Šifra Delastelle - BIFID

Jde o rozšíření textu o šifře BIFID z knihy P.Vondruška: Kryptologie, šifrování a tajná písma, edice OKO, Albatros, Praha 2006 (http://crypto-world.info/oko/index.php).

Systém vysvětlíme na příkladu zašifrování otevřeného textu: NOVY TYP SIFRY.

1) Převod otevřeného textu na dvojice čísel
Nejprve se vytvoří tabulka pro převod otevřených znaků na dvojici čísel.

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

Tento převod musí splňovat podmínku, že pokud se objeví nějaká hodnota řádkové souřadnice, pak musí být tato hodnota použita i jako sloupcová souřadnice a naopak. Lze proto pro realizaci s výhodou použít Polybiův čtverec ([1], str.35, 42, 201), kde řádky a sloupce mají stejné souřadnice a znaky otevřené abecedy (písmena) jsou ve čtverci rozházeny nebo zapsány podle nějakého hesla (zde ALBATROS) .

Hodnoty se (po převodu pomocí tabulky) zapisují do dvou řádků. Do prvního řádku budeme zapisovat řádkovou souřadnici určující pozici písmene v tabulce (např. pro N to bude 4) a do druhého řádku sloupcovou souřadnici (pro N to je 3).

(Lze samozřejmě postupovat i opačně tj. do prvního řádku se zapisuje sloupcová souřadnice určující pozici písmene v tabulce (např. pro N to je 3) a do druhého řádku řádková souřadnice (pro N to je 4)).

Podle tohoto pravidla dostaneme pro námi zvolený otevřený text následující vyjádření:

```
Otevřený text:            NOVY TYP SIFRY
Přepis podle tabulky:     (N=43, O = 21, V=51 …)
1. řádek                  4255 154 23315
2. řádek                  3114 444 24154
```

2) Rozdělení na skupiny
Kdybychom nyní použili Delastellovu koncepci zašifrování souřadnic (viz část 3), získal by eventuální luštitel řadu informací o otevřeném textu a systém by měl závažné bezpečnostní vady. Např. by luštitel znal délku jednotlivých slov otevřeného textu, v případě samostatně stojícího písmene by nedošlo k jeho přešifrování a stejná slova by se zašifrovala vždy stejně. Z těchto důvodů se proto nyní otevřený text dělí do skupin. Často používaná dělba byla po pěti písmenech ve skupině, ale jsou možné i dělby na jiný počet písmen (např. po osmi znacích). Je také možné u krátkých textů vypustit všechny mezery v otevřeném textu a dále text již nedělit a zacházet s ním při přešifrování jako s celkem.

Příprava textu – dělba na pět znaků:

```
Otevřený text:          NOVY TYP SIFRY
Po úpravě:              NOVYT YPSIF RY
Přepis podle tabulky:   (N=43, O = 21, V=51 …)
1. řádek                42551 54233 15
2. řádek                31144 44241 54
```

3) Delastellova koncepce sdružování

Šifra BIFID je založena na následující Delastellově koncepci sdružování souřadnic a jejich zpětném převodu na šifrový text.

Delastelle navrhl domluveným způsobem sdružovat jednotlivé souřadnice textu na dvojice čísel a tyto skupiny převést podle převodové tabulky zpět na písmena, která vytvoří výsledný šifrový text.

Sdružovat souřadnice lze různým způsobem, v případě šifry BIFID jsou nejčastěji používány tři postupy: „vodorovně“, „šikmo nahoru“ a „šikmo dolů“.

3 a) sdružování „vodorovně“

Seskupování se provádí v rámci jednoho číselného vyjádření skupiny, jestliže vyčerpáme v tomto vyjádření v prvním řádku všechny číslice, pokračujeme v sestavování dvojic v řádku druhém a to opět od začátku skupiny.

Delastellovo přešifrování (vodorovné sdružování):

```
1.řádek          42551 54233 15
2.řádek          31144 44241 54
```

Výsledek:
sdružení v prvé skupině: 42, **55**, 13, 11, 44 , ve druhé: 54, **23**, 34, 42, 41 třetí: 15, 54

Převod pomocí tabulky : M Z B Y C I R
A P M K Y

Výsledný šifrový text : MZBAP YCIMK RY

3 b) sdružování „šikmo nahoru“

Mimo vodorovného sdružování se používá i sdružování směrem šikmo nahoru.

Prvá varianta. Dolní znak se sdružuje se znakem horním, který stojí šikmo nad ním. První horní znak v prvé skupině je využit až pro poslední sdružení v této skupině.

