Cairo University
Faculty of Computers and Artificial Intelligence
Information Technology Department
IT423 - Information and Computers Networks Security
Spring 2022

Lab Assignment (4)

<u>Assignment deadline</u>: - 28/12/2022

Implement ElGamal encryption algorithm.

Input: -
1- Plain text of any size (characters)□ text to be encrypted

Output: -
1- *Prime Number (P)*
2- Z_p^* *and* Primitive Element (α)
2- Private Key at each party (d and K_M)
3- Generated (i) for each character in the input text, and the Ephemeral Key (K_E)
3- Cipher Text (hexadecimal)
4- K_M^{-1} and the Plaintext after decryption (Character)

Read the hints which are mentioned through this document carefully.

Hint 1: -
- For step 1 in key generation p & α must satisfy the following:-
1- p is random prime number $1 < p < 2^{500}-1$
2- α is random integer such that $\alpha \in Z^*_p$
- Check if p is prime or not using Fermat Primality Test

Hint 2:-
In Fermat Primality Test do the following
- Step 1: s = 100
- Step 1.2: is computed by using the square-and-multiply algorithm

Hint3: -
- Generate i for each character in the input text

Hint4: -
- Generate K^{-1}_M using EEA

Grading Criteria: (Total Mark 7)

- P & α generation ➔ 1 mark
- Private key calculation ➔ 2 mark
- Generated i for each character ➔ 1 mark
- Cipher Text ➔ 1 mark
- Inverse K_{M-1} ➔ 1 mark
- Plain Text ➔ 1 mark