No. of Printed Pages : 3

CST-303

00841

ADIT / BIT PROGRAMME

Term-End Examination

December, 2011

CST-303 : INFORMATION SYSTEM SECURITY

Time : 3 hours *Maximum Marks : 75*

Note : *There are **two Sections** in this paper. All questions in **Section A** are **Compulsory**. Answer **any three** questions from **Section B**.*

SECTION - A

1. For each of the following statement, state whether it is ***true*** or ***false*** : **1x10=10**

(a) RSA stands for Rivest Security Algorithm.

(b) Kerberos is not a Security tool.

(c) Virus appends itself to a file, therefore, it becomes easy to detect it.

(d) Diffie - Hellman algorithm is used for key exchange.

(e) Euler totient function is used in RSA algorithm.

(f) In Public key system encryption key and decryption key are different.

(g) Digital signature standard is an example of public cryptography system.

(h) DES encrypts blocks of 128 bits.

(i) Firewalls provides no protection against external threats.

(j) X· 509 defines the standard for digital signature certificate.

2. What do you understand by 'Authentication' and 'Encryption' in the context of system security ? Explain. **10**

3. Discuss how kerberos protocol achieves authentication. **10**

SECTION - B

4. (a) Describe how PGP is used to provide secure e-mail communication. **10**

   (b) Differentiate between active attacks and passive attacks. **5**

5. (a) Describe the importance of digital signature in banking and insurance sector. **10**

   (b) Discuss the Caesar Cipher technique. **5**

6. Perform the encryption and decryption using RSA algorithm for the following : **15**
   P = 7, q = 17, plain text input 'M' = 19 and d = 77.
   p and q are two prime numbers.

7. Write a brief note on each of the following : **5x3=15**
   (a) IP Sec
   (b) Substitution Cipher
   (c) Logic Bomb
   (d) Virus
   (e) SSL