TD 8: Public Key Encryption

Exercise 1.
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 2.
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 $m \leftarrow \mathcal{U}(\mathcal{M})$ 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.

Exercise 3.
Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a Public-Key encryption scheme. Let us define the following experiments for $b \in \{0,1\}$ and $Q = \mathsf{poly}(\lambda)$.

$\mathsf{Exp}_b^{\text{many-CPA}}$

$\mathcal{C}$		$\mathcal{A}$
$(pk, sk) \leftarrow \mathsf{KeyGen}(1^\lambda)$		
	$\xrightarrow{pk}$	
		Choose adaptively $(m_0^{(i)}, m_1^{(i)})_{i=1}^Q$
	$\xleftarrow{(m_0^{(i)}, m_1^{(i)})_{i=1}^Q}$	
$(c_i = \mathsf{Enc}(pk, m_b^{(i)}))_{i=1}^Q$		
	$\xrightarrow{(c_i)_{i=1}^Q}$	
		Output $b' \in \{0,1\}$

The advantage of $\mathcal{A}$ in the many-time CPA game is defined as

$$\mathsf{Adv}^{\text{many-CPA}}(\mathcal{A}) = |\Pr(\mathcal{A} \xrightarrow{\mathsf{Exp}_1^{\text{many-CPA}}} 1) - \Pr(\mathcal{A} \xrightarrow{\mathsf{Exp}_0^{\text{many-CPA}}} 1)|.$$

1. Recall the definition of CPA-security that was given during the lecture. What is the difference?

2. Show that these two definitions are equivalent.

3. Do we have a similar equivalence in the secret-key setting?