Univerzita Hradec Králové
Přírodovědecká fakulta
Katedra informatiky

Luštění transpozičních šifer s podporou počítače

Bakalářská práce

Autor: Sabina Hájková

Studijní program: B1101 Matematika

Studijní obor: Matematika se zaměřením na vzdělávání,
Informatika se zaměřením na vzdělávání

Vedoucí práce: PhDr. Michal Musílek, Ph.D.

Hradec Králové duben 2015

Univerzita Hradec Králové

Přírodovědecká fakulta

Zadání bakalářské práce

Autor:	Sabina Hájková
Studijní program:	B1101 Matematika
Studijní obor:	Informatika se zaměřením na vzdělávání Matematika se zaměřením na vzdělávání
Název práce:	Luštění transpozičních šifer s podporou počítače
Název práce v AJ:	Deciphering of transposition ciphers with computer support
Cíl a metody práce:	Cílem práce je posoudit možnosti využití počítače jako pomůcky k luštění klasických transpozičních šifer různých tipů. Práce se podrobněji zaměří na konkrétní typ šifer a metodu jejich analýzy, například na luštění jednoduché sloupcové transpozice nebo Fleissnerovy mřížky na základě slovníkového útoku využívajícího pouze krátkých slov. Praktickým výstupem práce budou jednoduché programy (např. makra vytvořená ve VBA pro MS Excel), využitelné při luštění transpozičních šifer.
Garantující pracoviště:	Katedra informatiky, Přírodovědecká fakulta
Vedoucí práce:	PhDr. Michal Musílek, Ph.D.
Oponent:	Ing. Petr Voborník, Ph.D.
Datum zadání práce:	1. 4. 2014
Datum odevzdání práce:	

PROHLÁŠENÍ:

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně a že jsem v seznamu použité literatury uvedla všechny prameny, ze kterých jsem vycházela.

V Hradci Králové dne Sabina Hájková

PODĚKOVÁNÍ:

Ráda bych poděkovala PhDr. Michalu Musílkovi, Ph.D. za odbornou pomoc, cenné rady a vstřícný přístup během vedení mé bakalářské práce.

ANOTACE

HÁJKOVÁ, S. *Luštění transpozičních šifer s podporou počítače*. Hradec Králové, 2014. Bakalářská práce na Přírodovědecké fakultě Univerzity Hradec Králové. Vedoucí bakalářské práce PhDr. Michal Musílek, Ph.D. 41 s.

Bakalářská práce je zaměřena na transpoziční šifry. V teoretické části jsou stručně popsány dějiny kryptologie, dále je uveden přehled různých šifrových systémů a způsobů šifrování, dešifrování a luštění. Praktickou částí bakalářské práce jsou jednoduchá makra vytvořená v editoru jazyka Visual Basic for Applications v aplikaci Microsoft Excel. Cílem jednotlivých maker je usnadnit práci s transpozičními šiframi. V závěru bakalářské práce jsou shrnuty výhody i nevýhody použití počítače při šifrování, dešifrování a luštění transpozičních šifrových systémů.

KLÍČOVÁ SLOVA

kryptografie, transpoziční šifra, šifrování, luštění, VBA, Excel

ANNOTATION

HÁJKOVÁ, S. *Deciphering of transposition ciphers with computer support*. Hradec Králové, 2014. Bachelor Thesis at Faculty of Science University of Hradec Králové. Thesis Supervisor PhDr. Michal Musílek, Ph.D. 41 p.

The Bachelor thesis is focused on transposition ciphers. The theoretical part includes the brief history of cryptology, description of various cipher systems as well as encryption, decryption and deciphering methods. The practical part deals with simple macros made in editor of Visual Basic for Applications in Microsoft Excel. Individual macros enable an easier work with transposition ciphers. The final part of Bachelor thesis summarizes advantages and disadvantages of using computers for encryption, decryption and deciphering methods of the transposition cipher systems.

KEYWORDS

cryptography, transposition cipher, encryption, deciphering, VBA, Excel

OBSAH

ÚVOD

Bakalářská práce se zabývá šifrováním, dešifrováním a luštěním transpozičních šifer. Práce je rozdělena na teoretickou a praktickou část. Obě tyto části jsou zaměřeny na odvětví kryptologie, tedy na kryptografii a kryptoanalýzu. Cílem bakalářské práce je seznámit se s transpozičními šiframi a pro usnadnění práce s nimi vytvořit jednoduchá makra v aplikaci MS Excel. Tyto aplikace jsou podrobně rozebrány v praktické části.

Cílem teoretické části bakalářské práce je podat základní informace z oblasti kryptografie. V první kapitole jsou zavedeny základní pojmy, které jsou důležité pro porozumění a práci s šiframi. Jsou zde vysvětleny i významy pojmů kryptologie, kryptografie, kryptoanalýza a steganografie. Cílem další kapitoly je zobrazit nejvýznamnější osobnosti a mezníky v dějinách kryptologie.

Kapitola s názvem Substituční šifry popisuje šifrovací algoritmy a pravidla pro šifrování a dešifrování pomocí substituce. V této kapitole se seznámíme s některými konkrétními substitučními šiframi, jako například s jednoduchou substitucí nebo Vigenèrovou šifrou.

Nejdůležitější kapitolou bakalářské práce je kapitola nazvaná Transpoziční šifry, která je rozdělena do jednotlivých podkapitol, které nesou názvy konkrétních transpozičních šifer. Cílem této kapitoly je postupné seznámení s jednoduchými transpozičními systémy, sloupcovou transpozicí a Fleissnerovou mřížkou. U každé z těchto šifer je uveden princip šifrování a dešifrování a názorný příklad.

Poslední kapitola teoretické části popisuje způsob luštění transpozičních šifer za pomoci tužky a papíru tak, abychom v konečné fázi dokázali jednoduché šifry prolomit. V jedné z podkapitol jsou uvedeny poznatky o frekvenční analýze, bez které se úspěšní luštitelé neobejdou. V dalších podkapitolách je podrobněji rozepsán způsob luštění konkrétních transpozičních šifer.

Cílem praktické části bakalářské práce je vytvoření algoritmů a jednoduchých maker pro usnadnění šifrování, dešifrování a luštění transpozičních šifer pomocí počítače. V první kapitole této části se seznámíme s programovacím jazykem Visual Basic for Application, který byl použit při vytváření maker v MS Excel. Další kapitola obsahuje tři podkapitoly, které jsou nazvány podle příslušných maker. V každé této podkapitole se nachází popis funkce programu a návod pro práci s konkrétním programem. V přílohách jsou navíc umístěny vývojové diagramy některých funkcí.

Na závěr bude provedeno shrnutí poznatků, se kterými se seznámíme v teoretické části, a zhodnocení výsledků praktické části bakalářské práce. Budou zde také sepsány výhody a nevýhody využití počítače pro práci s uvedenými šifrovými systémy.

1 TEORETICKÁ ČÁST

V teoretické části budou vysvětleny nejzákladnější pojmy z oblasti šifrování, mezi které patří například i šifra, kód, luštění nebo dešifrování. Budou zde uvedeny i rozdíly a vztahy mezi kryptologií, kryptografií a kryptoanalýzou. Dále se budeme zabývat historií kryptologie a důležitými jmény, jejichž nositelé stojí za vznikem jednotlivých šifer.

Podle způsobu šifrování dělíme šifry na substituční a transpoziční. V práci bude uvedeno pár poznatků o substitučních šifrách. Podrobněji se ale budeme věnovat jednotlivým transpozičním šifrám, na které je bakalářská práce zaměřena.

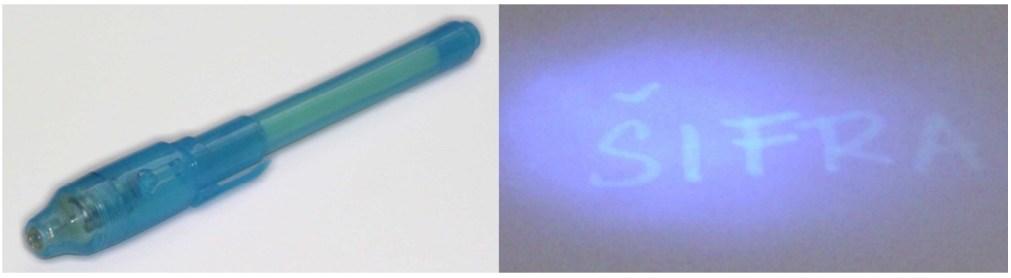
1.1 Základní pojmy

Nejzákladnějším pojmem v oblasti tajné komunikace je **kryptologie** neboli věda o šifrování. Kryptologie bývá rozdělena na dvě odvětví – kryptografii a kryptoanalýzu.

Název **kryptografie** vznikl z řeckého slova *kryptos*, což znamená skrytý. Kryptografie je souhrn metod jak utajit obsah zprávy tak, aby v rukou nepovolaného člověka byla nečitelná. Děje se tak pomocí šifrování, to znamená, že si účastníci tajné komunikace smluví určitá pravidla, na jejichž základě potom pozmění text zprávy. Luštění takovéto zprávy je pro člověka, který pravidla šifrování nezná, velmi obtížné. (Singh, 2009)

Opakem kryptografie je **kryptoanalýza**, která se zabývá luštěním tajných zpráv. Kryptoanalytici hledají způsob, jak šifru prolomit a přečíst si text zprávy i bez znalosti šifrovacího klíče. Simon Singh ve své knize uvádí, že prvními úspěšnými kryptoanalytiky byli Arabové. (Singh, 2009)

Vedle kryptografie vznikla také **steganografie**, jejíž název byl odvozen ze dvou řeckých slov *steganos*, v překladu schovaný, a *graphein*, neboli psát. Jak už z těchto slov vyplývá, steganografie je druh komunikace, jejíž členové se snaží tajit existenci svých zpráv, aby o nich nevěděl nikdo jiný. Samotný text zprávy ale nemusí být nijak pozměněn. Janeček například uvádí příběh Histiaia, který svému poslovi oholil hlavu, vytetoval na ni zprávu a počkal, až mu vlasy opět narostou. Potom ho se zprávou vyslal do Řecka za svým zeťem. Aby si mohl Aristagoras Milétský tuto zprávu přečíst, musel si posel znovu oholit hlavu. (Janeček, 1998) Tajnou zprávu lze ale zapsat i jednoduše speciálním fixem s neviditelným inkoustem, na který pak stačí pouze posvítit UV baterkou a text se objeví (viz obrázek 1).



Obrázek 1 – Dětský UV fix a tajný text napsaný neviditelným inkoustem

K samotnému šifrování je ale nutné znát význam dalších pojmů. Jedním z nich je nepochybně **šifra**. Šifrou rozumíme nahrazování písmen zprávy, kterou chceme utajit, jinými písmeny, číslicemi nebo symboly. Jestliže například písmena v abecedě očíslujeme od 0 do 25 a zašifrujeme slovo SOBOTA, získáme 1814114190.

Podobný význam jako šifra má i pojem **kód**, což je slovo, číslo nebo symbol, kterým jsme nahradili jiné slovo nebo skupinu slov. Například v knize Marka Bowdena Černý jestřáb sestřelen se můžeme dočíst, že vojáci pro odstartování mise použili heslo IRENA. (Bowden, 2008)

Text, který chceme zašifrovat, se nazývá **otevřený text**, je to text psaný v běžném jazyce a pro každého člověka srozumitelný. Kdežto **šifrový text** je již výsledná podoba textu po zašifrování, jeví se jako náhodná kombinace znaků.

Důležitým pojmem je také **klíč**, což je souhrn pravidel, podle nichž probíhá šifrování. Například kterými znaky budou nahrazena písmena otevřeného textu nebo jaké heslo bude při šifrování použito. Je zřejmé, že klíč musí znát jak odesílatel, tak příjemce zašifrované zprávy a musí být bezpečně utajen, aby se k němu nedostal nepovolaný člověk. Postup vytváření šifrového textu se nazývá **šifrovací algoritmus**.

