Begin each problem on a separate page.

**Problem 1  Hard-Core Predicates**

(a) Let $f$ be a (strong) one-way function. Consider $g(x_1 x_2 \cdots x_n) = f(x_2 x_3 \cdots x_n)$ (where each $x_i$ is a bit). Show that $g$ is also a one-way function and has a hard-core bit.

(b) Assume the existence of one-way functions. Show that there does not exist a single hard-core predicate that works for every one-way function.

**Problem 2  Trapdoor One-Way Functions**

Let $f$ be a one-way permutation. In this problem, we will use $f$ to construct a family of trapdoor one-way functions $G$ (not one-way permutations!). The idea is to evaluate the function $f$ as usual. The only exception is that when the input is a special value $\alpha$, then $g$ operates in a way that makes it easy to invert. Define $G = \{ g_\beta \}_{\beta \in \{0,1\}^*}$ as follows: $g_\beta$ is a function $\{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$, where $|\beta| = n$.

$$g_\beta(e,v) = \begin{cases} v & \text{if } f(e) = \beta \\ f(v) & \text{otherwise} \end{cases}$$

Define Gen and the sampling function for the domain of $g_\beta$ and prove that $G$ is a collection of trapdoor one-way functions. (You can think about how to extend this argument when $f$ is any one-way function.)

**Problem 3  Pseudorandom Generators**

Let $f : \{0,1\}^n \rightarrow \{0,1\}^{m(n)}$ and $g : \{0,1\}^{n'} \rightarrow \{0,1\}^{m'(n)}$ be two pseudo-random generators, where $m$ and $m'$ are polynomials. Prove or disprove the following:

(a) The function $h$ defined as $h(x) = g(f(x))$ is a PRG.

(b) The function rev$(f)$ defined as rev$(f)(x) = (f(x))^R$ is a PRG, where $y^R$ stands for the reverse of the string $y$.

(c) The function $h$ defined as $h(x) = f(x) \oplus g(x)$ is a PRG ($\oplus$ is bitwise xor) $m$ and $m'$ are the same polynomial.

(d) The function $h$ defined as $h(s\|s') = s\|f(s')$, where $|s| = |s'| = n$ is a PRG.

(e) The function $h$ defined as $h(s\|s') = s\|f(s\|s')$, where $|s| = |s'| = \frac{n}{2}$ is a PRG.
Problem 4 Pseudorandom Functions

Let \( \mathcal{F} = \{ f_s : \{0, 1\}^{|s|} \to \{0, 1\}^{|s|}, s \in \{0, 1\}^* \} \) be a PRF. Let \( \mathcal{G} = \{ g_s : \{0, 1\}^{l(|s|)} \to \{0, 1\}^*, s \in \{0, 1\}^* \} \). Prove or disprove that \( \mathcal{G} \) is a PRF in the following cases. For all \( s \in \{0, 1\}^* \), \( x \in \{0, 1\}^{l(|s|)} \) define \( g_s \) as:

(a) \( g_s(x) = f_s(x) \| f_s(x + 1 \mod 2^{|s|}) \) where \( l(n) = n \).

(b) \( g_s(x) = f_{0^{|s|}}(x) \| f_s(x) \) where \( l(n) = n \).

(c) \( g_s(x) = f_{s_1}(x) \| f_{s_2}(x + 1 \mod 2^{|s|}) \), where \( s_1 \) is the first \( |s|/2 \) bits of \( s \), \( s_2 \) is the second \( |s|/2 \) bits of \( s \), and \( l(n) = n/2 \).

(d) \( g_s(x) = f_s(x) \oplus s \)

Problem 5 Secure Encryption

Definition 1 Given two strings \( x, y \) of length \( n \), the Hamming distance between \( x \) and \( y \), denoted by \( H(x, y) \), is the number of positions in which \( x \) and \( y \) differ, e.g., \( H(00, 01) = 1, H(01010, 11110) = 2 \).

Let us give possible definitions of next-message secure encryption schemes. For each of the cases given below, determine whether the private-key encryption scheme is secure. Prove or provide a counter-example. An encryption scheme \((\text{Gen}, \text{Enc}, \text{Dec})\) is next-message secure iff

(a) For all messages \( m_0 \) and \( m_1 \) such that \( H(m_0, m_1) = 1 \), the encryptions of \( m_0 \) and \( m_1 \) are indistinguishable. Formally, for all distinguishers \( D \), there exists a negligible function \( \epsilon(\cdot) \), such that for all \( n \), and \( m_0, m_1 \in \{0, 1\}^n \) such that \( H(m_0, m_1) = 1 \),

\[
\left| \Pr[D(\text{Enc}(m_0)) = 1] - \Pr[D(\text{Enc}(m_1)) = 1] \right| \leq \epsilon(n)
\]

(b) For all messages \( m \) (\( m \neq 1^n \)), the encryptions of \( m \) and \( m + 1 \) are indistinguishable.