Total No. of Questions : 10]

SEAT No. : ____

P3174

[Total No. of Pages : 2

[5354]-691

B.E. (Information Technology)

INFORMATION AND CYBER SECURITY

(2012 Pattern) (Semester - I)

Time : 2½ Hours] ***[Max. Marks :70***

Instructions to the candidates:

1) ***Answer Q1 or Q2, Q3 or Q4, Q5 or Q6, Q7 or Q8, Q9 or Q10.***
2) ***Figures to the right indicate full marks.***

Q1) a) Distinguish between Symmetric and Asymmetric key cryptography. Explain the principle of one time pad with example. **[6]**

b) In RSA, if public key e = 7 and modulus n = 33, calculate private key d. **[4]**

OR

Q2) a) Draw AES block diagram and state the general steps in detail. **[6]**

b) Using Euclidean algorithm calculate following **[4]**

i) GCD (88, 220)

ii) GCD (25, 60)

Q3) a) Explain X.509 standard for digital certificate. **[6]**

b) Find the value of x using Chinese remainder theorem: **[4]**
$x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 5$, $x \equiv 2 \bmod 7$

OR

Q4) a) Explain the difference between MAC and Message Digest with example. **[6]**

b) Compare and contrast MD5 and SHA1. **[4]**

Q5) a) How AH and ESP are differs while working under transport and tunnel mode. **[8]**

b) Explain different IDS methods with one example each. **[8]**

P.T.O.

OR

Q6) a) Define IKE protocol and explain its aggressive mode and quick mode in brief. **[8]**

b) Explain SSL hand shake and SSL Record protocol in detail with neat sketch. **[8]**

Q7) a) Describe the classification of cybercrime. **[10]**

b) Describe the Indian and global legal perspective on cyber-crime **[6]**

OR

Q8) a) What is cyber stalking? Explain the types of stalkers. **[10]**

b) Address security issues in cloud computing. **[6]**

Q9) a) Describe following in detail **[12]**

i) Indian IT ACT 2000 and its challenges.

ii) SQL injection.

b) Distinguish between phishing and pharming? Describe key loggers and Spywares in brief. **[6]**

OR

Q10)Write short note on following : **[18]**

a) Different ways of password cracking

b) Host based malicious programs: Trap Door, Logic Bombs and Trojan horse

c) Proxy server and an anonymizer

❖❖❖❖