Total No. of Questions : 10]

SEAT No. :

P1870

[Total No. of Pages : 2

[4859]-1058

B.E. (Information Technology)

INFORMATION AND CYBER SECURITY

(2012 Course) (Semester - I) (New)

Time : 3 Hours] *[Max. Marks : 70*

Instructions to the candidates:

1) ***Answer Q.1 or Q.2, Q3 or Q.4,Q.5 or Q.6, Q.7 or Q.8,Q9 or Q.10***
2) ***Neat diagrams must be drawn wherever necessary.***
3) ***Figures to the right indicate full marks.***
4) ***Assume suitable data, if necessary.***

Q1) a) State the Chinese Remainder theorem with example. **[6]**

b) In a public key cryptosystem using RSA, given N=187 and the encryption key (E) as 17, find out the corresponding private key (D). **[4]**

OR

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

b) Define following. **[4]**

i) Discrete logarithm

ii) Fermat theorem

Q3) a) Explain X.509 standard for Digital Certificate. **[6]**

b) Explain permutation and substitution steps in DES algorithm. **[4]**

OR

Q4) a) Using Euclidean algorithm calculate **[4]**

i) GCD (48, 30)

ii) GCD (105, 80)

b) What problem was Kerberos designed to address. Describe Kerberos realm. **[6]**

P.T.O.

Q5) a) Define IKE protocol and illustrate IKE format in detail. **[8]**

b) Discuss SSL with respect to four phases **[8]**

i) Establish security capabilities

ii) Server authentication and key exchange

iii) Client authentication and key exchange

iv) Finish

OR

Q6) a) Explain various categories of Intrusion Detection system (IDS) **[8]**

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

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

b) Define cyber security and information security with example. **[6]**

OR

Q8) a) Explain with example how social engineering is playing wide role in cyber crime. **[10]**

b) Write a short note on Indian legal perspective. **[6]**

Q9) a) What is SQL injection? Explain in detail. **[8]**

b) Write short note on: **[10]**

i) Indian IT act

ii) Different ways of password cracking

OR

Q10) Define and differentiate

a) Proxy server and an anonymizer. **[6]**

b) DOS and DDOS **[6]**

c) Virus and worm. **[6]**