



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



# Kryptologie

## *Klasická kryptografie: Substituční šifry II*

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

- **Polygrafická substituce**
  - Playfair (anglický čtverec)
  - Bifid/Trifid
  - Hillova šifra
- **Ostatní substituce**
  - Polybiův čtverec
  - Tabulkové substituce (tzv. jedno a dvoumístné šifry)
  - Autokláv (Autoklíč)

# 1. Polygrafické substituce

# Polygrafické substituce: Playfair

- Digramová šifra (šifrují se vždy 2 písmena)
- Využití klíčového slova
- Používá tabulku 5x5 - nutno vynechat jeden znak,
  - v CZ jazyce: V = W (K = Q)
  - v EN jazyce I = J

# Polygrafické substituce: Playfair

- V každém digramu musí být různé znaky - pokud není splněno, vložíme vhodný znak např. „x“.
- Při lichém počtu znaků v OT (až po případném doplnění znaku do stejné dvojice!!) doplníme na konci zvoleným znakem.

**povinné ➡ povinne ➡ po vi nx nx ex**

# Polygrafické substituce: Playfair

- Do tabulky nejprve zapíšeme heslo (klíč).
- Opakující znaky hesla jsou vynechány. ALFA ➡ ALF
- Tabulky doplníme podle abecedy s vynecháním znaků již použitých v hesle.
- Tabulka pojme 25 znaků => jeden znak vynecháme

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

*Příklad dle: [1]*

# Polygrafické substituce: Playfair

- Jestliže leží dva znaky na stejném řádku, každé se nahradí písmenem ležícím o jedno napravo.
- Pokud je písmeno úplně vpravo, nahradí se prvním na stejném řádku (rotace na řádku).

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

Např.:

**CA → AB**

**FM → GD**

# Polygrafické substituce: Playfair

- Jestliže leží dva znaky ve stejném sloupci, každé se nahradí písmenem ležícím o jedno **níže**.
- Pokud je písmeno úplně dole, nahradí se **prvním ve stejném sloupci** (rotace ve sloupci).

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

Např.:

EI → IF

CX → GT



# Polygrafické substituce: Playfair

- Jestliže leží dva znaky **na různých řádcích a sloupcích**, každé se nahradí písmenem ležícím na stejném řádku, ale ve sloupci jako druhé z dvojice.
- Hledáme tak protilehlou diagonálu obdélníku.

Šifrovací pomůcka:

První je řádek, potom sloupec.

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

Např.:

KO → EU

# Polygrafické substituce: Playfair

Šifrovací pomůcka:  
První je řádek, potom sloupec.

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

Např.:

IS → AO

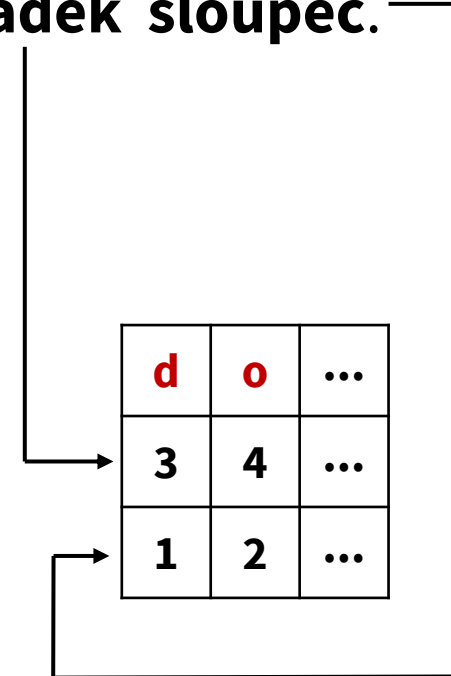
# Polygrafické substituce: Bifid

- Šifra „playfair“ typu.
- Opět i zde je využito klíčového slova.
- Používá tabulku 5x5 - nutno vynechat jeden znak.
  - používáme v **CZ jazyce** V = W a v **EN jazyce** I = J
- Slova OT dělíme po pěticích.
- Pro každý znak pod sebe zapisujeme souřadnice **řádek sloupec**.

# Polygrafické substituce: Bifid

- Pro každý znak pod sebe zapisujeme souřadnice **řádek** **sloupec**.

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



# Polygrafické substituce: Bifid

- Následně vzniklé pětice čísel spojíme a znovu rozdělíme do dvojic a vyhledáme odpovídající znaky, které představují šifru.

