Cryptography

Problem set 1 - 27-28 III 2013

Definition 1. An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ is **perfectly secret** if for every probability distribution over $\mathcal{M}$, every messsage $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $P[C = c] > 0$:

$$P[M = m|C = c] = P[M = m].$$

Definition 2. An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ is **perfectly secret** if and only if for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$:

$$P[C = c|M = m] = P[C = c].$$

Definition 3. An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ is **perfectly secret** if for every probability distribution over $\mathcal{M}$, every $m_0, m_1 \in \mathcal{M}$, and every $c \in \mathcal{C}$:

$$P[C = c|M = m_0] = P[C = c|M = m_1].$$

Problem 1 Prove or refute: definitions 1 and 2 are equivalent.

Problem 2 Prove or refute: definitions 2 and 3 are equivalent.

Problem 3 Prove or refute: definitions 1 and 3 are equivalent.

Problem 4 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 $c \in \mathcal{C}$:

$$P[M = m|C = c] = P[M = m'|C = c].$$

Problem 5 1. Prove that the *shift cipher* is perfectly secure if only a single character is encrypted.

2. Prove that One Time Pad is perfectly secure.