

Total No. of Questions : 12]

SEAT No. :

P864

[4659] - 244

[Total No. of Pages : 3

**B.E (Computer Engineering)
d- INFORMATION SECURITY
(2008 Course) (Semester - II) (Elective - IV)**

Time : 3 Hours]

[Max. Marks : 100

Instructions to the candidates:

- 1) *Answer any three questions from each section.*
- 2) *Neat diagrams must be drawn wherever necessary.*
- 3) *Figures to the right side indicate full marks.*

SECTION - I

- Q1)** a) What are the different categories of security services defined by x.800? Discuss each in detail. [8]
- b) What are different types of cryptography? Explain Hill Ciphering developed by Lester Hill in detail with suitable example. [10]

OR

- Q2)** a) What is masquerade? Discuss it with suitable example. Is it active attack? Justify your answer. [8]
- b) What is Rotor machine? Discuss Rotor Machine with wiring representation [10]

- Q3)** a) Draw and explain the internal structure of single round of DES algorithm. [8]
- b) What is stream Ciphering? Discuss any one stream ciphering in detail. [8]

OR

- Q4)** a) What is diffusion and confusion? Differentiate diffusion and confusion. [8]
- b) Draw and explain key distribution scenario using private key cryptography. [8]

P.T.O.

- Q5)** a) What is a one way and trapdoor one way function? Explain each in detail. [8]
- b) Perform encryption and decryption using RSA algorithm for following value of keys message. Discuss each step in detail. [8]
- i) $p = 3, q = 11, e = 7, m = 5$
- ii) $p = 17, q = 31, e = 7, m = 2$

OR

- Q6)** a) How the key management is done using private key cryptography? Discuss any one method for key management. [8]
- b) What is elliptic curve? Explain zero point of elliptic curve. Consider Diffie-Hellman scheme with a common prime number $q = 1$ and a primitive root $\alpha = 2$. If user A has private key $Y_A = 9$, what is private key X_A . [8]

SECTION - II

- Q7)** a) What types of attacks are addressed by message authentication? Enlist and explain in detail. [8]
- b) What message digests? Explain all steps of MD5 algorithm for message digesting. [10]

OR

- Q8)** a) What is HMAC? Discuss different objectives of HMAC. Explain HMAC algorithm in brief. [8]
- b) What is Digital Signature? Explain DSA algorithm in detail. Enlist all algorithms which can use for digital signature. [10]

- Q9)** a) Enlist and explain the services provided IPSec. What are the benefits of IPSec? [8]
- b) Explain SSL architecture with suitable diagram. [8]

OR

- Q10)** a) What is IDS? Differentiate statistical Anomaly detection and rule base intrusion detection. [8]
- b) What is packet filtering? Differentiate packet filtering router and stateful inspection firewall. [8]

- Q11)a)** What are the different principal services provided by PGP? Discuss each service in detail. **[8]**
- b) Explain the format of text message of email defined by RFC 822 in detail. **[8]**

OR

- Q12)a)** Enlist and discuss security services provided by X.500 in detail. **[8]**
- b) Write short notes on the following (any two). **[8]**
- i) PEM
 - ii) Electronic Commerce Security
 - ii) Web and Email security.

