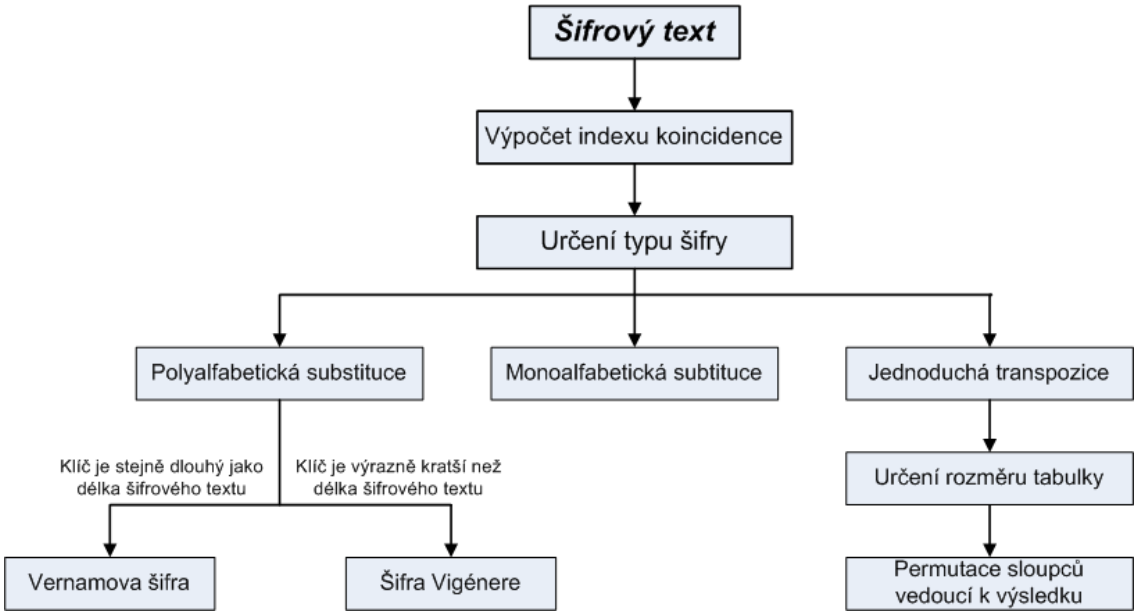
Útok postranními kanály Tímto způsobem se kryptoanalytik obvykle snaží získat klíč nebo přímo otevřený text. Informace mohou unikat pomocí elektromagnetického vyzařování, měřením spotřeby proudu a času apod.

Korupční kryptoanalýza V případě korupční kryptoanalýzy dojde k úniku informací (klíčů, algoritmů, otevřeného textu..) na základě selhání lidského faktoru - to znamená, že díky podplácení, krádežím atd. má kryptoanalytik k dispozici potřebné údaje, na jejichž základě rozluští šifrový text.

Výše popsané metody luštění lze ještě jemněji dělit podle určitých kritérií, pro prvotní přiblížení je však tento výčet dostatečný. Následující text popisuje postup při luštění šifer na základě znalosti šifrového textu.

2.4.1 Obecný postup luštění klasických šifer

Obrázek 2.4 demonstruje možný obecný postup při luštění klasických šifer.



Obr. 2.4: Obecný postup při luštění klasických šifer

Pro žádnou z výše popsaných šifer neexistuje jednoznačný postup, který by vedl vždy k přesnému vyluštění. Existují určité metody, které luštění usnadňují, ve skutečnosti však vždy hraje větší či menší roli vlastní úvaha kryptoanalytika.
Pro kryptoanalýzu jsou podstatné dvě informace:

- znalost kryptosystému (substituce, transpozice...)

- znalost parametrů spjatých s tímto kryptosystémem (parametr posunu…)

Postup při luštění klasických šifer může být následující:
Nejprve je třeba vypočítat *index koincidence* upraveného šifrového textu (tj. zbaveného mezer). Pomocí něj se provede prvotní odhad typu šifry, případně jazyka otevřeného textu (viz obrázek 2.3). V případě monoalfabetické substituce a jednoduché transpozice se dále provede srovnání četnosti výskytu jednotlivých znaků šifrového textu a očekávaného jazyka otevřeného textu. Pokud je četnost znaků šifrového textu a předpokládaného jazyka otevřeného textu stejná, zřejmě se bude jednat o transpozici - v opačném případě o substituci.
V případě polyalfabetické šifry je třeba určit délku šifrovacího klíče - podle něj se provede rozdělení na šifru Vigénere nebo Vernamovu šifru (která je obecně nerozluštitelná).

2.4.2 Luštění monoalfabetické substituce

Pro luštění jednoduché substituce je nutné disponovat dostatečně dlouhým šifrovým textem - obvykle by měl mít alespoň 200 znaků. Za úplné minimum (které však nemusí mít jednoznačné řešení) se považuje text o délce 50 znaků [8].
Vzhledem k tomu, že pro abecedu o velikosti 26 znaků existuje $\approx 4 \cdot 10^{26}$ možností, ani pro současnou výpočetní techniku není reálné vyzkoušet je všechny v rozumném čase. Jak již bylo řečeno v kapitole 2.1, jednoduchá záměna je charakteristická některými statistickými rysy. V případě, že luštitel určí (např. za pomocí indexu koincidence), že daná šifra je pravděpodobně jednoduchou záměnou, lze pro získání otevřeného textu využít metodu *frekvenční analýzy* (viz 2.10).
Samotná monoalfabetická substituce se rozpadá na několik poddruhů (viz 2.1). Počátek luštění je pro všechny stejný (kryptoanalytik neví, která z šifer byla použita): nejprve je třeba určit frekvenci výskytu jednotlivých hlásek šifrové abecedy (to již pravděpodobně bylo učiněno při rozpoznávání typu šifry). Dále se vyberou nejčetnější znaky šifrového textu a mapují se na nejčetnější znaky očekávané abecedy otevřeného textu. Vzhledem k tomu, že v českém jazyce je nejčetnějším písmenem *e* (viz tabulka 2.11), ve většině případů se začíná právě s ním. Čím více písmen se na základě četnosti výskytu podaří namapovat, tím snažší je pokračování luštění - při dostatečně dlouhém textu je možno obvykle namapovat 5 nejčetnějších (e, a, o, i, n) a 5 nejméně četných písmen (q, w, x, f, g).

Jednoduchý posun

Dále se luštitel může pokusit vyjádřit rozdíl pozic písmen šifrové a nové namapované abecedy. V případě, že je původní text zašifrován substitucí s jednoduchým posu-

nem, u správně namapovaných znaků se tento rozdíl projeví právě jako parametr posunu. Čím více znaků se luštitel pokusí namapovat, tím pravděpodobněji správně určí parametr posunu (tzn. pokud je např. suverénně nejčastějším písmene v šifrové abecedě - s četností přes 10% - písmeno **n**, zřejmě bude odpovídat písmenu **e** v oteřené abecedě, a rozdíl mezi indexy těchto písmen je 9 - to je zmiňovaný parametr posunu).

Euklidův algoritmus

Pokud metoda vyjádření rozdílu selže, je možno použít algoritmus pro luštění afinní šifry. Pro dešifrování lze použít tuto formuli:

$$O(x) = (a' \cdot S(x) + b') \ mod \ 26 \tag{2.7}$$

kde a' je tzv. mutiplikativní inverze a v Z_{26} [12] a

$$b' = -a^{-1} \cdot b \tag{2.8}$$

To ale platí pouze tehdy, když největší společný dělitel $nsd(a, 26) = 1$ (pro abecedu o 26ti znacích; v opačném případe nelze O vyjádřit jako funkci S - jednomu znaku šifrové abecedy by odpovídalo více znaků abecedy otevřeného textu, tzn. šifrový text nelze jednoznačně dešifrovat). Největší společný dělitel dvou čísel se dá vypočítat např. pomocí Euklidova algoritmu [13].
Modulární multiplikativní inverzi čísla a v Z_{26} lze vyjádřit jako

$$a^{-1} \equiv x \ mod \ 26 \tag{2.9}$$

což je ekvivalentní s

$$a \cdot x \equiv 1 \ mod \ 26 \tag{2.10}$$

Jak již bylo řečeno, tato inverze existuje pouze v případě, že $nsd(a, 26) = 1$. Konkrétní příklad výpočtu multiplikativní inverze:

$$3^{-1} \equiv x \ mod \ 26 \tag{2.11}$$

tedy

$$3 \cdot x \equiv 1 mod \ 26 \tag{2.12}$$

Nejmenším x, které řeší tuto rovnici, je 9 (protože $(3 \cdot 9) \ mod \ 26 = 1$. Rovnici řeší také čísla 35, 61 - zkráceně množina všech čísel $\{9 + n \cdot 26\}$, kde $n \in N_0$. Tato inverze se dá mj. vypočítat pomocí rozšířeného Euklidova algoritmu [13].
Luštitel stojí před úkolem odhadnout parametry a^{-1} a b. Postup je následující:
nejprve je třeba pomocí pravidel frekvenční analýzy (viz kapitola 2.3.2) namapovat

alespoň 2 písmena šifrové abecedy na původní abecedu otevřenou (obvykle se začíná nejčetnějšími písmeny - *e, a, o*). Pomocí nich se sestaví soustava dvou rovnic o dvou neznámých pro šifrování:

$$s_1 = (a \cdot o_1 + b) \ mod \ 26$$
$$s_2 = (a \cdot o_2 + b) \ mod \ 26 \tag{2.13}$$

kde o_1, o_2 jsou písmena otevřeného textu, s_1, s_2 odpovídající písmena šifrového textu. Pomocí ekvivalentních úprav (obvykle sčítání a odčítání) je třeba z rovnic vyjádřit a, např. odečtením:

$$s_2 - s_1 = (o_2 - o_1) \cdot a \ mod \ 26 \Rightarrow (s_2 - s_1) \cdot (o_2 - o_1)^{-1} = a \ mod \ 26 \tag{2.14}$$

kde $(o_2 - o_1)^{-1}$ je již výše zmíněná multiplikativní inverze. Výsledné a se dosadí do libovolné ze dvou původních rovnic, čímž se vyjádří druhý parametr b. V tuto chvíli jsou již známy parametry šifrového systému a je možno zašifrovaný text dešifrovat pomocí rovnice 2.7.
Vzhledem k tomu, že luštění afinní šifry není zpočátku zcela triviální, je demonstrováno na příkladu v příloze B.

