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** | 2020-21 | **Batch** | 2018-22 | **Date** | **29.9.20** | **FN** |
| **Time: 90 Minutes** | **Answer All Questions** | | | | **Maximum: 50 Marks** | |

Part – B Answer all the questions (2×5 = 10 Marks)

|  |  |  |
| --- | --- | --- |
| <KL3> | 1 a. Give an example what is vrfyk(m,t) in MAC algorithm. (2)  b. When m=2 bits, t=2 bits, k=2 bits, List all the possible m,t and k.(2)  c. What is meant by oracle in the context of adversary. (1) | <CO3> |
| <KL2> | 2. a. What is avalanche effect. (2)  b.How to derive sub-keys from master key. Give an example. (2)  c. What is meant by one round in feistel network? (1) | <CO2> |

Part – C Answer any TWO questions (2×10 = 20 Marks)

|  |  |  |
| --- | --- | --- |
| <KL3  > | 3 a. With m=2 bits, t=2 bits, what is meant by unforgery?(1)   1. Draw a flowchart combining Mac-forgeA, 𝜋 and Mac(Gen, Mac, Vrfy) scheme. (3) 2. What is chosen message attack and adaptive chosen message attack in the context of adversary? Which one is best for him?(2) 3. Give a scenario validating the Mac-sForge scheme.(2) 4. if k=3 bits, T=4 bits, M=8 bits. For T=1110, M=10110110, what is meant by brute force attack on MAC.(2) | <CO3> |
| <KL3  > | 4 a. List out all combination of message tag pair if T=2, M=4 bits. How many repetition you can find? (1)   1. Give some sample data for the following scheme. (3)  1. What are the cases CBC - MAC is secure and when it is not secure. (2) 2. What is collision and collision resistent ? Give an example (2) 3. How is it possible to forge a valid tag by adversary ? (2) | <CO3> |
| <KL2  > | 5. a. What is meant by Inverting a Feistel network ? (2)   1. List out the procedure in one round DES function. (2) 2. In what cases DES is more vulnerable to attacks? (2) 3. Give two differences of AES and DES (2). 4. What are weak keys in DES? (2) | <CO2> |