Cryptology: Assignment 2

Topics: Symmetric Key Encryption, Computational Security, PRG, PRF

1. Are the following functions negligible or not? Justify your answer.
   (a) $\mu_1(n) := \nu_1(n)/\nu_2(n)$, for any negligible functions ν_1 and ν_2 with $\nu_2(n) > 0$, for all n.
   (b) $\mu_2(n) := \nu_1(n) \,.\, \nu_2(n)$, for any negligible functions ν_1 and ν_2.
   (c) $\mu_3(n) := n \log n \,.\, \nu(n)$, for any negligible function ν.
   (d) $\mu_4(n) := n^{100},\ \mu_5(n) := n^{\log n}$.

2. Let us consider two problems based on the hardness of Discrete Logarithm problem.

   Definition 1 (Computational Diffie–Hellman (CDH))**.** Let $G = \langle g \rangle$ be a cyclic group of prime order $q > 2$. The *Computational Diffie–Hellman (CDH) problem* is:

   $$\text{Given } (g, g^a, g^b),\ a, b \xleftarrow{\$} \mathbb{Z}_q, \text{ to compute } g^{ab}.$$

   Definition 2 (Squared Diffie–Hellman (SDH))**.** Let $G = \langle g \rangle$ be a cyclic group of prime order q. The *Squared Diffie–Hellman (SDH) problem* is:

   $$\text{Given } (g, g^a),\ a \xleftarrow{\$} \mathbb{Z}_q, \text{ compute } g^{a^2}.$$

   Show that if CDH is hard in G, then SDH is also hard in G. [Hint: Can you show computing the square root of any element $h \in G$ is easy?]

3. Let G be a pseudorandom generator (PRG) with expansion factor $\ell(n) > n + 1$.
   (a) Show that $G_1(s) = G(s_1 s_2 \dots s_{n-1}) \| s_n$ is PRG, where $s = s_1 s_2 \cdots s_n$.
   (b) Prove that $G_2(s) = G(s) \| G(\overline{s})$ is not a PRG. [Hint: Can you use the previous result?]

4. Prove that if F is a pseudorandom function (PRF) defined over $(\{0,1\}^n, \{0,1\}^n, \{0,1\}^n)$, then
   $$G(s) := F_s(1) \| F_s(2) \| \cdots \| F_s(\ell)$$
   is a pseudorandom generator (PRG) with expansion factor $n\ell$.

5. Let F be a secure PRF defined over $(\{0,1\}^n, \{0,1\}^n, \{0,1\}^n)$.
   (a) Prove that $\widetilde{F}_k(x) := F_k(x) \oplus x$ is a secure PRF.
   (b) Prove that $\widetilde{F}_{(k,k')}(x) := F_k(x) \oplus F_{k'}(x)$ is a secure PRF.
   (c) Show that $\widetilde{F}_k(x) := F_k(x) \oplus F_k(x \oplus 1^n)$ is not a secure PRF.
   (d) Show that $\widetilde{F}_k(x) := F_k(x) \| F_k(F_k(x))$ is not a secure PRF.

6. Let F be a secure PRF defined over $(\{0,1\}^n, \{0,1\}^n, \{0,1\}^n)$. Justify whether the following constructions are PRF or not.

   (a) $\widetilde{F}_k(x) := F_k(0\|x) \parallel F_k(1\|x)$.

   (b) $\widetilde{F}_k(x) := F_k(0\|x) \parallel F_k(x\|1)$.

7. Consider the following definition of a weak pseudorandom function (weak PRF), which intuitively is like a PRF but has a weaker oracle access: it only allows you to get the PRF output on a uniform random input (similar to how you see the PRG output only on a random input). A family of functions $\mathcal{F} := \{F_k : \{0,1\}^n \to \{0,1\}^n\}_{k\in\mathcal{K}}$ is called a *weak PRF* if for every PPT distinguisher $\mathcal{D}$, there exists a negligible function $negl$ such that $\forall\ n$:

$$\left|\Pr_k[\mathcal{D}^{F_k(\$)} = 1] - \Pr_f[\mathcal{D}^{f(\$)} = 1]\right| \leq negl(n)\,,$$

   where $f_k(\$)$ and $f(\$)$ are modified oracles that output $(r, F_k(r))$ and $(r, f(r))$, respectively, for $r \leftarrow_\$ \{0,1\}^n$.

   (a) Prove that if $\mathcal{F}$ is a PRF then $\mathcal{F}$ is a weak-PRF.

   (b) Let $\mathcal{F} := \{f_k : \{0,1\}^n \to \{0,1\}^n\}$ be a PRF. We define $\mathcal{G} := \{g_k : \{0,1\}^n \to \{0,1\}^n\}$ as follows:

$$g_k(x) = \begin{cases} 0^n, & \text{if } x = 0^n, \\ f_k(x), & \text{otherwise.} \end{cases}$$

   Prove that $\mathcal{G}$ is weak-PRF but not a PRF.

8. Let us consider the following two notions of Indistinguishability.

   Definition 3 (Left-or-Right (LOR) Indistinguishability)**.** Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme. The LOR game chooses a random bit $b \leftarrow \{0,1\}$ and a key $K \leftarrow \mathsf{Gen}(1^n)$. Given equal-length messages (m_0, m_1), the challenger returns $C \leftarrow \mathsf{Enc}_K(m_b)$. The adversary $\mathcal{A}$ returns b' and wins if it correctly guesses $b' = b$. The LOR advantage of $\mathcal{A}$ is

$$\mathsf{Adv}^{\mathrm{LOR}}_{\Pi}(\mathcal{A}) = \left|\Pr[b' = b] - \frac{1}{2}\right|.$$

   The encryption scheme Π is called LOR-indistinguishable if this advantage is negligible for every PPT adversary $\mathcal{A}$.

   Definition 4 (Real-or-Random (ROR) Indistinguishability)**.** Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme. The ROR game chooses a random bit $b \leftarrow \{0,1\}$ and a key $K \leftarrow \mathsf{Gen}(1^\lambda)$. Given a message m, the challenger returns $C \leftarrow \mathsf{Enc}_K(m)$, if $b = 0$. Otherwise, it returns a ciphertext of length $|m|$, chosen uniformly at random string. The adversary $\mathcal{A}$ returns a bit b' and wins if it correctly guesses $b' = b$. The ROR advantage of $\mathcal{A}$ is

$$\mathsf{Adv}^{\mathrm{ROR}}_{\Pi}(\mathcal{A}) = \left|\Pr[b' = b] - \frac{1}{2}\right|.$$

   The encryption scheme is ROR-indistinguishable if this advantage is negligible for every PPT adversary $\mathcal{A}$.

   Prove that an encryption scheme Π achieves LOR indistinguishability if and only if Π achieves ROR indistinguishability.

9. Let F be a pseudorandom function from n-bits to n-bits and G be a pseudorandom generator with expansion factor $n+1$. For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of (i) an eavesdropper and (ii) chosen plaintext adversary.

   (a) $Enc_k(m) := \langle r,\ G(r) \oplus m \rangle$, where $m \in \{0,1\}^{n+1}$, $r \leftarrow_{\$} \{0,1\}^n$.

   (b) $Enc_k(m) := m \oplus F_k(0^n)$.

   (c) $Enc_k(m) := \langle r,\ m_1 \oplus F_k(r),\ m_2 \oplus F_k(r+1) \rangle$, where $r \leftarrow_{\$} \{0,1\}^n$, where $m = m_1 \| m_2$, $|m_1| = |m_2| = n$.