OT		d	o	c	k	e		j	c	a	s	u		j	a	k	o	h		u	s	a	k	l		a	s	u
ř.		3	4	2	1	1		2	2	2	4	4		2	2	1	4	3		4	4	2	1	2		2	4	4
sl.		1	2	β	5	2		2	3	4	4	5		2	4	5	2	4		5	4	4	5	1		4	4	5



34	21	11	23	52		22	24	42	34	45		22	14	32	45	24		44	21	25	44	51		24	44	45
H	L	P	C	W		I	A	O	H	U		I	R	F	U	A		S	L	B	S	V		A	S	U

*Příklad dle: [1]*

# Polygrafické substituce: Bifid

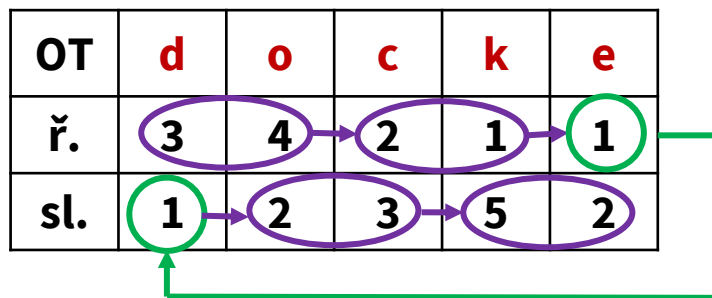
- Šifrování

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

Zašifrovaná první pětice:

34	21	11	23	52
H	L	P	C	W

OT	d	o	c	k	e
ř.	3	4	2	1	1
sl.	1	2	3	5	2



# Polygrafické substituce: Bifid

- Dešifrování

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

Zašifrovaná první pětice:

34	21	11	23	52
H	L	P	C	W

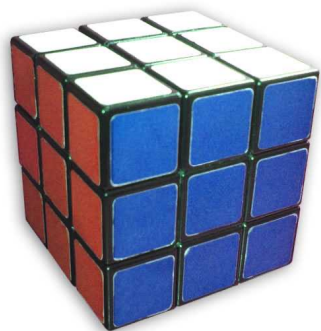
Směr dešifrování:



OT	d	o	c	k	e
ř.	3	4	2	1	1
sl.	1	2	3	5	2

# Polygrafické substituce: Trifid

- Podobný princip má šifra Trifid [1].
- Zápis do trojrozměrné tabulky o 27 prvcích (tři tabulky - vrstvy o rozměru 3x3).
- Každý znak je reprezentován trojicí čísel (č.vrstvy, řádek, sloupec).





# Polygrafické substituce: Hillova Šifra

- Matematická šifra
- Znaký abecedy převedeme na čísla 0 – 25
- Klíčem je náhodně zvolená matice  $A$ :
  - je stupně  $n$  ( $n$  řádků,  $n$  sloupců)
  - nesmí být singulární  $\Rightarrow$  determinant nesmí být roven nule
- Text rozdělíme do bloků o délce  $n$  a převedeme na číselné vektory  $v$

# Polygrafické substituce: Hillova Šifra

- Matice  $A$  a vektor  $v$

- Abeceda:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Klíč:

$$\begin{pmatrix} F & A & I \\ U & T & B \\ K & R & Y \end{pmatrix} \asymp \begin{pmatrix} 5 & 0 & 8 \\ 20 & 19 & 1 \\ 10 & 17 & 24 \end{pmatrix} = A$$

$$\text{OT: EVA} \asymp \begin{pmatrix} 4 \\ 21 \\ 0 \end{pmatrix} = v$$

# Polygrafické substituce: Hillova Šifra

- Determinant matice  $A$

$$A = \begin{pmatrix} 5 & 0 & 8 \\ 20 & 19 & 1 \\ 10 & 17 & 24 \end{pmatrix}, \det A = 3395 \Rightarrow \det A \neq 0$$

Input interpretation:
$\begin{vmatrix} 5 & 0 & 8 \\ 20 & 19 & 1 \\ 10 & 17 & 24 \end{vmatrix}$
Result:
3395

Nejedná se o singulární matici => řádky matice jsou lineárně nezávislé => můžeme pokračovat

*Zdroj výpočtu: [2]*



# Hilova šifra: šifrování

## ○ Postup

- Nejprve provedeme výpočet  $A \cdot v$  (násobení matice vektorem)
- Následně provedeme  $(A \cdot v) \bmod 26$  (aplikace modulární aritmetiky)

