EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Kryptologie

Klasická kryptografie: Transpoziční šifry

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204

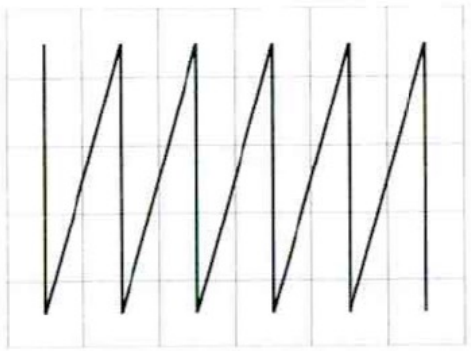
Doc. Ing. Roman Šenkeřík, Ph.D.
FAI, Ústav informatiky a umělé inteligence

Obsah prezentace

- Transpoziční šifry.
  - Obecná transpozice v tabulce
  - Jednoduchá transpozice v tabulce s klíčem
  - Dvojitá transpozice (případně se dvěma klíči)
  - Zubatka
  - Ostatní
- Hybridní šifry (transpozice/substituce).
  - ADFGVX šifra

1. Transpoziční šifry

Transpoziční šifry: Obecná transpozice v tabulce



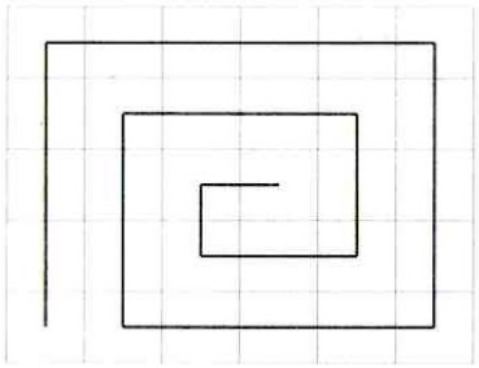
K	N	Z	E	Y	D
D	I	A	N	T	N
O	D	J	E	I	E
H	V	I	C	Z	H
O	A	C	H	A	O

KNZEYDDIANTNODJ
IEHVICZHOACHAO

Příklad dle: [1]

Základním principem je určitým způsobem zapsat text a jiným jej zase přečíst.

Transpoziční šifry: Obecná transpozice v tabulce



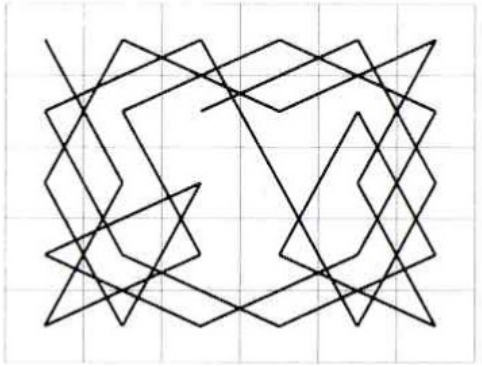
D	A	Z	I	T	Y
N	A	V	D	I	H
E	Z	D	K	N	C
H	A	O	H	O	E
O	J	I	C	E	N

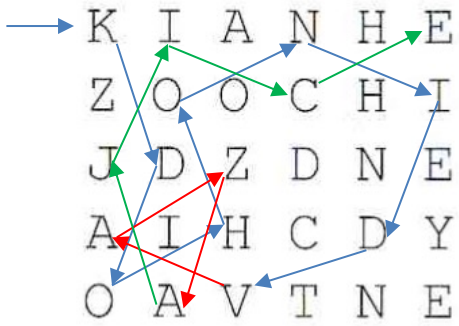
DAZITYNAVDIHEZD
KNCHAOHOEOJICEN

Příklad dle: [1]

Základním principem je určitým způsobem zapsat text a jiným jej zase přečíst.

Transpoziční šifry: Obecná transpozice v tabulce





KIANHEZOOCHIJDZ
DNEAIHCDYOAVTNE

Příklad dle: [1]

Základním principem je určitým způsobem zapsat text a jiným jej zase přečíst.

Transpoziční šifry: Jednoduchá transpozice v tabulce s klíčem

- Využívá klíč - počet sloupců = počet znaků klíče
- Zápis po řádcích, čtení po sloupcích (šifrování)
- Sloupce jsou setříděny podle pořadí znaků v klíči

P	E	T	R	K	L	I	C
K	D	O	H	O	N	I	D
V	A	Z	A	J	I	C	E
N	E	C	H	Y	T	I	Z
A	D	N	E	H	O	K	E

Šifrování probíhá, tak že jsou sloupce seřazeny podle abecedy

⇒

C	E	I	K	L	P	R	T
D	D	I	O	N	K	H	O
E	A	C	J	I	V	A	Z
Z	E	I	Y	T	N	H	C
E	D	K	H	O	A	E	N

Příklad dle: [1]

- Tabulku je nutno (“na konci”) doplnit vhodně zvolenými znaky

Transpoziční šifry: Dvojitá transpozice (případně se dvěma klíči)

- Na stejném principu je založena dvojitá transpozice, postup je pouze 2x zopakovaný.

- Postup je sice stejný **ALE** druhou tabulku již není možné doplnit dodatečnými znaky, tj délka “mezišifry” a délka klíče č. 2 musí být dělitelná beze zbytku!

Např.: délka „mezišifry“ ms = 20 a délka klíče k = 5.

