2. PŘEHLED KLASICKÝCH ŠIFROVÝCH SYSTÉMŮ

ATBAŠ-ALBAM-ATBAH

Tyto systémy vynalezli a prokazatelně používali hebrejci. Z hlediska konstrukce šifry jsou všechny tři systémy jednoduché substituce, kde šifrová abeceda používá znaky otevřené abecedy. Vztah mezi otevřenou a šifrovou abecedou není zcela „náhodný“, ale je dán určitými pravidly, která umožňují sestavit příslušné převodové tabulky. Ve všech třech případech je zachován princip vzájemné záměny, tj. je-li šifrový znak X záměna otevřeného znaku Y, pak také platí, že šifrový znak Y je záměna otevřeného znaku X.

ATBAŠ

Šifra spočívá v tom, že se vezme písmeno, spočítá se jeho vzdálenost od začátku abecedy, a nahradí se písmenem, které se nachází v téže vzdálenosti od konce abecedy. Podle popsaného postupu dostala šifra také své jméno atbaš, neboť první písmeno hebrejské abecedy je *alef* a je nahrazeno posledním písmenem *tav,* druhé písmeno *bet* se nahrazuje předposledním písmenem hebrejské abecedy – *šin* atd.

Pro mezinárodní abecedu by podle tohoto pravidla vypadala převodová tabulka takto:

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

(kde OT používáme k označení otevřené abecedy a ŠT k označení šifrové abecedy)

Vzhledem k principu vzájemné záměny otevřeného a šifrového znaku abecedy se převodová tabulka často uvádí ve zkráceném tvaru:

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

V případě použití hebrejské abecedy by vypadala převodová tabulka šifry atbaš tak, jak je uvedeno na obrázku. Znaky v tabulce jsou seřazeny podle toho, jak se píše v hebrejštině, tj. zprava doleva:

11	10	9	8	7	6	5	4	3	2	1
כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
12	13	14	15	16	17	18	19	20	21	22

Příklad použití:

```
Otevřený text  OKO ALBATROS
Šifrový text   LPL ZOYZGILH
```

ALBAM

Jedná se o obdobný systém jako atbaš, ale pravidla pro převod znaků otevřeného textu na šifrový znak jsou tvořena jiným způsobem. Hebrejská abeceda byla rozdělena na dvě poloviny, kde se první písmeno první poloviny nahrazovalo prvním písmenem druhé poloviny, druhé písmeno první poloviny nahrazovalo druhé písmeno druhé poloviny. Tedy prvé písmeno abecedy *alef* nahrazuje první písmeno druhé poloviny *lamed* a opačně, *beth* nahrazuje druhé písmeno druhé poloviny *mem* atd. V mezinárodní abecedě by to odpovídalo A = N, B = O, C = P….

Převodová tabulka sestavená dle tohoto pravidla by pro mezinárodní abecedu vypadala takto:

```
OT:  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
ŠT:  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
```

Převodová tabulka se dá vzhledem k principu vzájemné záměny převodu mezi otevřeným a šifrovým znakem uvést v následujícím zkráceném tvaru:

```
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
```

Příklad použití:

```
Otevřený text  OKO ALBATROS
Šifrový text   BXB NYONGEBF
```

ATBAH

Tak jako dva předchozí, definuje tento systém vzájemný převod mezi znaky otevřeného textu a šifrového textu. Systém se opírá o hebrejské číslovky, které se podobně jako římské číslovky psaly pomocí písmen hebrejské abecedy. Prvních 9 písmen hebrejské abecedy bylo šifrováno tak, že se písmena očíslovala od 1 do 9 a nahradila znakem, jenž měl pořadové číslo odpovídající doplňku čísla do 10. Tudíž *alef,* první písmeno, se nahradilo *teth,* které je v pořadí deváté a opačně. Dalších 9 písmen substituce bylo nahrazeno obdobným způsobem, byly doplněny do hebrejské číslice 100. V desítkové soustavě by to znamenalo, že by se dělal doplněk do čísla 28. Tudíž *mem,* třináctě písmeno, a *samekh,* písmeno patnácté, se vzájemně nahrazují. V naší abecedě by toto odpovídalo A = I, B = H, C = G, D = F, …. H = B, I = A, J = R, K = Q, ….. Q = K, R = J. Co by se stalo se znaky, které by odpovídaly číslům od 19 výše, není jasné.

Převodová tabulka sestavená podle tohoto neúplného pravidla by pro mezinárodní abecedu vypadala následovně:

```
OT:  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
ŠT:  I H G F N D C B A R Q P O E M L K J
```

Aby mohla být převodová tabulka používána i pro zbývající znaky, vžilo se následující doplnění, které zachovává vzájemnou záměnu znaků otevřeného textu a šifrových znaků:

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

Takto upravená a doplněná převodová tabulka se dá vzhledem k principu vzájemné záměny mezi otevřeným a šifrovým znakem uvést v následujícím zkráceném tvaru:

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

Příklad použití:

```
Otevřený text  OKO ALBATROS
Šifrový text   MQM IPHIYJMZ
```

Polybiův čtverec

Řecký historik Polybios vynalezl kódový systém vhodný pro signalizaci. Seřadil písmena do čtverce a jednotlivé řady a sloupce očísloval. Každé písmeno lze kódovat pomocí dvou čísel – číslem řady a číslem sloupce. Polybios doporučoval, aby tato čísla byla předávána pomocí pochodní. Např. písmeno v prvém řádku a pátém sloupci by bylo odesláno pomocí jedné pochodně v levé ruce a pěti pochodní v pravé ruce. Zprávy tak mohly být odeslány bezpečně a rychle na velké vzdálenosti.

