Question 1

We show that IND-CCA security implies IND-CPA security by showing that if an IND-CPA adversary can win with non-negligible advantage, then it can be used to build an IND-CCA adversary who can win with non-negligible advantage.

The key generation routines are identical between the IND-CPA and the IND-CCA game. When $\mathcal{A}_{\text{IND-CCA}}$ receives the keypair, it directly passes it to $\mathcal{A}_{\text{IND-CPA}}$. $\mathcal{A}_{\text{IND-CPA}}$ can use the public key to perform encryption queries but does not submit any decryption queries.

When $\mathcal{A}_{\text{IND-CPA}}$ generates the challenge plaintext m_0, m_1, $\mathcal{A}_{\text{IND-CCA}}$ passes them to the IND-CCA challenger and receives the challenge ciphertext c_b. $\mathcal{A}_{\text{IND-CCA}}$ passes c_b to $\mathcal{A}_{\text{IND-CPA}}$ and receives the guess b^* from $\mathcal{A}_{\text{IND-CPA}}$.

Because both the IND-CPA and the IND-CCA games are played with identical keypairs, $\mathcal{A}_{\text{IND-CPA}}$'s guess is correct if and only if b^* is equal to b. Therefore, $\mathcal{A}_{\text{IND-CCA}}$'s advantage is equal to $\mathcal{A}_{\text{IND-CPA}}$'s advantage, meaning that if $\mathcal{A}_{\text{IND-CPA}}$ has non-negligible advantage, then $\mathcal{A}_{\text{IND-CCA}}$ has non-negligble advantage.