

Domácí úkol 4

Úloha 1 (8 bodů). Uvažujme následující způsob šifrování textových zpráv. Každému písmenu A až Z přiřadíme čísla 1 až 26.

A → 1	H → 8	O → 15	V → 22
B → 2	I → 9	P → 16	W → 23
C → 3	J → 10	Q → 17	X → 24
D → 4	K → 11	R → 18	Y → 25
E → 5	L → 12	S → 19	Z → 26
F → 6	M → 13	T → 20	
G → 7	N → 14	U → 21	

Tím pádem místo vstupního textu máme posloupnost čísel. Niní rozdělíme posloupnost do n -tic. Každá n -tice odpovídá vektoru $v = (v_1, \dots, v_n)^T \in \mathbb{R}^n$. Šifrujeme tak, že vektor přenásobíme předem danou regulární maticí $A \in \mathbb{R}^{n \times n}$, tedy každou n -tici v zašifrujeme na n -tici Av .

Příjemce pak naši zprávu dešifruje tak, že rozdělí posloupnost čísel na n -tice a každou n -tici w vynásobí maticí A^{-1} a dostane $A^{-1}w$. Pak zase přeloží čísla na znaky podle tabulky výše.

Dešifrujte posloupnost čísel

$$31, 53, 54, 87, 28, 47, 15, 29, 30, 55, 15, 29, 38, 67, 53, 85,$$

za předpokladu, že $n = 2$ a podařilo se nám zjistit, že slovo „PIVO“ se zašifruje jako 34, 59, 52, 89.

Úloha 2 (4 body). V grupě (G, \circ) s neutrálním prvkem e dokažte

- (a) $e^{-1} = e$,
- (b) $(a^{-1})^{-1} = a$,
- (c) $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$,
- (d) pokud $a \circ b = a$, pak $b = e$.

Úloha 3 (5 bodů). Ukažte, že pro $n \geq 2$ je počet lichých a sudých permutací v S_n stejný.