UG/PG ODD SEMESTER EXAMINATION, 2022

COMPUTER SCIENCE

7th Semester /1st Semester

Course No. : MCS-503

(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 are replay attacks? Give an example of replay attack. 4

   (b) Encrypt "MY NAME IS ATUL" with Playfair cipher using key "PLAYFAIR EXAMPLE". Explain the steps involved. 5

   (c) What is the difference between Substitution Cipher and Transposition cipher? 5

2. (a) Discuss the concept s of Phishing and Pharming. 4

(b) What will be the ciphered text if the plain text "CAT" is encrypted using Hill cipher with keyword as "GYBNQKURP"? Explain the steps involved 5

(c) Discuss the algorithm for Rail Fence Technique. 5

UNIT-II

3. (a) Distinguish between streams and block ciphers. 5

(b) What is the idea behind meet-in-the-middle attack? 4

(c) Explain Double DES and Triple DES. 5

4. (a) Explain any two data encryption modes. 4

(b) Distinguish between Symmetric and Asymmetric key cryptography 5

(c) Explain the main concepts in DES. 5

UNIT-III

5. (a) What is the IDEA algorithm? Explain the details of one round in IDEA algorithm. 7

(b) Explain the encryption and decryption process of Blowfish algorithm? 7

6. Explain Dippie-Hellman keye exchanghe/ agreement algorithm in detail. 14

UNIT-IV

7. (a) Describe the advantage and disadvantages of symmtric and symmetric-key cryptography. 14

(b) Can we combined the symmetric-key cryptography and asymmetric-key cryptography? If yes, explain in detail. 4

(c) Given two prime number P-17 and Q-29, find out N, E and D in a RSA encryption process. 6

8. Explain the working of MD-5 algorithm in detail. 14

UNIT-V

9. Explain Kerberos V_4 authentication protocol in detail. 14

10. Write short notes on the following : 4+5+5=14

(i) IP Security

(ii) Digital Envelope

(iii) Digital Signature

****