Odesílatel pomocí klíče a šifrovacího algoritmu převede otevřený text na šifrový, to znamená, že ho **zašifruje**. Příjemce šifrové zprávy musí použít opačný algoritmus, aby si mohl obsah zprávy přečíst, bude tedy zprávu **dešifrovat**. Příjemce má ovšem k dispozici stejný klíč a pravidla šifrování, jaká použil odesílatel zprávy. Pokud se ovšem zpráva dostane do rukou cizího člověka, který ji dokáže přečíst i bez znalosti klíče a pravidel, říká se tomuto procesu **luštění**.

1.2 Dějiny kryptologie

Je zřejmé, že lidé začali utajovat zprávy až po vzniku písma. Janeček uvádí, že první pokusy o tajnou komunikaci se objevily již v pátém století před naším letopočtem. V té době se ale jednalo spíše o ukrývání samotných zpráv než o jejich šifrování. (Janeček, 1998)

Nejstarší šifrou vůbec je pravděpodobně **atbaš**, pomocí níž byly ve Starém zákoně šifrovány části textu. Jedná se o substituci, která nahrazovala první písmeno hebrejské abecedy za poslední, druhé za předposlední a tak dále. Podobné šifře atbaš jsou také hebrejské šifrovací systémy **atbah** a **albam**.

Jedním z nejstarších šifrovacích systémů je **Skytala**, který používali Sparťané. Jedná se o dvě naprosto stejné hole, neboli skytalé. Jednu hůl měl odesílatel zprávy a druhou příjemce. Odesílatel navinul na hůl pruh látky, papyru nebo nějaký pásek, potom na něj napsal zprávu a po odvinutí předal pásku svému poslovi, který ji mohl použít například jako opasek, aby zabránil objevení existence zprávy. Příjemce si text mohl přečíst teprve ve chvíli, kdy pásek navinul na hůl o stejném průměru, jaký měla hůl odesílatele (viz obrázek 2). Tento způsob tajné komunikace je kombinací kryptografie a steganografie.

Obrázek 2 – Skytala

Jedním z významných šifrovacích systémů v dějinách kryptografie byla také **Polybiova šifrovací mřížka**. Abeceda se zapsala do tabulky s očíslovaným vodorovným i svislým záhlavím a každému písmenu pak byla přiřazena dvojice čísel, tedy číslo řádku a sloupce, ve kterém se písmeno nacházelo. Tento způsob šifrování umožnil předávání šifrové zprávy pomocí pochodní. Počtem pochodní v jedné ruce odesílatel ukazoval číslo řádku a počtem pochodní v druhé ruce číslo sloupce. (Vondruška, 2006)

Gaius Julius Ceasar často používal k šifrování vojenských zpráv **jednoduchou substituci**, tedy nahrazoval písmena otevřeného textu řeckými písmeny. Později své šifrovací systémy zdokonalil, například každé písmeno otevřeného textu zaměnil za písmeno, které od něj v abecedě leželo o tři pozice dále, a takto postupoval, dokud nezašifroval celou zprávu. Vondruška ve své knize píše, že Ceasarův syn Augustus zase nahrazoval písmena těmi, které stály v abecedě za ním. Poslední písmeno v abecedě Z zaměňoval za dvojici písmen AA. (Vondruška, 2006)

V Čechách pravděpodobně začal jako první šifrovat Mistr Jan Hus, jehož šifrovací systém spočíval v nahrazování samohlásek otevřeného textu písmeny, které stály v abecedě hned za nimi. Tuto šifru použil v dopisech, které posílal z vězení v Kostnici.

Největší rozkvět kryptografie nastal v 16. století v souvislosti s velkým počtem válek, rozvojem vědy a techniky. Například i alchymisté šifrovali své nápady a pokusy, aby je uchránili před zneužitím. Největší zájem o utajenou komunikaci však byl v politických řadách.

V roce 1500 napsal německý opat Johannes Trittheim (1462 – 1518) první knihu o šifrování. Kryptografii obohatil také několika vlastními šifrovacími systémy, jako je například **tabulka se složitou substitucí** nebo **tříčíselná substituce**, která každému písmenu otevřené abecedy přiřadí trojici čísel složenou z číslic 1, 2 a 3. Trittheim je také autorem známé tabulky utvořené z 26 abeced, zvané **tabula recta**. Trittheimovo dílo se ovšem znelíbilo panským rodům, proto bylo zničeno a jeho autor byl obviněn z čarodějnictví. (Janeček, 1998)

Velkým přínosem pro kryptografii byla tzv. **Cardanova mřížka**, která dostala jméno po svém autorovi Hieronymu Cardanovi. Jedná se o čtvercovou desku, ve které jsou na různých místech vyřezány otvory, do nichž se po přiložení mřížky na papír zapíše otevřený text. Po odejmutí desky se volná místa mezi písmeny otevřeného textu zaplní jinými náhodnými písmeny. Tím se otevřený text ukryje ve změti náhodných písmen,

jedná se tedy o steganografickou metodu. Příjemce šifrového textu musí vlastnit stejnou mřížku, aby zprávu dokázal přečíst. Tato mřížka byla později zkoumána a vylepšována dalšími kryptografy, mezi které patřil například známý generál Paul von Hindenburg nebo plukovník Eduard Fleissner von Wostrovitz, který je autorem **otočné mřížky**. (Kajínek, 2008)

Předchůdcem sloupcové transpozice v tabulce byla **řádková transpozice podle hesla**, kterou používal francouzský šlechtic a kardinál Armand-Jean du Plessis de Richelieu (1585 – 1642).

S tabulkou složitější substituce, podobné tabulce Trittheimově, přišel i francouzský diplomat Blaise de Vigenère (1523 – 1596), který vycházel z prací kryptografů Giovanniho Porta, Leona Battisty Albertiho a právě Johanna Trittheima. Výsledkem byla **Vigenèrova šifra** a **Vigenèrův čtverec** (viz obrázek 3), který se skládá z 26 šifrových abeced, přičemž každá následující je vzhledem k předchozí abecedě posunuta o jedno písmeno. (Singh, 2009) Princip šifrování pomocí Vigenèrova čtverce si ukážeme v kapitole o substitučních šifrách.

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

Obrázek 3 – Vigenèrův čtverec (převzato z wikipedia.org)

Angličan Francis Bacon (1561 – 1626) se také zajímal o kryptografii a vynalezl **binární šifrování**. Bacon každé písmeno abecedy vyjádřil pěticí znaků složenou z písmen **a** a **b**. To znamená, že písmeno A mělo kód aaaaa, písmeno B se rovnalo kódu aaaab, C bylo přepsáno na aaaba, atd. Tento systém se stal základním kamenem pro pozdější moderní kódování. (Janeček, 1998) V dnešní době se místo písmen **a** a **b** používají nejčastěji znaky 0 a 1.

Kryptografií se zabýval i bývalý americký prezident Thomas Jefferson, který vynalezl populární šifrovací nástroj, známý jako **Jeffersonova disková šifra**. Nástroj měl tvar válce, který se skládal z 36 disků, a na každém z nich bylo 26 znaků. S těmito disky se pak libovolně otáčelo tak, aby v jednom z 26 řádků po celé délce válce vznikl otevřený

text. V některém ze zbylých řádků se četl šifrový text. Každý disk byl pochopitelně očíslovaný, aby příjemce mohl snadno zprávu dešifrovat.

Obrázek 4 – Jeffersonova disková šifra (převzato z monticello.org)

Charles Wheatstone (1802 – 1875) zavedl v roce 1854 šifru **Playfair**, která však dostala jméno po svém propagátorovi Lyonu Playfairovi. Jedná se o šifrovací čtverec o velikosti 5 x 5, pomocí něhož se bigramy (dvojice písmen) otevřeného textu zaměňují za bigramy šifrového textu. Pro určování těchto bigramů existují určitá pravidla, která si vysvětlíme v kapitole Substituční šifry.

Trittheimovu tabulku tabula recta využil i **Francis Beaufort** (1774 – 1857), který si ale vytvořil vlastní vzorec šifrování. Ve svislém záhlaví četl písmeno otevřeného textu, ve stejném řádku pak vyhledal písmeno hesla a nad ním ve vodorovném záhlaví četl písmeno šifrového textu.

V roce 1888 francouzský kryptolog **De Viaris** sestavil vzorce pro snadnější používání Vigenèrovy a Beaufortovy šifry. Ve vzorcích uvedených níže značí písmeno O otevřený text, písmeno Š značí šifrový text a H je znakem pro heslo. V tabulce vzorců je uveden ještě systém Sestri-Beaufortův, který vymyslel Giovanni Sestri. Pomocí této šifry se získává šifrový text způsobem jako Vigenère zprávy dešifroval a naopak.

	šifrování	**dešifrování**
Vigenère	O + H = Š	Š – H = O
Beaufort	H – O = Š	H – Š = O
Sestri-Beaufort	O – H = Š	Š + H = O

Historie kryptografie se dále vyvíjela, šifry byly zdokonalovány, aby nedocházelo k jejich prolamování. S vývojem techniky začaly vznikat i šifrovací stroje. Prvním takovým zařízením byly dva elektrické psací stroje spojené soustavou 26 vodičů. Každé písmeno na jednom stroji bylo spojeno s jiným písmenem na stroji druhém. Proslulým šifrovacím strojem byla **Enigma**, kterou používali Němci za druhé světové války. Boris Hagelin zase sestrojil několik verzí šifrovacího stroje, které pojmenoval po sobě, tedy **Hagelin**.

Jak již bylo řečeno, prvními úspěšnými kryptoanalytiky byli Arabové. Dnes již velice známou a pro kryptoanalýzu velmi důležitou **frekvenční analýzu** poprvé popsal v 9. století našeho letopočtu Abú Jusúf Jaqúb ibn Isháq ibn as-Sabbáh ibn'Omrán ibn

Ismail al-Kindí, který začal zkoumat výskyt jednotlivých hlásek v textu. Jednoduchá záměna, která byla dlouhá staletí považována za bezpečnou, byla tak díky frekvenční analýze prolomena. (Singh, 2009)

Na používání jednoduchého šifrového systému doplatila i Marie Stuartovna, která z vězení posílala zašifrované zprávy svému obdivovateli a spiklenci Anthonymu Babingtonovi. K šifrování používali **nomenklátor**, tedy seznam znaků, ve kterém byly uvedeny nejen symboly k nahrazení písmen abecedy, ale také některých (často se opakujících, nebo zvlášť důležitých) slov a frází. Babington ve svém dopise popsal plánované Mariino vysvobození a spiknutí proti anglické královně Alžbětě I. a zprávu zašifroval. Dopis se ale dostal k tajemníkovi Alžběty I., který ho předal svému luštiteli Thomasu Phelippesovi, a tajný text byl rozluštěn. Tyto dopisy byly použity jako usvědčující důkaz a Marie a její spiklenci byli popraveni. (Singh, 2009)

Známými kryptoanalytiky byli Antoine a Bonaventure Rosignolové (otec a syn), kteří na základě svých luštitelských zkušeností sestrojili šifrový systém s názvem **Velká šifra**. Oba Rosignolové pracovali u dvora Ludvíka XIV. a šifrovali jeho tajné dokumenty. Po jejich smrti však jejich šifru nedokázal nikdo zlomit. Podařilo se to až po dvou stech letech Étiennu Bazeriesovi, který jako první dokázal Ludvíkovy dokumenty přečíst. Mezi tyto dokumenty patřil i dopis, který prozradil tajemství Muže se železnou maskou. Názory, zda je tento dopis pravdivý či nikoli, se ovšem liší.

Do dějin kryptoanalýzy se také zapsal Charles Babbage svým úspěšným prolomením Vigenèrovy šifry, která byla dlouhou dobu považována za nerozluštitelnou a díky tomu často nazývána jako Le chiffre indéchiffrable (nerozluštitelná šifra).

