Indian Institute of Technology Kharagpur
Department of Computer Science and Engineering

CS60088 Foundations of Cryptography **Spring 2026**

Mid-Semester Examination **26 February, 9 AM – 11 AM** **Marks = 60**

*Answer **any four** questions. State all assumptions you make. Keep your answers concise.*

1. (a) Consider a private key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ defined as follows:

   $\mathsf{Gen}(1^\lambda)$: $k \xleftarrow{\text{U}} \{0,1\}^{\lambda/2}$, $\mathcal{M} = \mathcal{C} = \{0,1\}^\lambda$.
   $\mathsf{Enc}(k, m)$: $c \leftarrow m \oplus (k||k)$
   $\mathsf{Dec}(k, m)$: $m \leftarrow c \oplus (k||k)$

   If this scheme perfectly secure? Justify.

   (b) Consider the following security definition for private-key encryption: an encryption scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over key space $\mathcal{K}$ and message space $\mathcal{M}$ is perfectly secure against key recovery if the following holds for any algorithm $\mathscr{A}$ and any distribution D over the message space $\mathcal{M}$:

   $$\Pr[\mathscr{A}(c) = k \mid k \xleftarrow{\text{U}} \mathcal{K}; m \xleftarrow{\text{D}} \mathcal{M}; c \longleftarrow \mathsf{Enc}(k, m)] \leq \frac{1}{|\mathcal{K}|}.$$

   Show that the above definition is not necessary for perfectly secure encryption i.e., show that there exists an encryption scheme which is perfectly secure, but not perfectly secure against key recovery.

   (c) Show that the above definition is not sufficient for perfectly secure encryption i.e., show that there exists an encryption scheme which is perfectly secure against key recovery, but not perfectly secure.

   5+5+5 = 15

2. (a) Define IND-EAV-security (indistinguishable encryptions under the presence of an eavesdropper) for symmetric key encryption.

   (b) Show how to construct IND-EAV-secure encryption from pseudorandom generators. Prove security of your construction.

   (c) Define IND-CPA-security. Is your construction from part (b) IND-CPA-secure? Justify.

   3+7+5 = 15

3. Let $\mathcal{SE} = (\mathsf{Gen}_1, \mathsf{Enc}, \mathsf{Dec})$ be an IND-CPA-secure symmetric encryption scheme and $\Pi = (\mathsf{Gen}_2, \mathsf{Mac}, \mathsf{Vrfy})$ be an EUF-CMA-secure message authentication code. Suppose that Alice and Bob share a key $k = (k_1, k_2)$ generated as $k_1 \longleftarrow \mathsf{Gen}_1(1^\lambda)$, $k_2 \longleftarrow \mathsf{Gen}_2(1^\lambda)$. Alice wants to send a message m to Bob in a private and authenticated way. To this end, consider her sending the following. For each choice, write down the steps of decryption and state whether the method achieves both privacy and authentication and justify your answer (there is no need for a proof, just the intuition will do).

   (a) $\mathsf{Mac}(k_2, \mathsf{Enc}(k_1, m))$

   (b) $\mathsf{Enc}(k_1, m), \mathsf{Mac}(k_2, m)$

   (c) $\mathsf{Enc}(k_1, m), \mathsf{Enc}(k_1, \mathsf{Mac}(k_2, m))$

(d) $m, \mathsf{Mac}(k_2, \mathsf{Enc}(k_1, m))$

(e) $c, \mathsf{Mac}(k_2, c)$, where $c = \mathsf{Enc}(k_1, m)$

$\boxed{3 \times 5 = 15}$

4. For a function $g : \{0,1\}^\lambda \to \{0,1\}^\lambda$, let $g^\$$ be an oracle that, whenever queried, chooses $x \xleftarrow{\text{U}} \{0,1\}^\lambda$ and returns $(x, g(x))$. We say a keyed function $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ is weakly pseudorandom if there exists a negligible function negl such that for all probabilistic polynomial time (in λ) algorithms $\mathscr{D}$,

$$|\Pr[\mathscr{D}^{F_k^\$(\cdot)} = 1] - \Pr[\mathscr{D}^{f^\$(\cdot)} = 1]| \leq \mathsf{negl}(\lambda),$$

where $k \xleftarrow{\text{U}} \{0,1\}^\lambda$ and f is chosen uniformly at random from the set of all functions from $\{0,1\}^\lambda$ to $\{0,1\}^\lambda$.

