Pracovní list číslo 3: Polygrafické substituce

Další možností, jak zvýšit bezpečnost substituce, je aplikovat substituci nikoli na jednotlivá písmena, ale na větší bloky písmen. Stejný blok nového textu se sice vždy zobrazí na stejný blok šifrovaného textu, ale protože bloků je daleko více než písmen, je frekvenční analýza podstatně náročnější. Uvedeme si zde tři šifry tohoto typu: Playfair, bifid a hillovu šifru. Tyto šifry jsou již technicky náročnější, zejména výklad Hillovy šifry vyžaduje základní znalost lineární algebry.

Šifra Playfair

Z praktických důvodů se myšlenka substituce větších bloků uplatnila hlavně pro digramy (dvojice písmen). Protože diagramů je již poměrně hodně (26 x 26 = 676), nastává problém se zapamatování zvolené substituce. Přímočarým řešením je mít slovník digramů, který bude udávat substituci pro každou dvojici. Toto řešení však nese klasické nevýhody spojené s existencí psaného klíče. Jak udělat substitucí digramů pomocí snadno zapamatovatelného klíče, řeší šifra *Playfair*. Autorem této šifry je sir Charles Wheeeatstone. Lyon Playfair, po kterém je pojmenována, pouze prosazoval její používání.
Šifra Payfair je založena na substituci digramů. Klíčem k této šifře je tabulka 5 x 5, která obsahuje všechna písmena (používáme abecedu se sjednocenými písmeny *i* a *j*). Zprávu rozdělíme na dvojice písmen. Pokud některou dvojici tvoří dvě stejná písmena, vložíme mezi ně písmeno *x*. Pokud je počet písmen lichý, doplníme na konec písmeno *x*. Každou dvojici písmen nyní zakódujeme následovně:

- Pokud se obě písmena nacházejí v tabulce na stejném řádku, každé se nahradí písmenem ležícím o jedno napravo. Pokud je písmeno úplně vpravo, nahradí se prvním písmenem na tomto řádku.
- Pokud se obě písmena nacházejí v tabulce ve stejném sloupci, každé se nahradí písmenem ležícím o jedna dolů. Pokud je písmeno úplně dole, nahradí se prvním písmenem v tomto sloupci.
- Pokud se písmena nacházejí v různých řádcích i sloupcích, pak se každé nahradí písmenem, které leží na stejném řádku, avšak ve sloupci, kde leží druhé písmeno z dvojice. Pokud si představíme obdélník vytyčený nešifrovanými písmeny, pak zašifrovaná písmena jsou zbylé dva vrcholy obdélníku.

Ukažme si, jak se pomocí šifry Playfair zašifruje „Dočkej času jako husa klasu“ s klíčem „Petrklíč“. Z klíče vyrobíme šifrovací tabulku standartním způsobem – nejdříve napíšeme písmena klíče a pak doplníme v abecedním pořadí všechna zbývající písmena. S pomocí této tabulky text zašifrujeme následovně.

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

do	ck	ej	ca	su	ja	ko	hu	sa	kl	as	ux
FN	BT	IF	AB	UN	CB	EU	MS	YH	PB	HY	QZ

Mgr. Irena HENCOVÁ, MBA, LL. M. 725 037 081
irena.hencova@ddmporuba.cz

O kvalitě této šifry svědčí její používání až do druhé světové války. Inspirovala také několik podobných šifer založených na digramech, které na jednu stranu používají více šifrovacích abeced pro zlepšení bezpečnosti a na druhou stranu mají jednodušší pravidla než Playfair. Příkladem takové variace je šifra „čtyř čtverců“. Dva z čtverců se používají pro nalezení písmen holého textu, další dva pro nalezení odpovídajících šifrovaných písmen.

Šifra bifid

I s pomocí jednoho čtverce však můžeme provádět polygrafickou substituci na delších skupinách písmen. K tomu slouží šifra *bifid*, jejímž autorem je Felix Delastelle; byla vytvořena kolem roku 1901. Opět si vezmeme čtverec 5 x 5 polí a očíslujeme řádky i sloupce čísly 1 až 5. Pak rozdělíme zprávu na skupinky pevné délky, řekněme po pěti písmenech. Pod každé písmeno napíšeme pod sebe řádkovou a sloupcovou souřadnici:

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

d	o	c	k	e		j	c	a	s	u		j	a	k	o	h		u	s	a	k	l		a	s	u
3	4	2	1	1		2	2	2	4	4		2	2	1	4	3		4	4	2	1	2		2	4	4
1	2	3	5	2		2	3	4	4	5		2	4	5	2	4		5	4	4	5	1		4	4	5

Nyní v rámci každé skupiny přepíšeme čísla po řádcích. Potom tato čísla rozdělíme do dvojic a pomocí tabulky přepíšeme zpět na písmena.

3421112352 2224423445 2214324524 4421254451 244445
H L P C W I A O H U I R F U I S L B S V A SU

Podobná je šifra *trifid* od stejného autora. Trifid používá tříčíselné kódy z čísel 1, 2, 3, která kódují písmena v trojrozměrné tabulce o 27 polích.

