

Total No. of Questions :10]

SEAT No. :

P3632

[4959]-1121

[Total No. of Pages :2

B.E. (Information Technology)
INFORMATION AND CYBER SECURITY
(2012 Pattern) (End-Sem.) (Semester -I) (414453)

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) Neat diagrams must be drawn wherever necessary.
- 3) Figures to the right side indicate full marks.
- 4) Assume suitable data if necessary.

Q1) a) Explain the following terms with example. [5]

Confusion and diffusion

b) State the Euclids algorithm with example. [5]

OR

Q2) a) Draw block diagram of SHA-1 and state the general step in the process. [5]

b) State and prove Fermat's theorem. [5]

Q3) a) What is Needham Schroeder protocol? Explain with sequence diagram. [5]

b) Explain one way and mutual authentication. [5]

OR

Q4) a) What is mean by modular arithmetic and exponentiation? [5]

b) What are the possible attacks on DES? [5]

P.T.O.

- Q5)** a) Explain SSL hand shake and SSL Record protocol in detail with neat sketch. [8]
b) Differences between. [8]
i) HIDS and NIDS.
ii) IDS and IPS.

OR

- Q6)** a) List the benefits of IPSec. Distinguish between tunnel and transport mode in IPSec [8]
b) What is the purpose of the SSL record layer protocol and handshake protocol? [8]
- Q7)** a) Describe the Indian and global legal perspective on cyber crime. [8]
b) Explain the types of cyber crime in detail. [8]

OR

- Q8)** a) What is Cyber stalking? Types of stalkers (online and offline). [8]
b) Explain what are the different attacks launched with attack vector. [8]

- Q9)** a) What is the difference between proxy servers and an anonymizers? [8]
b) Explain phishing and password cracking. [10]

OR

- Q10)** Write short note on following. [18]
a) Key loggers and Spywares.
b) Indian IT Act and its challenges.
c) SQL Injection and Digital signatures.

