C. Olivier-Anclin

Session 2 - Security notions

Exercise 1 (Negligible functions)
Let f and g be two negligible functions. Prove that:

1. $f \cdot g$ is negligible.
2. For any $k > 0$, f^k is negligible.
3. For any $\lambda, \mu \in \mathbb{R}$, $\lambda, \mu > 0$, $\lambda \cdot f + \mu \cdot g$ is negligible.

Exercise 2 (DL, CDH, DDH assumptions)
Recall DL, CDH, and DDH assumptions and prove that:

1. Solving DL $\Rightarrow$ Solving CDH.
2. Solving CDH $\Rightarrow$ Solving DDH.

Exercise 3 (Play with IND-CPA definition)
Let $E = (\mathsf{Enc}, \mathsf{Dec})$ be an IND-CPA secure encryption scheme. For each of the following encryption algorithms, determine whether it is IND-CPA secure. Either provide an adversary with a strong advantage, or prove that the advantage function is similar to the advantage function of E.

1. $\mathsf{Enc}_1^k(m) = 0 \| \mathsf{Enc}_k(m)$ (where $\|$ denotes concatenation)
2. $\mathsf{Enc}_2^k(m) = \mathsf{Enc}_k(m) \| m^{\oplus}$ where $m^{\oplus} = \bigoplus_i m[i]$.
3. $\mathsf{Enc}_3^k(m) = \mathsf{Enc}_k(m)^{\leftarrow}$ where $c^{\leftarrow}$ is the reverse of c, defined as $c^{\leftarrow}[i] = c[\#c - i - 1]$ for $0 \leq i < \#c$.
4. $\mathsf{Enc}_4^k(m) = \mathsf{Enc}_k(m^{\leftarrow})$.
5. $\mathsf{Enc}_5^k(m) = \mathsf{Enc}_k(m) \| H(m)$, H be a public hash function (*i.e.,* H is deterministic and hard to invert).

Exercise 4 (Deterministic Asymmetric Encryption Scheme)
Let $\Pi = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ be a deterministic asymmetric encryption scheme. Prove that Π is not IND-CPA.

Exercise 5 (One-way security)
Let f be a one-way function, we construct the encryption E as follows:

- Pick a random value x in the domain of f.
- The encryption of m is $\langle f(x), x \oplus m \rangle$

Prove that: if f is a one-way function, then E is a OW-CPA encryption scheme.