Problem a: Block Ciphers

Consider the following definition of a block cipher. This definition is equivalent to the one in the lecture slides.

Definition 1. A function $E : \mathcal{K} \times X \to Y$ is called a block cipher if:

1. $X = Y$ and
2. for all $K \in \mathcal{K}$, $E_K : X \to X$ is an efficiently computable permutation on the set X.

Here, $E_K(x) = E(K, x)$ for all $x \in X$, which is a common shorthand notation.

Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher.

(a) Analysis of F_1

Let the function $F_1 : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be defined by:

$$F_1(K, x) = E(K, x) \oplus x.$$

Is F_1 a block cipher? Prove your answer.

(b) Analysis of F_2

Let the function $F_2 : (\{0,1\}^k \times \{0,1\}^n) \times \{0,1\}^n \to \{0,1\}^n$ be defined by:

$$F_2((K_1, K_2), x) = E(K_1, K_2 \oplus x).$$

The keyspace of F_2 is $\{0,1\}^k \times \{0,1\}^n$. Show that F_2 is a block cipher and that it is PRP-secure assuming that E is PRP-secure.

Problem b: IND-CPA Security

Suppose $SE = (\text{KGen}, \text{Enc}, \text{Dec})$ is an IND-CPA secure encryption scheme with key space $\mathcal{K}$ and message space $\mathcal{M}$, such that $\mathcal{K} = \mathcal{M} = \{0,1\}^n$ for some even integer n. You can assume that messages of the same length have equally-sized ciphertexts (if not stated otherwise). Which of the following encryption algorithms are guaranteed to represent correct encryption schemes with IND-CPA security?

1. $\text{Enc}_a(K, m) = \text{Enc}(K, (m, r))$. Here, the message space for Enc_a is $\{0,1\}^{n/2}$, r is a random $n/2$-bit string, and (m, r) is the concatenation of m and r.
2. $\text{Enc}_b(K, m) = \text{Enc}(K, m) \oplus \text{Enc}(K, 0^n)$.
3. $\text{Enc}_c(K, m) = (\text{Enc}(K, m), m[1])$. Here, $m[1]$ is the first bit of m.