TD 7: Hash Functions, PKE

Exercise 1.
Suppose $h_1 : \{0,1\}^{2n} \to \{0,1\}^n$ is a collision-resistant hash function.

1. Define $h_2 : \{0,1\}^{4n} \to \{0,1\}^n$ as follows: Write $x = x_1 \| x_2$ with $x_1, x_2 \in \{0,1\}^{2n}$; return the value $h_2(x) = h_1(h_1(x_1) \| h_1(x_2))$. Prove that h_2 is collision-resistant.

2. For $i \geq 2$, define $h_i : \{0,1\}^{2^i n} \to \{0,1\}^n$ as follows: Write $x = x_1 \| x_2$ with $x_1, x_2 \in \{0,1\}^{2^{i-1}n}$; return $h_i(x) = h_1(h_{i-1}(x_1) \| h_{i-1}(x_2))$. Prove that h_i is collision-resistant.

Exercise 2.
Pedersen's hash function is as follows:

- Given a security parameter n, algorithm $\mathtt{Gen}$ samples (G, g, p) where $G = \langle g \rangle$ is a cyclic group of known prime order p. It then sets $g_1 = g$ and samples g_i uniformly in G for all $i \in \{2, \ldots, k\}$, where $k \geq 2$ is some parameter. Finally, it returns $(G, p, g_1, \ldots, g_k)$.
- The hash of any message $M = (M_1, \ldots, M_k) \in (\mathbb{Z}/p\mathbb{Z})^k$ is $H(M) = \prod_{i=1}^{k} g_i^{M_i} \in G$.

1. Bound the cost of hashing, in terms of k and the number of multiplications in G.

2. Assume for this question that G is a subgroup of prime order p of $(\mathbb{Z}/q\mathbb{Z})^\times$, where $q = 2p + 1$ is prime. What is the compression factor in terms of k and q? Which k would you choose? Justify your choice.

3. Assume for this question that $k = 2$. Show that Pedersen's hash function is collision-resistant, under the assumption that the Discrete Logarithm Problem (DLP) is hard for G.

4. Same question as the previous one, with $k \geq 2$ arbitrary.

Exercise 3.
Let $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be a correct public-key encryption scheme. Let us assume moreover that Enc is deterministic.

1. Show that this scheme is not CPA-secure.

Exercise 4.
Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a public-key encryption scheme. The One-Wayness against Chosen Plaintext Attack (OW-CPA) security notion is the following. The challenger samples $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$ and $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$, where $m \leftarrow U(\mathcal{M})$ and $\mathcal{M}$ is the message space. The adversary wins if it outputs a message m' such that $m = m'$.
A scheme is said OW-CPA secure if no ppt adversary wins with non-negligible probability.

1. Write a formal definition of the OW-CPA security. Can a scheme be OW-CPA secure if the message space is $\mathcal{M} = \{0,1\}$?

2. Show that if $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is IND-CPA secure and has exponential message space, then it is OW-CPA secure.

3. Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an IND-CPA secure encryption scheme with message space $\mathcal{M}$ such that it has cardinality $|\mathcal{M}| = 2^\lambda$, where λ is the security parameter. Show that a small modifiction of the scheme leads to an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}', \mathsf{Dec}')$ that is OW-CPA secure but not IND-CPA secure anymore.