# Tutorial-VI (Public Key Cryptosystem)

1. (i)Given n=221 and e=5 find d in RSA cryptosystem.
   (ii) In ElGamal given prime p= 31 , choose an appropriate $e_1$ and d , then calculate $e_2$.

2. Alice uses Bob's RSA public key (e=7, n=143) to send plaintext P=8 encrypted as cipher text C=57. Show how eve can use the chosen-ciphertext attack if she has access to Bob's computer to find the plaintext.

3. Alice uses Bob's RSA public key (e=3, n=3) and sends the ciphertext 22 to Bob. Show how Eve can find the plaintext using cycling attack.