ECE4802/CS4801 Assignment #4

Due: Apr 27, 2023, 11:59pm.

1. D-H Key Exchange: Alice and Bob want to generate a common key. They agreed to use prime number $p = 709$ and generator $\alpha = 2$. Alice's private key= 17, Bob's private key= 41.
   Find the the followings and show every intermediate step:

   a. Alice's public key.
   b. Bob's public key.
   c. Common key generated by Alice and Bob.
   d. Explain how Alice and Bob establish the key.

2. ElGamal Encryption: Encrypt and decrypt the following messages using ElGamal Encryption for $\mathbb{Z}_{971}^{*}$ and $g = 314$ and show every intermediate step:
   a. Private key $a = 23$, random parameter $k = 21$, message $m_1 = 49$. (Hint: Find private and public keys first.)
   b. Encryption of m_2 is given as (285,849) for the same key.
      i. Find the encryption of $m = m_1 . m_2$ using homomorphic property of ElGamal Encryption. Note that m_1 is the message in part a and use the ciphertext you found in part a.
      ii. Decrypt the ciphertext you find in part i and verify that message you find is equal to the multiplication of m_1 and m_2 , i.e., $m = m_1 . m_2$. Note that, you are supposed to decrypt the given ciphertext to find m_2.