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

P613

[Total No. of Pages : 2

BE/Insem/APR - 246
B.E. (Computer Engineering)
INFORMATION AND CYBER SECURITY
(2015 Pattern) (Semester - II)

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

Instructions to the candidates :

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

Q1) a) Explain Operational Security Model for Network Security. **[5]**

b) How Information Security attacks are classified? Give example for each. **[5]**

OR

Q2) a) What are different security policies? Explain. **[5]**

b) List the differences between Security & Privacy. **[5]**

Q3) a) Use PlayFair Cipher to encrypt the message "This is a columnar transposition". Use key - APPLE. **[5]**

b) Explain following algorithm modes **[5]**

i) ECB

ii) OFB

OR

Q4) a) Explain the operation of DES algorithm in detail. **[5]**

b) Explain Monoalphabetic & Polyalphabetic ciphers with appropriate examples. **[5]**

P.T.O.

CFGP013091 49.248.216.238 12/03/2019 13:27:05 static-238

https://www.sppuonline.com/

Q5) a) Find the key exchanged between Alok and Bobby considering following data.

i) n = 11

ii) g = 5

iii) X = 2, Y = 3

Find value of A, B and secret key K. **[5]**

b) What is Kerberos? Explain operation in detail. **[5]**

OR

Q6) a) Given two Prime Numbers P = 17 & Q = 29 find out N, E, & D in an RSA encryption process. **[5]**

b) Explain in details the need & implementation of one way hash function (MD5). **[5]**

CEGP013091 49.248.216.238 12/03/2019 13:27:05 static-238

https://www.sppuonline.com/