

Total No. of Questions : 6]

SEAT No. :

P100

[Total No. of Pages : 2

Oct.-16/BE/Insem.- 158
B.E. (I.T)
INFORMATION AND CYBER SECURITY
(2013 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. [6]
 b) Define congruence and compare it with equality. [4]

OR

- Q2)** a) Find the value of x using chinese reminder theorem: [6]
 $x \equiv 2 \pmod{7} : x \equiv 2 \pmod{7}, x \equiv 3 \pmod{9}.$
 b) Compare symmetric and asymmetric key cryptography. [4]

- Q3)** a) What is double DES? What kind of attack on double DES makes it useless? [6]
 b) In CFB mode, how many blocks are affected by a single bit error in transmission? [4]

OR

- Q4)** a) Perform encryption and decryption using RSA algorithm. $p=7, q=11, e=17$ and $M = 8$. [6]
 b) Which transformations defined in AES change the contents of bytes and which one do not change the contents of bytes. [4]

P.T.O.

- Q5)** a) Explain any one digital signature format with neat diagram. [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) In context of Kerberos what is a realm. [4]



www.sppuonline.com