S rostoucí úrovní výpočetní techniky byly postupně kladeny vyšší a vyšší nároky na šifrovací systémy. Doposud zdánlivě nerozluštitelné systémy byly prolomeny, a proto se spousta kryptografů snažila vynalézt bezpečný šifrovací systém. Aby se zašifrovaná zpráva stala nerozluštitelnou, muselo být při jejím šifrování použito náhodné heslo stejné délky, jako byla délka otevřeného textu, a nesmělo být použito vícekrát než jednou. Nerozluštitelnost takového systému dokázal americký matematik a kryptolog Claude Elwood Shannon. Tento systém je znám pod názvem **One-time pad** nebo také **jednotkové přičtení hesla**. (wikipedia.org)

Příprava a distribuce dlouhých a dokonale náhodných hesel je velmi náročná, proto se v praxi využívají systémy nikoliv nerozluštitelné, ale obtížně luštitelné. To znamená, že kryptoanalytikovi trvá velmi dlouho, než vyzkouší všechny možné varianty hesla. Průměrná doba k prolomení šifry je tak dlouhá, že obsah zašifrované zprávy mezitím ztratí svoji aktuálnost a význam.

1.3 Substituční šifry

Mezi nejznámější a nejvíce využívané šifrovací systémy patří substituční šifry. Slovem **substituce** rozumíme záměnu znaků otevřeného textu za znaky šifrové abecedy. Šifrování může probíhat různými způsoby, například celý otevřený text můžeme zašifrovat pomocí jediné šifrovací abecedy nebo každé písmeno otevřeného textu

zašifrujeme odlišnou šifrovací abecedou, apod. Také šifrová abeceda mívá různé podoby, písmena otevřeného textu můžeme nahradit například řeckými písmeny, číslicemi, skupinou čísel nebo různými symboly.

Substituční šifry lze rozdělit na jednoduchou záměnu, někdy též monoalfabetickou šifru, homofonní substituci, polyalfabetickou substituci, polygramovou substituční šifru a digrafickou substituční šifru. (Vondruška, 2006)

Jednoduchá záměna (monoalfabetická substituce) je šifrovací systém, který všechny znaky otevřeného textu zaměňuje za znaky **jediné** šifrovací abecedy. Šifrovací abeceda se může skládat ze znaků otevřené abecedy, ale mohou ji tvořit také symboly, číslice a další.

Příkladem jednoduché záměny je například již zmíněná šifra typu atbaš, která nahrazuje první písmeno abecedy za poslední, druhé za předposlední a tak dále. Můžeme využít pomocnou tabulku:

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

Například slovo SUBSTITUCE zašifrujeme pomocí této tabulky jako FHOFGVGHPR. Pro dešifrování používáme stejnou tabulku.

Také velmi známé kódování pomocí Morseovy abecedy patří do kategorie monoalfabetické substituce. Každý znak Morseovy abecedy je vytvořen z určitého počtu teček a čárek, například znak — • představuje písmeno N. Nejedná se ovšem o šifrování, zpráva je pouze převedena do podoby vhodné pro vysílání elektrických, zvukových nebo optických signálů.

Homofonní substituce je šifra, u které se pro vybraný znak používá více šifrových znaků. Šifrové znaky se stejným významem se nazývají homofony.

Polyalfabetickou substitucí rozumíme několik jednoduchých substitucí, které jsou podle domluvy postupně aplikovány na jednotlivá písmena otevřeného textu. Typickým příkladem tohoto šifrovacího systému je Vigenèrova šifra.

Otevřený text zbavíme diakritiky a mezer a zvolíme heslo. Naším otevřeným textem bude například *Bakalářská práce z informatiky* a heslem *Substituce*. Otevřený text upravíme a nad něj napíšeme heslo tolikrát, abychom získali stejný počet znaků, jako má otevřený text.

```
SUBSTITUCESUBSTITUCESUBSTIT
BAKALARSKAPRACEZINFORMATIKY
```

Potom se ve Vigenèrově čtverci šifrový znak nachází na průsečíku řádku začínajícím prvním písmenem hesla a sloupce začínajícím prvním písmenem otevřeného textu.

```
TULSE IKMME HLBUX HBHHS JGBLB SR
```

Takto pokračujeme dále, až získáme šifrový text, který ještě rozdělíme do pětimístných skupin.

Při dešifrování hledáme v řádku označeným písmenem hesla písmeno šifrového textu a nad ním se v prvním řádku tabulky nachází znak otevřeného textu.

Polygramová substituční šifra je obecný název pro šifry, které zaměňují skupiny znaků otevřeného textu za skupiny znaků šifrové abecedy. Jestliže nahrazujeme dvojice znaků, tato šifra se nazývá **bigramová substituční šifra**, pokud pracujeme s trojicemi znaků, šifra se nazývá **trigramová substituce** atd.

V kapitole Dějiny kryptologie jsme se zmínili o šifře Playfair, což je příklad bigramové substituční šifry. Pro šifrování je důležité znát heslo, které se vepíše do tabulky 5 x 5 a zbylá políčka doplníme písmeny v abecedním pořadí, která se však již nenacházejí v domluveném hesle. V tabulce navíc vynecháme písmeno Q, protože se v českém jazyce vyskytuje velmi málo. Otevřený text upravíme na tvar bez diakritiky, bez mezer a písmeno Q nahradíme písmenem K. Vzniklý text ještě rozdělíme do skupin po dvou znacích, pokud máme lichý počet znaků, doplníme text o písmeno, které se v češtině příliš nepoužívá, například X nebo Z. Jestliže se v některé dvojici vyskytne jeden znak dvakrát, vložíme mezi ně opět písmeno X nebo Z. Samotný převod otevřeného textu na šifrový se řídí třemi pravidly:

- jestliže se obě písmena jednoho bigramu otevřeného textu nacházejí v tabulce ve stejném sloupci, písmena šifrového textu čteme pod těmito písmeny, v případě, že je některé písmeno na konci sloupce, šifrovým znakem je první písmeno tohoto sloupce
- pokud se obě písmena nacházejí v jednom řádku, šifrové znaky čteme vpravo od těchto písmen, jestliže je některé písmeno na konci řádku, šifrovým znakem je první písmeno tohoto řádku
- v případě, že se každé písmeno bigramu nachází v jiném řádku a v jiném sloupci, znaky šifrového textu se nacházejí v průsečíku řádku prvního písmene a sloupce druhého písmene a v průsečíku řádku druhého písmene a sloupce prvního písmene (záleží na pořadí!)

Způsob šifrování si ukážeme na názorném příkladu. Jako heslo zvolíme slovo *Kniha* a otevřeným textem bude *Zítra večer u starého dubu*. Vytvoříme převodovou tabulku a upravíme otevřený text na požadovaný tvar.

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

OT: ZI TR AV EC ER US TA RE HO DU BU

ŠT: XA US KZ FD CT PT UH TC AM FS FP

Posledním typem substituce je **digrafická substituční šifra**, jejíž princip jasně ukazuje šifrování pomocí Polybiovy mřížky, která každé písmeno otevřeného textu nahrazuje dvojicí číslic. Digrafická substituce tedy znamená záměnu jednotlivých znaků otevřeného textu za dvojice znaků šifrové abecedy. Šifrová abeceda se nemusí skládat jen z číslic, mohou ji tvořit symboly i znaky otevřené abecedy.

1.4 Transpoziční šifry

Princip **transpozičních šifer** spočívá ve změně pořadí znaků v otevřeném textu. Změna pořadí probíhá podle předem daných pravidel. Je tedy zřejmé, že tvar a počet znaků v šifrovém textu je stejný jako v otevřeném textu. Mezi nejjednodušší transpozice patří například psaní slov nebo celých textů pozpátku. Například slova *Dnes večer* můžeme zašifrovat jako *Send rečev*.

V následujících podkapitolách budou popsány typické transpoziční šifrovací systémy a způsoby jejich šifrování a dešifrování. Budou zde zahrnuty i systémy, které nejsou šiframi v pravém slova smyslu, jsou totiž veřejně známé a postrádají tajný klíč. Jejich luštění tedy není nijak složité.

1.4.1 Nejjednodušší transpozice

Jednoduché transpoziční šifry, které si zde uvedeme, jsou často nazývány jako dětské šifry, protože jsou hojně využívány při dětských hrách, na táborech nebo k posílání tajných psaníček.

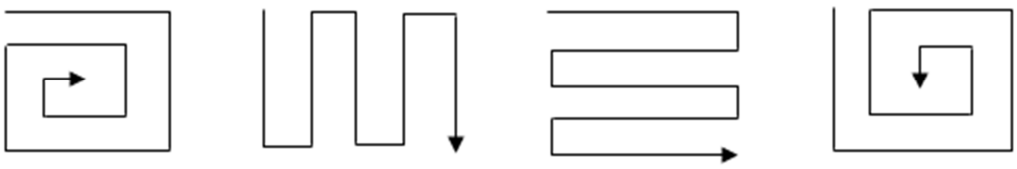
Do této kategorie transpozičních šifer patří například systém, který zapisuje jednotlivé znaky otevřeného textu postupně na přední a zadní pozice řádku připraveného pro šifrový text. Například text *Dnes večer* přepíšeme do tvaru bez diakritiky a mezer a po zašifrování získáme text DEVCREESN.

Velmi oblíbený je také systém **Podle plotu**. Otevřený text se zapíše „podle plotu“ do dvou nebo více řádků. Jako příklad použijeme otevřený text *Šifrový systém podle plotu* a zapíšeme ho následujícím způsobem do tří řádků:

S				O				Y				M				L				O		
	I		R		V		S		S		E		P		D		E		L		T	
		F				Y				T				O				P				U

Šifrový text získáme vypsáním jednotlivých řádků za sebe a rozdělením do pětimístných skupin. Příjemce zprávy tedy dostane text SOYML OIRVS SEPDE LTFYT OPU.

Zprávu můžeme zašifrovat také tak, že ji zapíšeme do tabulky nebo nějakého obrazce. Jednotlivé znaky textu zapíšeme do tabulky po sloupcích nebo podle předem dohodnutého pravidla, například ve spirále, shora dolů a podobně (viz obr. 5). Šifrový text pak čteme z tabulky po řádcích.



Obrázek 5 – Některé z možností zápisu otevřeného textu do tabulky

Pomocí tohoto systému zašifrujeme text *Sejdeme se dnes v sedm hodin u studny* a pro zápis do tabulky využijeme druhý tvar na obrázku 5.

S	E	S	U	S
E	N	V	N	T
J	D	S	I	U
D	E	E	D	D
E	S	D	O	N
M	E	M	H	Y

Výsledný šifrový text: SESUS ENVNT JDSIU DEEDD ESDON MEMHY

Tyto šifrovací systémy nejsou příliš bezpečné, protože postrádají tajný klíč, který by ztížil práci luštitelům. U posledního typu, který jsme zde zmínili, však klíčem může být způsob zápisu textu do tabulky nebo obrazec, do kterého se otevřený text zapisuje.

1.4.2 Jednoduchá sloupcová transpozice

Nejvyužívanějším transpozičním systémem je sloupcová transpozice podle hesla. Jedná se o šifrový systém, který k převodu otevřeného textu na šifrový text využívá heslo a tabulku. Podle toho, zda otevřený text v tabulce doplníme náhodnými znaky či nikoli, budeme rozlišovat sloupcovou transpozici s úplnou a neúplnou tabulkou.

Způsob šifrování si ukážeme na názorném příkladu a využijeme k tomu **sloupcovou transpozici s úplnou tabulkou**. K určení velikosti tabulky je důležité znát heslo, které udává počet sloupců tabulky. Každému písmenu hesla přiřadíme číslo v abecedním pořadí, pokud se některé písmeno vyskytne ve slově (nebo frázi) vícekrát, menší hodnotu bude mít ten znak, který se vyskytuje jako první.

Naše heslo: T A R A N T U L E

Permutační vyčíslení: 7 1 6 2 5 8 9 4 3

Takto získaný klíč (permutační vyčíslení) zapíšeme do záhlaví tabulky, která má stejný počet sloupců, kolik máme číslic. Pod heslo zapisujeme po řádcích otevřený text bez mezer a bez diakritiky. V případě, že v tabulce zbydou v posledním řádku volná políčka, doplníme otevřený text náhodnými znaky tak, aby byla tabulka úplná, například písmeny Q, X, W.

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

Náš otevřený text: Změna plánu! Tajná operace proběhne podle původní dohody. Přijď včas!

Upravený otevřený text:
ZMENAPLANUTAJNAOPERACEPROBEHNEPODLEPUVODNIDOHODYPRIJDVCAS

Šifrový text vypisujeme po sloupcích od 1 do *n*, kde *n* je délka hesla. V našem případě je *n* = 9. Nakonec šifrový text rozdělíme do skupin po pěti znacích.