Ostatní systémy

V případě, že se nepodařilo rozluštit jednoduchou substituci jako posun ani jako afinní šifru, luštiteli nezbývá než se snažit ručně mapovat co nejvíce písmen šifrové abecedy na abecedu otevřenou, přičemž k tomu využívá poznatky popsané v kapitole 2.3.2.

2.4.3 Luštění polyalfabetické substituce

Prvním úkolem při luštění tohoto typu šifry je určení délky klíče. Metod pro určení je několik, následuje popis tří nejpoužívanějších:

Kasiského metoda Má-li kryptoanalytik k dispozici dostatečně dlouhý text, začne v něm hledat opakující se polygramy (čím delší, tím lepší - nejfrekventovanější však jsou obvykle bigramy). Pokud jejich výskyt není náhodný, tj. odpovídá stejnému otevřenému textu, musí být vzdálenost těchto polygramů rovna násobku délky klíče - a to proto, že se jedná o stejný otevřený text zašifrovaný stejným úsekem hesla. Pro jednotlivé opakující se polygramy se určí jejich vzdálenost. Skutečná délka klíče pak bude s největší pravděpodobností největším společným dělitelem těchto vzdáleností. Při tomto postupu je třeba mít na vědomí, že opakované bigramy mohou v šifrovém textu vzniknout i náhodně, a ne všechny vzdálenosti opakovaných bigramů

musí být násobkem délky klíče (delších polygramů se to v drtivé většině případů netýká).
V tuto chvíli již je známá délka klíče, zbývá určit jeho podobu. Myšlenka spočívá v tom, že v šifrovém textu se pravidelně opakují skupiny znaků (s periodou délky hesla), které jsou zašifrovány jednoduchým posunem. Parametrem posunu je písmeno hesla (resp. jeho index v abecedě). To znamená, že pro délku klíče x bude posunutí o x_1 aplikováno na skupiny znaků s indexem polohy v textu{*1, x+1, 2x+1...*} *atd.*, posunutí o x_2 bude aplikováno na skupiny znaků s pořadovým číslem {*2, x+2, 2x+2*} *atd.* - přičemž x_1 značí posun o tolik pozic, kolik je pořadí v abecedě prvního písmena klíče, x_2 je posun o tolik pozic, kolik je pořadí druhého písmena klíče atd. Tedy $x_1, x_2, x_3...$ odpovídají parametrům jednoduchých posunů. Tento fakt je vysvětlen na následujícím příkladě:
třípísmenným klíčem *sen* je zašifrovaný text *diplomová práce* - výsledkem je řetězec *vmcds zgznh vnui*. Písmena otevřeného textu *d, l, o, p, c* jsou posunuta o stejný parametr (konkrétně o 18, což je pozice prvního písmena klíče - **s**). Dále písmena *i, o, v, r, e* jsou posunuta o 4 a zbylá písmena o 13 (k určení pozice může být nápomocná tabulka 2.6). Šifrový text se rozdělil do tří skupin (obecně do tolika, kolik znaků obsahuje klíč). Každá tato skupina je charakteristická konkrétním posunem - dá se na ní nahlížet jako na monoalfabetickou šifru s jednoduchým posunem (v podstatě je to varianta Ceasarovy šifry, pouze parametr posunu nemusí být roven třem). Postup luštění takové šifry byl přiblížen v kapitole 2.4.2. Tímto způsobem se vyluští každá skupina zvlášť, přičemž jsou zjištěna jednotlivá písmena hesla.
Výše popsaná metoda se nazývá *Kasiského metoda*. Je pojmenovaná podle pruského důstojníka Fridricha W. Kasiského, který ji zavedl již roku 1863. Za pomoci této metody luštění je možné prolomit text o délce 50 krát délka klíče (a to v případě, že je znám pouze šifrový text). Pokud kryptoanalytik zná zároveň i otevřený text, k určení klíče mu stačí text o délce dvou klíčů [9].

Průměrný index koincidence Pro zjištění velikosti klíče se dá také použít index koincidence (viz 2.3.1). Při použití polyalfabetické šifry se text rozpadá do několika skupin (tolika, kolik je délka klíče). Každá taková skupina má přibližně stejný index koincidence, jako je IC jazyka otevřeného textu (důvod je prostý - jedná se vlastně o monoalfabetickou šifru, jejíž IC odpovídá IC otevřeného textu). Aritmetický průměr všech IC jednotlivých skupin se tak právě blíží IC použitého jazyka. Zná-li útočník jazyk otevřeného textu, stačí vyzkoušet všechny pravděpodobné možnosti velikosti klíče a pro každou z nich spočítat průměry jednotlivých indexů koincidence. Klíč bude mít nejpravděpodobněji takovou délku, pro kterou se průměrný IC nejvíce blíží IC jazyka otevřeného textu [9].

Odhad indexu koincidence Variantně se však můžeme pokusit o hrubý odhad délky klíče za pomocí očekávané hodnoty IC:

$$E(IC) = \frac{1}{t} \cdot \frac{L-t}{L-1} \cdot \kappa_p + \frac{t-1}{t} \cdot \frac{L}{L-1} \cdot \kappa_r \tag{2.15}$$

kde L je délka šifrového textu, t je délka klíče, κ_p a κ_r hodnoty z tabulky 2.9. Pro jednotlivé periody (t = 1,2…20,…50..) dosazujeme do vzorce (2.15) a výsledek porovnáváme s hodnotou IC šifrového textu vypočítaného dle vzorce (2.3). Hodnota t, pro kterou se $E(IC)$ nejvíce blíží IC šifrového textu, přibližně odpovídá délce klíče.

2.4.4 Luštění jednoduché transpozice

V případě, že luštitel pomocí indexu koincidence a statistického rozložení znaků určí, že šifrový text byl vytvořen pomocí jednoduché transpozice, dalším krokem je odhadnutí rozměrů původní tabulky.

Šifra obvykle vypadá jako běžný text - řádky s mezerami, rozdělené na *slova* atd. Nejprve je třeba tento text zbavit mezer (šifrový text *OAOED VMCPP LRIA* - viz šifrování kapitola 2.2.2 - bude po úpravě vypadat *OAOEDVMCPPLRIA*). Následně se spočítají všechny znaky textu. Tento počet (v tomto případě 14) se rozloží na součin prvočísel, ze kterých se poté odhaduje rozměr šifrové tabulky. Číslo 14 lze rozložit pouze dvěmi možnostmi: 1x14 a 2x7. Více pravděpodobná se jeví být varianta 2x7, v prvním případě by délka permutačního klíče byla rovna jedné, a to je poměrně netypická varianta (tuto možnost sice nelze zcela vyloučit, ale s ohledem na pravděpodobnost se obvykle analyzuje až jako druhá v pořadí).

Pro lepší ilustraci ještě jeden příklad: šifrový text o délce 60 znaků se dá rozložit na prvočíselný součin: $60 = 2 \cdot 2 \cdot 3 \cdot 5$. V úvahu tedy připadají tabulky 1x60, 60x1, 2x30, 30x2, 3x20, 20x3, 4x15, 15x4, 5x12, 12x5, 6x10, 10x6, celkem 12 variant. Některé z nich se však dají rovnou vyloučit (nebo alespoň odsunout na pozdější testování pro případ, že by jiné varianty neuspěly) - a to 1x60, 2x30, 3x20, 4x15. Permutační klíč je totiž u těchto tabulek poměrně krátký a lze předpokládat, že autor šifrového textu použil delší, „bezpečnější“ klíč. Naopak varianty 60x1 a 30x2 jsou velmi netypické - první z nich by znamenala permutační klíč o stejné délce, jako je samotný otevřený text. Těmito úvahami lze vyloučit hned polovinu možných rozměrů tabulek.

Zachycený šifrový text se dále vepisuje po sloupcích do jednotlivých tabulek. Jako další pomůcka může sloužit jedna z vlastností jednoduché záměny - protože transpozice otevřeného textu dle permutačního klíče probíhá na úrovni řádků, měl by v nich zůstat zachován poměr samohlásek a souhlásek tak, jak je běžné v textu (pro český jazyk je to 40:60). Tabulka, která tento poměr splňuje nejlépe, je nejpravděpodobnější variantou. V následujícím kroku však nezbývá než zkoušet možnosti

přeházení sloupečků tak, aby z nich vznikl otevřený text - obvykle za pomocí pravidel frekvenční analýzy (bigramové a trigramové vazby atd.).

3 REALIZACE A POPIS APLIKACE

Pro účely softwarové podpory výuky kryptoanalýzy byla vytvořena aplikace a podpůrné webové stránky s teorií. Aplikace si neklade za cíl plně rozluštit zadané šifrové texty. Měla by spíše studentům umožnit pochopení podstaty luštění šifrových systémů a nabídnout jim potřebné pomůcky - tak, aby studenti sami luštění dokončili. Vzhledem k tomu, že většina dnešních šifrových systémů (včetně moderních) obsahuje ve svých základech monoalfabetickou šifru a jednoduchou transpozici (byť v pozměněné formě), byly právě tyto zvoleny pro navrhovaný software, a zároveň k nim pro svou názornost a dobrou algoritmizovatelnost přidána polyalfabetická šifra Vigénere. Tyto šifry jsou relativně srozumitelné a zřejmě nejsnáze demonstrovatelné, díky tomu lze lépe pochopit jejich podstatu.

