Cryptography

Problem set 1

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 $c \in \mathcal{C}$:

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

Definition 4. A function f is negligible if for every polynomial $p(\cdot)$ there exists an N such that for all integers $n > N$ it holds that $f(n) < \frac{1}{p(n)}$.

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 Consider the following definition of perfect secrecy for the encryption of two messages. An encryption scheme $\langle \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec} \rangle$ over a message space $\mathcal{M}$ is perfectly-secret for two messages if for all distributions over $\mathcal{M}$, all $m_0, m_1 \in \mathcal{M}$, and all $c_0, c_1 \in \mathcal{C}$ with $P(C_0 = c_0 \wedge C_1 = c_1) > 0$:

$$P(M_0 = m_0 \wedge M_1 = m_1 | C_0 = c_0 \wedge C_1 = c_1) = P(M_0 = m_0 \wedge M_1 = m_1),$$

where m_0 and m_1 are sampled independently from the same distribution over $\mathcal{M}$.

Prove that no encryption scheme satisfies this definition (hint: take $m_0 \neq m_1$ but $c_0 = c_1$).

Problem 6
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.

Problem 7 The best algorithm known today for finding the prime factors of an n-bit number runs in time $2^{cn^{\frac{1}{3}}(\log n)^{\frac{2}{3}}}$. Assuming $4GHz$ computers and $c = 1$ (and that the units of the given expression are clock cycles), estimate the size of numbers that cannot be factored for the next 100 years.

Problem 8 Let f, g be negligible functions. Show that:

1. The function $h(n) = f(n) + g(n)$ is negligible .
2. For any positive polynomial p, the function $h(n) = p(n) \cdot f(n)$ is negligible .

Problem 9 (2 points) Let $\Pi_1 = \langle Gen_1, Enc_1, Dec_1 \rangle$, $\Pi_2 = \langle Gen_2, Enc_2, Dec_2 \rangle$ be the two private-key encryption schemes. Show how to construct Π – a *CPA-secure* private-key encryption scheme by combining schemes Π_1 and Π_2. You may assume that Π_i is *CPA*-secure but you do not know which one.

Assuming that an adversary can win the *CPA* experiment with an advantage ϵ_i for the scheme Π_i, evaluate adversary's advantage for the scheme Π.