Výsledný šifrový text: MTANV DANJE PDPQN EEPHV QAPBE ODWAN PONRX EACEO YSZUR HUOCP ARDII WLOOL DJX

Dešifrování zprávy je velice snadné. Příjemce zašifrované zprávy spočítá délku textu a vydělí ji délkou smluveného hesla. Tak získá počet řádků v tabulce, počet sloupců je daný počtem znaků hesla. Dešifrant potom vepisuje šifrový text do připravené tabulky po sloupcích a začíná sloupcem označeným číslem 1, pokračuje sloupcem označeným číslem 2, až vepíše celý text do tabulky. V řádcích tabulky si pak přečte čitelný text zprávy.

Šifrování pomocí **sloupcové transpozice s neúplnou tabulkou** probíhá identicky, rozdílem jsou pouze zbylá políčka v posledním řádku tabulky, která necháváme volná. Užití neúplné tabulky při šifrování je bezpečnější než šifrování s úplnou tabulkou, protože případný luštitel bude mít větší práci s určováním velikosti tabulky a doplňováním šifrového textu. Nebude totiž vědět, kolik sloupců je kratších než ostatní sloupce.

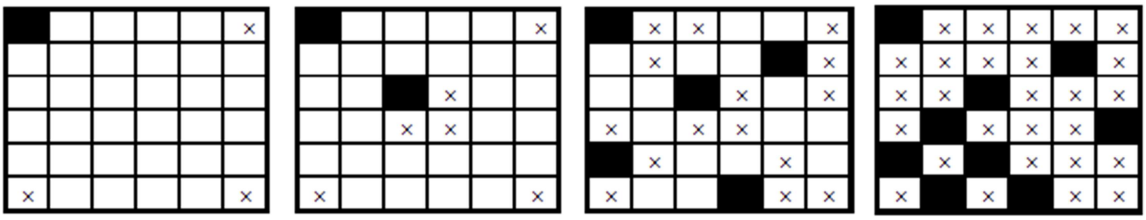
V minulosti se často používala **dvojitá transpozice**, která je mnohem odolnější než předchozí dva typy šifrovacích systémů. K šifrování byla potřeba dvě různá hesla. Otevřený text se napsal do tabulky podle prvního hesla, po sloupcích byl získán text, který byl vepsán do tabulky podle druhého hesla. Výsledný šifrový text se opět vypisoval po sloupcích v určitém pořadí. (Vondruška, 2006)

1.4.3 Fleissnerova otočná mřížka

V kapitole Dějiny kryptologie jsme se zmiňovali o otočné mřížce, která je známá také jako **Fleissnerova mřížka**, jelikož byla pojmenována po svém objeviteli plukovníku Eduardu Fleissneru von Wostrovitz.

Fleissnerova mřížka je vlastně čtverec s určitým počtem políček. V mřížce se vystřihne čtvrtina políček tak, aby po čtyřech otočeních o 90° odkryla všechna zbylá políčka čtverce. Do prázdných políček se potom vepisuje text, který má být zašifrován.

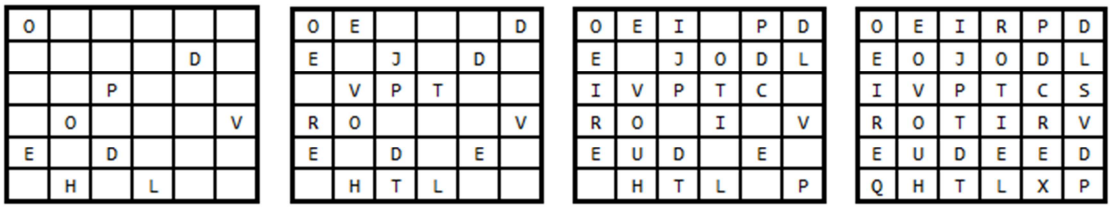
Výroba otočné mřížky je snadná, postup si ukážeme na čtverci o rozměrech 6 x 6, který tedy bude mít 36 políček. Jelikož vystřihujeme čtvrtinu z celkového počtu políček, v našem čtverci musí být vystřiženo 9 políček, aby po všech otočeních byla odkryta celá tabulka. Po vystřižení každého okénka označíme všechny jeho polohy po otočení nějakým znakem (na obrázku 6 jsou vystřižená políčka značena černou barvou a jejich pozice po otočení symbolem ×).



Obrázek 6 – Výroba Fleissnerovy otočné mřížky

Odesílatel i příjemce zprávy musí vlastnit shodnou mřížku, také se musí dohodnout na jejím výchozím otočení při prvním přiložení na papír. Odesílatel pak mřížku položí podle dohodnuté pozice na papír a do prázdných políček vepíše znaky zprávy, po zaplnění všech políček mřížku otočí o 90° a pokračuje v psaní zprávy. Mřížka je následně otočena ještě dvakrát. Pokud je délka otevřeného textu menší než je celkový počet políček, šifrant doplní prázdná políčka náhodnými znaky. Jestliže je naopak délka textu zprávy delší, použije další čtverec a zašifruje zbytek zprávy. Jestliže členové tajné komunikace zvolí mřížku s lichým počtem okének, zůstává prostřední okénko nevyužité a musí být doplněno náhodným znakem.

Pomocí naší tabulky zašifrujeme následující text: *Odpověď hledej v třetí polici uprostřed*. Jednotlivá písmena bez diakritických znamének budeme zapisovat do mřížky a zbylá políčka doplníme znaky Q a X (postup plnění tabulky je vidět na obrázku 7).



Obrázek 7 – Šifrování pomocí Fleissnerovy mřížky

Výsledný šifrový text získáme vypsáním řádků tabulky a rozdělením do skupin po pěti znacích. Náš šifrový text bude mít tedy tvar: OEIRP DEOJO DLIVP TCSRO TIRVE UDEED QHTLX PXXXX (poslední skupinu jsme doplnili znakem X).

Příjemce zašifrovaného textu nebude mít s jeho dešifrováním velkou práci. Pouze zapíše všechny znaky po řádcích do tabulky (jejíž velikost zná díky mřížce shodné s mřížkou odesílatelovou) a vynechá poslední přebytečné znaky, které odesílatel umístil na konec šifrového textu, aby doplnil poslední skupinu na pět míst. Potom přiloží mřížku ve výchozí poloze na tabulku a zapíše si znaky, které vidí ve vystřižených okénkách, následně otočí mřížku o 90° a opět zapíše viditelné znaky, dešifrant postup zopakuje ještě dvakrát a nakonec si přečte srozumitelný text tajné zprávy.

1.5 Ruční luštění transpozičních šifer

Cílem této kapitoly, jak již název napovídá, bude ukázat způsob luštění základních transpozičních šifer, konkrétně jednoduché sloupcové transpozice a Fleissnerovy mřížky. Luštění znamená získávání srozumitelného sdělení z šifrového textu bez znalosti klíče. Důležitou součástí této kapitoly je také seznámení s frekvenční analýzou, která má pro luštění šifer velký význam. Význam a využití frekvenční analýzy při luštění transpozičních šifer bude demonstrováno na konkrétních příkladech u každého z uvedených šifrových systémů.

1.5.1 Frekvenční analýza

S pojmem frekvenční analýza jsme se seznámili již v kapitole Dějiny kryptologie, kde jsme se také dozvěděli, že prvním, kdo tuto techniku popsal a využil ji k luštění šifer, byl arabský učenec al-Kindí.

Frekvenční analýza zkoumá výskyty a četnosti jednotlivých písmen v daném jazyce. Například v českém jazyce se nejvíce vyskytují písmena E, A, O, I, N, nejčastějšími bigramy jsou například ST, NI, PO, OV, CH, RO, EN, NA a nejpoužívanějšími trigramy (trojice písmen) jsou PRO, OVA, OST, STA atd. Nejčetnějším trigramem složeným ze souhlásek je STR. Na základě těchto poznatků dokáže kryptoanalytik rozluštit mnohé zašifrované zprávy. Je ovšem zřejmé, že luštitel musí daný jazyk dobře ovládat, neboť úspěšné luštění závisí i na jeho intuici a správných odhadech. (Vondruška, 2006)

Tabulku četností získáme tak, že v libovolném textu zjistíme počet jednotlivých znaků. Je ovšem důležité, aby byly zkoumány rozsáhlejší úseky textů, jedině tak získáme přesnější hodnoty četností. V krátkých úsecích nemusí obvyklá četnost platit. Například v textu *Tři sta třicet tři stříbrných stříkaček stříkalo přes tři sta třicet tři stříbrných střech* je frekvence znaků odlišná od obvyklé frekvence v českém jazyce.

Porovnáním četností znaků v kterémkoli otevřeném textu s frekvencí znaků v šifrovém textu dokáže luštitel zjistit, zda byla zpráva zašifrována pomocí substituce nebo transpozice. Pokud například bude v nějakém nám srozumitelném textu prvním nejpočetnějším písmenem E, druhým A, třetím O a v šifrovém textu jim budou přibližně odpovídat četnosti písmen P, N a T, pak je zřejmé, že písmeno E bylo při šifrování zaměněno za písmeno P, písmeno A za N a O za T. Jednalo by se tedy o substituční šifru. Jestliže ale budou znaky s odpovídajícími si četnostmi shodné, pak se bude jednat o transpozici. (Singh, 2009)

Po určení šifrovacího systému se pak kryptoanalytik snaží na základě znalosti častých bigramů, trigramů a zákonitosti střídání samohlásek se souhláskami objevit otevřený text zprávy.

1.5.2 Jednoduchá sloupcová transpozice

Prvním krokem při luštění textu, o kterém se kryptoanalytik domnívá, že byl zašifrován pomocí jednoduché sloupcové transpozice, je provedení frekvenční analýzy, z které nejen zjistí, v jakém jazyce je otevřený text zprávy napsán, ale také si ověří, zda se opravdu jedná o transpozici.

Luštitel také z frekvenční analýzy zjistí celkový počet znaků šifrového textu. Získané číslo rozdělí na součin dvou čísel, jedno číslo představuje počet sloupců a druhé počet řádků tabulky. Ze všech možných rozkladů čísla je vybrán ten nejpravděpodobnější a podle něho je sestavena tabulka.

Do tabulky je pak postupně po sloupcích vepsán šifrový text. Kryptoanalytik tabulku rozstříhá na jednotlivé sloupce a pak se snaží různým přeskupováním nalézt správné

pořadí sloupců tak, aby byl schopen v řádcích tabulky přečíst otevřený text zprávy. Při hledání správného pořadí využívá znalosti častých bigramů a trigramů daného jazyka. (Vondruška, 2006)

Popsaný postup luštění jednoduché sloupcové transpozice aplikujeme na konkrétní příklad. Naším úkolem bude rozluštit tento šifrový text:

NSITE AOATU EBEYO NITAI LESSO SESZA NEAIO **X**PLEL EYLYJ AOTHL JMD**X**M DIAEN UEMKV BEDKN P**X**IIA APEIT JVIEY AZKRC ODARA TYACD AAAAU AAVJT ZNEBZ AETPD RZTEO ADYLA TRDKH RNOKL SJCAE ETNOA VJSUE ODASF R**X**EED ELNMB AHDAI HBYM**X** ZKCPR SLTII NLTCP TMO

Nejprve provedeme frekvenční analýzu, tedy určíme absolutní či relativní četnost písmen a odtud zjistíme, že frekvence znaků šifrového textu jsou přibližně stejné jako frekvence znaků v českém jazyce. Navíc znaky s nejvyššími počty výskytu se také příliš neliší, a tedy na základě úvah z předešlé podkapitoly můžeme vyloučit substituci. Absolutní a relativní četnosti jednotlivých znaků jsou uvedeny v následující tabulce.

A	B	C	D	E	F	G	H	I	J	K	L	M
27	5	5	11	22	1	0	4	12	6	6	10	6
13,6	2,5	2,5	5,6	11,1	0,5	0	2	6,1	3	3	5,1	3
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
10	11	6	0	7	9	14	4	4	0	5	7	6
5,1	5,6	3	0	3,5	4,5	7,1	2	2	0	2,5	3,5	3

Z tabulky je zřejmé, že se v textu vyskytuje pětkrát písmeno X, které je pro český jazyk netypické. Budeme tedy předpokládat, že posledních pět sloupců tabulky bylo doplněno tímto znakem a v šifrovém textu ho vyznačíme tučně.

