Homework 2
Due at the beginning of class on Sept. 29

1. (Exercise 2.2.) Prove or refute: For every encryption scheme that is perfectly secret, it holds that for every distribution over the message space $\mathcal{M}$, every $m, m' \in \mathcal{M}$, and every $c \in C$:

$$\Pr[M = m \mid C = c] = \Pr[M = m' \mid C = c].$$

2. (Exercise 2.9.) Consider the following definition of perfect secrecy for the encryption of two messages. An encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ over a message space $\mathcal{M}$ is perfectly-secret for two messages if for all distributions over $\mathcal{M}$, all $m, m' \in \mathcal{M}$, and all $c, c' \in C$ with $\Pr[C = c \land C' = c'] > 0$:

$$\Pr[M = m \land M' = m' \mid C = c \land C' = c'] = \Pr[M = m \land M' = m'],$$

where $m$ and $m'$ are sampled independently from the same distribution over $\mathcal{M}$. Prove that no encryption scheme satisfies this definition. (Hint: Take $m \neq m'$ but $c = c'$.)

3. Define $G : \{0,1\}^* \rightarrow \{0,1\}^*$ by $G(x_1, \ldots, x_n) = x_1 \oplus x_2, x_1, \ldots, x_n$. (Note that the output of $G$ is one bit longer than its input.) Prove that this $G$ is not a pseudorandom generator.

4. Define $F : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ as follows: $F_k(x) = k \oplus x$. In class we proved that this $F$ is not a pseudorandom function by showing an algorithm that could distinguish $F$ from random using two queries. Can you construct a distinguishing algorithm that uses only one query? Either describe and analyze such an algorithm, or argue informally why no such algorithm exists.

5. Define $F : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}$ as follows: $F_{k_1, \ldots, k_n}(x_1, \ldots, x_n) = \bigoplus_i k_i x_i$, where $k_i, x_i \in \{0,1\}$. (Note that, different from the usual convention, $F$ takes an $n$-bit key and an $n$-bit input, but has only a single-bit output.) Prove that this $F$ is not a pseudorandom function.