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

Šifra se z tohoto kódu stane, pokud písmena nejsou ve čtverci vepsána abecedně, ale utajeně – tedy způsobem, který je znám pouze odesílateli a příjemci. Dohoda na obsahu čtverce může probíhat různě. Buď si obě strany vymění celý čtverec s vepsanou abecedou nebo (což byl běžnější způsob) se pouze dohodnou na klíči. Klíčem je nějaké slovo, pomocí kterého se potom vytvoří obsah čtverce. Slovo se nejprve vepíše do prvních políček čtverce (pokud se v hesle některé písmeno opakuje, pak se použije pouze poprvé) a zbytek čtverce se doplní zbývajícími znaky abecedy, a to v abecedním pořadí. Vzhledem k tomu, že mezinárodní abeceda má 26 znaků a čtverec má 25 pozic, je zvykem dva nejméně používané znaky sloučit do jedné buňky. V anglic-

kém jazyce se slučuje I a J, v českém jazyce to může být např. X a Y, jak je uvedeno v našem příkladu.

Takto konstruovaný šifrový systém je klasickým představitelem **digrafické šifry.** Tedy šifry, kdy je každý znak otevřené abecedy nahrazen dvojicí znaků šifrové abecedy. Současně se lze na tuto šifru dívat jako na jednoduchou záměnu, kde abeceda šifrového textu je tvořena 25 hodnotami čísel (11, 12, .. , 15, 21, 22, … ,25, …, 51, …55).

Polybiův čtverec, který umožňuje převod písmen na číslice, se stal základem mnoha dalších šifrových systémů.

Příklad

Heslo: PAVEL

Převodová tabulka sestavená pomocí hesla PAVEL

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

Otevřený text: KNIHA ŠIFER

Šifrování: K = 34 (souřadnice řádku a sloupce, kde je písmeno uvedeno v převodové tabulce), atd.

Šifrový text: 34 41 32 31 12 45 32 24 14 44

Šifra ťuk-ťuk (knock cipher)

Tento šifrový systém snad pochází původně z věznic carského Ruska, kde jej používali vězňové z řad anarchistů. Jeho použití popisuje i Alexander Solženicyn ve slavné knize *Souostroví Gulag*. Šifra se rozšířila postupně do věznic celé Evropy. Jak vypadá? Je založena na využití upraveného Polybiova čtverce. Vězňové se dohodnou na převodové tabulce. K sestavení tabulky se používalo domluvené heslo. V případě ruských anarchistů měla tabulka 6 řádků a 6 sloupců, neboť ruská abeceda má více znaků než mezinárodní abeceda. Zpráva se z cely do cely předává ťukáním na stěnu. Odtud její název. Nejprve se vyťukávají řádkové souřadnice písmene a potom sloupcové souřadnice. Tento způsob komunikace byl poměrně pomalý a pracný.

Na závěr malá ukázka – vyťukání zašifrovaného slova OKO (k převodu použita tabulka z minulého příkladu):

ťuk-ťuk-ťuk-ťuk ťuk-ťuk ťuk-ťuk-ťuk ťuk-ťuk-ťuk-ťuk ťuk-ťuk-ťuk-ťuk ťuk-ťuk

Caesarova šifra

Jedná se o dva tisíce let starý šifrový systém, který bezesporu patří mezi nejznámější šifrové systémy vůbec. Zavedení šifry se připisuje římskému císaři Caesarovi. Známý životopisec Suetonius popisuje, jak jím zavedený systém přesně vypadal. Každé písmeno zprávy bylo zaměněno za písmeno, které leželo o tři místa dále v abecedě. Z konce abecedy se přejde opět (cyklicky) na začátek abecedy. Z hlediska zařazení mezi šifrové systémy se jedná o jednoduchou záměnu. Systém nemá klíč. Klíčem by mohlo být např.

různé posunutí šifrové abecedy vůči abecedě šifrové. Znamená to, že pokud neoprávněná osoba jednou zjistí, že je používána ke komunikaci Caesarova šifra a jak je konstruována (např. vyluští konkrétní zprávu), pak snadno dešifruje všechny následující zprávy. Jedná se tedy o tzv. omezený algoritmus **(restricted algorithm).**

Způsob šifrování si předvedeme na následujícím otevřeném textu – citátu S. Branta: *Mundus vult decipi.* (Svět chce být klamán)

Otevřený text se nejprve přepíše do mezinárodní abecedy:
MUNDUS VULT DECIPI SVET CHCE BYT KLAMAN

Caesarova šifra																									
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
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

A potom se každé písmeno zprávy zamění za písmeno, které leží o tři místa dále v abecedě. K záměně lze také s výhodou použít převodovou tabulku.

Dostaneme následný šifrový text (Caesarův systém):
PXQGXV YXOW GHFLSL VYHW FKFH EBW NODPDQ