Z analýzy šifrového textu jsme také zjistili, že celkový počet znaků je 198. Toto číslo rozložíme na součin prvočísel: 198 = 2 x 3 x 3 x 11, abychom mohli určit rozměry tabulky. Získáme několik pravděpodobných možností rozměrů tabulky a to 9 x 22, 18 x 11 nebo 22 x 9, 11 x 18 (první číslo vždy udává počet sloupců). Ostatní možnosti nebudeme uvažovat, protože jsou velmi nepravděpodobné (například 2 x 99).

Nyní si všimneme umístění znaků X v šifrovém textu, ve většině případů je následující písmeno X od předchozího vzdáleno o 18 písmen, třetí a čtvrté X je od sebe vzdáleno o 90 písmen. Obě tato čísla, tedy 18 a 90, jsou násobky čísel 9 a 18, nikoli čísel 11 a 22. Můžeme tedy vyloučit tabulky o rozměrech 9 x 22 a 18 x 11.

Nyní vepíšeme po sloupcích šifrový text do zbylých pravděpodobných tabulek a u každé tabulky určíme poměr samohlásek a souhlásek v jednotlivých řádcích. Mělo by platit samohlásky / souhlásky = 40 / 60. (Vondruška, 2006)

Tabulka 22 x 9 s předpokládaným poměrem hlásek 8,8 / 13,2

NUASPAMKIVODJTDREUEHZI	9/13
SEIZLODVIIDATPYNEEEDKN	10/12
IBLAETIBAEAAZDLOTODACL	11/11
TEENLHAEAYRANRAKNDEIPT	10/12
EYSEELEDPAAAEZTLOALHRC	11/11
AOSAYJNKEZTUBTRSASNBSP	7/15
ONOILMUNIKYAZEDJVFMYLT	9/13
AISOYDEPTRAAAOKCJRBMTM	9/13
TTEXJXMXJCCVEAHASXAXIO	7/15

Tabulka 11 x 18 s předpokládaným poměrem hlásek 4,4 / 6,6

NAPMIOJDEEZ	5/6
SILDIDTYEEK	5/6
ILEIAAZLTDC	5/6
TELAARNANEP	5/6
ESEEPAETOLR	6/5
ASYNETBRANS	4/7
OOLUIYZDVML	5/6
ASYETAAHJBT	5/6
TEJMJCEKSAI	4/7
USAKVDTRUHI	4/7
EZOVIAPNEDN	5/6
BATBEADOOAL	6/5
ENHEYARKDIT	5/6
YELDAAZLAHC	5/6
OAJKZUTSSBP	3/8
NIMNKAEJFYT	4/7
IODPRAOCRMM	4/7
TXXXCVAAXXO	3/8

Z uvedených poměrů samohlásek a souhlásek je zřejmé, že nejvíce vyhovuje tabulka o rozměrech 11 x 18. Doplníme tedy do jednotlivých sloupců této tabulky šifrový text a tabulku po sloupcích rozstříháme. Sloupce budeme postupně přeskupovat tak, abychom v jednotlivých řádcích získali otevřený text. Můžeme při tom využít poznatku, že posledních pět sloupců bylo doplněno písmeny X. Práci si také usnadníme, pokud budeme vyhledávat pro češtinu typické bigramy a trigramy. Vznikne nám tabulka s následujícím pořadím sloupců.

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

Otevřeným textem tajné zprávy je úryvek z knihy Jiřího Janečka: *„Již od nepaměti, kdy se lidé začali dělit na přátele a nepřátele, se obě strany snažily domlouvat tak, aby se jejich tajemství druhá skupina nedozvěděla. Oba tábory také ihned začaly hledat způsob, jak se k tajným informacím dopracovat.“* (Janeček, 1998)

1.5.3 Fleissnerova otočná mřížka

Při luštění zprávy zašifrované pomocí Fleissnerovy mřížky opět nejdříve provedeme frekvenční analýzu, abychom zjistili jazyk otevřeného textu a zda se jedná o transpozici. Již jsme ale také v předchozích podkapitolách zjistili, že výsledky frekvenční analýzy jsou tím přesnější, čím je zkoumaný text delší, proto se nedoporučuje provádět analýzu u příliš krátkých textů. Výsledky by totiž mohly luštitele spíše zmást než mu pomoci.

Je důležité si uvědomit, že mřížka je symetrická a vždy se skládá z *n* x *n* políček (*n* je libovolné). Proto je tedy možné rozdělit šifrový text do řádků po *n* znacích. Vznikne nám tabulka o *n* řádcích a *n* sloupcích.

Dále také víme, že v mřížce je vystřižena vždy čtvrtina políček. Luštitel tedy může snadno určit počet znaků viditelných při každém otočení. Pavel Vondruška v časopise Crypto-World uvádí, že průměrně se v každém řádku vyskytuje jeden znak otevřeného textu. Na základě těchto poznatků se potom kryptoanalytik snaží hledat nějaký čitelný úsek otevřeného textu a svůj odhad si kontroluje tak, že otáčí mřížkou a zjišťuje, jaká slova by vznikla. Ze zbylých písmen dává dohromady další slova nebo úseky textu. Nakonec všechny úseky pospojuje a výsledkem je čitelný text zprávy. (Vondruška, 2004)

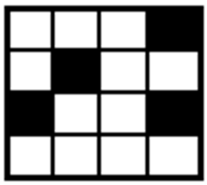
Uvedený postup luštění si ukážeme na jednoduchém příkladu. Naším úkolem je rozluštit obsah této zašifrované zprávy: EEZH DLJP EEAD RPMO.

Frekvenční analýzu v tomto případě provádět nebudeme, protože text je příliš krátký a údaje by byly nepřesné. Celkový počet znaků je 16, tedy víme, že byla použita tabulka 4 x 4. Šifrový text zapíšeme do řádků po 4 znacích.

```
E E Z H
D L J P
E E A D
R P M O
```

Víme, že v každé otočné mřížce je vystříhána čtvrtina políček, v našem případě tedy bude mít tabulka čtyři vystřižená okénka. Pomocí výše uvedených pravidel budeme ve vzniklé tabulce hledat čtyřmístné sekvence znaků, které dohromady dají čitelný text a jejich pozice umožní otáčení mřížky tak, aby byla využita všechna políčka. Svoje odhady zkontrolujeme otočením mřížky.

Mohlo by se například zdát, že čtyři písmena ZLED dávají dohromady čitelný úsek textu, avšak při otočení takto vzniklé mřížky o 90°, 180° a 270° nebude pokryta celá mřížka. Vyzkoušíme řadu znaků HLED, po otočení získáme skupinu písmen EJPO. Pokud tyto dvě skupiny spojíme, dostaneme text HLEDEJPO, z něhož jasně vidíme čitelné slovo *hledej*, můžeme tedy pokračovat v odhalování textu. Po dokončení otáčení získáme text HLED EJPO DPAR EZEM, který upravíme, a výsledkem je otevřený text tajné zprávy: Hledej pod pařezem. Na obrázku 8 je vyvedena podoba mřížky, kterou používali odesílatel a příjemce při tajné komunikaci.



Obrázek 8 – Hledaná otočná mřížka

Člověk, který šifruje zprávu pomocí otočné mřížky, by měl být obezřetný při výběru rozměrů tabulky. Jestliže se stane, že počet znaků zprávy je menší než je počet políček v mřížce, šifrant musí tabulku doplnit náhodnými znaky. Naneštěstí se nejčastěji pro doplnění zprávy používá znak X, který však případnému nepříteli hned odkryje některé pozice okének v mřížce. Nejvhodnějším způsobem šifrování je tedy najít správný rozměr mřížky, popřípadě zprávu doplnit od sebe odlišnými znaky.

2 PRAKTICKÁ ČÁST

V rámci praktické části bakalářské práce budou vytvořena makra v editoru jazyka Visual Basic for Applications v aplikaci Microsoft Excel. Úkolem těchto maker je usnadnění šifrování, dešifrování a luštění vybraných transpozičních šifer.

V první kapitole této části se krátce seznámíme s původem jazyka Visual Basic for Applications, jeho strukturou a využitím. V další kapitole budou již popsána jednotlivá vytvořená makra, jejich funkce a také návody pro práci s nimi.

2.1 Visual Basic for Applications

Visual Basic for Applications (dále jen VBA) je programovací jazyk, který je součástí kancelářské sady aplikací Microsoft Office (Word, Excel, Access …). Jeho základním stavebním kamenem je jazyk BASIC (**B**eginner's **A**ll-purpose **S**ymbolic **I**nstruction **C**ode), který byl určen pro výuku programování na univerzitách. (Walkenbach, 1999)

Obrázek 9 – Logo jazyka Visual Basic for Applications (převzato z wikipedia.org)

Každá aplikace Microsoft Office obsahuje objekty, se kterými VBA pracuje. Například v aplikaci Excel jsou objekty jednotlivé pracovní listy, tabulky, grafy apod. VBA umožňuje vytváření jednoduchých maker, která automaticky provádějí operace a činnosti, které by člověk musel opakovaně a zdlouhavě vykonávat ručně (např. výpočty prováděné na velkém množství dat, přeskupování buněk, úprava textů). Makra jsou sestavena z funkcí, procedur a formulářů a každá tato funkce nebo procedura obsahuje různé podmínky, cykly, příkazy a proměnné, které určují, co má uvedené makro provádět. Každý formulář obsahuje tlačítka, textová pole a další prvky potřebné k zadávání výchozích dat uživatelem.

2.2 Luštění transpozičních šifer s podporou počítače

Z názvu této kapitoly je patrné, že následující stránky bakalářské práce se budou týkat způsobu, jak usnadnit proces luštění, ale i šifrování a dešifrování transpozičních šifer využitím počítače. Za tímto účelem byla vytvořena makra, se kterými se podrobněji seznámíme v následujících podkapitolách.

V každé podkapitole bude uveden návod k obsluze příslušného makra, dále popis jeho funkce a struktury. Nejdůležitější funkce nebo části maker budou znázorňovány pomocí vývojových diagramů, které jsou součástí příloh.

2.2.1 Frekvenční analýza

S pojmem frekvenční analýza a s jeho úlohou jsme se seznámili již v předchozích kapitolách. Tedy víme, že počítání jednotlivých znaků textu pouze za pomoci tužky a papíru je zdlouhavé a velmi snadno se můžeme dopustit chyby. Využití počítače a aplikace Microsoft Excel umožňuje vytvoření makra pro rychlejší a snazší výpočet četností znaků.

