Roll No. .... Total Pages : 03

BT-7/D-18 37151

CRYPTOGRAPHY AND INFORMATION SECURITY

CSE-419N

Time : Three Hours] [Maximum Marks : 75

Note : Attempt *Five* questions in all, selecting at least *one* question from each Unit.

Unit I

1. (a) What is Shannon's theorem for perfect secrecy ? 3

   (b) What is the difference between : 6

   (i) Polyalphabetic and mono-alphabetic ciphers

   (ii) Public and private key crytography ?

   (c) Use the playfair cipher to encipher and decipher the message "the key is hidden under the door pad" using the key GUIDANCE. 6

2. (a) Discuss various active and passive attacks. 5

   (b) What is the difference between threat and an attack ? 2

   (c) What do you understand by CIA Security ? 3

Previous Pathshala

(d) Define Kerchhoff's and Avalanche principle in context to cryptography. Give example. 5

Unit II

3. (a) How key expansion takes place in :

   (i) AES

   (ii) DES ? 6

   (b) Draw a single round of DES with clear description of mangler function. How many XOR operations are used in DES. 6

   (c) What is the difference between Tiger hash and Gear hash ? 3

4. (a) Performance RSA encryption for $p = 17$, $q = 11$, $e = 7$ and $M = 88$. Find out the cipher text by showing each step. Also, perform decryption to verify your calculation. 7

   (b) Draw and explain the modes of cipher that can be used in a stream cipher mode. 5

   (c) Discuss briefly PKI. 3

Unit III

5. (a) How key exchange takes place in DH algorithm ? Explain man-in-the-middle attack on DH algorithm with the help of example. 8

Previous Pathshala

(b) Draw an overview of Kerberos illustrating all the message exchanges. 7

6. (a) Write notes on the following :

(i) PGP

(ii) SSL. 8

(b) Elaborate CCA-secure encryption. 7

Unit IV

7. Explain the following : 15

(a) Rabin fingerprint algorithm

(b) DSS

(c) MD5.

8. (a) Explain any *two* intrusion systems in detail. 10

(b) How digital certificates provide security ? 5

Previous Pathshala