Delastellovo přešifrování (sdružování šikmo nahoru, prvá varianta):

```
1.řádek          42551 54233 15
2.řádek          31144 44241 54
```

Výsledek:
sdružení v prvé skupině: 32 , 15, 15, 41, 44 , ve druhé: 44, 42, 23, 43, 15, třetí: 55, 41

Převod pomocí tabulky : GRRKP PMCNR ZK
Výsledný šifrový text : **GRRKP PMCNR ZK**

Druhá varianta. Existuje i upravená varianta sdružování směrem šikmo nahoru. Úprava spočívá v tom, že se začne posledním dolním znakem v každé skupině a ten se sdruží s prvním horním znakem skupiny, dále se již postupuje pravidelně zdola šikmo nahoru až nakonec skupiny.
Delastellovo přešifrování (sdružování šikmo nahoru, druhá varianta):

```
1.řádek          42551 54233 15
2.řádek          31144 44241 54
```

Výsledek:
sdružení v prvé skupině: 44, 32 , 15, 15, 41, ve druhé: 15, 44, 42, 23, 43, třetí: 41, 55

Převod pomocí tabulky : PGRRK RPMCN KZ
Výsledný šifrový text : **PGRRK RPMCN KZ**

Poznámka: Tento způsob šifrování byl použit při sestavování úlohy č.29 (BIFID) v knize Kryptologie, šifrování a tajná písma, str. 308. Při převodu písmen na zlomky a zpět byla využívána převodová tabulka tak, že se nejprve udávaly souřadnice sloupku a pak řádku. Tedy opačně než v této ukázce.

3 c) sdružování „šikmo dolů“:
Dalším možným typem sdružování je sdružování směrem šikmo dolů.
Prvá varianta. Horní znak se sdružuje se znakem, který leží od něj šikmo dole. První dolní znak v prvé skupině je použit až pro poslední sdružení v této skupině.
Delastellovo přešifrování (sdružování šikmo dolů, prvá varianta):

```
1.řádek          42551 54233 15
2.řádek          31144 44241 54
```

Výsledek:
sdružení v prvé skupině: 41, **21**, 54, 54, 13 , ve druhé: 54, **42**, 24, 31, 34, ve třetí: 14, 55

Zpětný převod pomocí tabulky : KOYYB YMDFI TZ
Výsledný šifrový text : **KOYYB YMDFI TZ**

Druhá varianta. Existuje i upravená varianta sdružování směrem šikmo nahoru. Úprava spočívá v tom, že se začne posledním dolním znakem v každé skupině a ten se sdruží s prvním horním znakem skupiny, dále se již postupuje pravidelně zdola šikmo nahoru až nakonec skupiny.

Delastellovo přešifrování (sdružování šikmo dolů, druhá varinta):

```
1.řádek          42551 54233 15
2.řádek          31144 44241 54
```

Výsledek:
sdružení v prvé skupině: 13, 41, **21**, 54, 54 , ve druhé: 34, 54, **42**, 24, 31 , ve třetí: 55,14.

Zpětný převod pomocí tabulky : BKOYY IYMDF ZT
Výsledný šifrový text : **BKOYY IYMDF ZT**

Poznámka (rozdílné převodové tabulky):
Zpětná převodová tabulka v části 3 může být pro větší bezpečnost odlišná od prvé převodové tabulky v části 1.

Lze také použít stejná převodová tabulka, ale při převodu znaků na čísla a zpět se použije jiné pořadí souřadnic (např. při převodu písmen na číslice [řádek, sloupek], při zpětném převodu [sloupec, řádek]).

4) Dešifrování
Příjemce musí znát použitou převodovou tabulku v části 1 a v části 3 (pokud byla odlišná) a způsob převodu znaků na číslice (zda se nejprve používá při jeho určení řádek nebo sloupek). Dále musí být s odesílatelem domluven na délce použité dělby otevřeného textu (např. podle slov - nedoporučuje se, délka 5, délka 8, celý text) a přesný způsob sdružování souřadnic (vodorovně, šikmo dolů, šikmo nahoru).
Příjemce (dešifrant) přijaté znaky šifrového textu nahradí číslicemi podle druhé převodové tabulky, provede správné uspořádání číslic do dvou řádků a převede s využitím známého sdružování souřadnic dvoumístné skupiny čísel zpět pomocí prvé tabulky na otevřené znaky.

[1] P.Vondruška: Kryptologie, šifrování a tajná písma, edice OKO, Albatros, Praha 2006
http://crypto-world.info/oko/index.php
[2] P.Vondruška: Šifra Delastelle – BIFID, root.cz, 5.12.2006
http://www.root.cz/clanky/sifra-delastelle-bifid/
[3] Wilhelm M. Plotz, CipherClerk,
http://members.aon.at/cipherclerk/Doc/DelastelleFract.html#Bifid