# Hillova šifra – výpočet $A \cdot v$

## ○ Výpočet

$$A \cdot v = \begin{pmatrix} 5 & 0 & 8 \\ 20 & 19 & 1 \\ 10 & 17 & 24 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 21 \\ 0 \end{pmatrix} = \begin{pmatrix} 20 \\ 479 \\ 397 \end{pmatrix}$$



Zdroj výpočtu: [2]  
Univerzita Jiřího Běty ve Zlíně  
Fakulta humanitních studií

# Hilova šifra: šifrování

- aplikace mod 26

$$(A \cdot v) \bmod 26 = \begin{pmatrix} 20 \\ 479 \\ 397 \end{pmatrix} \bmod 26 = \begin{pmatrix} 20 \\ 11 \\ 7 \end{pmatrix}$$

$$\check{S}T = \begin{pmatrix} 20 \\ 11 \\ 7 \end{pmatrix} \asymp \begin{pmatrix} U \\ L \\ H \end{pmatrix}$$

$$20 \bmod 26 = 20$$

$$479 \bmod 26 = 11$$

$$397 \bmod 26 = 7$$

# Hilova šifra: dešifrování

## ○ Postup

- Nejprve provedeme výpočet  $A^{-1} \cdot \mathbf{št}$  (násobení inverzní matice vektorem)
- Následně provedeme  $(A \cdot \mathbf{št}) \bmod 26$  (aplikace modulární aritmetiky)

# Hilova šifra: dešifrování

- **inverzní matice  $A^{-1}$**

- Pro inverzní matici platí:

$$A^{-1} \cdot A = I, \text{ kde } I \text{ je jednotková matice}$$

Input:

$$\begin{pmatrix} \frac{439}{3395} & \frac{136}{3395} & -\frac{152}{3395} \\ -\frac{94}{679} & \frac{8}{679} & \frac{31}{679} \\ \frac{30}{679} & -\frac{17}{679} & \frac{19}{679} \end{pmatrix} \cdot \begin{pmatrix} 5 & 0 & 8 \\ 20 & 19 & 1 \\ 10 & 17 & 24 \end{pmatrix}$$

---

Result:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$



# Hilova šifra: dešifrování

- inverzní matice  $A^{-1}$

$$A^{-1} = \begin{pmatrix} \frac{439}{3395} & \frac{136}{3395} & -\frac{152}{3395} \\ -\frac{94}{679} & \frac{8}{679} & \frac{31}{679} \\ \frac{30}{679} & -\frac{17}{679} & \frac{19}{679} \end{pmatrix}$$

- Vytkneme společnou část všech prvků matice:

$$\begin{pmatrix} \frac{439}{3395} & \frac{136}{3395} & -\frac{152}{3395} \\ -\frac{94}{679} & \frac{8}{679} & \frac{31}{679} \\ \frac{30}{679} & -\frac{17}{679} & \frac{19}{679} \end{pmatrix} = \frac{1}{3395} \begin{pmatrix} 439 & 136 & -152 \\ -470 & 40 & 155 \\ 150 & -85 & 95 \end{pmatrix}$$

# Hilova šifra: dešifrování

- úprava  $A^{-1}$

$$A^{-1} = \frac{1}{3395} \begin{pmatrix} 439 & 136 & -152 \\ -470 & 40 & 155 \\ 150 & -85 & 95 \end{pmatrix} = 3395^{-1} \begin{pmatrix} 439 & 136 & -152 \\ -470 & 40 & 155 \\ 150 & -85 & 95 \end{pmatrix} =$$

inverze

$$= 7 \begin{pmatrix} 439 & 136 & -152 \\ -470 & 40 & 155 \\ 150 & -85 & 95 \end{pmatrix} = \begin{pmatrix} 3073 & 952 & -1064 \\ -3290 & 280 & 1085 \\ 1050 & -595 & 665 \end{pmatrix}$$

- Aplikace modulární aritmetiky (mod 26) na inverzní matici  $A^{-1}$ :

$$A^{-1} \bmod 26 = \begin{pmatrix} 3073 & 952 & -1064 \\ -3290 & 280 & 1085 \\ 1050 & -595 & 665 \end{pmatrix} \bmod 26 = \begin{pmatrix} 5 & 16 & 2 \\ 12 & 20 & 19 \\ 10 & 3 & 15 \end{pmatrix}$$

