Cryptography and Network Security/Computer and Information Security

(B.Tech.CS 6th Sem,MSc.CS 4th sem)

1st Mid semester

Full Marks: 30 **Time: 1.00 Hrs**

(Question 1 is compulsory and Answer any two questions from rest)

1.(i)what are the services provided by cryptography? [2*5]

(ii) Distinguish between mono alphabetic substitution and poly alphabetic substitution.

(iii) How many keys will be needed if 10 people want to communicate using public key cryptography?

(iv) What is the importance of padding?

(v) What is the difference between substitution cipher and transposition cipher

2.What do you mean by symmetric key algorithm?Discuss DES algorithm with suitable diagram? [10]

3.(i)What is the purpose of Diffie-Hellman key exchange protocol? Briefly discuss Diffie_Hellman Key exchange protocol

(ii)) What is the value of symmetric key in Diffie-Hellman protocol if g=7,p=23,x=3 and y=6? [6+4]

4.(i) Briefly discuss RSA algorithm [5]

(ii) In RSA given two prime numbers p=23,q=19.Find out the private key and public key [5]