Domácí úkol 4: Podmíněná entropie a perfektní šifry

V následujících úlohách značíme $\mathbf{K}$, $\mathbf{P}$ a $\mathbf{C}$ diskrétní náhodné veličiny, které odpovídají volbě klíče, volbě otevřeného textu a výslednému šifrovému textu. Předpokládáme, že $\mathbf{P}$ a $\mathbf{K}$ jsou nezávislé.

Úloha 1. Máme dva stejně silné týmy A a B, které spolu hrají na 4 vítězné zápasy. Náhodná veličina X reprezentuje průběhy série, tj. označíme-li A vítězství týmu A a označíme-li B vítězství týmu B, pak X nabývá např. AAAA, AAABBBB, ABABABA, ... Náhodná veličina Y reprezentuje počet odehraných zápasů. Spočítejte $\mathrm{H}(X)$, $\mathrm{H}(Y)$, $\mathrm{H}(X \mid Y)$, $\mathrm{H}(Y \mid X)$.

Úloha 2. Dokažte, že pro každou šifru platí $\mathrm{H}(\mathbf{K} \mid \mathbf{C}) \geq \mathrm{H}(\mathbf{P} \mid \mathbf{C})$. Co říká tato nerovnost slovy/významem?

Úloha 3. Nechť $(\mathcal{P}, \mathcal{C}, \mathcal{K}, E, D)$ je šifra, kde $\mathcal{P} = \{0,1\}^{10}$, $\mathcal{K} = \{0,1\}^5$ a $\mathcal{C} = \{0,1\}^{10}$. Diskrétní náhodné veličiny $\mathbf{P}$ a $\mathbf{K}$ mají rovnoměrné rozdělení. Kdykoliv zašifrujeme jeden otevřený text dvěma různými klíči, výsledkem jsou dva různé šifrové texty. Spočítejte průměrnou informaci o otevřeném textu a o klíči extrahovanou útočníkem z šifrového textu (kolik informace o klíči a otevřeném textu se v průměru dozví z šifrového textu, tj. $I(\mathbf{P}; \mathbf{C})$ a $I(\mathbf{K}; \mathbf{C})$).

Úloha 4. Množina otevřených textů obsahuje tři stejně pravděpodobné zprávy a, b a c. Množina šifrových textů je shodná s množinou otevřených textů. Používáme tři stejně pravděpodobné klíče $\{k_1, k_2, k_3\}$ a platí: $E_{k_1} : a \mapsto c$, $b \mapsto a$, $c \mapsto b$; $E_{k_2} : a \mapsto b$, $b \mapsto c$, $c \mapsto a$; $E_{k_3} : a \mapsto c$, $b \mapsto b$, $c \mapsto a$. Je tato šifra perfektní? Pokud ne, jakou jednoduchou změnu byste provedli, aby šifra perfektní byla?