3.1 Realizace

Následující oddíl se zabývá realizací software pro podporu výuky klasické kryptoanalýzy. S ohledem na požadavky zadání (interaktivita, názornost, grafické příp. webové rozhraní a lokálně - bez serveru - běžící aplikace) byla jako programovací jazyk zvolena Java. Jako vývojové prostředí bylo vybráno NetBeans, které umožňuje uživatelsky komfortní návrh grafických rozhraní. Zároveň pro podporu výuky byly vytvořeny webové stránky, obsahující základní poznatky klasických šifer, vytvořenou aplikaci a návod na její používání. Samotný program je určen pro dvě základní činnosti: šifrování otevřeného textu a luštění/dešifrování (resp. jeho podpora) šifrového textu.

3.1.1 Zdrojový kód

Zdrojový kód vytvořeného programu je okomentován pomocí tzv. Javadoc [14], což je nástroj pro vytváření API[1] dokumentace v HTML formátu. S ohledem na jeho rozsah je pouze součástí přiloženého CD.

GUI[2] bylo vytvářeno pomocí funkce návrháře v IDE[3] Netbeans. Skládá se z menu, pomocí kterého jsou voleny jednotlivé funkce, které program může vykonávat; dále ze dvou hlavních textových oken, několika pomocných tlačítek a informativních navěští. Toto grafické rozhraní je v projektu striktně odděleno od tříd obsahujících

[1] API = Application Programming Interface, označuje v informatice rozhraní pro programování aplikací.

[2] GUI = Graphical User Interface je uživatelské rozhraní, které umožňuje ovládat počítač pomocí interaktivních grafických ovládacích prvků.

[3] Integrated Development Environment = vývojové prostředí

jednotlivé šifrovací (a další) funkce - aby v případě úpravy těchto funkcí nedošlo k nechtěnému ovlivnění rozhraní. Díky této hierarchii je případně možno v budoucnu přidávat další šifrovací (či jiné) funkce, aniž by to znamenalo výraznější zásah do kódu.
V projektu byly vytvořeny jednotlivé balíky sdružující třídy, které k sobě logicky svým obsahem patří. Např. balík s názvem *sifry* obsahuje třídy pro jednotlivé typy šifer - konkrétně *JednoduchyPosun*, *VigenereAutoklic*, *AfinniSifra* atd. Všechny tyto šifry dědí ze společného předka *Sifra*.
Následuje stručná ukázka kódu, konkrétně jde o metodu pro vytvoření šifrové abecedy v případě (de)šifrování pomocí jednoduchého posunu (monoalfabetická šifra). Pomocí takto vytvořené abecedy se v jiné metodě může zadaný text zašifrovat (případně dešifrovat). Metoda na vstupu očekává pole s původní abecedou a zároveň parametr posunu, na výstupu pak vrací pole s nově vytvořenou abecedou.

```
public static char[] posunAbecedu(char[] abeceda, int posun) {
    if (posun < 0 || posun > abeceda.length) {
        throw (new IllegalArgumentException ("Maximalni posun je "
        + abeceda.length + ", " + "minimalni posun je 0 (zadano: "
        + posun + ")"));
    }

    char[] result = new char [abeceda.length];

    for (int i = 0; i < abeceda.length; i++) {
        result[i] = abeceda [(i + posun < abeceda.length) ?
        (i + posun) : (i + posun - abeceda.length)];
    }

    return result;

}
```

Značná pozornost byla při programování věnována ošetření vstupů. Program je schopný provádět zvolené operace nad textem tvořeným pouze mezinárodní abecedou - v případě jakýchkoliv uživatelských vstupů je kontroluje a případně upravuje na požadovaný formát.
Podrobnější popis jednotlivých tříd a metod obsahuje již zmíněný Javadoc.

3.1.2 HTML stránky

Vzhledem k tomu, že v dnešní době se zřejmě nejčastějším způsobem vyhledávání a čtení informací stalo prohlížení www stránek, teorie klasických šifer, popsaná v kapitole 1, byla zpracována právě do podoby html stránek. To umožňuje snadnou dostupnost poznatků - buď jejich zpřístupněním na lokálních discích počítačů, nebo přímo zveřejněním do sítě Internet.
Stránky jsou rozděleny na jednotlivé sekce, korespondující s teorií popisovanou v kapitole .
Ze zdrojového kódu aplikace byl vytvořen jar soubor, který agreguje více souborů (tříd) do jednoho (obvykle se používá pro distribuci java aplikací). Tento soubor je umístěný na jedné z webových stránek (ve formě spustitelné aplikace) včetně popisu jak ho používat. Zároveň jsou doplněny příklady luštění několika šifrových textů.
Webová prezentace je součástí přiloženého CD.

3.2 Popis aplikace

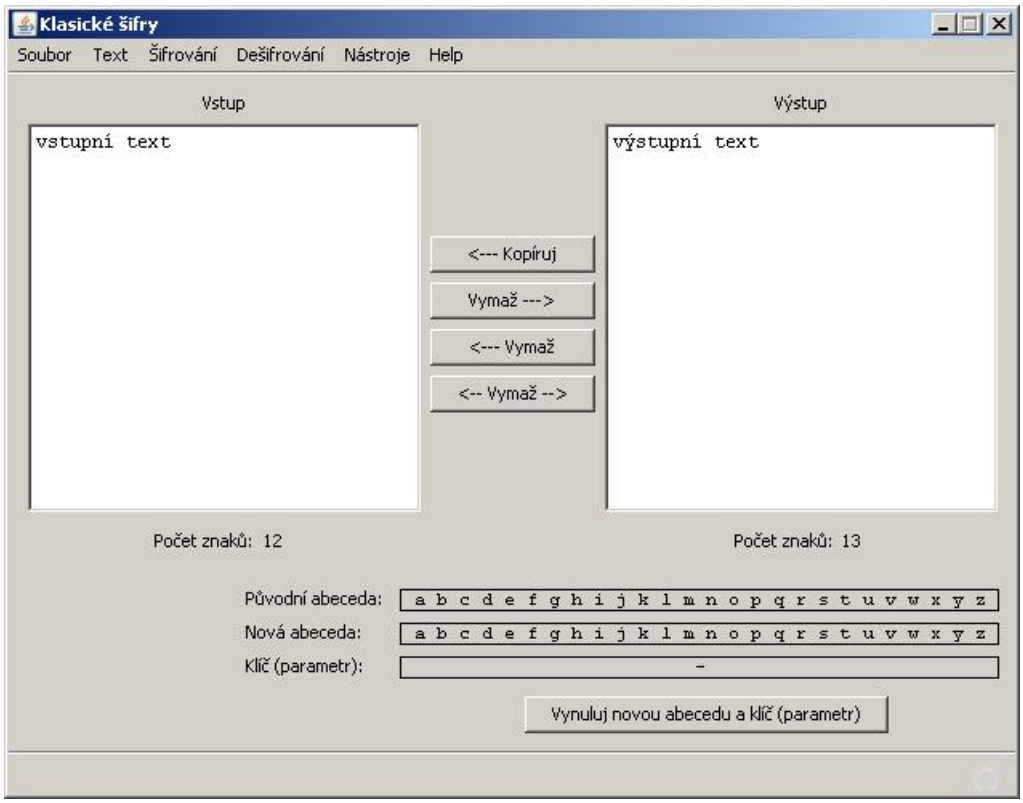
Hlavním účelem vytvořeného programu je (de)šifrovat zadané texty a poskytovat podpůrné funkce pro luštění (samotné luštění ale zůstává na uživateli programu). Program pracuje s textovými vstupy, nad kterými provádí vybrané operace. Konkrétně s šifrovým textem je to několik různých operací - například zobrazení jeho statistických vlastností (výpočet indexu koincidence, frekvenční analýza).
Pro jednotlivé šifry bylo nutno vytvořit příslušné funkce provádějící zašifrování/ dešifrování (včetně možnosti volby parametrů). Dále byly vytvořeny nástroje, pomocí nichž mohou studenti jednotlivé šifry luštit.
Program na vstupu očekává pouze český text. Šifrovat a dešifrovat lze text v jakémkoliv jazyce používajícím mezinárodní abecedu, nicméně některé statistické funkce (frekvenční analýza) jsou uzpůsobeny českému jazyku (četnost rozložení hlásek atd.).

3.2.1 Vstupy a výstupy

Software pracuje s textovými vstupy a výstupy. Vstupem (ať už jde o otevřený nebo šifrový text) může být textový soubor, který se dá otevřít pomocí menu *Soubor* → *Otevřít*. Textový vstup se dá mimo to také přímo zapsat/vložit do pracovního okna. Vzhledem k tomu, že program má být výukový, tj. má sloužit hlavně k demonstraci kryptoanalýzy/kryptografie, parametry jednotlivých šifrových systémů jsou vždy omezeny - např. délka hesla pro šifru Vigénere je max. 30 znaků.

3.2.2 Hlavní panel

Po spuštění aplikace dojde k zobrazení hlavního okna, které znázorňuje obrázek 3.1. Obsahuje dvě textové oblasti, menu a návěstí s informacemi. Následuje popis a funkce jednotlivých prvků menu.



Obr. 3.1: Hlavní okno aplikace

Soubor

Menu Soubor obsahuje položky Otevřít, Uložit a Konec.

- **Otevřít** - pomocí této položky lze do textové oblasti *Vstup* načíst libovolný soubor umístěný na disku. Jednotlivé šifrovací funkce programu pracují pouze se znaky mezinárodní abecedy, tzn. má smysl pracovat pouze s textovými soubory (*.txt) - filtr po otevření toho menu je nastaven na zobrazení adresářů a textových souborů.
- **Uložit** - umožňuje uložit obsah textových oblastí (v závislosti na poloze kurzoru) do souboru na disk.
- **Konec** - ukončí program.

Text

Menu Text obsahuje položky Editace, Kopírovat, Vložit, Vybrat vše a Smazat.

