# Zgoščevalne funkcije, lastnost popolne tajnosti

1. Naj bo $f : \{0,1\}^n \to \{0,1\}^n$ bijektivna enosmerna funkcija in $H : \{0,1\}^{2n} \to \{0,1\}^n$ kompresijska funkcija definirana s

$$H(x_1||x_2) = f(x_1 \oplus x_2).$$

   Katere od lastnosti ima funkcija $H$: odpornost praslik, odpornost 2-praslik, odpornost na trke?

2. **Kompresijska funkcija Chaum, van Heijst, Pfitzmann**. Naj bo $p$ takšno praštevilo, da je tudi $q = (p-1)/2$ praštevilo. Naj bo $a$ generator grupe $\mathbb{Z}_p^*$ in $b$ naključno izbran element grupe $\mathbb{Z}_p^*$. Kompresijsko funkcijo $h : \mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{Z}_p^*$ definiramo takole:

$$h : (x_1, x_2) \mapsto a^{x_1}\, b^{x_2} \bmod p.$$

   (a) Naj bo $p = 23$, $q = 11$, $a = 5$ in $b = 4$. Izračunajte $h(5, 10)$.

   (b) Pokažite, da je ta kompresijska funkcija odporna na trke, če predpostavimo, da je problem diskretnega logaritma v grupi $\mathbb{Z}_p^*$ težek.

   (c) Za $q = 11$, $p = 23$, $a = 5$ in $b = 4$ izračunajte $h(5, 10)$. Iz trka $((4, 9), (6, 3))$ izračunajte diskretni logaritem elementa 4 z osnovo 5.

3. V nekem jeziku so le 3 črke: $A, B$ in $H$. V spodnji tabeli so podane frekvence digramov:

| | A | B | H |
|---|---|---|---|
| A | 0 | 0.17 | 0.02 |
| B | 0.03 | 0.02 | 0 |
| H | 0.71 | 0.01 | 0.04 |

   Besedilo zakodiramo tako, da vsaki črki priredimo številko: $A \mapsto 0$, $B \mapsto 1$, $H \mapsto 2$. Nato besedilo $b = b_1 b_2 \dots b_n \in \mathbb{Z}_3^n$ zašifriramo s ključem $k = k_1 k_2 \dots k_n \in \mathbb{Z}_3^n$ v kriptogram $c = c_1 c_2 \dots c_n \in \mathbb{Z}_3^n$, kjer je $c_i = b_i + k_i \bmod 3$.

   Trije kriptogrami $BA$, $AH$ in $BB$ so zašifrirani z istim ključem. Kateri ključ je bil najverjetneje uporabljen? Dešifrirajte kriptograme.

4. Kriptosistem $\mathcal{S} = (\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ opremimo z verjetnostnimi porazdelitvami $B$, $C$ in $K$ na množicah $\mathcal{B}$, $\mathcal{C}$ in $\mathcal{K}$. Pokažite, da ima kriptosistem $\mathcal{S}$ lastnost popolne tajnosti natanko tedaj, ko

   (a) za vsak $b \in \mathcal{B}$ in za vsak $c \in \mathcal{C}$ velja $P[C = c|B = b] = P[C = c]$.

   (b) za vsak par $b, b' \in \mathcal{B}$ in za vsak $c \in \mathcal{C}$ velja $P[C = c|B = b] = P[C = c|B = b']$.