| Reg.No. |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**INTERNAL ASSESSMENT TEST -II**

**CB3491 –CRYPTOGRAPHY AND CYBER SECURITY**

**Academic Year: 2023-24 (ODD Semester)**

**A**

**Year/Semester & Branch: III Year/ V Semester**

**Faculty Name: Dr.G.Sivaraman Date: 01/11/23**

**Max. Marks: 50 Time: 90 mins**

| **Course Outcome(s)** | **Question Numbers** | **Bloom's Taxonomy Level** |
| --- | --- | --- |
| **CO 3:** Develop cryptographic algorithms for information security. | 1 2 3 6  8 | RE -Remembering  UN -Understanding  AP -Applying  AN -Analyzing  EV –Evaluating  CR –Creating |
| **CO 4:** Comprehend the various types of data integrity and authentication schemes | 4 5 7  9 |

**PART-A Answer ALL Questions (5x2=10 Marks)**

1. What are the strengths of DES algorithm ?**[RE]**
2. How is S-box constructed in DES? **[RE]**
3. State Fermat’s and Euler’s theorem .**[UN]**
4. Evaluate 1113 mod 53 using modular exponentiation.[**RE]**
5. What are the function for message authentication .**[RE]**

**PART-B Answer ALL Questions (2 X 13=26 Marks)**

1. Detail about the Data Encryption Standard with suitable diagrams .(13) [UN]
2. Explain Diffie-Hellman Key exchange with its pros and cons .(13)**[UN]**

**PART-C Answer the Questions (2X7=14 marks)**

**(Application/Design/Analysis/Evaluation/Creativity/Case Study)**

1. Explain the Chinese Remainder Theorem (7) **[UN]**
2. Detail about the Hash Function (7) **[UN]**

**Prepared by** **Verified by**  **Approved**

**(Dr.G.Sivaraman) (Ms.M.Anitha)**

**AP/CSE HOD/CSE PRINCIPAL**

| Reg.No. |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**INTERNAL ASSESSMENT TEST -II**

**CB3491 –CRYPTOGRAPHY AND CYBER SECURITY**

**Academic Year: 2023-24 (ODD Semester)**

**B**

**Year/Semester & Branch: III Year/ V Semester**

**Faculty Name:Dr.G.Sivaraman Date: 01/11/23**

**Max. Marks: 50 Time: 90 mins**

| **Course Outcome(s)** | **Question Numbers** | **Bloom's Taxonomy Level** |
| --- | --- | --- |
| **CO 3:** Develop cryptographic algorithms for information security. | 1 2 3 6  8 | RE -Remembering  UN -Understanding  AP -Applying  AN -Analyzing  EV –Evaluating  CR –Creating |
| **CO 4:** Comprehend the various types of data integrity and authentication schemes | 4 5 7  9 |

**PART-A Answer ALL Questions (5x2=10 Marks)**

1. What are discrete logarithms **?[RE]**
2. List out the different techniques of distributing public keys. **[RE]**
3. What types of attacks are addressed by message authentication? [**UN]**
4. Differentiate Hash function and MAC?[**RE]**
5. List out the applications of the public key cryptosystems.**[RE]**

**PART-B Answer ALL Questions (2 X 13=26 Marks)**

1. Detail about the AES with suitable diagrams.(13) **[UN]**
2. Explain Diffie-Hellman Key.(13) **[UN]**

**PART-C Answer the Questions (2X7=14 marks)**

**(Application/Design/Analysis/Evaluation/Creativity/Case Study)**

1. Detail about Primes .(7) **[UN]**
2. Explain about the Hash function of Authentication function. (7) **[UN]**

**Prepared by** **Verified by**  **Approved**

**(Dr.G.Sivaraman) (Ms.M.Anitha)**

**AP/CSE HOD/CSE PRINCIPAL**

| Reg.No. |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |