PG Even Semester Examination, September, 2023

COMPUTER SCIENCE

(10th Semester)

Course No.: MCSCC-1003 / MS-403

(Cryptography)

Full Marks: 70

Pass Marks: 28

Time: 3 hours

The figures in the margin indicate full marks for the questions.

Answer any five questions, taking one from each unit.

UNIT-I

1. (a) What is the difference between Host and Network security? In which model a system is secure because no one knows about its presence and contents? 3+1=4

   (b) State if the following are true or false with proper explanation (any two) : 2+2=4

   (i) Substitution techniques involve permutation and comibations to produce cipher text.

   (ii) In simple columnar technique we write down the plaintext message as a sequance of diagonals.

UNIT-V

9. (a) Write a technical note on types of Digital watermarking, their uses and advantages? 7

   (b) What are the significance of digital significance and certificates? 7

10. (a) What is PGP? Explain its significance. 5

    (b) With proper diagram explain the working of Kerberos. 9

****

(iii) Concepts of symmetric key criptography and public key cryptography are opposite to each other.

(c) Discuss the different attack that compromises the principals of security. 6

2. (a) Using mono-alphabetic cipher, with key= 9 encrypt the message "This is a book on security". Discuss the problem in the above question. 2+2=4

(b) The number of possibilities required to break mono-alphabetic cipher is ____. Explain why? 2+2=4

(c) What are the differences between substitution and transposition techniques? Explain with examples. 6

UNIT-II

3. State if the following are true or false with proper explanation: 2x7=14

(i) "Block cipher can consist of ony 64 bits."

(ii) "MCC can have 27 different combination".

(iii) In DES *Initial permutations* and *final permutations* are optional steps.

(iv) In Double DES S-Box substitution is not required.

(v) Double DES brings together concepts of Substitution and Transposition

(vi) Block cipher Decryption consist of decypting one bit at a time.

(vii) DES a block cipher algorithm.

4. What are strength of DES? What are modes of operations of DES? 7+7=14

UNIT-III

5. Explain in details how IDEA and BLOWFISH works. 7+7=14

6. (a) Explain the main features of AES. Discuss the steps of AES. 7

(b) Explain the concepts of Linear Congruential Generators? 7

UNIT-IV

7. (a) Given two prime numbers, P=17, Q=29, find out N, D and E in RSA. 7

(b) Consider a plain text alphabet "G", using RSA algorithm and values E=3, D=11 and N=15, find out what this plain text alphabet encrypts to and verify that upon decryption it transforms to G. 7

8. (a) What is the name of the attack that creates problem for Deffie-Hellman key exchange algorithm? Explain with an example how this attack takes place. 1+5=6

(b) Compare the working of : MD5 and SHA. 4

(c) What is HMAC? 4