CS442: Introduction to Cryptography Instructor: Aarushi Goel

Homework 3

Due: April 5; 2026 (11:59 PM)

1 CPA Secure Encryption

Determine whether the following encryption schemes are CPA-secure. If you believe a scheme is CPA-secure, provide an intuitive explanation (a formal proof is not required). If you believe it is not secure, describe a concrete attack that violates CPA-security.

1. **(10 points)** Let $G : \{0,1\}^n \to \{0,1\}^{n+1}$ be a pseudorandom generator (PRG). Consider the following scheme for encrypting messages $m \in \{0,1\}^{n+1}$.

   - $\mathsf{KeyGen} \to k$: Sample a key $k \xleftarrow{\$} \{0,1\}^n$.
   - $\mathsf{Enc}(k, m) \to c$: Compute and output $c = m \oplus G(k)$.
   - $\mathsf{Dec}(k, c) \to m$: Compute and output $m = c \oplus G(k)$.

2. **(10 points)** Let $\{f_k\}_k$ be a family of pseudorandom functions (PRFs), where $f_k : \{0,1\}^n \to \{0,1\}^n$ and $k \in \{0,1\}^n$. Consider the following scheme for encrypting messages $m \in \{0,1\}^{2n}$.

   - $\mathsf{KeyGen} \to k$: Sample a key $k \xleftarrow{\$} \{0,1\}^n$.
   - $\mathsf{Enc}(k, m) \to c$: Parse $m = m_1 \| m_2$, where each $m_i \in \{0,1\}^n$, sample $r \xleftarrow{\$} \{0,1\}^n$, and output
     $$c = (r,\, m_1 \oplus f_k(r),\, m_2 \oplus f_k(r)) .$$
   - $\mathsf{Dec}(k, c) \to m$: Parse $c = (c_1, c_2, c_3)$, compute $m_1 = c_2 \oplus f_k(c_1)$ and $m_2 = c_3 \oplus f_k(c_1)$, and output $m = m_1 \| m_2$.

3. **(10 points)** Let $\{f_k\}_k$ be a family of pseudorandom functions (PRFs), where $f_k : \{0,1\}^n \to \{0,1\}^n$ and $k \in \{0,1\}^n$. Consider the following scheme for encrypting messages $m \in \{0,1\}^{2n}$.

   - $\mathsf{KeyGen} \to k$: Sample a key $k \xleftarrow{\$} \{0,1\}^n$.
   - $\mathsf{Enc}(k, m) \to c$: Parse $m = m_1 \| m_2$, where each $m_i \in \{0,1\}^n$, sample $r \xleftarrow{\$} \{0,1\}^n$, and output
     $$c = (r,\, m_1 \oplus f_k(r),\, m_2 \oplus f_k(r+1)) .$$
   - $\mathsf{Dec}(k, c) \to m$: Parse $c = (c_1, c_2, c_3)$, compute $m_1 = c_2 \oplus f_k(c_1)$ and $m_2 = c_3 \oplus f_k(c_1 + 1)$, and output $m = m_1 \| m_2$.

2 Modes of Operation

Let $\{f_k\}_k$ be a family of *pseudorandom permutations (PRPs)*, where $f_k : \{0,1\}^n \to \{0,1\}^n$ and $k \in \{0,1\}^n$. Consider the following mode of operation (a variant of counter (CTR) mode from Lecture 14) for encrypting arbitrarily long messages $m \in \{0,1\}^{nt}$, where t is arbitrary:

- $\mathsf{KeyGen} \to k$: Sample a key $k \xleftarrow{\$} \{0,1\}^n$.
- $\mathsf{Enc}(k, m) \to c$: Parse $m = m_1 \| \ldots \| m_t$, where each $m_i \in \{0,1\}^n$. Sample $\mathsf{ctr} \xleftarrow{\$} \{0,1\}^n$. For each $i \in [t]$, compute $c_i = f_k(\mathsf{ctr} + i + m_i)$. Output $c = (\mathsf{ctr}, c_1, \ldots, c_t)$.

1. **(5 points)** Describe the corresponding decryption algorithm.
2. **(10 points) Is this scheme CPA-secure?** If you believe it is CPA-secure, provide an intuitive explanation (a formal proof is not required). If you believe it is not secure, describe a concrete attack that violates CPA-security.
3. **(10 points)** Recall from Lectures 13 that a *ciphertext only attack (COA)-secure* encryption scheme is one where each key is used to encrypt only a single message. **Is this scheme COA secure?** If you believe it is secure, provide a formal proof. Otherwise, describe a concrete attack that violated COA security.

3 Message Authentication Codes

Let $\{f_k\}_k$ be a family of pseudorandom functions (PRFs), where $f_k : \{0,1\}^n \to \{0,1\}^n$ and $k \in \{0,1\}^n$. **Show concrete attacks demonstrating that each of the following schemes is NOT a many-time secure message authentication code.**

1. **(10 points)** Consider the following scheme for authenticating messages $m \in \{0,1\}^{nt}$, where t is arbitrary:
   - $\mathsf{KeyGen} \to k$: Sample a key $k \xleftarrow{\$} \{0,1\}^n$.
   - $\mathsf{Sign}(k, m) \to \sigma$: Parse $m = m_1 \| \ldots \| m_t$, where each $m_i \in \{0,1\}^n$. Compute
   $$\sigma = f_k(m_1) \oplus \cdots \oplus f_k(m_t).$$
   - $\mathsf{Verify}(k, m, \sigma) \to b$: Parse $m = m_1 \| \ldots \| m_t$, recompute the above value, and check if it equals σ. Output $b = 1$ if equal, and $b = 0$ otherwise.
2. **(10 points)** Let $\langle i \rangle$ denote an $n/2$-bit encoding of the integer i. Consider the following scheme for authenticating messages $m \in \{0,1\}^{nt}$:
   - $\mathsf{KeyGen} \to k$: Sample a key $k \xleftarrow{\$} \{0,1\}^n$.
   - $\mathsf{Sign}(k, m) \to \sigma$: Parse $m = m_1 \| \ldots \| m_{2t}$, where each $m_i \in \{0,1\}^{n/2}$. Compute
   $$\sigma = f_k(\langle 1 \rangle \| m_1) \oplus \cdots \oplus f_k(\langle 2t \rangle \| m_{2t}).$$
   - $\mathsf{Verify}(k, m, \sigma) \to b$: Parse $m = m_1 \| \ldots \| m_{2t}$, recompute the above value, and check if it equals σ. Output $b = 1$ if equal, and $b = 0$ otherwise.