Domácí úkol 2: Diskrétní pravděpodobnost

Úloha 1. Ukažte, že Hillova šifra a transpoziční šifra obecně nekomutují. Uvažujte například text délky 4 a matici řádu 2.

Úloha 2. Náhodný pokus probíhá tak, že házíme n-krát ideální mincí. Nechť $k \leq n$. Jaká je pravděpodobnost

(i) jevu, že při počátečních k hodech padne alespoň jednou rub;

(ii) jevu, že celkem k-krát padne rub.

Úloha 3. Házíme dvěma kostkami. Určete pravděpodobnost, že na kostkách padnou různá čísla za podmínky, že součet čísel bude sudý.

Úloha 4. Nechť $\mathcal{P} = \mathcal{C} = \{a, b, c, d, e\}$ je množina otevřených a šifrových textů. Pravděpodobnostní rozdělení otevřených textů je dáno tabulkou:

a	b	c	d	e
0,1	0,4	0,2	0,05	0,25

Množina klíčů je $\mathcal{K} = \{k_1, k_2, k_3\}$, všechny klíče jsou stejně pravděpodobné. Šifrování je určeno následující tabulkou:

Otevřený text	a	b	c	d	e
Zašifrování klíčem k_1	b	e	a	d	c
Zašifrování klíčem k_2	a	c	e	b	d
Zašifrování klíčem k_3	c	e	d	a	b

Určete pravděpodobnost, že šifrový text je roven d.