Jednoduché šifry

Tomáš Luczków

České vysoké učení technické v Praze
Fakulta jaderné a fyzikálně inženýrská

Obsah prezentace

Jednoduché šifry

- Caesarova šifra
- Afinní šifra
- Vigenerova šifra
- Permutační šifra
- Hillova šifra

Příklad

Zakóduj slovo KATERINA v Z_{27}
Kódová abeceda={a, b,..., y, z, “ “}
$c = 15$

Příklad - zakódování

α	K	A	T	E	R	I	N	A
α	10	0	19	4	17	8	13	0
$\alpha + c$	25	15	34	19	32	23	28	15
$\beta = mod(\alpha + c; 27)$	25	15	7	19	5	23	1	15
β	Z	P	H	T	F	X	B	P

Příklad - dekódování

$c = 15 \Rightarrow -c = 12$

β	Z	P	H	T	F	X	B	P
β	25	15	7	19	5	23	1	15
$\beta + (-c)$	37	27	19	31	17	35	13	27
$\alpha = mod(\beta + (-c))$	10	0	19	4	17	8	13	0
α	K	A	T	E	R	I	N	A

Příklad - sami

Dekóduj slovo BKASWGUJXB v Z_{27}
Kódová abeceda={a, b,..., y, z, “ “}
$c = 19$

Příklad

Zakóduj slovo FJFI CVUT v Z_{27}
Kódová abeceda={a, b,..., y, z, “ “}
$c = 10$

Příklad - zakódování

α	F	J	F	I		C	V	U	T
α	5	9	5	5	26	2	21	20	19
$\alpha * c$	50	90	50	80	260	20	210	200	190
β	23	9	23	26	17	20	21	11	1
β	X	J	X		R	U	V	L	B

Příklad - dekódování

$c = 10 \Rightarrow c^{-1} = 19$

β	X	J	X		R	U	V	L	B
β	23	9	23	26	17	20	21	11	1
$\beta * c^{-1}$	437	171	437	494	323	380	399	209	19
α	5	9	5	8	26	2	21	20	19
α	F	J	F	I		C	V	U	T

Příklad - sami

Dekóduj slovo ECHRFZY v Z_{27}
Kódová abeceda={a, b,..., y, z, “ “}
$c = 4$

Příklad

Zakóduj slovo PREZENTACE v Z_{27}
Kódová abeceda={a, b,..., y, z, " "}
$\gamma(BUDU\ SE\ Z\ NI\ UCIT)$
$\gamma(9)$

Příklad - zakódování

α	P	R	E	Z	E	N	T	A	C	E
$\gamma(9)$		N	I		U	C	I	T	B	U
α	15	17	4	25	4	13	19	0	2	4
$\gamma(9)$	26	13	8	26	20	2	8	19	1	20
$\alpha + \gamma(9)$	41	30	12	51	24	15	27	19	3	24
β	14	3	12	24	24	15	0	19	3	24
β	O	D	M	Y	Y	P	A	T	D	Y

Příklad - dekódování

β	O	D	M	Y	Y	P	A	T	D	Y
β	14	3	12	24	24	15	0	19	3	24
$\gamma(9)$		N	I		U	C	I	T	B	U
$\gamma(9)$	26	13	8	26	20	2	8	19	1	20
$-\gamma(9)$	1	14	19	1	7	25	19	8	26	7
$\alpha = \beta + (-\gamma(9))$	15	17	31	25	31	40	19	27	29	31
α	15	17	4	25	4	13	19	0	2	4
α	P	R	E	Z	E	N	T	A	C	E

Příklad- sami

Dekóduj slovo OSCRMZDBZFONOUPQ v Z_{27}
γ=ZASLOUZI SI HO
$\gamma = 3$

Příklad

Zakóduj slovo PERMUTACNI v Z_{27}
$\pi = 35214$
Kódová abeceda={a, b,..., y, z, “ “}

Příklad- zakódování

α	P	E	R	M	U	T	A	C	N	I
α	15	4	17	12	20	19	0	2	13	8

$$\beta_1 = \begin{pmatrix} 15 & 4 & 17 & 12 & 20 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 17 & 20 & 4 & 15 & 12 \end{pmatrix}$$

$$\beta_2 = \begin{pmatrix} 19 & 0 & 2 & 13 & 8 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 8 & 0 & 19 & 13 \end{pmatrix}$$

β	17	20	4	15	12	2	8	0	19	13

Příklad - dekódování

β	17	20	4	15	12	2	8	0	19	13

$$\alpha_1 = \begin{pmatrix} 17 & 20 & 4 & 15 & 12 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 15 & 4 & 17 & 12 & 20 \end{pmatrix}$$

$$\alpha_2 = \begin{pmatrix} 2 & 8 & 0 & 19 & 13 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 19 & 0 & 2 & 13 & 8 \end{pmatrix}$$

$\alpha = \alpha_1 + \alpha_2 =$	15	4	17	12	20	19	0	2	13	8
α	P	E	R	M	U	T	A	C	N	I

Příklad - sami

Dekóduj slovo 14 26 20 19 25 12 12 26 8 20 v Z_{27}
$\pi = 53142$
Kódová abeceda={a, b,..., y, z, “”}

Příklad

Zakóduj slovo FOTBAL v Z_{27}

$$\mathbf{H} = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

Příklad - zakódování

$$\mathbf{FO} = \begin{pmatrix} 5 & 14 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 33 & 38 \end{pmatrix} = \begin{pmatrix} 6 & 11 \end{pmatrix}$$

$$\mathbf{TB} = \begin{pmatrix} 19 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 21 & 40 \end{pmatrix} = \begin{pmatrix} 21 & 13 \end{pmatrix}$$

$$\mathbf{AL} = \begin{pmatrix} 0 & 11 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 22 & 22 \end{pmatrix} = \begin{pmatrix} 22 & 22 \end{pmatrix}$$

$$\beta = \begin{pmatrix} G & L & V & N & W & W \end{pmatrix}$$

Příklad - dekódování

$$\mathbf{H^{-1}} = \begin{pmatrix} 26 & 1 \\ 1 & 13 \end{pmatrix}$$

$$\begin{pmatrix} 6 & 11 \end{pmatrix} \cdot \begin{pmatrix} 26 & 1 \\ 1 & 13 \end{pmatrix} = \begin{pmatrix} 167 & 149 \end{pmatrix} = \begin{pmatrix} 5 & 14 \end{pmatrix}$$

$$\begin{pmatrix} 21 & 13 \end{pmatrix} \cdot \begin{pmatrix} 26 & 1 \\ 1 & 13 \end{pmatrix} = \begin{pmatrix} 559 & 190 \end{pmatrix} = \begin{pmatrix} 19 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 22 & 22 \end{pmatrix} \cdot \begin{pmatrix} 26 & 1 \\ 1 & 13 \end{pmatrix} = \begin{pmatrix} 594 & 308 \end{pmatrix} = \begin{pmatrix} 0 & 11 \end{pmatrix}$$

$$\alpha = \begin{pmatrix} F & O & T & B & A & L \end{pmatrix}$$

Příklad - sami

Dekóduj slovo PRHBDG
v Z_{27}
Kódová abeceda={a, b,..., y, z, " "}
$\mathbf{H} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$