ŠIFROVACÍ KROUŽEK - 8. hodina

Playfairova šifra je polyalfabetická šifra, kterou navrhl v roce 1854 britský vědec Charles Wheatstone. Pojmenovaná je podle největšího propagátora a britského poslance Lyona Playfaira. Byla používána jako vojenská polní šifra v omezené míře i za druhé světové války.

Více info: https://cs.wikipedia.org/wiki/Playfairova_%C5%A1ifra

Jak to funguje. K Playfairovi potřebujeme 25 písmen abecedy, tedy podobně jako u BIFIDu si zvolíme některou z možností (sloučit I a J, V a W, U a V nebo vypustit Q). V původní verzi této šifry se slučovalo I a J.

Vytvoříme si tedy opět čtverec 5 x 5, do kterého vepíšeme abecedu, buďto posloupně, nebo za principu zvolení klíčového slova, pokud prahneme po největší bezpečnosti, klíčem bude celá abeceda v náhodném pořadí, které zná jenom ten, kdo šifruje a ten kdo dešifruje.

Pro příklad použijeme nejjednodušší možnost, abecedu popořadě, kde slučujeme I a J.

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

I.Quest
Pořádá RADIOKLUB OK1KPI Písek

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 si zvolíme text, který šifrujeme, třeba náš obvyklý:

SIFROVACIKROUZEK

Playfairova šifra pracuje s tzv. Bigramy, neboli dvojicemi písmen, takže si nejprve rozdělíme text, který šifrujeme do bigramů:

SI FR OV AC IK RO UZ EK

Nyní šifrujeme postupně každou dvojici znaků a to podle následujících pravidel:

- Pokud obě písmena z bigramu leží na stejném řádku, nahradí se písmeny ležícími napravo od nich. Pokud je jedno z písmen poslední v řádku, nahradí se prvním ze stejného řádku.

- Pokud obě písmena leží ve stejném sloupci, nahradí se písmeny ležícími pod nimi. Pokud je jedno z písmen poslední ve sloupci, nahradí se prvním z téhož sloupce.

- Pokud obě písmena leží na jiném řádku a v jiném sloupci, je každé z nich nahrazeno písmenem ležícím na průsečíku řádku daného písmena a sloupce druhého písmena.

Takže jdeme na to: Písmena SI nejsou ve stejném řádku ani sloupci, takže je šifrujeme podle třetího pravidla, tedy podle průsečíků řádku a sloupce, výsledkem bude **TH**

Stejně bude probíhat i šifrování FR= **GQ**, OV = **LY**.

Další bigram je AC, zde jsou písmena ve stejném řádku, takže podle prvního pravidla budou výsledkem písmena vpravo od nich, tedy AC = **BD**.

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

Stejně tak IK podle prvního pravidla bude **KF**.

RO bude opět podle třetího pravidla **TM**.

UZ leží ve stejném sloupci, takže zde použijeme druhé pravidlo a výsledkem bude: **ZE**. Stejně tak EK bude **KP**.

Výsledný zašifrovaný text tedy bude:

THGQLYBDKFTMZEKP

Jelikož se jedná o polyalfabetickou šifru, je odolná proti frekvenční analýze.

Co se týče dešifrování, známe-li správný čtverec, postupujeme úplně stejně, akorát pravidlo 1 a 2 nám musí fungovat obráceně, tedy použijeme písmeno vlevo potažmo nad místo vpravo potažmo pod.

Cvičení 1:

Zkuste si zašifrovaný text opět rozšifrovat.

THGQLYBDKFTMZEKP

Cvičení 2:

Zašifruje do Playfaira text: VANOCEBYLYKRATKE a pouzijte ctverec se sloučeným I/J a klíčovým textem: ZASESETESIMENADALSI (pokud se nám v klíči opakují písmena, použijeme jen ty, které se neopakují, tedy: ZASETIMNDL)

Cvičení 3:

Zkusíme si rozšifrovat úkol z I.Questu 2015

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