Domácí úkol 5: DES

Úloha 1. Máme dán otevřený text a dva šifrové texty $x, y_1, y_2 \in \{0,1\}^{64}$ takové, že $y_1 = \mathrm{DES}(x,k)$ a $y_2 = \mathrm{DES}(\overline{x},k)$, kde klíč k je neznámý. Operace $x \mapsto \overline{x}$ značí bitovou negaci, např. $\overline{1101} = 0010$. Popište útok, kterým lze odhalit klíč k s průměrnou časovou složitostí 2^{54} šifrovacích operací šifry DES. Využijte toho, že $\overline{\mathrm{DES}(x,k)} = \mathrm{DES}(\overline{x},\overline{k})$ pro libovolný otevřený text x a šifrovací klíč k.

Úloha 2. Nechť k je šifrovací klíč a $k_1, k_2, \ldots, k_{16}$ jsou příslušné rundovní klíče šifry DES. Označme $(C_0, D_0) = \mathrm{PC1}(k)$. Dokažte, že platí-li $k_1 = k_2 = \cdots = k_{16}$, pak všechny bity v C_0 mají stejnou hodnotu a všechny bity v D_0 mají stejnou hodnotu.

Úloha 3. Říkáme, že klíč k je *slabý*, jestliže $\mathrm{DES}(x,k) = \mathrm{DES}^{-1}(x,k)$ pro všechna $x \in \{0,1\}^{64}$. Popište čtyři slabé klíče DESu.