

Register Number

|  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|

Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam – 603 110

(An Autonomous Institution, Affiliated to Anna University, Chennai)

Department of Computer Science and Engineering

Continuous Assessment Test – II

Question Paper

|                                      |  |       |         |      |                   |    |
|--------------------------------------|--|-------|---------|------|-------------------|----|
| Degree & Branch                      | B.E CSE  |       |         |      | Semester          | V  |
| Subject Code & Name                  | UCS1505 & INTRODUCTION TO CRYPTOGRAPHIC TECHNIQUES |       |         |      | Regulation: 2018  |    |
| Academic Year                        | 2022-23<br>ODD                                     | Batch | 2020-24 | Date | 19.10.2022        | FN |
| Time: 8.15 – 9.45 AM<br>(90 Minutes) | Answer All Questions                               |       |         |      | Maximum: 50 Marks |    |

## Part – A (6×2 = 12Marks)

|    |   |     |                |
|----|---|-----|----------------|
| K1 | 1. What is diffusion and confusion?                                       | CO1 | 1.4.1          |
| K2 | 2. Explain the avalanche effect.  | CO1 | 1.3.1          |
| K3 | 3. Apply Fermat's little theorem to find $2^{345} \text{ mod } 11$ .      | CO3 | 1.4.1          |
| K2 | 4. Compare DES and AES  | CO1 | 1.3.1<br>1.4.1 |
| K3 | 5. Apply Euclid's algorithm to find the gcd (1076, 1970)                  | CO3 | 1.3.1<br>2.1.3 |
| K2 | 6. Explain any two algebraic structures used in cryptographic algorithms. | CO3 | 1.4.1          |

## Part – B (3×6 = 18 Marks)

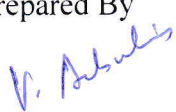
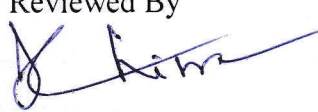
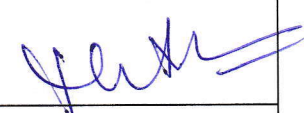
|    |   |     |                 |
|----|---|-----|-----------------|
| K2 | 7. What is a message authentication code? What is the difference between a message authentication code and a one-way hash function? | CO1 | 1.4.1           |
| K3 | 8. Solve using Euler's Totient function $\phi(440)$ , $\phi(27)$ and $\phi(231)$  | CO3 | 1.4.1<br>13.3.1 |
| K3 | 9. Apply extended Euclid algorithm to find the multiplicative inverse of 23 mod 100.  | CO3 | 1.4.1<br>13.3.1 |

## Part – C (2×10 = 20 Marks)

|    |   |     |       |
|----|---|-----|-------|
| K2 | 10. Alice wants to send message M to Bob, without Eve observing it. Alice and Bob have agreed to use a symmetric cipher Data Encryption Standard (DES). Key exchange has already been done, and so they share a key K for a specific encryption algorithm E.<br>a. Outline the steps that Alice must follow for encrypting M and sending it to Bob.<br>b. Outline the steps that Bob must follow for decrypting the received ciphertext C | CO1 | 1.4.1 |
|----|---|-----|-------|

OR

|    |  |     |                 |
|----|--|-----|-----------------|
| K2 | 11. What is double DES? What kind of attack on double DES makes it useless?<br>What is triple DES?   | CO1 | 1.4.1           |
| K3 | 12. Apply the Chinese remainder Theorem to solve the following congruences and explain the algorithm.<br>$x \equiv 1 \pmod{3}$ $x \equiv 4 \pmod{5}$ $x \equiv 6 \pmod{7}$   | CO2 | 2.1.3<br>13.3.1 |
| OR |  |     |                 |
| K3 | 13. Make use of a Feistel cipher composed of sixteen rounds with a block length of 128 bits and a key length of 128 bits. Suppose that, for a given $k$ , the key scheduling algorithm determines values for the first eight round keys,<br>$k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9 = k_8, k_{10} = k_7, k_{11} = k_6, k_{12} = k_5, k_{13} = k_4, k_{14} = k_3, k_{15} = k_2, k_{16} = k_1,$<br>Suppose you have a ciphertext $C$ . Explain how, with access to an encryption oracle, you can decrypt $C$ and determine $m$ using just a single oracle query. (5 Marks)<br>b. Consider a notion of indistinguishable encryption for multiple distinct messages, i.e., where a scheme need not hide whether the same message is encrypted twice. Give a suitable definition | CO3 | 2.1.3<br>13.3.1 |

|  |   |  |
|--|---|--|
| Prepared By<br> | Reviewed By<br> | Approved By<br> |
| Course Coordinator   | PAC Team  | HOD  |