- **Editace** - jednotlivé šifrovací a statistické funkce programu pracují pouze se základní mezinárodní abecedou (26 znaků). V případě, že uživatel na vstup zadá text obsahující jiné znaky (např. diakritika, číslice, interpunkce atd.), program při volání funkcí nad tímto textem vždy ohlásí nutnou úpravu, bez které nepovolí další pokračování. V případě, že uživatel úpravu odsouhlasí, program projde vstupní text pomocí metody s názvem

  `editujText()`

  a upraví ho na mezinárodní abecedu (pouze malá písmena, včetně odstranění mezer). Vynucená úprava textu následuje po každé změně v textové okně *Vstup*, lze ji však volat ručně právě pomocí tohoto menu.

- **Kopírovat, Vložit, Vybrat vše, Smazat** - provede příslušnou akci s obsahem textového okna, ve kterém je umístěný kurzor.

Šifrování

Menu Šifrování umožňuje zašifrovat vstupní otevřený text. Zahrnuje jednotlivé typy šifer: monoalfabetická substituce, polyalfabetická substituce a jednoduchá transpozice; u většiny z nich uživatel zadává na vstupu parametry šifrového systému.

- **Monoalfabetická šifra** - zadaný text (v textové oblasti *Vstup*) lze zašifrovat jednou z těchto možností (detailněji popisovaných v kapitole 2.1): posun o zadaný parametr, afinní šifra, použití klíče, náhodně vygenerovaná abeceda a abeceda zadaná uživatelem. Stručný komentář zdrojového kódu jednotlivých šifrovacích funkcí je obsahem Javadocu.

- **Polyalfabetická šifra** - zadaný text (v textové oblasti *Vstup*) lze zašifrovat jednou z těchto možností (detailněji popisovaných v kapitole 2.2.1): Vigénere nebo Vigénere autoklíč.

- **Jednoduchá transpozice** - vstupní text (v oblasti *Vstup*) lze zašifrovat pomocí zadání klíče. Šifrový systém je jednoduchá transpozice s úplnou tabulkou, to znamená že v případě chybějících písmen v otevřeném textu jsou nahrazeny znaky **x**.

Výstup jednotlivých šifrovacích transformací je vložen do textového okna *Výstup* a je ho možno uložit do souboru. Šifrový text je ještě předtím upraven do tzv. telegrafické konvence - rozdělen po pěticích. Zároveň se po zašifrování textu nastaví v informačním panelu nově vytvořená abeceda šifrového systému.

Dešifrování

Menu Dešifrování téměř kopíruje menu Šifrování. V případě, že se uživateli podaří zjistit pro zadaný šifrový text typ a parametry použitého šifrovacího systému, pomocí tohoto menu si může ověřit jejich správnost. Jednotlivé metody provedou nad vstupním textem operace inverzní k šifrování (jednou výjimkou je afinní šifra, u které se nezadávají původní parametry a,b, ale a^{-1},b.

Nástroje

Pro luštění šifer je zapotřebí používat různé výpočty nebo statistické funkce, které jsou shrnuty v menu Nástroje.

- **Index koincidence** - tato statistická funkce je detailně popisována v kapitole 2.3.1. Po zavolání funkce IC program zobrazí nové okno s vypočítaným indexem koincidence. Pomocí něj se uživatel může rozhodnout, jakým typem šifry je text šifrován. Průměr IC subtextů slouží pro určení délky hesla v případě šifry Vigénere (viz kapitola 2.4.3). Funkce E(IC) je popisována rovněž v kapitole 2.4.3.

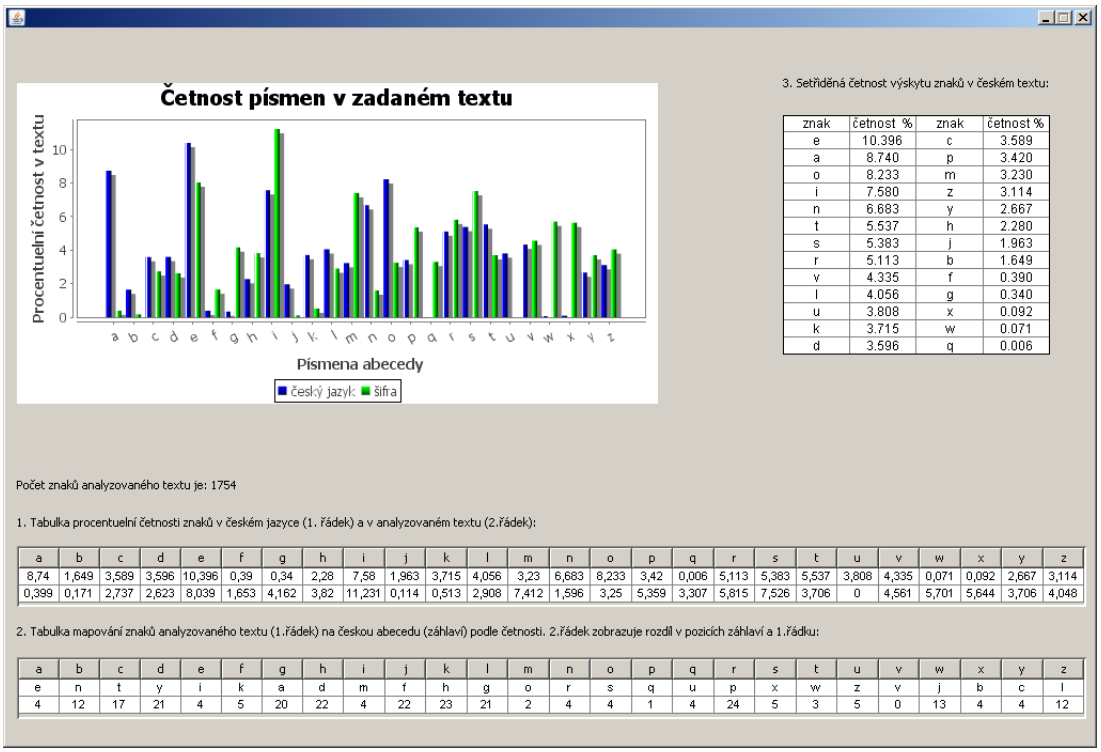
- **Euklides** - toto menu je používáno v případě luštění afinní šifry. Obsahuje dvě funkce - NSD (zjištění největšího společného dělitele dvou čísel (funguje na základě Euklidova algoritmu) a dále rozšířený Euklidův algoritmus, pomocí kterého je možno určit multiplikativní inverzi čísla. NSD je možno mj. využít při zjišťování délky hesla u šifry Vigénere.

- **Výměna znaků** - v případě luštění monoalfabetické substituce se může uživatel pokoušet zaměnit za sebe dva znaky šifrové a otevřené abecedy, k čemuž slouží menu „Výměna jednoho znaku“. Pokud zná luštitel již celou šifrovou abecedu (resp. její mapování na otevřenou), může pro dešifrovní textu použít položku menu „Výměna všech znaků“.

- **N-tice** - položky v tomto menu slouží pro vyhledání n-tic (dvojic až desetic) v analyzovaném textu a zároveň určení vzdálenosti shodných n-tic. Využívá se při určování délky hesla u šifry Vigénere.

- **Frekvenční analýza** - velmi důležitá položka (viz obrázek 3.2). Po vyvolání této nabídky dojde k otevření nového okna, které obsahuje některé statistické údaje o zadaném textu. Jedná se o soupcový graf zobrazující četnosti písmen v české abecedě (**modré sloupce**) a zároveň četnost písmen (procentuelní) v analyzovaném textu (zelené sloupce). Dále okno zobrazuje několik tabulek:

- tabulka obsahující četnost znaků v českém jazyce, setříděných sestupně podle výskytu
- tabulka obsahující četnost znaků v českém jazyce a zároveň četnost znaků v analyzovaném textu (v podstatě se jedná o data, kterými je naplněný graf)
- tabulka mapující znaky upraveného šifrového textu na znaky mezinárodní abecedy podle výskytu četnosti. Tato tabulka zároveň obsahuje údaj o posunutí jednotlivých znaků vůči sobě. Je použitelná při luštění jednoduchého posunu.



Obr. 3.2: Frekvenční analýza

- **Rozklad na prvočísla** - vrací prvočíselný rozklad zadaného čísla.
- **Převod do tabulky** - v případě, že uživatel chce luštit zadaný šifrový text jako jednoduchou transpozici, je potřeba převést ho do podoby tabulky. Po vyvolání této nabídky dojde k převodu textu v okně *Vstup* do tabulky o rozměrech zadaných uživatelem. Tabulka je zobrazena v novém okně; lze v ní vzájemně zaměňovat sloupce a řádky a tím postupně šifrový text luštit (na vstupu je očekávána šifra typu jednoduchá transpozice s úplnou tabulkou).
- **Vytvoření subtextu** - znamená, že aplikace z textu v okně *Vstup* vytvoří menší skupinu, a to na základě uživatelem zadaných parametrů. Těmi jsou

vzdálenost jednotlivých písmen v původním textu a dále odsazení (tzn. na které pozici leží první vybíraný znak).

- **Informace** - toto menu umožňuje zobrazit některé pomocné informace o českém jazyce: jedná se o tabulku výskytu nejčetnější bi- a trigramů a dále tabulku zobrazující index písmen v české abecedě.