# Hillova šifra: dešifrování

- **výpočet  $(A^{-1} \cdot \text{št}) \bmod 26$**

$$A^{-1} \cdot \text{št} = \begin{pmatrix} 5 & 16 & 2 \\ 12 & 20 & 19 \\ 10 & 3 & 15 \end{pmatrix} \begin{pmatrix} 20 \\ 11 \\ 7 \end{pmatrix} = \begin{pmatrix} 290 \\ 593 \\ 338 \end{pmatrix}$$

- Aplikace mod 26:

$$(A^{-1} \cdot \text{št}) \bmod 26 = \begin{pmatrix} 290 \\ 593 \\ 338 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4 \\ 21 \\ 0 \end{pmatrix}$$

- Výsledek:

$$\begin{pmatrix} 4 \\ 21 \\ 0 \end{pmatrix} \asymp \begin{pmatrix} E \\ V \\ A \end{pmatrix}$$

## 2. Ostatní substituce

# Ostatní substituce: Přehled

- Více šifer za jedno písmeno (Tabulka 4 x 7 jedno a dvojmístné šifry a jiné)
- Autoklíč
- Využití nomenklátorů, klamačů, zkomolenin
- Knižní šifra

# Ostatní substituce - Polybiův čtverec

Polybiův čtverec je velmi jednoduchá šifra. Jde pouze o to, seřadit abecedu do čtvercové tabulky  $5 \times 5$  a očísloval její řádky a sloupce.

Každé písmeno původního textu pak nahrazuji dvojice písmen:

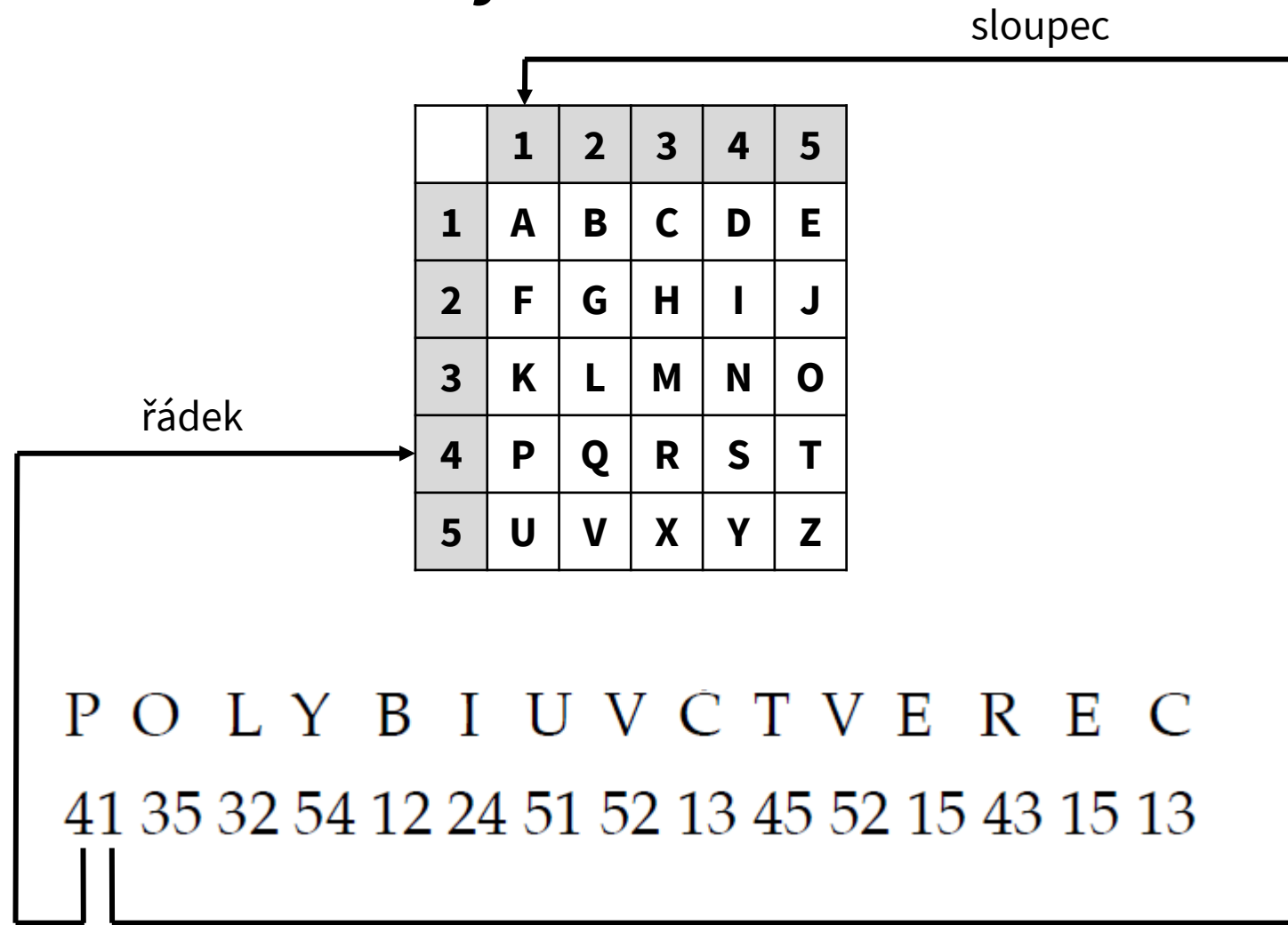
- nejprve číslo řady,
- pak číslo sloupce.

