ŠIFROVACÍ KROUŽEK - 4. hodina

1. **Polybiův čtverec** – Polybios (cca 230 př.n.l. – cca 120 př.n.l.) byl starověký řecký politik, historik, matematik a spisovatel.

   Polibiův čtverec je matice 5x5, do které vepíšeme 25 znaků abecedy. Tzn. že jedno z písmen chybí. V původní verzi se vypouštělo písmeno U (slučovalo se s V, které je podobné). Dnes se v podobných šifrách nejčastěji vypouští písmeno Q, nebo se slučují písmena I a J, případně se může vypouštět W (slučovat s V) a v závislosti na řeči, kterou šifrujeme. Také je možné abecedu různě přeházet a nebo použít klíč, tedy první slovo v abecedě, zbytek se pak doplní.

   Původní Polybiův čtverec (vypouštíme U – resp. slučujeme s V):

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

   Polybiův čtverec (vypouštíme W, resp. slučujeme s V):

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

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

I.Quest
Pořádá RADIOKLUB OK1KPI Písek

Polybiův čtverec (vypouštíme Q):

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

Polybiův čtverec (slučujeme I/J):

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

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

I.Quest
Pořádá RADIOKLUB OK1KPI Písek

Polybiův čtverec s klíčem (klíč je HESLO + vypouštíme Q):

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

Text, který budeme šifrovat je např.: **SIFROVACIKROUZEK**

Šifrujeme tak, že sbíráme souřadnice jednotlivých písmen v rámci daného čtverce, tedy obvykle první číslo řádku, druhé číslo sloupce. Podle druhu čtverce, který jsme použili pak můžeme dostat následující výsledky:

Původní Polybiův čtverec (vypouštíme U – resp. slučujeme s V):

`44 24 21 43 35 51 11 13 24 31 43 35 51 55 15 31`

Polybiův čtverec (vypouštíme W, resp. slučujeme s V):

`44 24 21 43 35 52 11 13 24 31 43 35 51 55 15 31`

Polybiův čtverec (vypouštíme Q):

`43 24 21 42 35 51 11 13 24 31 42 35 45 55 15 31`

Polybiův čtverec (slučujeme I/J):

`43 24 21 42 34 51 11 13 24 25 42 34 45 55 15 25`

Polybiův čtverec s klíčem (klíč je HESLO + vypouštíme Q):

`13 32 25 43 15 51 21 23 32 34 43 15 45 55 12 34`

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

I.QUEST
Pořádá RADIOKLUB OK1KPI Písek

Vidíme, že zašifrování i rozšifrování je jednoduché, nicméně vyžaduje znalost správného sestavení čtverce, kterých může být poměrně veliké množství.

Online tool: http://musilek.eu/michal/sifry-polybios.html?menu=cc&item=k&lang=cz

Další zajímavé šifry, tzv. Fraktálové, na základě Polybiova čtverce vymyslel Felix Delastelle (1840 – 1902). K jeho dalším šifrám, se podíváme později, ale nyní si jednu ukážeme, jmenuje se **BIFID**.

Bifid používá standardní Polybiův čtverec, použijeme příklad výše:

Polybiův čtverec s klíčem (klíč je HESLO + vypouštíme Q):

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

Výsledek je:

13 32 25 43 15 51 21 23 32 34 43 15 45 55 12 34

BIFID pak funguje tak, že sloučíme na jeden řádek souřadnice řádků (tedy první z cifru všech dvojic) do dalšího řádku pak souřadnice sloupců (tedy druhé číslo):

```
1324152233414513
3253511324355524
```

Tyto opět rozdělíme na dvojice a zapíšeme do jednoho řádku:

```
13 24 15 22 33 41 45 13 32 53 51 13 24 35 55 24
```

a za pomoci stejné tabulky převedem zpátky na písmenka:

Výsledek: **SDOBJNUSIXVSDMZD**

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

Online tool: http://musilek.eu/michal/sifry-delastelle.html?menu=cc&item=i&lang=cz

Cvičení:

1. Zašifrujte do Polybiova čtverce s klíčem „KOPRETINA"a sloučeným I/J text:

   NEJSTARSISIFRYJSOUZEGYPTA

2. Zašifrujte do BIFIDu se stejným čtvercem jako ve cvičení 1 text:

   PRISTESEBUDEMEUCITSUBSTITUCNISIFRY

Úkol:

1. Rozšifrujte následující šifru bez klíče, zkuste zjistit o jaký Polybiův čtvrerec se jedná.

   35 34 31 54 12 24 45 51 13 44 51 15 42 15 13 24 15 24 15 14
   33 11 55 33 15 24 43 44 11 42 43 24 13 23 43 24 21 15 42

2. Rozšifrujte tento BIFID, je použitý stejný čtverec jako v úkolu 1.

   IDSRGZQQMGDVYUDKPO

Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

I.QuEst
Pořádá RADIOKLUB OK1KPI Písek