Sešit s názvem *Frekvenční analýza* obsahuje makro, které po zadání nějakého textu uživatelem vypočítá absolutní a relativní četnosti znaků. Kliknutím na tlačítko „Provést analýzu!“ je vyvolán formulář, kam uživatel zadá požadovaný text. Po stisknutí tlačítka „OK“ se v tabulce umístěné v listu s názvem *Frekvenční analýza* zobrazí absolutní a relativní četnosti jednotlivých písmen zadaného textu. V tabulce se také pro porovnání nachází sloupec relativních četností typických pro český jazyk. (Havrlant)

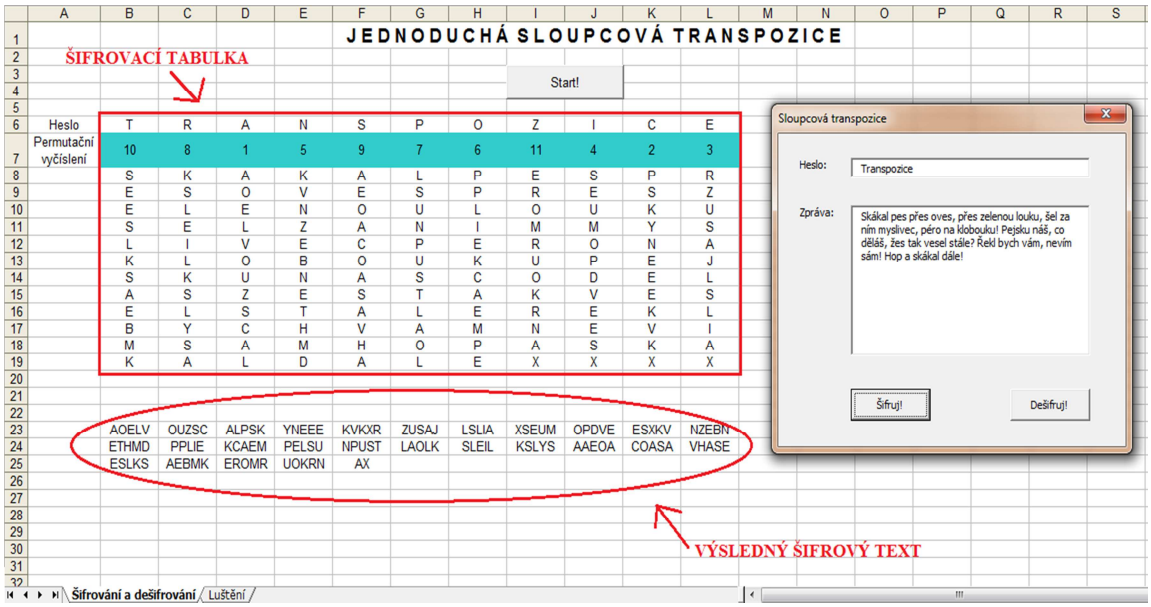
Tabulka obsahuje písmena mezinárodní abecedy, tj. bez diakritiky. Makro totiž před provedením analýzy upraví uživatelem zadaný text na tvar bez mezer a interpunkčních a diakritických znamének. Počet znaků takto upraveného textu se zobrazí v posledním řádku tabulky. Uživatel si však svůj text může připomenout v tabulce *Zkoumaný text*, kde se nachází jeho původní neupravený tvar, v jakém byl zapsán do formuláře.

Takto zpracované makro napomáhá uživateli při luštění šifer. Díky sloupci vzorových četností luštitel dokáže zjistit, zda je zpráva zašifrována transpozičním či substitučním systémem. Struktura funkce provádějící frekvenční analýzu je znázorněna vývojovým diagramem v příloze 1.

2.2.2 Jednoduchá sloupcová transpozice

V sešitu nazvaném *Jednoduchá sloupcová transpozice* se vyskytují dva listy. Makra v prvním listu převádí text nějaké zprávy pomocí sloupcové transpozice na zašifrovaný tvar, který pak dokáží i dešifrovat. Makro v druhém listu usnadňuje luštiteli práci při hledání otevřeného textu zprávy.

Pro šifrování textu sloupcovou transpozicí stačí uživateli kliknout v listu *Šifrování a dešifrování* na tlačítko „Start!“, čímž je vyvolán formulář, který vyžaduje zadání hesla a zprávy. Heslo musí mít minimálně pět znaků. Uživatel nemusí text zprávy ani heslo upravovat (tzn. odstraňovat diakritiku a interpunkční znaménka), úpravu totiž provede makro. Po stisknutí tlačítka „Šifruj!“ se v listu objeví šifrovací tabulka. V prvním řádku této tabulky je vypsáno heslo, ve druhém řádku najdeme permutační vyčíslení hesla (řádek je barevně odlišen) a pod ním je po řádcích vypsán otevřený text zprávy. Pod tabulkou je vypsán již výsledný šifrový text rozdělený do skupin po pěti znacích. Na obrázku 10 je zobrazen zmíněný formulář a šifrovací tabulka.



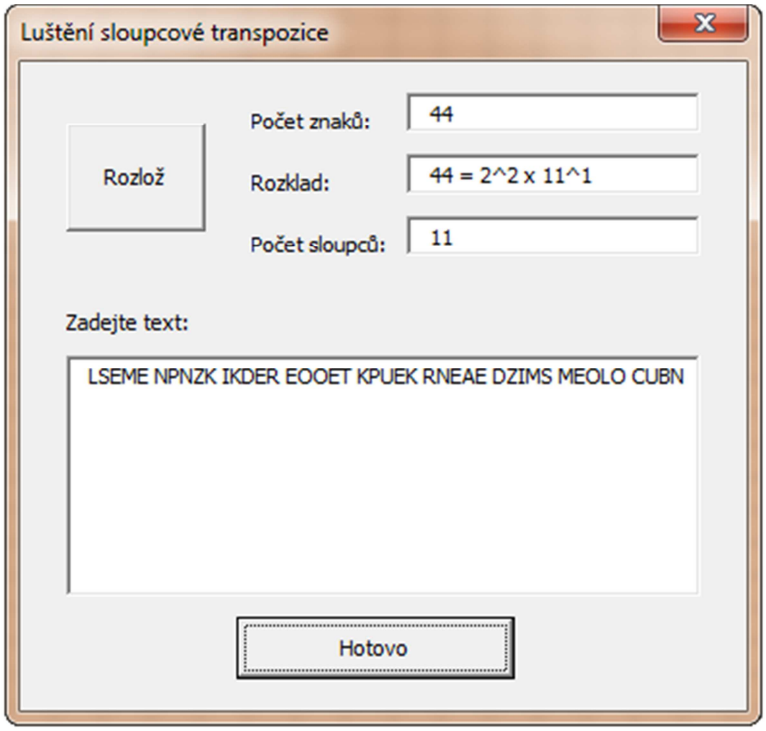
Obrázek 10 – Šifrování sloupcovou transpozicí pomocí makra

Pro dešifrování zprávy uživatel klikne opět na tlačítko „Start!“ a do zobrazeného formuláře napíše smluvené heslo a šifrový text zprávy. Tlačítko „Dešifruj!“ spustí dešifrování zprávy, v listu je tedy opět vytvořena tabulka, v jejímž prvním řádku se nachází heslo a ve druhém jeho permutační vyčíslení, které udává pořadí sloupců, do kterých je vepisován šifrový text. Pod tabulkou je vypsán otevřený text zprávy a je na uživateli, aby si text upravil do čitelné podoby, tzn. doplnil mezery a diakritiku.

V příloze 2 je vývojový diagram funkce, která provádí šifrování zprávy, tedy prochází jednotlivé sloupce a vypisuje z nich znaky podle pořadí, které bylo dáno permutačním vyčíslením. Funkce, která se podílí na dešifrování, je obdobná, liší se pouze tím, že znaky textu do sloupců podle daného pořadí zapisuje.

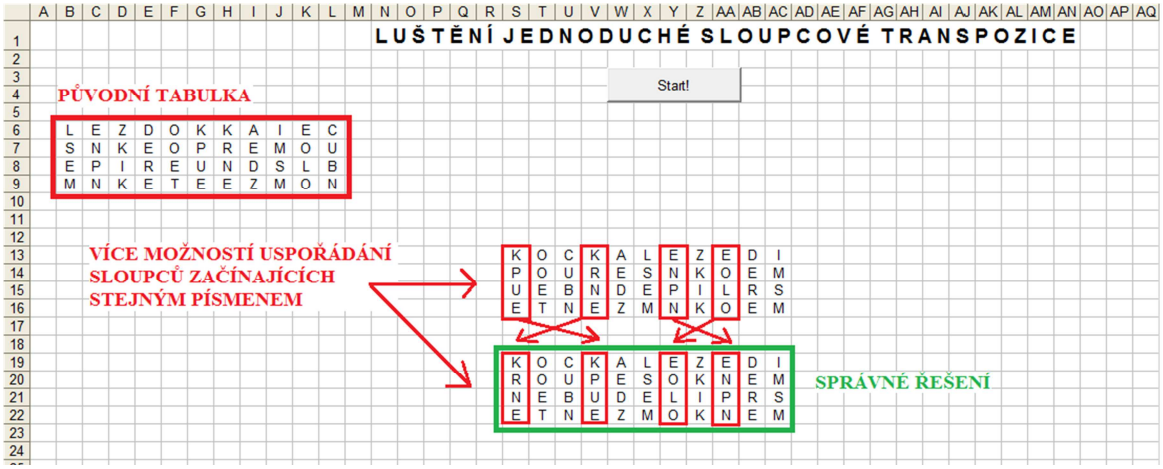
Nepostradatelnou součástí šifrování a dešifrování textů je permutační vyčíslení hesla. Funkce, která tento úkon provádí je znázorněna vývojovým diagramem v příloze 3. Funkce převede znaky hesla na hodnoty z ASCII tabulky a zkoumá, který znak má nejnižší hodnotu, potom jim podle toho přiřadí pořadí. Tato funkce pracuje již s upraveným heslem, to znamená, že heslo bylo zbaveno mezer a veškerých znamének.

Jak již bylo řečeno, sešit obsahuje dva listy. Druhý list je určen pro hledání otevřeného textu bez znalosti hesla. Potom, co uživatel provede frekvenční analýzu šifrového textu a zjistí, že se jedná o transpozici, klikne v listu nazvaném *Luštění* na tlačítko „Start!“. Objeví se formulář (viz obrázek 11), do kterého uživatel zapíše šifrový text a pak provede rozklad délky zprávy na prvočísla stisknutím tlačítka „Rozklad“. Po tomto kroku se ve formuláři vyplní políčka s celkovým počtem znaků zprávy a prvočíselným rozkladem. Z vypsaných prvočísel si uživatel sestaví hodnotu nejvhodnější pro počet sloupců tabulky a zapíše ji do příslušného políčka. Po stisknutí tlačítka „Hotovo“ je v listu vyrobena tabulka se zadaným počtem sloupců, do kterých je postupně vepsán text zprávy.



Obrázek 11 – Formulář pro luštění sloupcové transpozice

Luštitel se pak v tabulce snaží najít pravděpodobná slova nebo útržky slov hledaného otevřeného textu tak, že si jednotlivé sloupce tabulky kopíruje na libovolné místo v listu a mění jejich pořadí (viz obrázek 12). Pokud se rozměry tabulky jeví nesprávné, musí uživatel znovu zadat šifrový text do formuláře a zvolit jiný počet sloupců. Stejně by luštitel postupoval při ručním luštění, musel by však vyrobit několik tabulek, aby využil všechny pravděpodobné rozměry, a potom je ještě rozstříhat po jednotlivých sloupcích, což zabere spoustu času.



Obrázek 12 – Hledání otevřeného textu

2.2.3 Fleissnerova otočná mřížka

Za účelem šifrování, dešifrování a luštění textů pomocí Fleissnerovy mřížky byla vytvořena makra, která najdeme v sešitu *Fleissnerova otočná mřížka*. Sešit opět obsahuje dva listy, jeden zaměřený na šifrování a dešifrování a druhý na luštění.

V prvním listu se nachází dvě textové oblasti určené pro zadávaný a výsledný text. Do horní oblasti uživatel napíše otevřený nebo šifrový text podle toho, zda chce zprávu šifrovat nebo dešifrovat. Potom klikne na tlačítko „Návrh mřížky“ a v levé části se objeví čtverec složený z určitého počtu tlačítek (dále jen mřížka), který je dán délkou upraveného textu, tedy textu zbaveného mezer a interpunkčních znamének. Strana čtverce je omezena od 4 do 30 tlačítek, to znamená, že délka zprávy nesmí být delší než 900 (30 x 30) znaků. V opačném případě je uživatel upozorněn, že zpráva je příliš dlouhá, a je mu doporučeno text rozdělit na více částí a zašifrovat je samostatně.

Nezbytnou součástí šifrování a dešifrování je tvorba mřížky. Když uživatel klikne na některé z tlačítek mřížky, tlačítko se označí 0 a pozice po jeho otočení o 90°, 180° a 270° jsou v tomto pořadí označeny číslicemi 1, 2 a 3. Číslice 0 představuje vystřižené okénko. Pokud má mřížka lichý počet tlačítek, prostřední tlačítko je označeno křížkem. Jestliže uživatel klikne na tlačítko, které již bylo označeno (tzn. je popsáno nějakou číslicí), označení na těchto pozicích zmizí. Toho může uživatel využít tehdy, když není spokojen s uspořádáním „vystřižených“ okének v mřížce a chce je upravit (například dvě nuly vycházejí vedle sebe).

