INDIAN STATISTICAL INSTITUTE
Mid-Semester Examination
M. Tech. (CrS) I year, 2nd Sem, AY 2024-2025
Cryptology

Date: 24. 02. 2025
Time: 2 Hours (10:30 AM to 12:30 PM)

Total Marks: 60

Answer as many questions as possible. The max score you can achieve is 45.

---

1. (a) Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n$, and for $k \in \mathcal{K}$, the encryption rule is defined as $\mathcal{E}(k, m) = k + m \pmod{n}$. Key generation chooses a uniform $k \in \{0,1\}^n$ and outputs it. Show that this encryption scheme is perfectly secure for any plaintext probability distribution.

   (b) Show that Substitute cipher is not perfectly secure.

   [5+5=10]

2. (a) Let G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$. To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$. State whether the scheme has indistinguishable encryptions in the presence of an eavesdropper. Explain your answer.

   (b) Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom permutation. Consider the mode of operation in which a uniform value $ctr \in \{0,1\}^n$ is chosen, and the i-th ciphertext block c_i is computed as $c_i := F_k(ctr + i + m_i)$ where the addition is defined over $\mathbb{F}_{2^n}$. Show that this scheme does not have indistinguishable encryptions in the presence of an eavesdropper.

   [5+5=10]

3. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. For the following constructions of a keyed function $F' : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$, state whether F' is a pseudorandom function. If yes, prove it; if not, show an attack.

   (a) $F'_k(x) \stackrel{def}{=} F_k(0 \,\|\, x) \,\|\, F_k(1 \,\|\, x)$.

   (b) $F'_k(x) \stackrel{def}{=} F_k(0 \,\|\, x) \,\|\, F_k(x \,\|\, 1)$.

   [5+5=10]

4. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function and let $\Pi : \{0,1\}^n \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ be a permutation defined using F. For any key $k \in \{0,1\}^n$ and input strings $a, b \in \{0,1\}^n$, $\Pi : k \times (a, b) \mapsto (c, d)$, where $c, d \in \{0,1\}^n$ and are computed according to the definition in Figure 1.

   Prove that Π is not a pseudorandom permutation. [10]

5. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. Consider the following private-key encryption scheme $\mathcal{E} = (\mathsf{G}, \mathsf{E}, \mathsf{D})$ for messages of length n as follows:

   - G: on input 1^n, choose uniform $k \in \{0,1\}^n$ and output it.

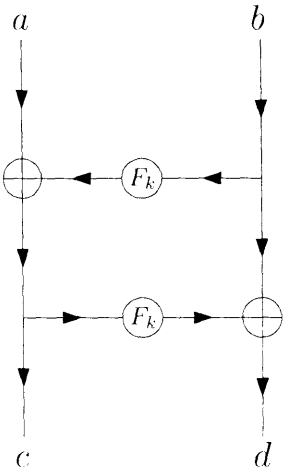


Figure 1: Π

- E: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext

$$c := \langle r, F_k(r) \oplus m \rangle.$$

- D: on input a key $k \in \{0,1\}^n$ and a ciphertext $c = \langle r, s \rangle$, output the plaintext message

$$m := F_k(r) \oplus s.$$

(a) Prove that if F is a pseudorandom function, then $\mathcal{E}$ is a CPA-secure private-key encryption scheme for messages of length n.

(b) Show that $\mathcal{E}$ is not CCA-secure.

[15+5=20]