

Total No. of Questions : 12]

SEAT No. :

**P715**

**[4458]- 781**

[Total No. of Pages : 2

**B.E. (Computer Engg.)**

**INFORMATION SECURITY**

**(Elective - IV) (410451) (Semester - II)(2008 Course)**

*Time : 3 Hours]*

*[Max. Marks : 100*

*Instructions to the candidates:*

- 1) *Answer three questions from Section-I and three questions from Section-II.*
- 2) *Figures to the right indicate full marks.*
- 3) *Assume suitable data, if necessary.*

**SECTION - I**

- Q1)** a) What are threats? Explain the different categories of threat. [6]  
b) Explain the four important functions of the information security performs in an organization. [12]

OR

- Q2)** a) Explain replay, modification of messages and denial of service attacks. [6]  
b) Explain in detail the Legal, Ethical and Professional issues during the security investigation. [12]

- Q3)** a) Write Characteristics of IDEA. Explain Encryption process of IDEA. [8]  
b) Explain with diagram steps involved in Automatic Key Distribution for Connection-Oriented Protocols. [8]

OR

- Q4)** a) Explain Control Vector Encryption and Decryption with diagram. [8]  
b) Describe Euclidean algorithm with the help of importance and pseudo code of algorithm. [8]

- Q5)** a) Briefly explain Diffie-Hellman key exchange. [8]  
b) In a public-key system using RSA, you intercept the ciphertext  $C = 10$  sent to a user whose public key is  $e = 5$ ,  $n = 35$ . What is the plaintext  $M$ ? [8]

OR

**P.T.O.**

- Q6)** a) Users A and B use the Diffie-Hellman key exchange technique with a common prime  $q = 71$  and a primitive root  $a = 7$ . [8]
- i) If user A has private key  $X_A = 5$ , what is A's public key  $Y_A$ ?
- ii) If user B has private key  $X_B = 12$ , what is B's public key  $Y_B$ ?
- iii) What is the shared secret key?
- b) Explain Elliptic Curve Cryptography in details. [8]

**SECTION - II**

- Q7)** a) What are the technical deficiencies in the Kerberos version 4 protocol. Explain how, Kerberos version 5 address these deficiencies. [8]
- b) Explain Digital Signature Algorithm. [8]

OR

- Q8)** a) Explain with the help of diagram X.509 certificate format. [8]
- b) Explain PKIX model Management Functions in details. [8]

- Q9)** a) What is Intrusion Detection System(IDS)? Explain different reasons for using IDS and different terminologies associated with IDS. [8]
- b) What are IPSec Services for IP layer? Explain SA parameters of IPSec. [8]

OR

- Q10)** a) What are the factors to be considered in selecting a right firewall? [4]
- b) How firewalls are configured and managed? [4]
- c) Draw SSL Protocol Stack and explain same. [8]

- Q11)** a) With help of diagram explain SET Participants. [8]
- b) Describes the functions of S/MIME. Also describes the functions of Cryptographic Algorithms Used in S/MIME. [10]

OR

- Q12)** a) Write short notes on : [12]
- i) PEM.
- ii) PGP.
- b) Describe Electronic commerce security issues from the perspective of customers and e-businesses. [6]

↑↑ ↑↑ ↑↑