Total No. of Questions : 6]

SEAT No. : □

P4873

[Total No. of Pages : 2

B.E./Insem. - 60

B.E. (Information Technology)

INFORMATION AND CYBER SECURITY

(2012 Pattern) (Semester - I)

Time : 1 Hour] *[Max. Marks : 30*

Instructions to the candidates:

1) ***Answer Q1 or Q2, Q3 or Q4, Q5 or Q6.***
2) ***Neat diagrams must be drawn wherever necessary.***
3) ***Figures to the right side indicate full marks.***
4) ***Assume Suitable data if necessary.***

Q1) a) Distinguish between Substitution and transposition ciphers. **[5]**

b) List and briefly define categories of security services. **[5]**

OR

Q2) a) Determine the value of x using Chinese remainder theorem. **[6]**

X = 1 (mod 5)

X = 6 (mod 7)

X = 8 (mod 11)

b) Discuss various attacks threatening integrity. **[4]**

Q3) Explain block cipher modes of operation (ECB, CBC, CFB, OFB and counter mode) with help of block diagram. **[10]**

OR

Q4) a) Describe advantages and disadvantages of DES algorithm. **[6]**

b) What is the significance of extended Euclidian algorithm with reference to RSA algorithm? Illustrate. **[4]**

P.T.O.

Q5) a) Let the given data be - Prime numbers p = 11, q = 19 and the plain text to be sent is 40. Assume public key e as 23. Using RSA algorithm determine the cipher text for the given plain text. Also perform the reverse process of finding the plain text from the cipher text. **[6]**

b) Compare and contrast MD5 and SHA1 **[4]**

OR

Q6) a) Explain man-in-the-middle attack in Diffie-Hellman key exchange. **[6]**

b) Discuss the key management with respect to following issues. **[4]**

i) Key generation

ii) Key distribution

iii) Key updation

● ● ●