Kapitola 4

Transpozice

Jak jednoduchá záměna tak Vigenèrova šifra spočívají v permutování abecedy, v záměně písmen otevřeného textu písmeny jinými písmeny šifrového textu. Jednoduchá záměna používá pouze jednu permutaci abecedy a její řešení je proto založené na znalosti frekvence jednotlivých písmen v přirozeném jazyce. Vigenèrova šifra sice frekvence jednotlivých písmen změní, nicméně pokud je klíčové slovo mnohem kratší než délka šifrového textu, lze využít opakované trigramy a obecně delší polygramy k určení délky klíče a po jejím určení můžeme pak použít frekvence jednotlivých písmen v přirozeném jazyce k doluštění šifrového textu. *Transpoziční systémy* jsou založené na jiné myšlence. Ponechávají jednotlivá písmena otevřeného textu beze změny, pouze je přeházejí ve snaze přetrhat bigramové vazby. Šifrový text je tak nějakou přesmyčkou, permutací, otevřeného textu. Mohou se v něm proto vyskytovat delší úseky tvořené samohláskami případně souhláskami.

Z tohoto popisu transpozičních šifer také vyplývá, jak poznat, že při šifrování byla použita nějaká transpozice. Frekvence jednotlivých písmen v šifrovém textu odpovídá frekvenci stejných písmen v otevřeném textu. Je proto také zachován poměr samohlásek a souhlásek, který je v češtině zhruba 2:3.

Jednoduchá transpozice

Nejjednodušším příkladem transpoziční šifry je *jednoduchá transpozice*. Její podstata spočívá v tom, že otevřený text napíšeme do tabulky s předem známým počtem sloupců, zatímco počet řádků může být buď také pevně daný nebo může záviset na délce otevřeného textu. Začneme jednoduchým příkladem. Zvolíme tabulku se šesti sloupci. Počet řádků bude záviset na délce otevřeného textu. Počet sloupců je dán délkou nějakého předem smluveného hesla nebo klíče, které je známé pouze odesílateli a zamýšlenému

adresátovi. Naším klíčem bude slovo `OSLICE`. Tento klíč si napíšeme nad tabulku s textem.

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

Text nyní zašifrujeme tak, že jej adresátovi odešleme po sloupcích, jejichž pořadí je určené pořadím písmen klíče v abecedě. V případě našeho klíče je tedy pořadí sloupců 5-6-4-3-1-2. Šifrový text pak vypadá následovně.

```
ACUOH REPJC NESNH NTOSK AETNC AKENH ETSVV AISVT
SEENA AAKND ALSIC AABTO TDHAE EVLSJ RVNEE OPU
```

Zamýšlený adresát pak text snadno dešifruje. Zapíše jej do šesti sloupců, neboť šest je délka klíče. Protože délka celého šifrového textu je 78 znaků, bude mít každý sloupec 13 znaků. Začne prvním sloupcem podle klíče, tj. pátým sloupcem. Pak pokračuje šestým sloupcem, čtvrtým, třetím, atd.

Řešení jednoduché transpozice

Jakkoliv je jednoduchá transpozice skutečně jednoduchá šifra, její luštění úplně jednoduché není. Napřed musíme určit rozměr tabulky, tj. počet sloupců. Poté hledáme pořadí jednotlivých sloupců pomocí frekventovaných bigramů v jednotlivých řádcích. Začneme opět jednoduchým příkladem v angličtině.

