TD 1 – Introduction

Exercise 1. *Perfect indistinguishability and information leak*
Let $(\mathsf{Enc}, \mathsf{Dec})$ be a perfectly indistinguishable encryption scheme. In all three cases below, prove that no adversary $\mathcal{A}$ can win the game with probability more that $\frac{1}{2}$. *Hint. Prove that if its probability of success is $p > \frac{1}{2}$, its probability of success in the indistinguishability game is also p.*

1. Given $c \leftarrow Enc_k(m)$, $\mathcal{A}$ must compute the least significant bit $m_{[0]}$ of m.
2. Given $c \leftarrow \mathsf{Enc}_k(m)$, $\mathcal{A}$ must compute the parity $\bigoplus_i m_{[i]}$ of m.
3. Given $c \leftarrow \mathsf{Enc}_k(m)$, $\mathcal{A}$ must tell whether m has more zeroes than ones.

Exercise 2. *Play with* $\mathsf{IND}-\mathsf{CPA}$ *definition*
Let $\mathcal{E} = (\mathsf{Enc}, \mathsf{Dec})$ be an $\mathsf{IND}-\mathsf{CPA}$ secure encryption scheme. For each of the following encryption algorithms, determine whether it is $\mathsf{IND}-\mathsf{CPA}$ secure: Either provide an adversary with a strong advantage, or prove that the advantage function is similar to the advantage function of $\mathcal{E}$.

1. $\mathsf{Enc}'_k(m) = 0 \| \mathsf{Enc}_k(m)$ where $\|$ denotes the concatenation.
2. $\mathsf{Enc}''_k(m) = \mathsf{Enc}_k(m) \| m^{\oplus}$ where $m^{\oplus} = \bigoplus_i m_{[i]}$.
3. $\mathsf{Enc}'''_k(m) = \mathsf{Enc}_k(m)^{\leftarrow}$ where $c^{\leftarrow}$ is the *reverse* of c, defined as $c^{\leftarrow}_{[i]} = c_{[\#c-i-1]}$ for $0 \leq i < \#c$.
4. $\mathsf{Enc}''''_k(m) = \mathsf{Enc}_k(m^{\leftarrow})$.

Exercise 3. *Other encryption schemes*

1. 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.
2. 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 $\Pr[\mathsf{Enc}_k(m) = c] = \frac{1}{n}$.
   iii. Prove that this encryption scheme is perfectly indistinguishable.
3. *(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 withnonzero 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).*