|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Roll No |  |  |  |  |  |  |  |  |  |  |  |  |

****

**Presidency University**

**Bengaluru**

**School Of Computer Science and Engineering & Information Science**

**Summer Term End-Term Examinations, August 2024**

**Date**: 06-08-2024

**Time**: 9:30AM – 12:30PM

**Max Marks**: 100

**Weightage**: 50%

**Odd Semester**: 2023 - 24

**Course Code**: CSE3078

**Course Name**: Cryptography and Network Security

**Department:** CSE

**Instructions:**

1. *Read the all questions carefully and answer accordingly.*
2. *Do not write any matter on the question paper other than roll number.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q.No** | **Questions** | **Marks** | **CO** | **RBT** |
| 1 | 1. To encipher the message “meet me after the DJ party” with a rail fence of depth 3. | 4 | CO1 | L1 |
| 1. Using the Vigenère cipher, encrypt the word “cryptographic” using the key “eng” | 6 | CO1 | L2 |
| 1. Construct a Playfair matrix with the key "cryptography". Make a reasonable assumption about how to treat redundant letters in the key Encrypt this message: "I only regret that I have but one life to give for my country" | 10 | CO1 | L3 |
| OR | | | | |
| 2 | 1. Apply Columnar Transposition Technique to encrypt the given plaintext.  Plain Text: "plan postponed until further order" Key: 4312567 | 4 | CO1 | L1 |
| 1. Compute the determinant of  \begin{bmatrix} 21 &12 &25 \\ 5&7 &18 \\ 3&14 &12 \end{bmatrix} mod 26 | 6 | CO1 | L2 |
| 1. Compute the corresponding ciphertext for the message “ATTACK” using the Hill cipher with the key | 10 | CO1 | L3 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3 | 1. State Fermat's little theorem and prove it for given data: p = 13 & a = 11. | 4 | CO2 | L1 |
| 1. Using the extended Euclidean algorithm, find the multiplicative inverse of 550 mod 1759. | 6 | CO2 | L2 |
| 1. A Box contains gold coins. If the coins are equally divided among three friends, two coins are left over, If the coins are equally divided among five friends, three coins are left over If the coins are equally divided among seven friends, two coins are left over. If the box holds smallest number of coins that meets these conditions, how many coins are there? (Hint : Use Chinese Remainder Theorem). | 10 | CO2 | L3 |

OR

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4 | 1. State the Euler's theorem and prove it for the given data: a = 3 & n=10. | 4 | CO2 | L1 |
| 1. Compute the output of the MixColumns transformation for the following sequence of input bytes “97 EC C3 95” using the key matrix. \begin{pmatrix} 2 &3 &1 &1 \\ 1 &2 &3 &1 \\ 1&1 &2 &3 \\ 3& 1 &1 &2 \end{pmatrix} | 6 | CO2 | L2 |
| 1. Given the plaintext {0F0E0D0C0B0A09080706050403020100} and the key {02020202020202020202020202020202} for Advanced Encryption Standard. i. Show the original contents of State, displayed as a 4 \* 4 matrix. ii. Show the value of State after initial AddRoundKey. iii. Show the value of State after SubBytes. | 10 | CO2 | L3 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5 | 1. Compare symmetric and asymmetric cryptography. | 4 | CO3 | L1 |
| 1. What is Digital Signature? Explain how it is created at the sender end and retrieved at receiver end differentiate digital signature from digital certificate. | 6 | CO3 | L2 |
| 1. Alice and Bob use the Diffie–Hellman key exchange technique with a common prime q = 157 and a primitive root ɑ= 5. i. If Alice has a private key XA = 15, find her public key YA. ii. If Bob has a private key XB = 27, find his public key YB. iii. What is the shared secret key between Alice and Bob? | 10 | CO3 | L3 |

OR

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 6 | 1. Describes a man-in-the-middle attack on the Diffie–Hellman key exchange protocol in which the adversary generates two public–private key pairs for the attack. | 4 | CO3 | L1 |
| 1. Analyze importance of HMAC and discuss about role of HMAC as authenticator through its functionality. | 6 | CO3 | L2 |
| 1. Brief about RSA Algorithm and also Compute encryption and decryption using RSA for the given data: p = 17, q = 31, e = 7 & M = 2 | 10 | CO3 | L3 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 7 | 1. Write short note on web security. | 4 | CO4 | L1 |
| 1. Evaluate the performance of S/MIME. Compare it with PGP. | 6 | CO4 | L2 |
| 1. Discuss the roles of the different servers in Kerberos protocol. How does the user get authenticated to the different servers? | 10 | CO4 | L3 |

OR

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8 | 1. Identify the benefits of IP Security. | 4 | CO4 | L1 |
| 1. Draw the flow diagram for Handshake protocol and its functionality in web client server application. | 6 | CO4 | L2 |
| 1. Explain the operational description of PGP cryptographic functions in detail with suitable block diagrams. | 10 | CO4 | L3 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 9 | 1. Brief about hash function will act as an authenticator in public key cryptography. | 4 | CO1 | L1 |
| 1. Illustrate the Message Digest Generation using SHA-512 with neat diagram and analyze it Complexity level of Security. | 6 | CO1 | L2 |
| 1. Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 11 and a primitive root ɑ = 2. i. If Bob has a public key YB = 3, what is Bob’s private key XB? ii. If Alice has a public key YA = 9, what is Alice’s private key XA? ii. what is the shared key K with Bob? | 10 | CO1 | L3 |

OR

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 10 | 1. Illustrate SSL Record Protocol Operation in web security. | 4 | CO2 | L1 |
| 1. Describe the key elements of the PKI Architectural Model with neat diagram. | 6 | CO2 | L2 |
| 1. Illustrate the Encapsulating Security Payload (ESP) security services and functionality with neat diagram in IPsec. | 10 | CO2 | L3 |