7E4104

Roll No. _____ [Total No. of Pages . 2]

7E4104

B. Tech. VII Semester (Back) Examination, Nov-Dec-2011

Information Technology

7IT5 Information Protection & Security

Time : 3 Hours **Maximum Marks : 80**

Min. Passing Marks : 24

Instructions to Candidates:

*Attempt any **five questions,** selecting **one** question from **each unit.** All questions carry **equal marks.** Schematic diagrams must be shown wherever necessary. Any data you feel missing suitably be assumed and stated clearly. Units of quantities used/calculated must be stated clearly.*

Unit - I

1. a) What do you understand about security attacks. Explain passive and active attacks in detail. **(8)**

   b) Explain the following cryptographic techniques

      i) Substitution techniques

      ii) Transposition techniques **(4+4=8)**

OR

1. a) What do you mean by block cipher? Explain different block cipher techniques. **(8)**

   b) Show that DES decryption is, in fact, the inverse of DES encryption. **(8)**

Unit - II

2. a) Explain the following with example

      i) Fermat's Little Theorem

      ii) Euler's Totient Function

      iii) Euler's Theorem **(8)**

   b) Write Euclid's algorithm to find the gcd of two integers and calculate the gcd (468, 24) and gcd (1970, 1066) **(8)**

OR

2. a) Explain the Diffie Hellman Key exchange algorithm with example? What is the man-in-the-middle attack problem in Diffie Hellman key exchange algorithm. **(8)**

   b) What is the roll of RSA algorithm in public key cryptography? Explain the RSA algorithm with example. **(8)**

Unit - III

3. a) Explain the concept of MAC and its function. **(8)**

   b) What is hash function? Why we need it for authentication. **(8)**

OR

3. a) What is message digest? Explain the detailed working of MD5 Message Digest algorithm. **(8)**

   b) Why we need SHA? Explain the working of SHA -1. **(8)**

Unit - IV

4. a) What is authentication? How Kerberos helps in authentication? Explain. **(8)**

   b) What is X-509 authentication service? Explain. **(8)**

OR

4. a) Why we need electronic mail security? Explain various services provided by PGP. **(8)**

   b) What is S/MIME? Explain its functionality. **(8)**

Unit - V

5. a) Why Internet security is important Explain the architecture of IP security. **(8)**

   b) What is security association (SA). Explain the Transport Mode and Tunnel mode security Associations. **(8)**

OR

5. a) Explain the working of Secure Electronic Transaction (SET) **(8)**

   b) Why we use firewalls? Explain the different types of firewalls. **(8)**