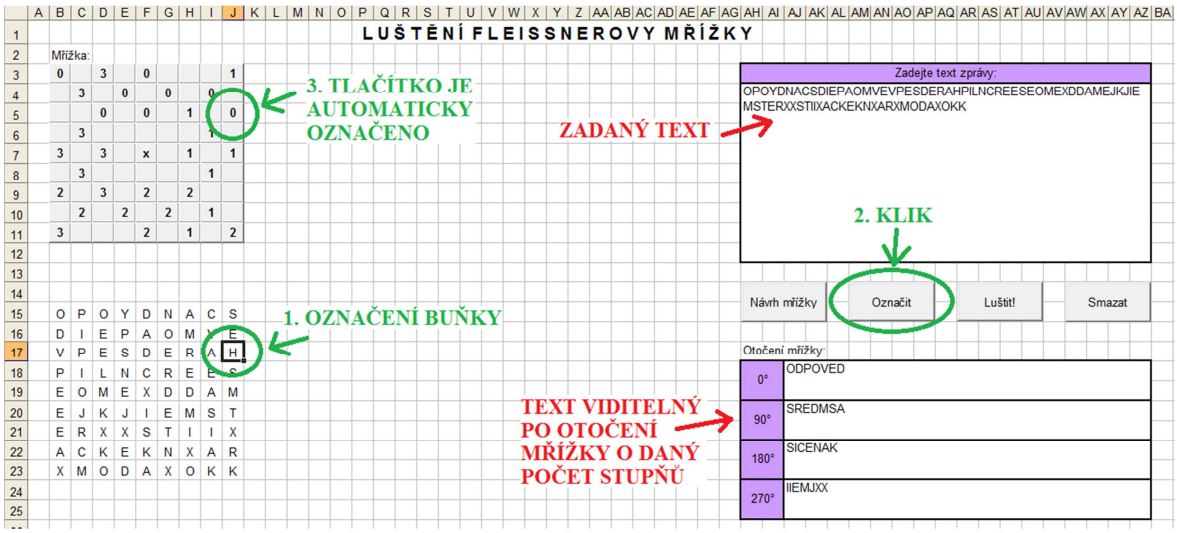
Dalším krokem po vytvoření mřížky je samotné šifrování, resp. dešifrování, které je spuštěno tlačítkem „Šifruj!“, resp. „Dešifruj!“. Mřížka však musí být zcela vyplněna číslicemi od 0 do 3, jinak je uživatel vyzván k doplnění mřížky. Po stisknutí jednoho z uvedených tlačítek je pod mřížkou vytvořen čtverec složený ze znaků zprávy (dále jen šifrovací čtverec). Pozice políček šifrovacího čtverce odpovídají pozicím jednotlivých tlačítek mřížky posunutým o tři řádky dolů. První část znaků zprávy je do šifrovacího čtverce zapisována na pozice, které odpovídají tlačítkům označených nulou, pozice dalších znaků odpovídají tlačítkům označeným jedničkou, atd. Jestliže je délka zprávy menší než počet okének v mřížce, zbylá políčka v šifrovacím čtverci jsou doplněna znakem X. Řádky vzniklého šifrovacího čtverce udávají již výsledný šifrový text, který je vypsán do textového pole s názvem *Výsledný text*. List obsahuje navíc ještě tlačítko „Smazat“, které smaže obsah obou textových oblastí, mřížku i šifrovací čtverec. Vše je pro lepší představu znázorněno na obrázku 13.

Obrázek 13 – Šifrování pomocí Fleissnerovy mřížky

Vývojový diagram v příloze 4 znázorňuje funkci, která provádí dešifrování zprávy, tedy vypisuje znaky šifrového textu do jednotlivých políček šifrovacího čtverce. Funkce nejdříve hledá tlačítka označená číslicí 0 a do políček odpovídajících těmto tlačítkům zapisuje znaky textu. Tento proces se opakuje celkem čtyřikrát, to znamená, že jsou vyhledávána postupně tlačítka označená 0, 1, 2 a 3. Znaky jsou zároveň ukládány a nakonec je celý řetězec vytištěn do odpovídající textové oblasti. Proces šifrování je téměř stejný, proto je zde uveden pouze diagram pro dešifrování.

Druhý list sešitu slouží uživateli k luštění různých textů a informací, u nichž nezná tvar šifrovací mřížky. Stejně jako v prvním listu i v tomto najdeme dvě textové oblasti a několik tlačítek. Druhá z oblastí je však rozdělena na čtyři díly podle stupňů otočení mřížky.

Pro zahájení procesu luštění je opět nutné zadat text do horního textového pole. Následuje kliknutí na tlačítko „Návrh mřížky“, po kterém se zobrazí odpovídající mřížka (rozměr mřížky je dán délkou textu) a pod ní šifrovací čtverec, ve kterém je po řádcích vypsán zadaný text. Pokud uživatel klikne na tlačítko „Luštit!“ před tím, než je vytvořena mřížka, zobrazí se mu chybová hláška a je vyzván k jejímu vytvoření.



Obrázek 14 – Postup označování tlačítek mřížky

Vytvořený šifrovací čtverec znaků tajného textu je dále zkoumán uživatelem, který v něm hledá případná slova nebo části slov. Aby si mohl uživatel svoje odhady ověřit, musí označit tlačítka mřížky, která odpovídají pozicím jednotlivých znaků, o kterých je uživatel přesvědčen, že tvoří slovo. Označení tlačítek může být provedeno dvěma způsoby. Uživatel buď přímo označí tlačítko v mřížce, které odpovídá políčku v šifrovém čtverci, nebo označí buňku, ve které se příslušný znak nachází, a klikne na tlačítko „Označit“. Odpovídající tlačítko se samo označí. Druhý postup je znázorněn zelenou barvou na obrázku 14. Po kliknutí na tlačítko „Luštit!“ jsou do dolní textové oblasti vyplněny znaky, které jsou viditelné po jednotlivém otočení mřížky. Tedy v poli 90° se nacházejí znaky, které odpovídají tlačítkům označených nulou, atd. Uživatel tentokrát není nucen označovat všechna tlačítka v mřížce, musí však počítat s tím, že vypsané znaky v odpovídající textové oblasti na sebe nebudou navazovat (tj. jestliže

v mřížce není označeno některé tlačítko, nemůže být vytvořen souvislý text). Pokud se tvar aktuální mřížky jeví jako nesprávný, uživatel může chybná tlačítka „odznačit“ a postup opakovat s novou mřížkou.

Pozor! V listu se opět nachází tlačítko „Smazat“, které se však chová stejně jako v listu předchozím. Není určeno pouze k mazání dolního textového pole, nýbrž k čištění celého listu! Obsah zmiňovaného pole je mazán automaticky při kliknutí na tlačítko „Luštit!“.

Aplikace byly odladěny pro Microsoft Excel 2003, proto autor nezaručuje korektní chování v jiných verzích tohoto programu.

Kód pro úpravu textů (odstranění mezer a znamének), který je využit ve všech zmiňovaných aplikacích, byl převzat z webu vedoucího této bakalářské práce. (Musílek, 2012)

Některá pravidla psaní příkazů a správné syntaxe jazyka VBA při tvoření veškerých maker byla čerpána z různých webových stránek a diskusí, které jsou uvedeny v seznamu literatury.

ZÁVĚR

Cílem bakalářské práce bylo podat základní informace o transpozičních šifrových systémech a využít počítač pro zjednodušení a zefektivnění práce s těmito systémy. Za tímto účelem byla v rámci praktické části bakalářské práce vytvořena jednoduchá makra, která jsou zaměřena na šifrování, dešifrování a luštění konkrétních transpozičních šifer, tedy jednoduchou sloupcovou transpozici a Fleissnerovu otočnou mřížku. Pro usnadnění luštění bylo také vytvořeno makro, které provádí frekvenční analýzu textu. Všechna tato makra byla zpracována v tabulkovém editoru Microsoft Excel, který je pro práci se zmíněnými šiframi nejvhodnější.

Bakalářská práce se skládá ze dvou částí. Cílem první teoretické části bylo seznámit čtenáře nejprve se základními pojmy z oblasti kryptologie, které je nutné znát pro správné pochopení a následné praktické využití šifrových systémů. V další kapitole této části je čtenář obeznámen se stručnými dějinami steganografie, kryptografie a kryptoanalýzy. Dále se také dozví několik informací o substitučních šifrách jakožto dalším druhu šifrových systémů. Nejrozsáhlejší část teoretické části je však věnována transpozičním šifrám a jejich principům šifrování a dešifrování a v neposlední řadě jsou uvedeny i způsoby luštění konkrétních šifrovacích systémů. Pro lepší pochopení a snazší představu byly jednotlivé systémy doplněny o praktické ukázky.

Pevně doufám, že po přečtení první části bakalářské práce bude čtenář schopen zašifrovat nebo dešifrovat nějaký text pomocí uvedených šifrových systémů nebo dokonce rozluštit nějakou tajnou zprávu pouze za použití tužky, papíru a nabytých znalostí.

Druhá část bakalářské práce má pak čtenáři tuto práci s šiframi usnadnit, neboť jsou v ní uvedeny návody k použití vytvořených aplikací. Jednotlivá makra byla napsána v programovacím jazyku Visual Basic for Applications, kterému se věnuje jedna z kapitol praktické části. Další kapitoly mají za cíl poučit čtenáře, jak daná makra fungují, jaké funkce byly použity při jejich tvorbě a jak má s jednotlivými aplikacemi pracovat. Pro lepší názornost byly některé funkce znázorněny pomocí vývojových diagramů. Čtenář po přečtení této části dokáže ovládat zmiňované aplikace a pomocí nich šifrovat, dešifrovat nebo luštit různé texty.

Ruční používání zmíněných šifrových systémů je mnohdy velmi zdlouhavé a náročné. Například výroba otočné mřížky zabere spoustu času, navíc podle zásad správného šifrování by každá mřížka měla být použita pouze jednou. U zpracovávání permutačního vyčíslení se zase šifrant může velmi snadno dopustit chyby, druhý účastník komunikace tak bude jen těžko hledat otevřený text zprávy. Nebo v případě rozsáhlého textu bude luštitel s velkými obtížemi počítat relativní četnost každého znaku. Proto věřím, že čtenáři, který se o šifry a s nimi spojenou problematiku zajímá, zpracované aplikace velmi pomohou, protože mu mimo jiné ušetří čas, hlavně však snižují riziko vzniku chyb v průběhu šifrování a s tím spojené narušení případné tajné komunikace.

Využití počítače při luštění nebo dešifrování má však i svou nevýhodu, která spočívá v hledání nebo úpravě otevřeného textu. Aby program samostatně upravil dešifrovaný text podle jednotlivých slov, vložil mezery na správná místa a doplnil diakritiku a interpunkční znaménka, musel by obsahovat velmi rozsáhlou databázi slov, podle níž by byl text upravován. Stejně tak jednotlivé úseky slov při luštění by musely být porovnávány se slovy z databáze. Z tohoto důvodu byla část práce při luštění a dešifrování přenechána uživateli.

Vytyčené cíle bakalářské práce byly splněny. Vytvořená makra mohou sloužit například při řešení úkolů v různých soutěžích zaměřených na transpoziční šifry. Pomocí programu *Frekvenční analýza* zase uživatel může provádět různé analýzy textů, apod. Makra mohou být také dobrým pomocníkem při řešení rébusů a šifer v populární celosvětové hře Geocaching.

SEZNAM OBRÁZKŮ

SEZNAM POUŽITÉ LITERATURY

Algoritmy.net: Příručka vývojáře. [online]. [cit. 2014-11-24]. Dostupné z: http://www.algoritmy.net/

BERGER, Roman. Lekce VBA. *Jak Programovat* [online]. 2012–2015 [cit. 2015-03-28]. Dostupné z: http://www.jakprogramovat.cz/lekce-vba

BIGGS, Norman L. *Codes: An introduction to information communication and cryptography*. 1. vyd. London: Springer, 2008. ISBN 978-1-84800-272-2

BITTO, Ondřej. *Historie kryptologie*. [online]. [cit. 2014-11-24]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003/xbitto.htm

BOWDEN, Mark. *Černý jestřáb sestřelen: Příběh moderní války*. 2. vyd. Praha: Academia, 2008. 363 s. ISBN 978-80-200-1602-7.