Hillova šifra

Hillovou šifru můžeme vnímat jako přípravu na moderní šifry, protože pracuje s číselnou reprezentací zprávy. Šifra je založena na lineární transformaci bloku zprávy, respektive jeho číselné reprezentace, pomocí násobení maticí. Postup šifrování je následující:

- Zvolíme délku bloku *n*. Zprávu si zapíšeme pomocí číselné reprezentace a rozdělíme bloky zvolené délky.
- Jako klíč si zvolíme matici A stupně *n*. Zvolená matice nesmí být singulární.
- Každý blok zprávy zašifrujeme tak, že ho vezmeme jako vektor a vynásobíme ho maticí A. Výsledek uvažujeme modulo 26 a zapíšeme pomocí písmen.

Rozšifrování probíhá tak, že jednotlivé bloky zašifrované zprávy násobíme inverzní maticí A^{-1}. Šifru si opět ukážeme na příkladu „ Dočkej času jako husa klasu“. Budeme používat bloky délky 3 a jako klíč zvolíme matici:

$$\begin{pmatrix} 1 & -2 & 1 \\ 2 & 0 & 1 \\ 2 & -1 & 1 \end{pmatrix}$$

Přepíšeme si zprávu na čísla a rozdělíme na trojice:

d	o	c		k	e	j		c	a	s		u	j	a		k	o	h	…
3	14	2		10	4	9		2	0	18		20	9	0		10	14	7	…

Každou trojici nyní zašifrujeme pomocí násobení trojic se zvolenou maticí. Pro první trojici dostáváme:

$$\begin{pmatrix} 1 & -2 & 1 \\ 2 & 0 & 1 \\ 2 & -1 & 1 \end{pmatrix} \text{x} \begin{pmatrix} 3 \\ 14 \\ 2 \end{pmatrix} = \begin{pmatrix} -23 \\ 8 \\ -6 \end{pmatrix}$$

Takže písmena *doc* se nám zašifrovala na *(-23, 8, -6),* což můžeme převést na *(3, 8, 20),* tedy na písmena *CIU* – k záporným číslům jsme přičetli 26, abychom dostáli čísla z intervalu 0 – 26, a ta jsme převedli na písmena. Rozšifrování probíhá s využitím inverzní matice následovně:

$$\begin{pmatrix} -1 & -1 & 2 \\ 0 & 1 & -1 \\ 2 & 3 & -4 \end{pmatrix} \text{x} \begin{pmatrix} 3 \\ 8 \\ 20 \end{pmatrix} = \begin{pmatrix} 29 \\ -12 \\ -50 \end{pmatrix}$$

Převodem na čísla v intervalu 0 – 26 získáme zpět *(3, 14, 2),* tedy písmena *doc.*

ŠIFRY – řešením rčení/citáty slavných

Příklad 1 (Nápověda: Řešení začíná: „Pokud nezměníme …..“)

Následující text je zašifrován šifrou Playfair. Jako tahák máte k dispozici částečnou znalost klíče (navíc víte, že klíč byl vytvořen z jednoslovného hesla standartní metodou):

S				U
		G		
V				Z

QP CE FS UX GU HF GU UD HQ LS UK US XU TC XU GU EL PS BM QZ PC GC CF EH BU KU GU GY MR

Mgr. Irena HENCOVÁ, MBA, LL. M. 725 037 081
irena.hencova@ddmporuba.cz

Příklad 2 (Nápověda: Řešení začíná: „A dej mi sílu unést všechno, co změnit nemám sil. Odvahu ……..“)

Následující text je zašifrován šifrou Playfair.

BEHOO MCTIQ KPFAM XAFHU WAAIV INWML WNOBT BMIME WBUZS AZRFI AWSBF SSBMO WELTO LTAWD OFNTV INWMI SOBND OINGB TAOSR VHUWU ROEAF BDAFO LAIWH WWERY

Příklad 3 (Nápověda: Klíč použitý k vytvoření šifrovací tabulky je „demokracie“.)

Následující text je zašifrován šifrou Bifid. Řešení začíná: „Jestliže prohlásíme, že to, co společnost …..“

AFTTS WBDOQ FSCGT GRVBP TFQFT TPCFE SFTOY DBWZT AVBEP VEAFT VTIFW CDPVW APADO WFIDR VEQPQ OAEKD GTIWC VOWYP PGPGP EBDAP WCVCQ CEPBQ WTMBW WSGGM RDPQG PIDAV YSGRG SEYTX TQW

Přezdívka	**Jméno**	**Příjmení**	**Věk** (např. 10 let)	**Kontakt**
Název	**Řešení šifry**			**Počet bodů**
Příklad 1				
Příklad 2				
Příklad 3				

Mgr. Irena HENCOVÁ, MBA, LL. M. 725 037 081
irena.hencova@ddmporuba.cz