Total No. of Questions : 6]

SEAT No. :

P5780

[Total No. of Pages : 1

B.E./Insem./Oct.-594

B.E.(Information Technology)

INFORMATION AND CYBER SECURITY

(2015 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) Differentiate between passive and Active Attack? **[5]**

b) Explain different Goals of Security? **[5]**

OR

Q2) a) Explain with diagram security Architecture and Operational Models. **[5]**

b) What is IDS (Intrusion Detection System)? Explain Function and types of IDS. **[5]**

Q3) a) Explain with diagram DES Encryption Algorithm. Explain Advantages and Drawbacks of DES. **[5]**

b) Perform Encryption and Decryption using RSA algorithm for following values p= 17,q=11,e=7,M=2. **[5]**

OR

Q4) a) Draw AES block diagram and state the general steps in detail. **[5]**

b) Explain Diffie-Hellman key exchange algorithm with example. **[5]**

Q5) a) Explain with diagram functioning of SHA-1 Algorithm. **[5]**

b) Describe briefly how IPSec Mechanism works and enlist its applications? Distinguish between tunnel and transport mode of IPSec. **[5]**

OR

Q6) a) Explain with diagram kerberos v4 authentication protocol. **[5]**

b) Explain SSL handshake and SSL record protocols with diagram. **[5]**