Claude Shannon. In: *Wikipedia: The free encyclopedia* [online]. [cit. 2014-12-07]. Dostupné z: http://en.wikipedia.org/wiki/Claude_Shannon

Crypto-World [online]. [cit. 2014-12-07]. Dostupné z: http://crypto-world.info/

Excel Easy: #1 Excel tutorial on the net [online]. 2010–2015 [cit. 2015-03-28]. Dostupné z: http://www.excel-easy.com/

HAVRLANT, Lukáš. Kryptografie a šifrování: Frekvenční analýza. In: *Matematika.cz* [online]. [cit. 2015-03-08]. Dostupné z: http://www.matematika.cz/frekvencni-analyza

JANEČEK, Jiří. *Gentlemani (ne)čtou cizí dopisy*. 1. vyd. Brno: BOOKS, 1998. 176 s. ISBN 80-85914-90-5.

KAJÍNEK, Milan. *Tajemství šifer - po stopách kryptografie a steganografie V*. [online] *The Epoch Times*. [cit. 2014-11-21]. Dostupné z: http://www.velkaepocha.sk/200807295638/Tajemstvi-sifer-po-stopach-kryptografie-a-steganografie-V.html

LASÁK, Pavel. *Jak na Excel: VBA v Excel* [online]. 2004–2015 [cit. 2015-03-28]. Dostupné z: http://office.lasakovi.com/excel/vba/

MSDN: The Microsoft developer network [online]. 2015 [cit. 2015-03-28]. Dostupné z: https://msdn.microsoft.com/en-US/

MUSÍLEK, Michal. *Informatika*. [online]. 2012 [cit. 2015-04-02]. Dostupné z: http://www.musilek.eu/michal/inf.html?menu=ict&lang=cz

MUSÍLEK, Michal. *Kapitoly z dějin informatiky*. 1. vyd. Univerzita Hradec Králové: Gaudeamus, 2011. 193 s. ISBN 978-80-7435-129-7.

MUSÍLEK, Michal. *Šifry a kódy*. [online]. 2012 [cit. 2015-04-02]. Dostupné z: http://www.musilek.eu/michal/sifry.html?menu=cc&lang=cz

One-time pad. In: *Wikipedia: The free encyclopedia* [online]. [cit. 2014-12-07]. Dostupné z: http://en.wikipedia.org/wiki/One-time_pad

PIPER, Fred; MURPHY, Sean. *Kryptografie: Průvodce pro každého*. 1. vyd. Praha: Dokořán, 2006. 158 s. ISBN 80-7363-074-5.

Scienceworld. [online]. [cit. 2014-11-24]. Dostupné z: http://www.scienceworld.cz/

SINGH, Simon. *Kniha kódů a šifer: Tajná komunikace od starého Egypta po kvantovou kryptografii*. 2. vyd. Praha: Dokořán a Argo, 2009. 382 s. ISBN 978-80-7363-268-7 (Dokořán) a 978-80-257-0144-7 (Argo).

TŮMA, Jiří. *Transpozice*. [online]. [cit. 2014-11-24]. Dostupné z: http://www.karlin.mff.cuni.cz/~tuma/ciphers/Sifry4.pdf

Vigenère cipher. In: *Wikipedia: The free encyclopedia* [online]. [cit. 2014-11-24]. Dostupné z: http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

Visual Basic for Applications. In: *Wikipedia: The free encyclopedia* [online]. [cit. 2015-03-20]. Dostupné z: http://en.wikipedia.org/wiki/Visual_Basic_for_Applications

VONDRUŠKA, Pavel. *Fleissnerova otočná mřížka: Nápověda pro řešitele soutěže 2004*. *Crypto-World*. 2004, roč. 6, 11/2004. [online] [cit. 2015-02-04] Dostupné z: http://crypto-world.info/casop6/crypto11_04.pdf

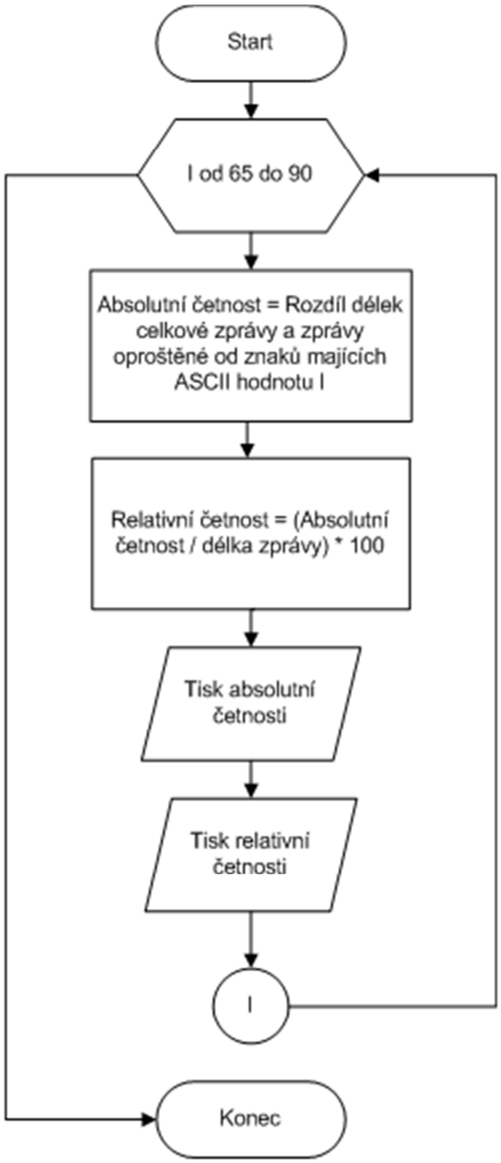
VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. 1. vyd. Praha: Albatros, 2006. 344 s. ISBN 80-00-01888-8.

WALKENBACH, John. *Microsoft Excel 2000 Programování ve VBA*. 1. vyd. Praha: Computer Press, 1999. 679 s. ISBN 80-7226-250-5.

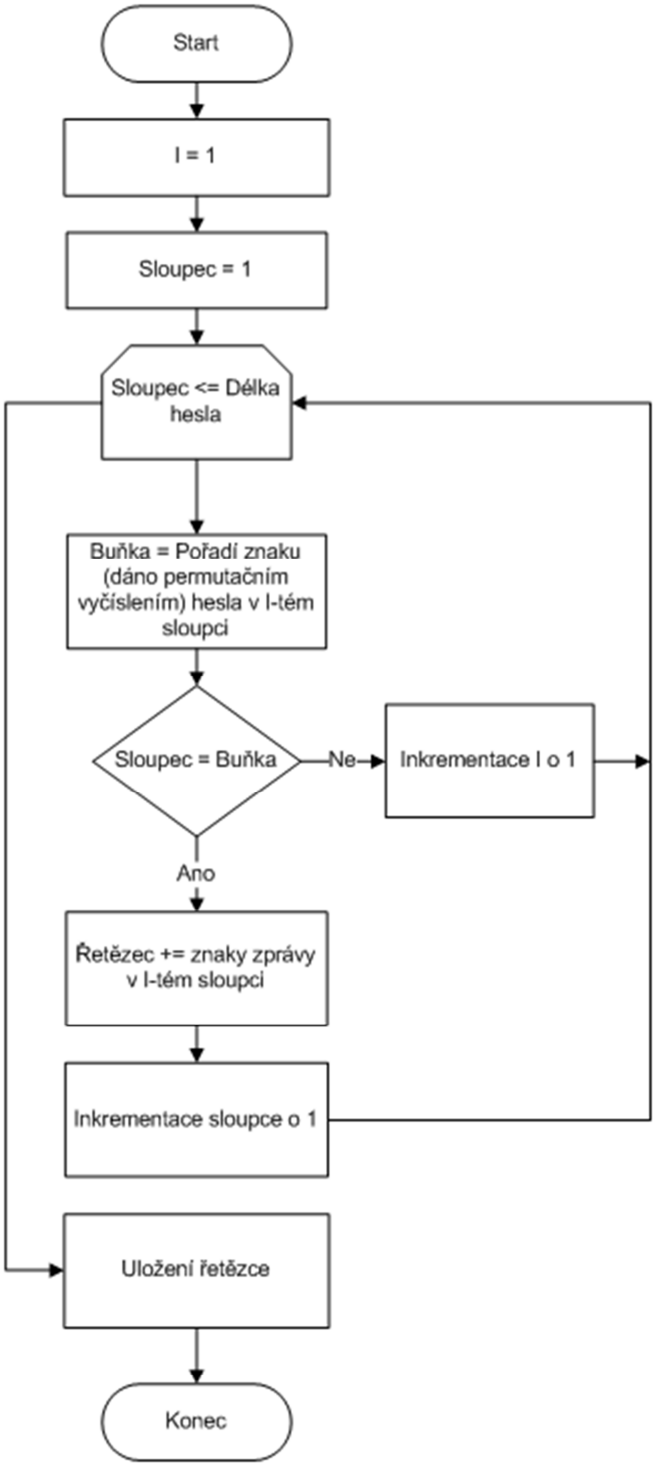
Wheel cipher. In: *Monticello* [online]. [cit. 2014-12-07]. Dostupné z: http://www.monticello.org/site/research-and-collections/wheel-cipher

SEZNAM PŘÍLOH

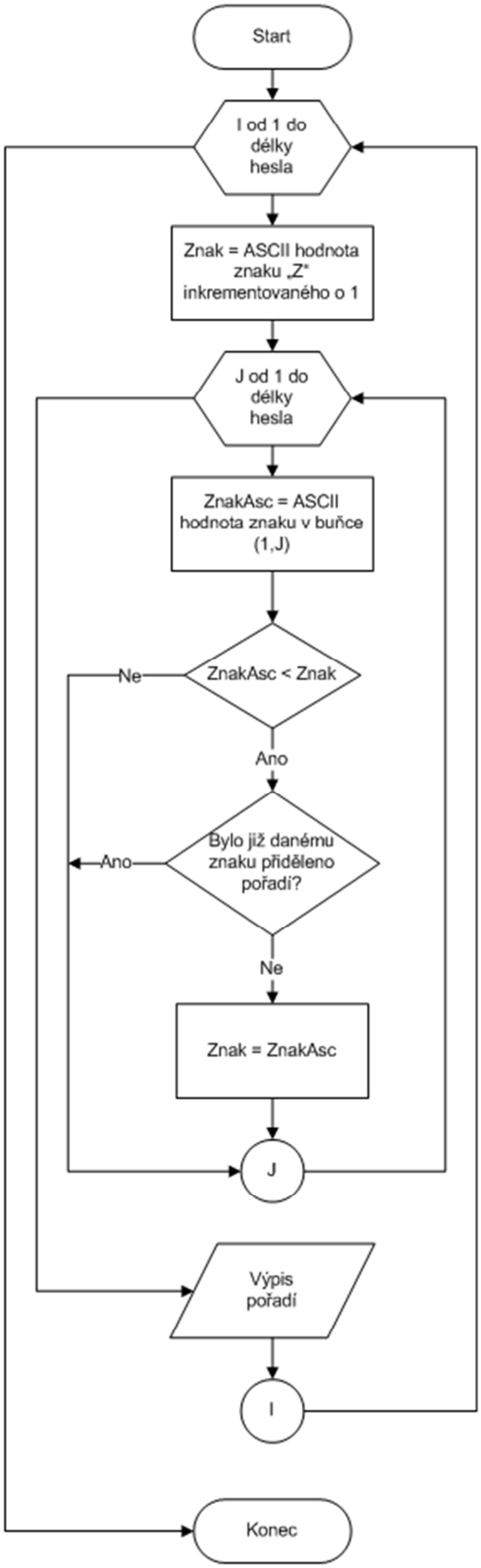
PŘÍLOHA 1 - Vývojový diagram frekvenční analýzy



PŘÍLOHA 2 - Vývojový diagram šifrování sloupcové transpozice



PŘÍLOHA 3 - Vývojový diagram permutačního vyčíslení hesla



PŘÍLOHA 4 - Vývojový diagram dešifrování pomocí Fleissnerovy mřížky