TD 1 – Introduction

Exercise 1. *Perfect indistinguishability and information leak*
Let $(\mathsf{Enc}, \mathsf{Dec})$ be a perfectly indistinguishable encryption scheme. Let $\mathcal{A}$ be an adversary that is given $c \leftarrow \mathsf{Enc}_k(m)$ where $k \twoheadleftarrow \mathcal{K}$ is uniformly sampled, and m is chosen by the challenger. In all three cases below, $\mathcal{A}$ tries to compute some information on m. Prove that in each case, the probability that $\mathcal{A}$ outputs the correct answer is $\leq \frac{1}{2}$. *Hint. Assume otherwise and prove that it contradicts the perfect indistinguishability.*

1. Information: the least significant bit $m_{[0]}$ of m.
2. Information: the parity $\bigoplus_i m_{[i]}$ of m.
3. Information: whether m has more zeroes than ones.

Exercise 2. *Perfectly indistinguishable?*

1. For the four encryption functions below where $\mathcal{K} = \mathcal{M} = \{0,1\}^n$, determine whether they define a perfectly indistinguishable encryption scheme. *Give either a proof or an adversary with non-zero advantage.*
   i. $\mathsf{Enc}^1_k(m) = 0 \| k \oplus m$ where $\cdot\|\cdot$ denotes string concatenation.
   ii. $\mathsf{Enc}^2_k(m) = k \oplus m \| m^{\oplus}$ where $m^{\oplus} = \bigoplus_{i=0}^{n-1} m_{[i]}$ is the XOR of the bits of m.
   iii. $\mathsf{Enc}^3_k(m) = (k \oplus m)^{\leftarrow}$ where $c^{\leftarrow}$ is the mirror of c, defined as $c^{\leftarrow}_{[i]} = c_{[\#c-i-1]}$ for $0 \leq i < \#c$.
   iv. $\mathsf{Enc}^4_k(m) = k \oplus m \| k^{\oplus}$.
2. Consider any encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$, and redefine Enc^1, Enc^2, Enc^3 and Enc^4 above by replacing the one-time pad $k \oplus m$ by $\mathsf{Enc}_k(m)$. What can be said of each the resulting scheme if:
   i. $(\mathsf{Enc}, \mathsf{Dec})$ is a perfectly indistinguishable encryption scheme?
   ii. $(\mathsf{Enc}, \mathsf{Dec})$ is IND-CPA secure?

Exercise 3. *Other encryption schemes*

1. Let $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0, \dots, n-1\}$ and let $\mathsf{Enc}_k(m) = m + k \bmod n$.
   - **i.** Describe Dec_k such that the encryption scheme is correct.
   - **ii.** Let $m \in \mathcal{M}$, $c \in \mathcal{C}$ and $k \twoheadleftarrow \mathcal{K}$. Prove that $\Pr\left[\mathsf{Enc}_k(m) = c\right] = \frac{1}{n}$.
   - **iii.** Prove that this encryption scheme is perfectly indistinguishable.
2. Caesar cipher with key $k \in \{0, \dots, 25\}$ encrypts a letter $\ell \in \{A, \dots, Z\}$ by replacing it with the letter k positions further along the alphabet. *Example with $k = 3$: $A \to D$, $B \to E$, …, $X \to A$, $Y \to B$, $Z \to C$.*
   - **i.** Prove that Caesar cipher is a perfectly indistinguishable encryption scheme for $\mathcal{M} = \{A, \dots, Z\}$.
   - **ii.** To encrypt a word, we apply the same encryption to each letter. Is the resulting scheme perfectly indistinguishable?
3. Let $\mathcal{M} = \mathcal{C} = \Sigma^\ell$, that is messages and ciphertexts are length-ℓ words over an alphabet Σ. The key space $\mathcal{K}$ is the set of all permutations on Σ: a key $k \in \mathcal{K}$ is a one-to-one mapping $k : \Sigma \to \Sigma$. We define $\mathsf{Enc}_k(m) = k(m_{[0]}) \| k(m_{[1]}) \| \cdots \| k(m_{[\ell-1]})$ where $\|$ is the concatenation.
   - **i.** Describe Dec_k such that the encryption scheme is correct.
   - **ii.** Prove that this encryption scheme is not perfectly indistinguishable.
4. *(at home)* Consider a variant of the first scheme where each key k is made of ℓ independent random permutations $k_{[0]}, \dots, k_{[\ell-1]}$ of Σ. The encryption is $\mathsf{Enc}_k(m) = k_{[0]}(m_{[0]}) \| \cdots \| k_{[\ell-1]}(m_{[\ell-1]})$.
   - **i.** Describe Dec_k such that the encryption scheme is correct.
   - **ii.** Prove that this encryption scheme is perfectly indistinguisable.

Exercise 4. *One-time pad for variable length messages*

Let us consider the space $\mathcal{M} = \{0,1\}^{\leq \ell}$ of binary string of length $\leq \ell$.

1. We consider the following encryption scheme: the key is uniformly sampled from $\mathcal{K} = \{0,1\}^\ell$ and we define $\mathsf{Enc}_k(m) = k_{[0,|m|[} \oplus m$ where $k_{[0,t[}$ is made of the first t bits of k.
   - **i.** Write the decryption algorithm.
   - **ii.** Prove that this scheme is not perfectly indistinguishable. *Give an intuitive explanation as well as an adversary with non-zero advantage in the indistinguishability game.*
2. Propose a perfectly indistinguishable encryption scheme for $\mathcal{M}$. *Provide the encryption and decryption algorithms, and prove that it is perfectly indistinguishable (using the result on the one-time-pad).*