ŠIFROVACÍ KROUŽEK - 9. hodina

Two square cipher

Další šífry z dílny Felixe Delastella (BIFID), jsou založené na úpravě mechanismu Playfairovy šifry. Jedná se o dvě šifry – Two Square Cipher a Four Square Cipher.

Nejprve k té první. Tato šifra funguje podobně jako Playfair, ale potřebujeme dva čtverce – dvě matice 5x5 s rozdílnými abecedami.

Jako příklad použijeme dvě klíčová slova, např.: PRVNICTVEREC a DRUHYCTVEREC

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

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

Budeme šifrovat náš oblíbený text: SIFROVACIKROUZEK, který si stejně jako u Playfaira rozdělíme na bigramy: SI FR OV AC IK RO UZ EK

Máme dvě možnosti, buď čtverce umístíme pod sebe, nebo vedle sebe, princip šifrování pak bude záležet právě na tomto umístění.

Nejprve tedy **pod sebou**:

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

I.Quest
Pořádá RADIOKLUB OK1KPI Písek

Šifrujeme tak, že první písmeno si najdeme v prvním čtverci, druhé ve druhém čtverci a spojíme si je obdélníkem, takže SI bude vypadat takto:

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

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

Výsledkem budou daná písmena ze stejného řádku, na okrajích obdélníku, tedy: **QK**

Stejným způsobem dále:

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

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

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

FR -> Pokud jsou obě písmena ve stejném sloupci, pak není kam posouvat v řádku a použijí se tedy tatáž písmenka: **FR**

Další text se šifruje stále stejně, výsledná šifra tedy bude:

QKFROVCEIKNMZQBG

Druhá možnost je šifrovat čtverce vedle sebe, postup je stejný, jen čtverce jsou vedle sebe:

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

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

SI -> KO

A stejným postupem i dále, výsledek bude:

KORFENACKYMHUZGA

Dešifrování pak probíhá stejným způbem – šifra je tedy **symetrická**.

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

Four square cipher

K této šifře potřebujeme čtyři čtverce, z nichž pravý horní a levý spodní mají standardní abecedu, zatímco zbylé dva jsou opět definovány klíčem (použijeme stejné klíče jako u two square cipher výše).

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

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

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

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

Nyní šifrujeme stejným způsobem, pouze tak, že šifrovaná písmenka hledáme v ve čtvercích se seřazenou abecedou, šifrovaná pak ve čtvercích s klíčovým slovem:

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

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

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

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

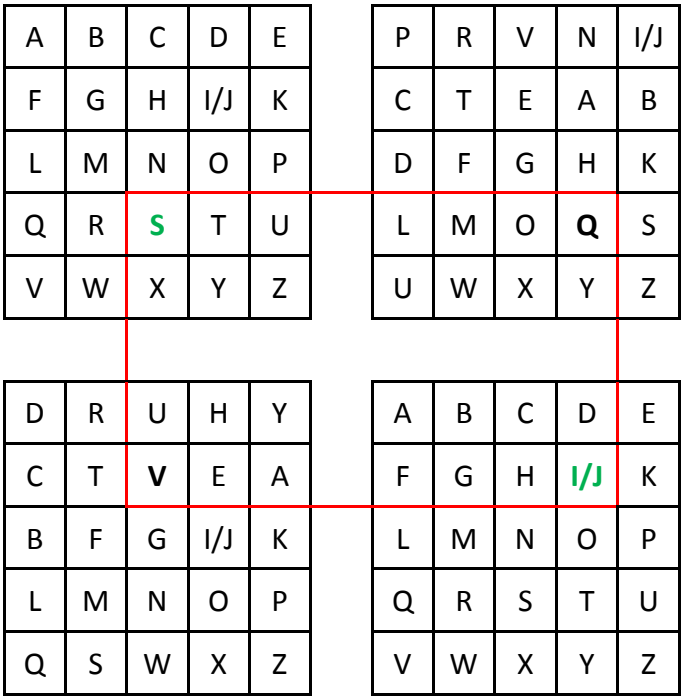
Kroužek vede: Richard Kába – RIK
Email: richard.kaba@centrum.cz
Tel.: +420 731 137 569
Kdykoli mě kontaktujte!

SI -> QV

Stejným způsobem i dále, výsledek pak bude:

QVTLDXVDBEQFSZIA

Při dešifrování musíme postupovat opačně, tedy šifrovaná písmenka hledat ve čtvercích s klíčem a výsledek ve čtvercích s běžnou abecedou.



QV -> SI

A stejným způsobem i nadále.

Cvičení:

Zašifrujte text: TESIMESENAVYSVEDCENI

První klíč: BUDOUJEDNICKY

Druhý klíč: NEBUDOUPETKY

Následujícími šiframi:

Two square cipher – vedle sebe
Two square cipher – pod sebou
Four square cipher

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