1. Show that RSA is not IND–CPA. The IND–CPA game is defined as follows

   (a) The challenger generates a new key pair PK, SK and publishes PK to the adversary, the challenger retains SK.

   (b) The adversary may perform a polynomially bounded number of calls to the encryption oracle or other operations.

   (c) Eventually, the adversary submits two distinct plaintexts M_0 and M_1 to the challenger.

   (d) The chellenger selects a bit $b \in \{0, 1\}$ uniformly at random, and sends the challenge ciphertext $C = E(PK, M_b)$ back to the adversary.

   (e) The adversary is free to perform any number of additional computations.

   (f) Finally, the adversary outputs a guess for the value b.

   A cryptosystem is said to be IND-CPA if that every probabilistic polynomial time adversary has only a negligible advantage over random guessing. Provide a description of the steps an adversary has to undertake in order to win the IND-CPA game and provide an assessment of the adversarial advantage, which is the difference probability of winning the IND-CPA game using the suggested method, and the probability of winning the IND-CPA game by random guessing. The IND-CPA property is also called *semantic security*, and showing that RSA is not IND-CPA is equivalent to stating that RSA is not semantically secure.

2. Show that RSA is not IND-CCA2. The IND-CCA2 game is defined as follows.

   (a) The challenger generates a new key pair PK, SK and publishes PK to the adversary, the challenger retains SK.

   (b) The adversary may perform any number calls to the encryption or decryption oracles, or other operations.

   (c) Eventually, the adversary submits two distinct chosen plaintexts M_0 and M_1 to the challenger.

   (d) The challenger selects a bit $b \in \{0, 1\}$ uniformly at random, and sends the challenge ciphertext $C = E(PK, M_b)$ back to the adversary.

   (e) The adversary is free to perform any number of additional computations, calls to the encryption and decryption oracles, but may not submit the challenge ciphertext C to the decryption oracle.

   (f) Finally, the adversary outputs a guess for the value b.

   Use the property properties of RSA, which is homomorphic w.r.t. multiplication, meaning that

$$\begin{cases} C_1 = m_1^e \bmod n \\ C_2 = m_2^e \bmod n \end{cases} \Longrightarrow C_1 \cdot C_2 = m_1^e \cdot m_2^e \bmod n = (m_1 m_2)^e \bmod n \ .$$

   Provide a description of the steps an adversary has to undertake in order to win the IND-CCA2 game and provide an assessment of the adversarial advantage, which is the difference probability of winning the IND-CCA2 game using the suggested method, and the probability of winning the IND-CCA2 game by random guessing.