Tutorial-V (Public Key Cryptosystem)

1. Consider the following scenario

   Bob chooses the following values to perform encryption/decryption using ElGamal cryptosystem.

   P=11, e1=2, d=3 and r=4

   (i)Show how encryption/ decryption takes place for given plaintext =7

   (ii) Show known Plaintext attack occurs in scenario

2. Bob Selects E_{67} (2,3) and chooses e1=(2,22),d=4 and r=2

   (i) Show how encryption/ decryption takes for plaintext (24,26) using elliptic curve based ElGamal cryptosystem

3. Perform the encryption/ decryption using RSA algorithm for the following

   (i)p=17, q=23, e=9 and M=7