CRYPTOGRAPHY AND

NETWORK SECURITY

Lab Task – 7

Q2)Elgamal cryptosystem and write remarks on what happens if C1 and C2 are swapped during the transmission.

- ElGamal encryption is a public-key cryptosystem. It uses asymmetric key encryption for communicating between two parties and encrypting the message.
- This cryptosystem is based on the difficulty of finding discrete logarithm in a cyclic group that is even if we know ga and gk, it is extremely difficult to compute gak.
- Let p be a large prime By "lArge" we mea n here a prime rather typicaL in length to that of an RSA modulus
- Select a special number g The number g must be a primitive elementmodulo p.

- Choose a private key x This can be any number bigger than 1and sma ller than p-1

- Compute public key y from x,p a nd g ◦The public key y is g raised to the power of the private key x modulo p.

  #ELGA MAL ENCRYPTION:-
  Generate a random number k

  Compute two values C
  1
  and C
  2
  , where

  C1
  = gk mod p and C2

  = Myk mod p

  Send the ciphertext C, which consists of the two
  separate values C1

  and C2
  .

  #ELGA MAL de-CRYPTION:-

• The receiver begins by using their private key x to transform C1
into something more useful:

c1x = (gk)x mod p

NOTE: c1x = (gk)x = (gx)k = (y)k = yk mod p
• - This is a very useful quantity because if you divide C2

by it you

get M. In other words:
C2

I yk =
(Myk) I yk M mod p

 IF C1==C2 THEN IT
WILL BE DECRYPTION
BECOMES DIFFICULT
& DIFFICULT TO
DECRYPT AT THE
RECEIVER END.