watIAM: sh2yap

student ID: 21111395

1. The encryption is trivial, as the attacker has public access to the public key, thus access to an “encryption oracle” is trivial. Attacker just needs to perform modular arithmetic to encrypt.
2. IND-CPA and IND-CCA for Elgamal PKES
   1. IND-CPA security game
      1. Setup: globally public prime p, globally public element g of large prime order q
      2. The challenger chooses x and set:
         1. kpublic =
         2. kprivate = x
      3. The adversary can select plaintexts m and random integer r to obtain corresponding ciphertext c = E(m) = (
      4. The adversary picks two messages m0 and m1 of the same length
      5. The challenger picks uniformly at random one of the messages, and encrypts it, the encrypted message is c.
      6. The adversary guesses which is which message m0 or m1 corresponds to the encrypted message c.
      7. If the guess is correct, the adversary wins.
   2. IND-CCA security game
      1. Same Setup as IND-CPA (step a.i, a.ii)
      2. The adversary can select ciphertexts c and random integer x , and feed into a Decryption oracle to obtain the corresponding plaintexts m. Note that, the adversary cannot ask to decrypt the challenge ciphertext.
      3. The adversary picks two messages m0 and m1 of the same length
      4. The challenger picks uniformly at random one of the messages, and encrypts it, the encrypted message is c.
      5. The challenger presents c to the adversary.
      6. Under IND-CCA2: Adversary can “perform additional operations in polynomial time, **including calls to the oracles, for ciphertexts different than**c.” ([Source](https://crypto.stackexchange.com/questions/26689/easy-explanation-of-ind-security-notions))
      7. The adversary guesses which is which message m0 or m1 corresponds to the encrypted message c.
      8. If the guess is correct, the adversary wins.
3. With reference to <https://people.eecs.berkeley.edu/~daw/teaching/cs276-s06/l19.pdf>

A close-up of a paper

Description automatically generated

A close-up of a paper

Description automatically generated