(a) Let F be a pseudorandom function. Define

$$F'_k(x) = \begin{cases} F_k(x) & \text{if } x \text{ is even} \\ F_k(x+1) & \text{if } x \text{ is odd} \end{cases}$$

Prove that F' is weakly pseudorandom but not pseudorandom.

(b) Consider the private-key encryption scheme described below.

$\mathsf{Gen}(1^\lambda)$**:** Choose key k as $k \xleftarrow{\text{U}} \{0,1\}^\lambda$.

$\mathsf{Enc}(k, m \in \{0,1\}^\lambda)$**:** Pick $r \xleftarrow{\text{U}} \{0,1\}^\lambda$ and compute ciphertext as $(r, F_k(r) \oplus m)$.

$\mathsf{Dec}(k, (r, c))$**:** Recover message m as $m = c \oplus F_k(r)$.

If F is weakly pseudorandom, then is the above scheme IND-CPA-secure? Justify.

$\boxed{6{+}9 = 15}$

5. Let $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ with $\mathcal{K} = \{0,1\}^n$ with IND-CPA security. Suppose we wish to split the ability to decrypt ciphertexts across two parties, Alice and Bob, so that both parties are needed to decrypt ciphertexts. For a key $k \xleftarrow{\text{U}} \mathcal{K}$, choose a random $r \xleftarrow{\text{U}} \mathcal{K}$ and define $k_a = r$ and $k_b = r \oplus k$. Now if Alice and Bob get together, they can decrypt a ciphertext c by first reconstructing the key k as $k = k_a \oplus k_b$ and then computing $\mathsf{Dec}(k, c)$. Our goal is to show that neither Alice nor Bob can decrypt ciphertexts on their own (i.e., decryption is not possible with only k_a or only k_b).

(a) Formulate a security notion that captures the advantage that an adversary $\mathscr{A}$ has in breaking IND-CPA security given Bob's key k_b; call this game 2SK. Denote this 2-way key splitting advantage as $\mathsf{Adv}^{\mathsf{2SK}}_{\mathcal{E},\mathscr{A}}$.

(b) Show that every 2-way key splitting adversary $\mathscr{A}$ running in time t, there is an IND-CPA adversary $\mathscr{B}$ running in time $t + O(n)$ such that $\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\mathcal{E},\mathscr{A}} = \mathsf{Adv}^{\mathsf{2SK}}_{\mathcal{E},\mathscr{A}}$.

$\boxed{6{+}9 = 15}$

6. Let $\mathsf{H} : X \to Y$ be a hash function with $|X| = n > m = |Y|$. An *r-way multi-collision* or *r-collision* is a set of r *distinct* points $x_1, x_2, \ldots, x_r \in X$ such that $\mathsf{H}(x_1) = \mathsf{H}(x_2) = \cdots = \mathsf{H}(x_r)$. Described below is a *generalised birhtday attack* that finds an r-collision for H (if it exists).

Pick $r-1$ distinct points $x_1, x_2, \ldots, x_{r-1}$ from X.
Set $i = r$ and $Q = \{x_1, \ldots, x_{r-1}\}$

repeat until $Q = X$
  Pick $x_i \in X \setminus Q$ and let $Q = Q \cup \{x_i\}$
  If $\exists\{x_{j_1}, \ldots, x_{j_r}\} \subseteq Q$ with $\mathsf{H}(x_{j_1}) = \mathsf{H}(x_{j_2}) = \cdots = \mathsf{H}(x_{j_r})$, then
    return $x_{j_1}, x_{j_2}, \ldots, x_{j_r}$
  $i = i + 1$
print 'no r-collisions exist'

The complexity of the attack is measured in terms of the number of points picked (i.e., the size of Q) for an r-collision to be found.

(a) For what values of n (in terms of m) will an r-collision necessarily exist?

(b) Let $q = |Q|$ denote the number of 'trials' required to find an r-collision. Suppose that H is a random function (i.e., for any $x \in X$, $y \in Y$, $\Pr[\mathsf{H}(x) = y] = 1/m$). Find an upper bound on the probability that an r-collision exists (in Q) after q trials.
Hint: Think union bound.

(c) Use solution to part (b) to show that the generalised birthday attack finds r-collisions with probability $\geq 1/2$ in time $\Omega(rm^{(r-1)/r})$. Again, assume H is a random function.

3+6+6 = 15