Příklad 4.1 *Následující šifrový text byl vytvořen z anglického textu jednoduchou transpozicí s úplnou tabulkou. Najděte otevřený text.*

```
EGBRA VITIO DENTM NLFYE HILNA LTYEW EITER
```

Řešení. Určení rozměru tabulky je v tomto případě jednoduché. Počet písmen v šifrovém textu je 35, tabulka má proto buď pět nebo sedm sloupců. Vycházíme z předpokladu, že tabulka byla úplná, po napsání otevřeného textu byly všechny sloupce stejně dlouhé. To obecně nemusí být pravda, je to ale vhodný první předpoklad. Zkusíme tedy 5 sloupců. Šifrový text si napíšeme do pěti sloupců po sedmi písmenech:

E	T	M	I	E
G	I	N	L	W
B	O	L	N	E
R	D	F	A	I
A	E	Y	L	T
V	N	E	T	E
I	T	H	Y	R

Dále bychom mohli pokračovat tak, že si papír rozstříháme po sloupcích a zkoušíme postupně všechny možnosti. V případě pěti sloupců je pouze 120 možných permutací sloupců a tak je můžeme všechny vyzkoušet. Pokud se ale pokoušíme šifru vyřešit ručně, může být zkoušení všech možných permutací sloupců, tj. řešení hrubou silou, příliš časově náročné. Řešení si můžeme usnadnit tak, že hledáme v jednotlivých řádcích nejfrekventovanější bigramy v angličtině a napíšeme si pro každý takový bigram, které dva sloupce by musely být sousední, aby se takový bigram skutečně v otevřeném textu objevil.

Řádek	Bigramy	Z nich plynoucí sousední sloupce
1	ME, TI, ET	3-1 nebo 3-5, 2-4, 1-2 nebo 5-2
2	IN, WI, NG	2-3, 5-2, 3-1
3	BE, ON, LE	1-5, 2-4, 3-5
4	RI, DA, ID	1-5, 2-4, 5-2
5	AT, ET, EA	1-5, 2-5, 2-1
6	VE, NT	1-3 nebo 1-5, 2-4
7	IT, TH, HI	1-2, 2-3, 3-1

Některé dvojice sousedních sloupců jsou vzájemně v rozporu, napíšeme si ale ty nejčastěji se vyskytující.

1-5, 2-4, 3-1, 5-2.

Tyto dvojice sousedních sloupců naznačují pořadí sloupců 3-1-5-2-4. Přehážeme sloupce v poslední tabulce podle tohoto pořadí a dostaneme

M	E	E	T	I
N	G	W	I	L
L	B	E	O	N
F	R	I	D	A
Y	A	T	E	L
E	V	E	N	T
H	I	R	T	Y

□

Tento příklad byl velmi jednoduchý tím, že počet písmen v textu byl součinem dvou prvočísel a tak, díky informaci, že byla použita úplná tabulka, byly pro rozměry této tabulky pouze dvě možnosti. Při hledání vhodného rozměru tabulky v méně jednoduchých případech můžeme využít očekávaný poměr samohlásek a souhlásek v otevřeném textu příslušného jazyka. Také následující příklad jsem přebral od Mgr. Pavla Vondrušky.

Příklad 4.2 *Šifrový text byl vytvořen z českého textu jednoduchou transpozicí s úplnou tabulkou. Najděte otevřený text.*

```
OTSEC NCNUX ATONO TOUTO KXUJU AILBX
UVPTD HSEOL KYREN EPSUK ZELID RZPAU
```

Řešení. První krok spočívá v určení rozměrů tabulky. Číslo 60 lze rozložit jako součin dvou čísel několika způsoby. Některé rozměry tabulek ale můžeme ihned vyloučit, neboť pro ně by luštění bylo příliš jednoduché. Můžeme určitě vyloučit tabulky s jedním, dvěma, třemi nebo čtyřmi sloupci. V těchto případech je totiž snadné vyzkoušet ručně všechny možnosti pořadí sloupců. Budeme proto uvažovat tabulky s aspoň pěti sloupci. Jejich rozměry jsou (první je počet sloupců) 5×12, 6×10, 10×6, 12×5, 20×3, 30×2. Napíšeme si pro každý z možných případů text do tabulky tak, že postupně zaplňujeme sloupce. V každém řádku potom spočítáme poměr samohlásek a souhlásek a porovnáme jej s očekávaným poměrem pro daný rozměr