Help

Menu Help obsahuje stručné info k ovládání programu (nikoliv teorii, která je zpracovaná formou webových stránek)

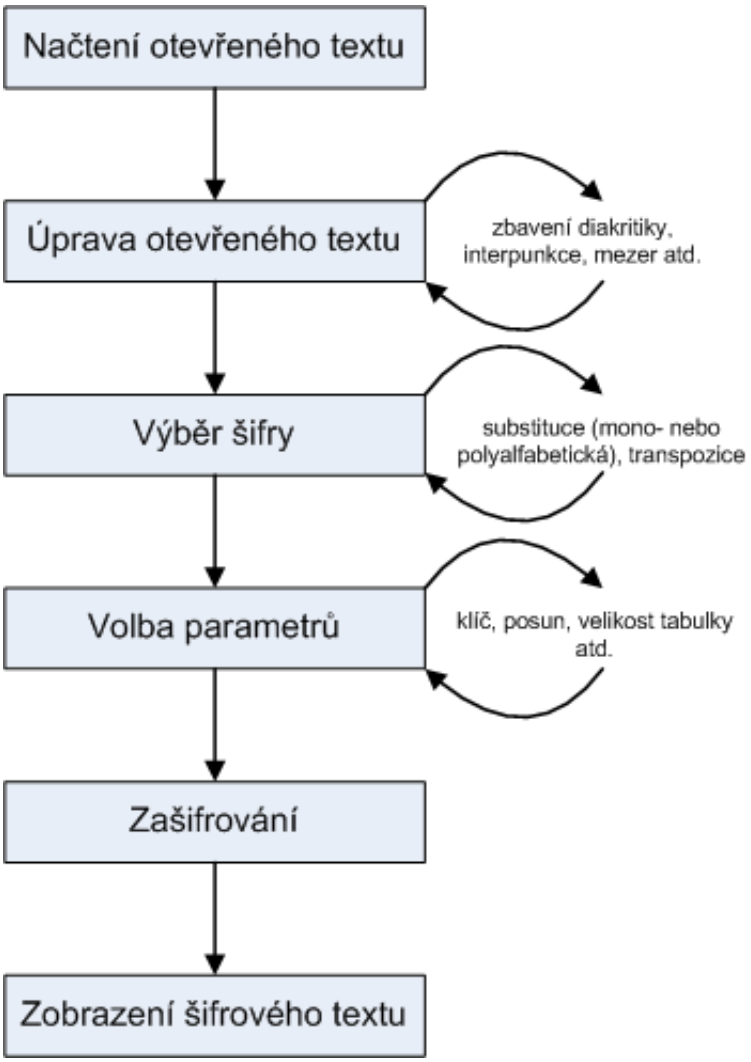
3.3 Šifrování pomocí vytvořené aplikace

Postup používání aplikace při zašifrování je jednoduchý, znázorňuje ho obrázek 3.3. Uživatel zadá do textového okna *Vstup* otevřený text (buď přímým zapsáním, nebo načtením ze souboru (viz 3.2.2). V menu Šifrování zvolí jednu z možných šifer, zadá potřebné parametry. Aplikace zkontroluje, zda text obsahuje nepovolené znaky (jiné, než základní mezinárodní abecedy) a v případě že ano, odstraní je. Výsledek šifrování se zobrazí v textovém okně *Výstup* a zároveň se (v případě, že to je možné), zobrazí v informačních návěštích hlavního panelu nová abeceda a parametry šifrového systému. Výsledek je opět možno uložit do souboru.

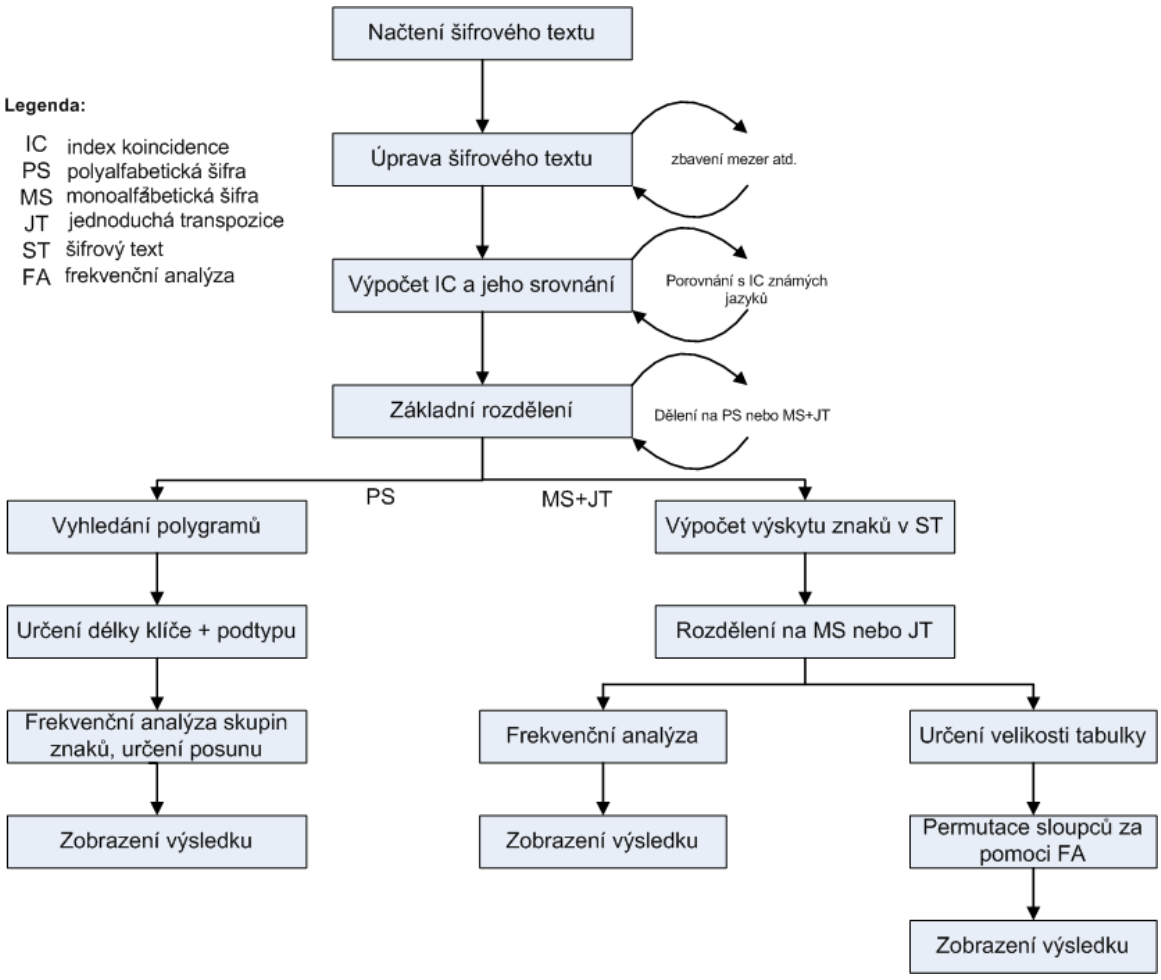
3.4 Luštění pomocí vytvořené aplikace

Následující kapitola popisuje postup luštění zadané klasické šifry pomocí vytvořené aplikace. Konkrétní příklady luštění jednotlivých typů šifer jsou zobrazeny v přílohách **A** a **B**.
Návrh postupu při luštění je znázorněn na obrázku 3.4. Pro úspěšné luštění (případně dešifrování) pomocí vytvořené aplikace by zadaná klasická šifra měla splňovat několik předpokladů (které však nezaručí skutečné vyluštění). Tyto předpoklady není nutné uvažovat v případě, že šifra byla vytvořena taktéž touto aplikací:

- Otevřený text byl zašifrován jedním z těchto druhů šifrových systémů: monoalfabetická substituce, polyalfabetická substituce nebo jednoduchá transpozice.
- klíč v případě monoalfabetické substituce (varianta *klíč*) je dlouhý 1 - 26 znaků.



Obr. 3.3: Šifrování pomocí softwaru



Obr. 3.4: Luštění pomocí softwaru

- V případě polyalfabetické substituce se jedná o systém Vigénere (s klíčem o délce 1 - 30 znaků) případně Vigénere varianta autoklíč, kde autoklíč je jeden znak mezinárodní abecedy.
- v případě jednoduché transpozice se jedná o variantu s úplnou tabulkou
- pro jednoznačné rozluštění by měl mít otevřený text alespoň 200 znaků

3.4.1 Analýza

Luštění šifry probíhá podle diagramu, který je zobrazen na obrázku č.3.4. Jako první je třeba vypočítat *index koincidence* (2.3.1). Lze ho zobrazit pomocí menu *Nástroje → Index koincidence (IC)*. Pomocí toto nástroje lze rozlišit, zda se jedná o šifru Vigénere, nebo jednu z možností monoalfabetická šifra a jednoduchá transpozice.
Pro rozlišení mezi jednoduchou transpozicí a monoalfabetickou šifrou je možno použít frekvenční analýzu - menu *Nástroje → Frekvenční analýza (FA)*. Pomocí zobrazeného grafu lze obvykle rozlišit mezi substitucí a transpozicí prakticky na první pohled - pokud barevné sloupce pro jednotlivé znaky spolu víceméně korespondují (tzn. četnost stejných písmen si odpovídá), jedná se o jednoduchou transpozici, v případě výraznější odlišnosti se jedná o substituci. Rozhodnutí, o kterou šifru se jedná, je pouze na uživateli.
Po provedení těchto kroků by měl být luštitel schopen odhadnout typ použitého šifrového systému, následujícím krokem je zjištění parametrů šifrového systému.

3.4.2 Parametry šifrového systému

Monoalfabetická substituce

V případě této šifry byl otevřený text zašifrován jednou z pěti možných variant: jednoduchý posun, afinní šifra, zadání klíče, zadání abecedy nebo náhodně vygenerovaná abeceda. Úkolem luštitele je určit šifrovou abecedu, použitou na zašifrování otevřeného textu.

- **jednoduchý posun** - jedná se zřejmě o nejsnáze luštitelnou variantu této šifry. Funkce menu *Nástroje → Frekvenční analýza (FA)* zobrazí nejen graf frekvenční analýzy, ale současně se ve spodní tabulce pokouší mapovat písmena šifrového textu dle četnosti na písmena základní abecedy. Současně zobrazuje rozdíl indexu (pořadí v abecedě) těchto znaků. Rozdíl indexu může být hledaným parametrem - obvykle to bývá rozdíl, který je stejný pro nejvíce písmen. Není to však podmínkou a někdy může být řešení touto metodou nejednoznačné. Je potřeba k němu přidat pravidla frekvenční analýzy (viz 2.3.2).

Obrázek č. 3.5 zobrazuje obsah tabulky pro text zašifrovaný posunem s parametrem 4. Je zřejmé, že vzájemný posun indexů o 4 se zobrazuje celkem u osmi mapování - což je poměrně vysoké číslo, na jehož základě se dá usuzovat právě na parametr 4.

