CS 409M : Introduction to Cryptography Fall 2024

Mid-sem Exam

Full Marks: 40, **Time**: 2 hours

Roll Number: ____________________ **Name:** ____________________

1. Answer each question on a new page of the answer booklet.
2. Do not use pencils. Pens only!
3. If you want, use me as your cheat sheet and ask me for definitions.
4. To give proof of security, an intuitive explanation will only get you part points. Give a complete security reduction or hybrid argument to get full marks.

Problem 1: [3 marks]

When using the one-time pad with the key $k = 0^\ell$, we have $\texttt{Enc}_k(m) = k \oplus m = m$, and the message is sent in the clear! Therefore, we modify the one-time pad by only encrypting with $k \neq 0^\ell$ (i.e., $\texttt{Gen}$ chooses k uniformly from the set of *nonzero* keys of length ℓ). Is this modified scheme still perfectly secure? Explain.

Problem 2: [9 marks (3+3+3)]

Let F be a pseudorandom function and G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$. In each case below, the shared key is a uniform $k \in \{0,1\}^n$. Against which of the following attacks is each encryption scheme below secure: ciphertext only attack (COA), chosen plaintext attack (CPA), and chosen ciphertext attack (CCA)? If secure, show proof of security; if not, show an attack.

a) To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.

b) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.

c) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 || m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0,1\}^n$ and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.

Problem 3: [6 marks (3+3)]

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. In each part below, is $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ EU-CMA secure? If yes, give proof of security; if not, show an attack.

a) Gen outputs a uniform $k \in \{0,1\}^n$. To authenticate a message $m_1 || m_2$ with $|m_1| = |m_2| = n$, Mac_k computes the tag $t = F_k(m_1) || F_k(F_k(m_2))$. Verification is the canonical verification.

b) Gen outputs a uniform $k \in \{0,1\}^n$. To authenticate a message m, Mac_k computes the tag $t = (F_k(m), F_k(m))$. Verification is the canonical verification.

Problem 4: [7 marks (2+2+3)]

Let $\Pi_E = (\mathsf{Gen}_E, \mathsf{Enc}, \mathsf{Dec})$ be a CPA-secure encryption scheme, and let $\Pi_M = (\mathsf{Gen}_M, \mathsf{Mac}, \mathsf{Vrfy})$ be an EU-CMA secure message authentication code. Consider the following authenticate-then-encrypt approach for encryption.

Authenticate-then-encrypt

Define $\Pi = (\mathsf{Gen}, \mathsf{AEnc}, \mathsf{ADec})$ as follows:

- $\mathsf{Gen}(1^n)$: Choose independent $k_E \leftarrow \mathsf{Gen}_E(1^n)$ and $k_M \leftarrow \mathsf{Gen}_M(1^n)$. Output (k_E, k_M).
- AEnc: on input a key (k_E, k_M) and a plaintext message m, compute $t \leftarrow \mathsf{Mac}_{k_M}(m)$ and $c \leftarrow \mathsf{Enc}_{k_E}(m||t)$. Output the ciphertext c.
- ADec: on input a key (k_E, k_M) and a ciphertext c, compute $\mathsf{Dec}_{k_E}(c) = m||t$. If $\mathsf{Vrfy}_{k_M}(m, t) = 1$, output m, else output $\perp$.

a) Prove that Π is a CPA-secure encryption scheme.

b) Prove that Π satisfies ciphertext integrity.

c) Is Π CCA secure? If yes, prove it, else, show an attack (for some Π_E and Π_M).

Problem 5: [5 marks]

Recall the Merkle-Damgård transform described below. Let (Gen, h) be a fixed-length collision resistant hash function for inputs of length $2n$ and with output length n.

Merkle-Damgård Transform

Construct the hash function (Gen, H) (with the same Gen) as follows:
H: on input a key k and a string $x \in \{0,1\}^*$ of length $L < 2^n$, do the following:

1. Set $B := \left\lceil \frac{L}{n} \right\rceil$ (i.e., the number of blocks in x). Pad x with zeroes so its length is a multiple of n. Parse the padded result as the sequence of n-bit blocks $x_1, \ldots, x_B$. Set $x_{B+1} := L$, where L is encoded as an n-bit string.
2. Set $z_0 := 0^n$. (also called the IV.)
3. For $i = 1, \ldots, B+1$, compute $z_i := h^k(z_{i-1}||x_i)$.
4. Output z_{B+1}.

For each of the following modifications to the Merkle-Damgård transform, determine whether the result is collision resistant. If yes, provide a proof; if not, demonstrate an attack.

a) Instead of using a fixed IV, set $z_0 := L$ and compute $z_i := h^k(z_{i-1}||x_i)$ for $i = 1, \ldots, B$. Output z_B.

b) Modify the construction so that instead of $z_{B+1} = h^k(z_B||L)$, the output is $z_B||L$.

Problem 6: [5 marks]

Let $(\mathsf{Gen}, \hat{h})$ be a fixed-length collision resistant hash function with input length $2n-1$ and output length $n-1$. Define (Gen, h) using the same Gen, on inputs of length $2n$ as:

$$h^k(b||x) := \begin{cases} b||\hat{h}^k(x), & \text{if } b = 0 \\ 1^n, & \text{otherwise} \end{cases}$$

a) Is (Gen, h) a collision resistant hash function?

b) Is the (Gen, H) obtained using Merkle-Damgård transform to (Gen, h) collision resistant?

Problem 7: [5 marks]

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a strong pseudorandom permutation (SPRP). Define the following encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$:

- $\mathsf{Gen}(1^n)$: Generate and output $k \in_R \{0,1\}^n$.
- $\mathsf{Enc}(k, m)$: For $m \in \{0,1\}^{n/2}$, generate a random $r \in_R \{0,1\}^{n/2}$ and output $c = F_k(m||r)$.
- $\mathsf{Dec}(k, m)$: Compute $m||r := F_k^{-1}(c)$, and output the first $n/2$-bits, m.

Prove that Π is CCA-secure but is not an authenticated encryption scheme.