Rozměr 5×12, očekávaný poměr samohlásek a souhlásek je 2:3

Text	Poměr
ONATK	2:3
AUHKE	3:2
ZRTCT	0:5
OXIVS	2:3
YPEZS	2:3
NOUUL	3:2
PERSL	1:4
PEUNT	2:3
JBTOE	2:3
UIACX	3:2
OOUXD	3:2
LNKDU	1:4

Rozměr 6×10, očekávaný poměr samohlásek a souhlásek je 2,4:3,6

Text	Poměr
OAKUKZ	3:3
TTXVYE	2:4
SOUPRL	2:4
ENJTEI	3:3
COUDND	2:4
NTAHER	2:4
COISPZ	2:4
NULESP	2:4
UTBOUA	4:2
XOXLKU	2:4

Rozměr 10×6, očekávaný poměr samohlásek a souhlásek je 4:6

Text	Poměr
OCOTUUSRUD	5:5
TNNOAVEEKR	4:6
SUOKIPONZZ	4:6
EXTXLTLEEP	3:7
CAOUBDKPLA	4:6
NTUJXHYSIU	4:6

Rozměr 12×5, očekávaný poměr samohlásek a souhlásek je 4,8:7,2

ONATKAUHKEZR	5:7
TCTOXIVSYPEZ	4:8
SNOUULPERSLP	4:8
EUNTJBTOEUIA	7:5
CXOOUXDLNKDU	4:8

Rozměr 15×4, očekávaný poměr samohlásek a souhlásek je 6:9

OCUOOKUBPSKNULZ	6:9
TNXNUXAXTEYEKIP	6:9
SCAOTUIUDORPZDA	7:8
ENTTOJLVHLESERU	5:10

Rozměr 20×3, očekávaný poměr samohlásek a souhlásek je 8:12

OECXOTTXULUTSLREUEDP	8:12
TCNANOOUABVDEKEPKLRA	8:12
SNUTOUKJIXPHOYNSZIZU	8:12

Rozměr 30×2, očekávaný poměr samohlásek a souhlásek je 12:18

OSCCUAOOOTKUUIBUPDSOKRNPUZLDZA	13:17
TENNXTNTUOXJALXVTHELYEESKEIRPU	11:19

Podíváme-li se na poměry počtu samohlásek a souhlásek v jednotlivých řádcích u tabulek, vychází nám jako nejpravděpodobnější rozměr 20×3, dále pak 6×10, 30×2, méně pravděpodobný je rozměr 10×6 a jako nejméně pravděpodobné jsou rozměry 5×12 a 15×4.

Čím více sloupců je v tabulce, tím je obtížnější najít jejich správné pořadí. Při ručním řešení je proto lépe začít u těch nejvíce pravděpodobných rozměrů s těmi, které mají nejméně sloupců. V našem případě je to rozměr 6×10, který po prozkoumání frekvencí bigramů vede ke správnému pořadí sloupců 4-5-2-6-3-1, což nám dá otevřený text

UKAZKO
VYTEXT
PROLUS
TENIJE
DNODUC
HETRAN
SPOZIC
ESUPLN
OUTABU
LKOUXX

□

Tyto dva příklady luštění jednoduché transpozice ukazují, že nejde o příliš bezpečný šifrovací systém. Jakkoliv řešení hrubou silou je nepříliš praktické pro delší klíče, zkoumání bigramů vede k cíli pro všechny délky klíče, které jsou prakticky použitelné. Kryptografové se proto vždy snažili nějak zakrýt délku hesla, například psaním otevřeného textu do tabulek nepravidelných tvarů nebo jiným pravidlem zápisu otevřeného textu do tabulky obdélníkového tvaru. Jinou a podstatně spolehlivější úpravou jednoduché transpozice je