2. Tabulka mapování znaků analyzovaného textu (1.řádek) na českou abecedu (záhlaví) podle četnosti. 2.řádek zobrazuje rozdíl v pozicích záhlaví a 1.řádku:

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
e	n	t	y	i	k	a	d	m	f	h	g	o	r	s	q	u	p	x	w	z	v	j	b	c	l
4	12	17	21	4	5	20	22	4	22	23	21	2	4	4	1	4	24	5	3	5	0	13	4	4	12

Obr. 3.5: Tabulka mapování znaků šifrového textu

- **afinní šifra** - zjištění parametrů tohoto systému není zcela triviální. Pomocí funkce menu *Nástroje → Frekvenční analýza (FA)* je třeba pokusit se namapovat dle četnosti alespoň dva znaky šifrového textu na základní abecedu. Nejsnáze se mapují znaky s nejčastějším a nebo naopak nejméně častým výskytem - jedná se o znaky *e, a, o* nebo *x, w, q*. Samozřejmě je možno určit překlad znaků i za pomocí jiných metod (např. pravidla frekvenční analýzy, viz 2.3.2) - základním předpokladem úspěchu vyluštění afinní šifry je ale správné určení mapování alespoň dvou znaků. Tyto znaky se potom použijí pro výpočet parametrů systému pomocí Euklidova algoritmu (viz 2.4.2), viz menu *Nástroje → Euklidův algoritmus*.
- **klíč, náhodná abeceda a zadání abecedy** jsou z pohledu luštitele totožné varianty - šifrová abeceda nebyla vytvořena systematicky, ale v podstatě náhodně. Jde o obtížnější systémy, luštitelné pouze pomocí pravidel frekvenční analýzy viz 2.3.2. Tato pravidla jsou mj. popsaná na vytvořených webových stránkách v sekci frekvenční analýza. Nejčastější bigramy a trigramy českého jazyka jsou zároveň zobrazitelné v menu *Nástroje → České dvojice + trojice*. Četnost znaků v české abecedě je zobrazena v tabulce v menu *Nástroje → Frekvenční analýza (FA)* (viz obrázek 3.2). Pro zkoušení záměn jednotlivých písmen bylo vytvořeno menu *Nástroje → Výměna jednoho znaku*, kdy se vzájemně vyměněné znaky pro přehlednost obarví červeně.

V případě určení šifrové abecedy systému lze správnost ověřit pomocí funkce menu *Dešifrování → Monoalfabetická šifra*, kde lze zadat parametry systému (pro posun, afinní šifru nebo klíč), případně je možno využít menu *Nástroje → Výměna všech znaků*, a to v případě znalosti šifrové abecedy.

Polyalfabetická substituce

V případě luštění šifry Vigénere je zapotřebí určit jediný parametr systému, a tím je heslo.

- **délka klíče**: u varianty Vigénere s periodickým heslem je prvním krokem zjištění délky klíče. Aplikace nabízí tři možnosti, pomocí kterých lze určit délku klíče:
  - E(IC) - funkce menu *Nástroje → Index koincidence (IC) → E(IC)* umožňuje vypočítat odhadovaný index koincidence na základě vzorce 2.15. Jeho porovnáním s indexem šifrového textu je možno zjistit přibližnou délku hesla (více viz kapitola 2.4.3).
  - odhad délky klíče pomocí průměru indexů koincidence sub-textu, který vznikne výběrem znaků původního textu (více viz kapitola 2.4.3) pomocí menu *Nástroje → Index koincidence (IC) → Průměr IC subtextů.*
  - Zřejmě nejspolehlivější metodou pro určení délky hesla je pomocí vzdálenosti opakujících se n-tic v analyzovaném textu. Pro zobrazení opakujících se dvojic až desetic písmen slouží tabulka v menu *Nástroje → N-tice → Vyhledání n-tic v textu.* Zároveň je možno zobrazit vzdálenost těchto opakujících se n-tic pomocí menu *Nástroje → N-tice → Hledej vzdálenoti n-tic.*
- **určení klíče**: jakmile luštitel zná délku použitého hesla, snaží se zjistit jeho podobu. Pomocí menu *Nástroje → Vytvoření subtextu* lze analyzovaný text rozpadnout na tolik skupin, kolik je znaků v textu - jednotlivé sub-texty jsou zašifrované stejným písmenem klíče. Díky tomu se problém redukuje na vyluštění zašifrování sub-textu jednoduchým posunem, který byl popsán v kapitole 2.4.3.
- varianta **autoklíč** není luštitelná jiným způsobem, než zkoušením jednotlivých možností autoklíče (tedy písmena a-z) pomocí menu *Dešifrování → Polyalfabetická šifra → Vigénere autoklíč.*

Jednoduchá transpozice

Pro luštění této šifry byla připravena funkce menu *Nástroje → Převod do tabulky.* Pomocí ní lze převést analyzovaný text z textového okna *Vstup* do tabulky o rozměrech, které uživatel zadá na vstupu (resp. zadává počet sloupců, počet řádků se dopočítá automaticky podle délky šifrového textu). Úkolem luštitele je odhadnout správně rozměry tabulky (viz kapitola 2.4.4) - pro tento odhad lze mj. využít funkci *Nástroje → Rozklad na prvočísla.*
V zobrazené tabulce lze vzájemně vyměňovat řádky a sloupce pomocí příslušných tlačítek, sloupce lze měnit i pomocí přetahování myší mezi sebou (v tom případě zůstává zachované pořadí záhlaví sloupců). Tato možnost je více doporučovaná,

protože díky záhlaví je vidět výsledné pořadí klíče. K přímému luštění je zapotřebí využít poznatků frekvenční analýzy (výskyt bigramů, trigramů atd.). Obsah tabulky lze zpětně nechat pomocí příslušného tlačítka vypsat do textového okna *Výstup* hlavního panelu.

3.5 Testování aplikace

V průběhu vytváření aplikace byla tato pravidelně testována se zaměřením na přehlednost a dále správnost výsledků při používání jednotlivých funkcí. Všechny nástroje, které aplikace nabízí, jsou plně funkční a při zadání korektních vstupů (což je ošetřeno přímo v aplikaci) vrací správné výsledky. Aplikace byla dále po vytvoření poskytnuta na testování několika studentům, kteří neprojevili vážnější výhrady.

3.6 Používání aplikace

Představa využití programu a webových stránek je následující:

- vyučující odprezentuje studentům látku týkající se klasické kryptografie/ kryptoanalýzy
- tato teorie bude k dispozici na připravených webových stránkách
- vyučující vybere otevřený text (článek atd.) a pomocí vytvořené aplikace jej zašifruje; výsledek uloží do textového souboru, který dá k dispozici studentům
- studenti budou mít za úkol pomocí teoretických poznatků zadaný text vyluštit, k čemuž budou používat program a zároveň v případě potřeby webové stránky
- výsledek si opět uloží do souboru a odevzdají vyučujícímu

4 ZÁVĚR

Jak bylo naznačováno již v úvodu, cílem této práce bylo prostudovat a stručně vysvětlit problematiku kryptoanalýzy vybraných klasických šifer a dále vytvořit podpůrnou aplikaci pro výuku klasické kryptoanalýzy. Za tímto účelem bylo vybráno několik základních druhů šifer - monoalfabetická substituce, polyalfabetická substituce a jednoduchá transpozice. Pro každou z nich je hlouběji zpracována teorie, zahrnující popis šifrového systému, jeho parametry a možnosti luštění. Jednotlivé šifry jsou demonstrovány na krátkých příkladech; v příloze práce jsou potom uvedeny dva příklady detailního luštění polyalfabetické a afinní šifry. Pozornost je zaměřena také na metody často vyžívané při samotném luštění - index koincidence a frekvenční analýza, a to včetně stručného matematického základu.

Poznatky z teorie šifrování a luštění, včetně příkladů, byly zpracovány do podoby webových stránek. Tyto stránky zajišťují jednoduchý přístup k informacím a díky své struktuře se zároveň dají v budoucnu snadno modifikovat (např. v případě doplnění nových druhů šifer).

Teorie kryptoanalýzy je velmi široká, k jejímu snadnějšímu zpřístupnění studentům dále byla vytvořena aplikace Klasické šifry. Tento software splňuje požadovaná kritéria - nepotřebuje pro svůj běh server a zároveň je součástí webových stránek. Funkce programu jsou detailněji popsány a je vysvětleno, jak se dají použít např. pro jednotlivé fáze luštění šifer. Pomocí tohoto programu si uživatelé (studenti) mohou teoretické poznatky ověřit v praxi. Naprogramovaná aplikace byla otestovaná na všech teoreticky popisovaných typech šifer, a to jako při jejich šifrování, tak luštění. Bylo ověřeno, že v kombinaci s webovými stránkami je dobře použitelná pro (de)šifrování a luštění popsaných klasických šifer. Aplikace je zároveň vytvořená strukturovaně tak, aby se v budoucnu dala případně doplnit o šifrování/luštění dalších druhů šifer, jako např. varianty šifry Vigénere nebo transpoziční šifry.

Vytvořený software by mohl být v budoucnu použit při výuce klasické kryptoanalýzy, např. jako jedna z laboratorních úloh - studenti dostanou k dispozici několik šifrových textů a za pomocí aplikace a webových stránek je budou luštit.

Při vytváření konceptu softwarové podpory výuky byl kladen důraz na přehlednost a strukturu - v budoucnu by toto zpracované téma mohlo být součástí většího edukativního celku, který by dále zahrnoval např. steganografii.

