**b)** To prove that the El Gamal encryption scheme is not CCA-secure, we need to construct an adversary that can win the CCA game with non-negligible probability.

Let A be the adversary that we construct as follows:

1. A receives the public key pk = h.
2. A chooses two messages m0 and m1 such that |m0| = |m1|.
3. A selects a random bit b ∈ {0,1} and encrypts mb using the encryption algorithm Ench(m) to obtain the ciphertext c.
4. A obtains the decryption of c by sending it to the oracle O to get either the decryption of c, or the encryption of m1.
5. A outputs 0 if oracle returns the decryption of c, else A outputs 1 if the oracle returns the encryption of m1.

The winning probability of A can be analyzed as follows:

Case 1: O returns the decryption of c. In this case, A knows that c encrypts mb, and can modify c to obtain a new ciphertext c\* = (c1, c2\*) where c2\* = c2 · gr' for some random value r' ∈ Zq. A sends c\* to the oracle O to obtain its decryption. Then, A can compute mb\* = m\* ⊕ m0, where m\* is the message obtained from the oracle. Since m0 and m1 have the same length, A knows that mb\* = m1 with probability 1/2. Thus, A outputs 1 with probability 1/2 in this case.

Case 2: O returns the encryption of m1. In this case, A knows that c does not encrypt m1, and can modify c to obtain a new ciphertext c\* = (c1, c2\*) where c2\* = c2 · gr' for some random value r' ∈ Zq. A sends c\* to the oracle O to obtain its decryption. Then, A can compute mb\* = m\* ⊕ m1, where m\* is the message obtained from the oracle. Since m0 and m1 have the same length, A knows that mb\* = m0 with probability 1/2. Thus, A outputs 0 with probability 1/2 in this case.

Pr[A wins] = ½

i.e., non-negligible.

Hence, the El Gamal encryption scheme is not CCA-secure.