

Total No. of Questions : 6]

SEAT No. :

P160

APR. - 16/BE/Insem. - 84

[Total No. of Pages : 1

**B.E. (Computer)
CYBER SECURITY**

(2012 Course) (Semester - II) (Elective - III)

Time : 1½ 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) *Use of logarithmic tables, slide rule, charts, electronic pocket calculator and steam tables is allowed.*
- 4) *Assume suitable data, if necessary.*

- Q1)** a) List and explain various elements of Information Security. [4]
b) What are the various security services. [4]
c) What are the security approaches used to implement security policy? [2]

OR

- Q2)** a) Draw and explain Operational Model of Network Security. [4]
b) List and explain different security Techniques. [4]
c) What is passive and active attack in information security explain with suitable example. [2]

- Q3)** a) Use Play fair cipher to encrypt the following message “This is a columnar transposition” use key - APPLE. [5]
b) Explain the operation of DES algorithm in detail. [5]

OR

- Q4)** a) Explain the operation of Cipher Block Chaining (CBC) Mode. [5]
b) Explain operation of AES algorithm and state its application. [5]

- Q5)** a) For the given parameters ‘P’ = 3 and ‘Q’ = 19 find the value of ‘e’ and ‘d’ using RSA algorithm & encrypt message ‘M’ = 6. [5]
b) What are the methods used in key distribution in public key cryptography. [5]

OR

- Q6)** a) Explain “Diffie-Hellmen” key exchange algorithm with suitable example. [5]
b) Explain operation of MD5 message digest algorithm. [5]