LITERATURA

[1] VONDRUŠKA, P. *Kryptologie, šifrování a tajná písma.* 1.vydání. Praha: Albatros nakladatelství, a.s., 2006. Edice OKO. ISBN 80-00-01888-8

[2] Singh, S. *Kniha kódů a šifer: utajování od starého Egypta po kvantovou kryptografii.* 2.vydání. Praha: Dokořán; Argo, 2009. Edice Aliter; sv.9. ISBN 978-80-7363-268-7

[3] ZELENKA, J., ČAPEK, J., FRANCEK, J., JANÁKOVÁ, H. *Ochrana dat: kryptologie.* 1.vydání. Hradec Králové: GAUDEAMUS, 2003. ISBN 80-7041-737-4

[4] *Index of coincidence - Wikipedia, the free encyclopedia* [online]. 2009, poslední aktualizace 10.12.2009 10:49. [cit. 1. 12. 2009]. Dostupné z URL: <http://en.wikipedia.org/wiki/Index_of_coincidence>.

[5] *Statistické charakteristiky češtiny - Centrum NLP* [online]. [cit. 12. 5. 2010]. Dostupné z URL: <http://nlp.fi.muni.cz/cs/stat_cestiny>.

[6] *Frekvence písmen, bigramů, trigramů, délka slov - Centrum NLP* [online]. [cit. 12. 5. 2010]. Dostupné z URL: <http://nlp.fi.muni.cz/cs/Frekvence_pismen_bigramu_trigramu_delka_slov>.

[7] TŮMA, J. *Kapitola 1: základní pojmy* [online]. [cit. 12. 5. 2010]. Dostupné z URL: <http://www.karlin.mff.cuni.cz/t̃uma/nciphers/nciphers1.pdf>.

[8] TŮMA, J. *Kapitola 2: jednoduchá záměna* [online]. [cit. 1. 12. 2009]. Dostupné z URL: <http://www.karlin.mff.cuni.cz/t̃uma/nciphers/nciphers2.pdf>.

[9] TŮMA, J. *Kapitola 3: periodický klíč* [online]. [cit. 12. 5. 2010]. Dostupné z URL: <http://www.karlin.mff.cuni.cz/t̃uma/nciphers/nciphers3.pdf>.

[10] *Dr. Tomáš Rosa - Kryptologie pro praxi* [online]. poslední aktualizace 2.11.2009. [cit. 12. 5. 2010]. Dostupné z URL: <http://crypto.hyperlink.cz/cryptoprax.htm>.

[11] *Ing. Tomáš Vaněk - Monoalfabetické substituční šifry* [online]. [cit. 12. 5. 2010]. Dostupné z URL: <http://www.comtel.cz/files/download.php?id=4091>.

[12] *Modular multiplicative inverse - Wikipedia, the free encyclopedia* [online]. 2009, poslední aktualizace 7.5.2010 10:49. [cit. 12. 5. 2010]. Dostupné z URL:<http://en.wikipedia.org/wiki/Modular_multiplicative_inverse>.

[13] *Pavel Mička - Euklidův algoritmus - Algoritmy.net* [online]. [cit. 12. 5. 2010]. Dostupné z URL: <http://www.algoritmy.net/article/44/Eukliduv-algoritmus>.

[14] *Javadoc Tool Home Page* [online]. [cit. 12. 5. 2010]. Dostupné z URL: <http://java.sun.com/j2se/javadoc/>.

[15] Menezes, Alfred J., van Oorschot, Paul C., Vanstone, Scott A. *Handbook of Applied Cryptography* 2.vydání. Boca Raton: CRC Press, 1997. ISBN 0-8493-8523-7

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

IC index koincidence

OT otevřený text

ST šifrový text

MS monoalfabetická šifra

PS polyalfabetická šifra

JT jednoduchá transpozice

HTML Hyper - Text Markup Language

API Application Programming Interface

GUI Graphical User Interface

IDE Integrated Development Environment

SEZNAM PŘÍLOH

A LUŠTĚNÍ POLYALFABETICKÉ ŠIFRY

Následující příklad představuje luštění konkrétního textu zašifrovaného polyalfabetickou šifrou s využitím vytvořeného programu. Zašifrovaný text je:

```
cstoc imkei kifpj hpcjp fpsvf ftlzz vkany hecew cmllb lnwya ldags
sqgns tmhcw ysrpb lvgkg hldlo wvgmw oedlb hqfzv hyjzj umusd ymryo
tcusn ueejq oskzp uskes jlbly fqtjz uehcw rpsoo iidvh lvqaf hgggo
szkac qifjq owllh lgzgs wvgdd lgzdc cildy llgdj hdmlb lfgpq vlfkw
gvspz lolpf ftjlq vzswg zcjtw cnwsc wvgdd lgzaf hgggo sseyc osfpn
ueejq owhzz btjlq vzfty bdhco csvlx zoqnv zpmks iyktz vzfpd vgwws
giepy vydtc trgsm jlkpr vdntr hqwus uhavm uevpq oykpb geuyc zxazy
vpfzg am
```

A.1 Index koincidence

Za pomoci menu Nástroje → Index koincidence → Index koincidence (IC) luštitel zjistí, že IC šifrového textu má hodnotu 0,0428. Tato hodnota je výrazně odlišná od IC českého jazyka, a ukazuje na polyalfabetickou šifru.

A.2 Určení délky klíče

Pro určení délky klíče byla vybrána metoda vzdálenosti n-tic v šifrovém textu. Pomocí menu Nástroje → N-tice → Vyhledání n-tic v textu je zobrazena tabulka n-tic. Pro luštitele jsou zajímavé ty nejdelší z nich, které se opakují alespoň dvakrát. Není třeba vybírat všechny n-tice, je vybráno v podstatě náhodně 6 z nich:

```
{afhgggos, nueejqo, wvgddlg, jlqvz, fft, cw}
```

Všechny vybrané n-tice se v textu vyskytují 2x, vyjma poslední která je v textu 3x. Pomocí menu Nástroje → N-tice → Hledej vzdálenosti n-tic je třeba zobrazit vzdálenosti jednotlivých n-tic, výsledkem je množina čísel:
{100, 160, 65, 55, 205, 80, 106}. Zjistíme největšího společného dělitele těchto vzdáleností (menu Nástroje → Euklides → nsd(a, b), kterým je číslo 5 (neodpovídá pouze poslední vybraná vzdálenost, která zřejmě vznikla náhodně). Délku klíče je možno ověřit přes Nástroje → Index koincidence → Průměr IC subtextů. Pro klíč o délce 5 vychází 0,0548, což je velmi blízké hodnotě IC českého jazyka (na rozdíl např. od délky 6, pro kterou je tento průměr 0,042).

A.3 Klíč

Klíč je možno určit pomocí rozpadu šifrového textu na 5 skupin (délka klíče). První skupinu luštitel získá pomocí menu Nástroje → Vytvoření subtextu zadáním vzdálenosti znaků 5 a odsazení 0. Výsledkem je

```
cikhffvhcllstylhwohhuytuoujfurilhsqolwlclhlvglfvzcwlhsouobvbczz
ivvgvtjvhuuogzva
```

Tato skupina znaků byla celá zašifrována jako jednoduchý posun - stačí určit parametr posunu. Zobrazíme frekvenční analýzu tohoto textu (menu Nástroje → Frekvenční analýza), konkrétně nás zajímá 3. tabulka: nejčastěji se vykytuje posun o

Tabulka mapování znaků analyzovaného textu (1.řádek) na českou abecedu (záhlaví) podle četnosti. 2.řádek zobrazuje rozdíl v pozicích záhlaví a 1.řádku:

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

Obr. A.1: Tabulka mapování znaků šifrového textu - první skupina

parametr 7, odpovídající písmenu **h** (viz obrázek A.1).
Obdobným způsobem pokračujeme u zbylých 4 znaků, např. třetí v pořadí: nejčastěji

Tabulka mapování znaků analyzovaného textu (1.řádek) na českou abecedu (záhlaví) podle četnosti. 2.řádek zobrazuje rozdíl v pozicích záhlaví a 1.řádku:

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
f	b	v	u	g	y	x	c	l	n	z	d	r	w	k	t	i	h	j	s	a	e	o	p	m	q
5	0	19	17	2	19	17	21	3	4	15	18	5	9	22	4	18	16	17	25	6	9	18	18	14	17

Obr. A.2: Tabulka mapování znaků šifrového textu - druhá skupina

se vyskytuje posun o parametr 18, odpovídající písmenu **s** (viz obrázek A.2).
Výsledkem je klíč „**heslo**“.

B LUŠTĚNÍ AFINNÍ ŠIFRY

Následující příklad představuje luštění konkrétního textu zašifrovaného afinní šifrou s využitím vytvořeného programu. Zašifrovaný text je:

```
cxgzj yzmxf zmhie hgohr yambk xgzco zuzeb ybczq zqxvr iamzf ymxnz ybozq
fhrfx qxfyx fkpvi gmbkh yoxvf ybkzv upamz gamko xvxym zoxoj pvzcx obkfy
xkxyc zjbmz ahjrg obamx jcbgi qxfyx kpffx jmzko xycbj ozuha mhucz vpfzf
mgnzv amxcx fkzcj bibyz ivriz faxfz rfjhg xyijr fzoph guhmo xjkbv obhab
jvriz ghahm rnxyq bjzgb kjpoz uhqbj zyzva hqzam hkbfq zfyzr ohfoz oziba
hvxoz qyzob yhizi uzebo xvrfx yzvxy amzgz kfxvm bghfy boxjh cxahn xyizk
ozquc xifxn evxor ybner vmzyz qbjoz vrizy zahab gohry gzney mzoxo jhkzg
bkjpm hiehg ozozf vxvzr fazne byrah ihmor qzjhm uzcvz ixqze hghah mrnzo
xabym xxyhi zfzam xymzo xojrv rfxvp fczyo bfazn xsxjb jbigz ehuzi nzjcx
gozfz amxyh vvriz fybyi zambk zkbfh mlbox fvrfb oxozu rgzam huzeb oxkeh
gozri arfhu zoamh yhizo bamxj cbgym axyzf oxizo hrxvr oxyhr igmbk xkbfa
mhfyz obymb yamxf yzrio zarfy xozuz iaznx ahfjh izoxj chrur qzbfx ozqnb
fyzqf xhubk bjyzm buzeb oxgha mhkbi xinbf yxqzy hambk gbinb fyxvp yrfam
bkgby hupkb ymzub amxab gznej gpfxn chkzj fobgk behrk zfymz goxne czyzn
ejhra xkymi oxnxo zuhfr azmvb mjzyr yzoxf jpiba bmfyh kzjbm hiehg ozfza
mzjho byfkr qhfhu oxmzj hmgob azyjx chvzy mr
```

