2017/EVEN/08/24/MCS–1003 (C)/
MS–403 (C)/575

PG Even Semester (CBCS) Exam., May—2017

COMPUTER SCIENCE

(10th Semester/4th Semester)

Course No. : MCS–1003 (C)/MS–403 (C)

(Cryptography)

Full Marks : 75
Pass Marks : 30

Time : 3 hours

The figures in the margin indicate full marks for the questions

Answer **five** questions, taking **one** from each Unit

UNIT—I

1. *(a)* What are the principles of security? Explain each of them with the attacks that compromise them. Use proper complies wherever needed. 12

(b) With an example, explain the simple columnar technique. 3

2. *(a)* Define the following : 4

(i) Brute force attack

(ii) Steganography

(iii) Host security

(iv) Security through obsecurity

(b) Consider a plain text message "I am a Hacker". Encrypt it with the following algorithm : 11

STEP *(i)* Replace each alphabet with its equivalent 7 bits ASCII code.

STEP *(ii)* Add a 0 bit as a left most bit to make each of the above bit patterns 8 bits long.

STEP *(iii)* Swap the 1st 4 bits with the last 4 bits for each alphabet.

STEP *(iv)* Write the hexadecimal equivalent of every 4 bits.

UNIT—II

3. *(a)* Compare and contrast between symmetric key and asymmetric key cryptography. 5

(b) Explain the concepts of symmetric key cryptography with proper diagram. 5

(c) Explain the concepts of stream cipher and block cipher with proper examples. 5

4. *(a)* What are the broad level steps of DES? Explain with proper diagram. 4+4=8

(b) Explain why and how every 8th bit of the original key of DES is discarded. Take help of a table to explain thus. 7

UNIT—III

5. *(a)* Explain the problem of key distribution faced in symmetric key cryptography. 2

(b) Explain the Diffie-Hellman key exchange algorithm. 9

(c) Alice and Bob want to establish a secret key using the Diffie-Hellman key exchange algorithm. Assuming $n = 11$, $g = 5$, $x = 2$ and $y = 3$, find out the values of a, b, k_1 and k_2. 4

6. *(a)* With proper diagram, explain the steps involved in AES. 10

(b) What is the idea behind meet-in-the-middle attack? 5

UNIT—IV

7. *(a)* Explain with diagrams how asymmetric key cryptography can help us to attain *(i)* confidentiality and *(ii)* authentication and non-repudiation. 4+6=10

(b) Explain the concept of message digests. 5

8. *(a)* Explain SHA. Compare between MD5 and SHA. 3+4=7

(b) Explain the RSA algorithm with an example. 8

UNIT—V

9. Write notes on the following : 7+8=15

(a) Digital watermarking

(b) Kerberos with diagram

10. *(a)* What are the advantages of using firewalls? What are its limitations? Discuss the two types of firewall with diagrams. 2+2+6=10

(b) Draw and explain in short the VPN architecture. 5

★ ★ ★