# Ostatní substituce - Polybiův čtverec

- Jednoduše se vepíše abeceda s vynecháním háčeků, čárek a písmen **Ch** a **W**.
- Někdy se vynechává **Q**, méně obvyklou možností je vynechat písmeno **J** (resp. považovat **J** a **I** za stejné písmeno), podobně jako se činí u šifry Playfair.

	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	X	Y	Z

# Ostatní substituce - Polybiův čtverec





# Ostatní Substituce - Tabulka 5 x 10

	1	2	3	4	5	6	7	8	9	0
1	A	Á	B	C	Č	D	Ď	E	É	Ě
2	F	G	H	I	Í	J	K	L	M	N
3	Ň	O	Ó	P	Q	R	Ř	S	Š	T
4	Ť	U	Ú	Ů	V	W	X	Y	Ý	Z
5	Ž	;	„	,	/	'	+	?	!	

Otevřený text:

P R A H A   J E   K R Á S N Á

Souřadnice z tabulky:

34 36 11 23 11 50 26 18 50 27 36 12 38 20 12

# Ostatní Substituce - Tabulka 4 x 7

		1	2	3	4	5	6
7	A	B	C	D	E	F	G
8	H	I	J	K	L	M	N
9	O	P	Q	R	S	T	U
0	V	W	X	Y	Z	/	+

Čísla 0, 7, 8, 9 znamenají řádky!

Otevřený text:

Souřadnice z tabulky:

Z	I	T	R	A		M	I		Z	A	V	O	L	E	J
04	81	95	93	7		85	81		04	7	0	9	84	74	82

Šifrovaný text: **04819 59378 58104 70984 7482**

# Ostatní substituce - Autokláv (Autoklíč)

Jedná se o modifikaci Polyalfabetické substituční šifry, jejímž cílem bylo zabránit opakování klíčového slova (tedy slabině).

Existují 2 verze:

- **Autokláv OT:** Klíčové slovo slouží k “nastartování” substituce, dále se jako klíčové slovo používá samotný otevřený text.
- **Autokláv ŠT:** Klíčové slovo slouží k “nastartování” substituce, dále se jako klíčové slovo používá samotná šifra.

# Ostatní substituce - Autokláv (Autoklíč)

Autokláv „OT“

OT:	A	H	O	J	P	E	P	O
Klíč:	K	L	I	C	A	H	O	J
ŠT:	K	S	W	L	P	L	D	X

Autokláv „ŠT“

OT:	A	H	O	J	P	E	P	O
Klíč:	K	L	I	C	K	S	W	L
ŠT:	K	S	W	L	Z	W	L	Z

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

# Ostatní substitute – SMS šifra

- Příklad:

**3 33 55 88 5 444 9999 2 7 666 9999 666 777 66 666 7777 8**

# Ostatní substituce – SMS šifra

- Jednoduchá “Mobilní” šifra
- Substituční šifra
- Každému znaku je přiřazen odpovídající počet stisků alfanumerické klávesnice mobilního telefonu - jako při psaní SMS bez slovníku (T9 a jiné...)
- A = jeden stisk dvojky (tj. A=2)
- E = dva stisky trojky (tj. E=33)
- ...

# 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] Wolfram Alpha. [online]. Dostupné z: <https://www.wolframalpha.com/>
- [3] JANEČEK, Jiří. Odhalená tajemství šifrovacích klíčů minulosti: ruční šifry. Praha: Naše vojsko, 1994. Mozaika (Naše vojsko). ISBN 80-206-0462-6.



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

**MŠMT**  
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



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