Total No. of Questions : 6] **SEAT No. :**

P5190 **[Total No. of Pages : 2**

B.E./Insem.-591
B.E. Information Technology (Semester-I)
INFORMATION AND CYBER SECURITY
(2012 Pattern)

Time : 1 Hour] ***[Maximum Marks : 30***

Instructions to the candidates:

1) ***Solve Q.1 or Q.2 Q.3 or Q.4 Q.5 or Q.6.***
2) ***Figures to the right indicate full marks.***
3) ***Assume suitable data if necessary.***

Q1) a) List and briefly define categories if passive and active security attacks. **[6]**

b) What are two problems with the one-time pad? **[4]**

OR

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

x = 3 (mod 5)

x = 7 (mod 8)

x = 5 (mod 7)

b) Differentiate between the following: **[4]**

i) Secret splitting and secret sharing

ii) Authentication and authorization

Q3) 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 reverse process of finding the plain text from the cipher text (use extended Euclidean algorithm to solve d) **[6]**

b) Explain CFB mode. And also how many blocks are affected by a single bit error in transmission? **[4]**

P.T.O

OR

Q4) a) Draw AES block diagram and explain the steps in details. **[6]**

b) Explain the avalanche effect. **[4]**

Q5) a) What are the key requirement of message digest and why SHA is more secure than MD5? **[6]**

b) Explain one way and mutual authentication. **[4]**

OR

Q6) a) Illustrate the Diffie Hellman key exchange protocol. **[6]**

b) Explain trap-door one-way function with example. **[4]**