Cryptography for Computer Scientists 2018/19	Oct 17, 2018

Exercises 3

Stefan Dziembowski MIM UW

Exercise 1: Pseudorandom functions from pseudorandom generators

Let $G : \{0,1\}^* \rightarrow \{0,1\}^*$ be a *length-doubling* pseudorandom generator, i.e., such that for every x we have $|G(x)| = 2 \cdot |x|$. Using G construct a pseudorandom function.
Hint: Consider using a binary tree.

Exercise 2: Pseudorandom functions

Let $f : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ and $g : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ be pseudorandom functions such that its input block length is equal to its key length and equal to its output block length. For h_i's defined as below decide if they are pseudorandom functions (if the answer is "yes" then give a proof, and otherwise provide a counterexample).

1. $h_1(k, (m_1, m_2)) := f(k, m_1) \oplus g(k, m_2)$,
2. $h_2(k, (m_1, m_2)) := f(k, m_1) \oplus g(k, m_1 \oplus m_2)$,
3. $h_3(k, m) = f(k, m) \oplus m$.

(above $|k_1| = |k_2| = |k| = |m_1| = |m_2|$)

Exercise 3: Complementarity of DES

Let $\overline{x}$ denote $y = (y_1, \ldots, y_n) \in \{0,1\}^*$ where each y_i is a negation of x_i (i.e. $y_i := 1 + x_i \bmod 2$). For $x = (x_1, \ldots, x_n) \in \{0,1\}^*$. Show that for every message m and every key k we have

$$\mathrm{DES}_k(m) = \overline{\mathrm{DES}_{\overline{k}(\overline{m})}}.$$

Show how to use this property to reduce the time of brute-force attack on DES by factor 2.