20 mod 4 = 0

Transpoziční šifry: Dvojitá transpozice (případně se dvěma klíči)

- Využívají se dva klíče.
- Zápis po řádcích, čtení po sloupcích.
- **První klíč** - počet sloupců
- **Druhý klíč** - počet řádků

Transpoziční šifry: Dvojitá transpozice (případně se dvěma klíči)

Sloupce jsou setříděny podle pořadí znaků v prvním klíči (“heslo”):

H	E	S	L	O
A	H	O	J	P
E	P	O	J	A
K	S	E	M	A
S	X	X	X	X

→

E	H	L	O	S
H	A	J	P	O
P	E	J	A	O
S	K	M	A	E
X	S	X	X	X

Řádky jsou “rozházeny” podle pořadí znaků v druhém klíči (“kafe”):

A	H	A	J	P	O
E	P	E	J	A	O
F	S	K	M	A	E
K	X	S	X	X	X

→

K	X	S	X	X	X
A	H	A	J	P	O
F	S	K	M	A	E
E	P	E	J	A	O

Zašifrovaný text: XHSPS AKEXJ MJXPA AXOEO

Transpoziční šifry: Zubatka

- Navazuje na jednoduchou transpozici v tabulce.
- Jestliže je délka textu velká tak, že délka sloupců tabulky převyšuje délku hesla a rozdělí se sloupce tabulky na dvě části podle příslušné hodnoty klíče.
- Text vpisujeme po řádcích shora dolů a to do první části této tabulky a potom do části druhé.

Zubatka: Příklad

Klíč:

S	E	D	M	I	K	R	A	S	K	A
10	4	3	8	5	6	9	1	11	7	2

	10	4	3	8	5	6	9	1	11	7	2
1	V	P	R	A	T	E	L	S	T	V	I
2	N	E	L	Z	E	N	I	r	C	P	O
3	V	A	Z	O	V	A	T	i	Z	A	t
4	Z	H	a	O	U	B	N	k	E	J	a
5	S	v	a	I	N	E	Z	n	P	O	i
6	C	x	c	H	i	L	E	c	B	O	e
7	V	r	o	A	x	p	N	o	I	L	t
8	I	a	j	C	i	p	H	r	O	i	t
9	C	e	l	e	n	a	E	p	N	o	m
10	I	i	n	e	j	a	l	e	A	v	e
11	r	e	j	n	e	c	h	v	P	a	l
12	s	e	n	e	c	a	x	x	x	x	x

V klíči očíslujeme písmena podle abecedy. Pokud se v klíči nachází stejné písmeno, pak bude mít druhý výskyt písmene hodnotu o 1 větší, než první výskyt (číslujeme zleva doprava)

OT: V přátelství nelze nic považovat za zhoubnější než pochlebování, lichocení a přitakávání.

Příklad dle: [2]

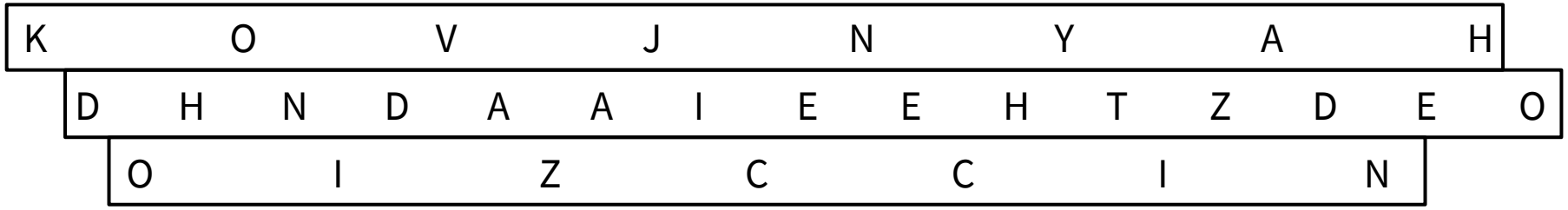
Transpoziční šifry: Ostatní

Transpozice typu “zábradlí” – lze využít například „*čtverečkovaný papír*“

K O V J N Y A H

D H N D A A I E E H T Z D E O

O I Z C C I N



Příklad dle: [1]

2. Hybridní šifry

ADFGVX šifra

- Šifry ADFGX či ADFGVX představovaly hybridní klasické (polní šifry).
- Hybridizací se v tomto případě myslí spojení substituce a transpozice do jednoho postupu. Jako hybridní šifra je někdy považován Bifid/Trifid.
- Hybridizace substituční tabulkové šifry (souřadnicového principu Polybiova čtverce a tabulky s klíčovým slovem „Playfair“ typu) a jednoduché transpozice s klíčem.
- Příklad a popis šifry dostupný zde: [3].

Seznam odkazů

[1] HANŽL, Tomáš, Radek PELÁNEK a Ondřej VÝBORNÝ. Šifry a hry s nimi: kolektivní outdoorové hry se šiframi. Praha: Portál, 2007. ISBN 978-80-7367-196-9.

[2] JANEČEK, Jiří. Odhalená tajemství šifrovacích klíčů minulosti: ruční šifry. Praha: Naše vojsko, 1994. Mozaika (Naše vojsko). ISBN 80-206-0462-6.

[3] Šifra ADFGX ADVGVX. [online]. Dostupné z: http://soutez2005.crypto-world.info/images/ADFGX.pdf

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Děkuji za pozornost

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204