Dvojitá transpozice

Ta spočívá v tom, že šifrový text ještě jednou zašifrujeme jednoduchou transpozicí s použitím stejného nebo jiného hesla (a tím také pomocí stejné nebo jiné tabulky). Ukážeme si to na původním anglickém textu se schůzkou v pátek v půl dvanácté. Jako druhý klíč použijeme posloupnost 3-5-2-6-4-1. Šifrový text z Příkladu 4.1 tak zapíšeme

3	**5**	**2**	**6**	**4**	**1**
E	G	B	R	A	V
I	T	I	O	D	E
N	T	M	N	L	F
Y	E	H	I	L	N
A	L	T	Y	E	W
E	I	T	E	R	

V tomto případě není tabulka úplná, jedno písmeno není vyplněné. V případě neúplné tabulky je nutné, aby odesílatel i adresát byly předem domluveni na tvaru tabulky, tj. nejen na počtu sloupců, ale také na jejich délce. Tato délka může být pro jednotlivé sloupce různá. Jen tak je možné zajistit

jednoznačné dešifrování. Text z druhé tabulky opět zapíšeme po sloupcích v pořadí daném klíčem. Šifrový text po použití dvojité transpozice pak vypadá

```
VEFNW BIMHT TEINY AEADL LERGT TELIR ONIYE
```

Dvojitá transpozice s různými klíči, případně jednoduchá transpozice s tabulkou nepravidelného tvaru, není snadno rozluštitelná. Pro její luštění je třeba mít k dispozici několik šifrových zpráv. Narozdíl od jednoduché transpozice s úplnou tabulkou, kdy stačí mít k dispozici dostatečně dlouhý šifrový text a použít frekvenční tabulky bigramů v přirozeném jazyce. Pokud je ale k dispozici jak otevřený tak odpovídající šifrový text, je i dvojitá transpozice řešitelná, obsahují-li oba texty nějaká písmena s malou frekvencí, která umožní určit některé odpovídající si dvojice písmen v otevřeném a šifrovém textu. Ani v tom případě ale není řešení jednoduché. Pokud si kryptoanalytik může zvolit otevřený text, který bude zašifrován, zvolí si pokud možno text, který obsahuje každé písmeno pouze jednou. Například

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

To mu umožní odhalit, které transpozice sloupců byly použity. V každém případě první úkol kryptoanalytika spočívá v nalezení délek klíčů. Dokud se mu to nepodaří, nemůže šifrový text rozluštit. Při nepříliš častém použití k šifrování zpráv, které mají nižší stupeň utajení, je dvojitá transpozice, při které se klíče navíc pravidelně mění, celkem použitelná. Pro pravidelné použití a k ochraně zpráv s vysokým stupněm utajení je ale nepřijatelná.

Obecně o dvojité transpozici

Dvojitá transpozice za normálních okolností zvýší bezpečnost, cenou ale je nebezpečí, že klíče budou použité v opačném pořadí. To vede k obecné otázce zdali šifrování jedné zprávy za použití dvou nebo více šifrovacích systémů zvýší bezpečnost přenášených zpráv. Na tuto otázku neexistuje jednoduchá odpověď, neboť ta závisí na použitých šifrovacích systémech. Tak například ničemu nepomůže použít dvakrát jednoduchou záměnu, neboť výsledkem je zase pouze jednoduchá záměna. Navíc použití dvou systémů s sebou nese nebezpečí, že budou použity v opačném pořadí. V takovém případě je vytvořen jiný šifrový text. To bude vadit příjemci zprávy, který po dešifrování dostane nesrozumitelný text. Pokud si vyžádá nové odeslání zprávy a kryptoanalytik zjistí, že má k dispozici dvě zašifrované verze téže zprávy, může to vést k jejímu rozluštění. Historie kryptologie zná takové případy.

Pokud se někdo rozhoduje, má-li zvýšit bezpečnost přenášených zpráv použitím dvou nebo více šifrovacích systémů, musí si odpovědět na několik otázek.