B.1 Index koincidence

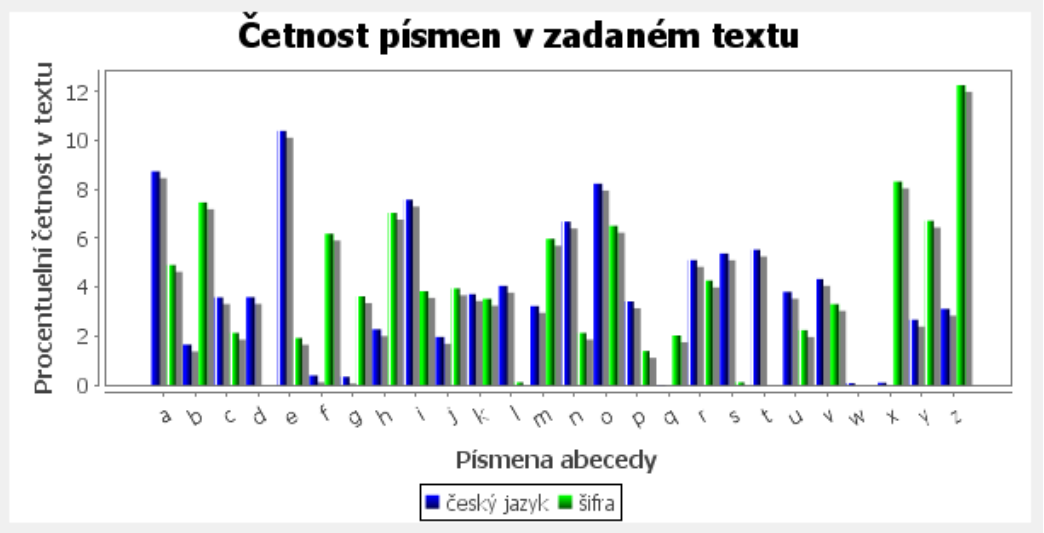
Za pomoci menu Nástroje → Index koincidence → Index koincidence (IC) luštitel zjistí, že IC šifrového textu má hodnotu 0,061. Tato hodnota je blízká českého jazyka, a ukazuje na monoalfabetickou šifru nebo transpozici.

B.2 Určení typu šifry

Při analýze grafu v okně Nástroje → Frekvenční analýza je vidět (viz obrázek B.2), že stejné znaky si neodpovídají svou četností, tzn. pravděpodobně se jedná o substituční šifru.

B.3 Podtyp šifry

Protože mapování šifrových znaků na abecedu otevřeného textu není zcela průkazné (viz obrázek B.2), jako další v pořadí se může luštitel pokusit prolomit afinní šifru. Jednou z možností je pouze uplatňovat na zachycený text pravidla frekvenční ana-



Obr. B.1: Graf frekvenční analýzy

Tabulka mapování znaků analyzovaného textu (1.řádek) na českou abecedu (záhlaví) podle četnosti. 2.řádek zobrazuje rozdíl v pozicích záhlaví a 1.řádku:

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	p	k	g	z	s	l	q	h	e	i	r	u	y	b	v	d	m	f	o	j	a	t	w	c	n
23	14	8	3	21	13	5	9	25	21	24	6	8	11	13	6	13	21	13	21	15	5	23	25	4	14

Obr. B.2: Tabulka mapování znaků šifrového textu

lýzy (viz kapitola 2.10), nebo se může pokusit vyluštit parametry afinní šifry.

B.4 Mapování písmen

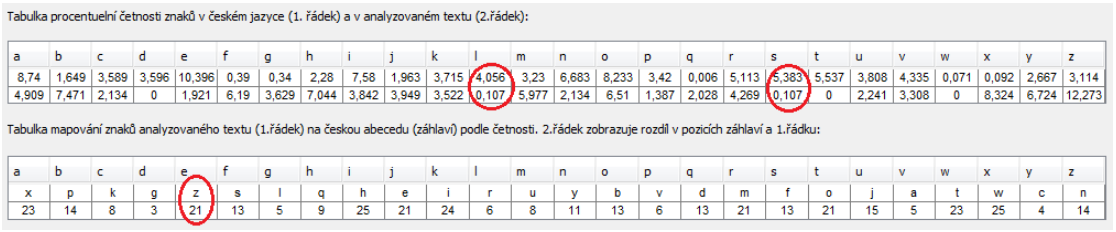
Pro úspěšné vyřešení afinní šifry je třeba namapovat alespoň dvě písmena šifrového textu. Na základě obrázku frekvenční analýzy B.2 je možno vybrat např. suverénně nejčetnější písmeno šifrového textu a mapovat ho, $\mathbf{z(25)} \rightarrow \mathbf{e(4)}$ (pozn. - číslo v závorce odpovídá indexu písmene v abecedě). Další písmeno by mohlo být např. **x** mapované na **a**, nicméně pro vyřešení soustavy rovnic je potřeba, aby alespoň jedno z vybraných písmen otevřené abecedy nemělo sudý index (nebo nebylo nulové).
Na obrázku B.3 je zobrazena setříděná četnost výskytu písmen v české abecedě. Z ní je mj. zřejmé, že písmena **f** a **g** mají téměř stejnou a ne příliš vysokou četnost výskytu. Dle obrázku B.4 je zřejmé, že v šifrovém textu by se mohlo jednat o písmena **l** nebo **s**. Zkusíme namapovat $\mathbf{f}(5) \rightarrow \mathbf{l}(11)$. Dostaneme (dle vztahu 2.13) soustavu dvou rovnic o dvou neznámých:

$$\begin{aligned} 25 &= 4 \cdot a + b \ mod\ 26 \\ 11 &= 5 \cdot a + b \ mod\ 26 \end{aligned} \tag{B.1}$$

Setříděná četnost výskytu znaků v českém textu:

znak	četnost %	znak	četnost %
e	10.396	c	3.589
a	8.740	p	3.420
o	8.233	m	3.230
i	7.580	z	3.114
n	6.683	y	2.667
t	5.537	h	2.280
s	5.383	j	1.963
r	5.113	b	1.649
v	4.335	f	0.390
l	4.056	g	0.340
u	3.808	x	0.092
k	3.715	w	0.071
d	3.596	q	0.006

Obr. B.3: Tabulka četnosti českých písmen


Tabulka procentuelní četnosti znaků v českém jazyce (1. řádek) a v analyzovaném textu (2.řádek):

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
8,74	1,649	3,589	3,596	10,396	0,39	0,34	2,28	7,58	1,963	3,715	4,056	3,23	6,683	8,233	3,42	0,006	5,113	5,383	5,537	3,808	4,335	0,071	0,092	2,667	3,114
4,909	7,471	2,134	0	1,921	6,19	3,629	7,044	3,842	3,949	3,522	0,107	5,977	2,134	6,51	1,387	2,028	4,269	0,107	0	2,241	3,308	0	8,324	6,724	12,273

Tabulka mapování znaků analyzovaného textu (1.řádek) na českou abecedu (záhlaví) podle četnosti. 2.řádek zobrazuje rozdíl v pozicích záhlaví a 1.řádku:

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	p	k	g	z	s	l	q	h	e	i	r	u	y	b	v	d	m	f	o	j	a	t	w	c	n
23	14	8	3	21	13	5	9	25	21	24	6	8	11	13	6	13	21	13	21	15	5	23	25	4	14

Obr. B.4: Rozložení četnosti šifrových písmen

Odečteme druhou rovnici od první a dostáváme:

$$\begin{aligned} 14 &= -1 \cdot a \ mod\ 26 \Rightarrow \\ 14 \cdot (-1)^{-1} &= a \ mod\ 26 \Rightarrow \\ 14 \cdot 25 &= a \ mod\ 26 \end{aligned} \tag{B.2}$$

Při tomto postupu byl použit výpočet multiplikativní inverze čísla -1 v Z_{26} pomocí menu Nástroje ⇒ Euklides ⇒ Euklidův algoritmus rozšířený. Výsledná rovnice ale na řešení nevede - jejím řešením je totiž sudé číslo **a**, které ovšem z definice afinní šifry nemohlo být použito.
Zkusíme druhou možnost, a to mapování $\mathbf{f}(5) \rightarrow \mathbf{s}(18)$. Dostáváme

$$\begin{aligned} 25 &= 4 \cdot a + b \ mod\ 26 \\ 18 &= 5 \cdot a + b \ mod\ 26 \end{aligned} \tag{B.3}$$

Opět odečteme druhou rovnici od první a dostáváme:

$$\begin{aligned} 7 &= -1 \cdot a \ mod\ 26 \Rightarrow \\ 7 &= 25 \cdot a \ mod\ 26 \Rightarrow \\ 7 \cdot 25^{-1} &= a \ mod\ 26 \Rightarrow \end{aligned}$$

$$\begin{aligned} 7 \cdot 25 &= a \ mod\ 26 \Rightarrow \\ 175 &= a \ mod\ 26 \Rightarrow \\ 19 &= a \ mod\ 26 \end{aligned} \tag{B.4}$$

Nejmenší **a** řešící tuto rovnici je $a = 19$. Dále dosadíme do první rovnice:

$$\begin{aligned} 25 &= 4 \cdot 36 + b \ mod\ 26 \Rightarrow \\ -51 &= b \ mod\ 26 \Rightarrow \\ 27 &= b \ mod\ 26 \Rightarrow \\ b &= 1 \end{aligned} \tag{B.5}$$

Parametry šifrového systémů jsou $a = 19, b = 1$, výsledek můžeme ověřit dešifrováním textu pomocí menu Dešifrování ⇒ Monoalfabetická šifra ⇒ Afinní šifra.