1. Zvýší se skutečně bezpečnost nového systému?
2. Pokud je šifrování a dešifrování prováděno ručně, nebude nový systém příliš pracný?
3. Pokud jsou šifrovací systémy použity v nesprávném pořadí, zvýší se kryptoanalytikova šance na rozluštění zprávy?

Další příklady šifer

Všechny příklady šifer, které jsme si dosud uvedli, zaměňují jedno písmeno nějakým jiným písmenem. To samozřejmě není jediná možnost. Lze například zaměnit písmeno za dvojici písmen pomocí následující tabulky. V této tabulce je zapsáno 25 písmen, vynecháno je písmeno `X`, které v případě potřeby můžeme v otevřeném textu nahradit bigramem `KS`.

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

Šifrování probíhá tak, že každé písmeno otevřeného textu najdeme v tabulce a nahradíme jej v šifrovém textu dvojicí písmen, která označují řádek a sloupec, ve kterém příslušné písmeno leží. Tak například písmeno `H` nahradíme bigramem `BC`. Výsledný šifrový text má proto dvojnásobnou délku oproti původnímu otevřenému textu. Tak například

```
VESELE VANOCE
```

zašifrujeme jako

```
EBAED DAECB AEEBA ACDCE ACAE
```

V této podobě jde o velmi slabou šifru jejíž bezpečnost lze o něco zvýšit tak, že abecedu v tabulce přeházíme a poté použijeme nějakou transpozici. Prvního z těchto cílů můžeme částečně dosáhnout pomocí klíčového slova, které napíšeme na začátek tabulky a ostatní místa tabulky pak doplníme zbývajícími písmeny abecedy. Například heslo `UTERY` vede k následující tabulce.

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

Přání `VESELE VANOCE`

pomocí takto upravené tabulky zašifrujeme jako

`ECACE BACDA ACECB ADCDD BCAE`

a poté uděláme transpozici v pořadí 5-1-4-2-3. Jeden sloupec je kratší, odesílatel i adresát musí být domluveni předem, že to bude sloupec s číslem 5. Z tabulky

5	1	4	2	3
E	C	A	C	E
B	A	C	D	A
A	C	E	C	B
A	D	C	B	D
	B	C	A	E

tak dostaneme šifrový text

`CACDB CDCBA EABDE ACECC EBAA`

Tímto způsobem se nám podařilo zpřetrhat všechny bigramové vazby. Stále je ale vidět, že šifrový text obsahuje pouze 5 písmen a lze tedy odhadnout, že byla použita šifra, která nahrazuje jednotlivá písmena pomocí dvojic písmen-bigramů. Tomu ale snadno odpomůžeme tak, že použijeme původní tabulku, pomocí které jsme náhradu monogram-bigram dělali, ke zpětné náhradě bigramů pomocí jednotlivých písmen. Pro každý bigram najdeme řádek a sloupec, které písmena bigramu označují (v tomto pořadí!) a nahradíme tento bigram písmenem, které leží v příslušném řádku a sloupci. Například první bigram `CA` nahradíme písmenem `G`, které leží v řádku `C` a sloupci `A`. Z přání `VESELE VANOCE` po zašifrování dostaneme

`GJCNA QDQKI SU`

Tímto způsobem zakryjeme použitou šifru. Vztah mezi jednotlivými písmeny otevřeného a šifrového textu je dosti komplikovaný. Transpozice uvnitř

postupu je podstatná, protože bez ní bychom opakovaným použitím tabulky pro převod bigramů na monogramy dostali zpět původní otevřený text. Tuto šifru můžeme zkráceně označit **MBTM-šifra**, neboť šifrování probíhá způsobem

monogram-**b**igram-**t**ranspozice-**m**onogram.

Šifry tohoto typu byly používány jak vrchním velením německé armády během první světové války tak japonskou armádu v průběhu druhé světové války. Rozluštění japonské šifry, známé jako JN40, v listopadu 1942 mělo velký vliv na další průběh války v Tichomoří.