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



 **PRESIDENCY UNIVERSITY**

  **Bengaluru**

|  |
| --- |
| **End - Term Examinations – JANUARY 2025** |
| **Date:** 11 - 01- 2025 **Time:** 09:30 am – 12:30 pm |

|  |  |
| --- | --- |
| **School:** SOCSE | **Program:** B.Tech - COM/CSE/CEI |
| **Course Code:** CSE3078 | **Course Name:** Cryptography and Network Security |
| **Semester**: V | **Max Marks**: 100 | **Weightage**: 50% |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CO - Levels** | **CO1** | **CO2** | **CO3** | **CO4** |
|  **Marks** | **24** | **24** | **26** | **26** |

**Instructions:**

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

**Part A**

|  |
| --- |
| **Answer ALL the Questions. Each question carries 2marks. 10Q x 2M=20M** |
| **1** | How secure is the one-time pad cipher. | **2 Marks** | **L1** | **CO1** |
| **2** | How do you encipher a message using an autokey system. | **2 Marks** | **L1** | **CO1** |
| **3** | Calculate the determinant mod 26 of $\begin{matrix}23&5\\13&7\end{matrix}$ | **2 Marks** | **L2** | **CO2** |
| **4** | S-Boxes inputs are s1{011011} & s2{110010} using DES. Find the outputs. | **2 Marks** | **L2** | **CO2** |
| **5** | What is the role of a compression function in a hash function? | **2 Marks** | **L1** | **CO3** |
| **6** | How does HMAC ensure message integrity and authenticity? | **2 Marks** | **L1** | **CO3** |
| **7** | Which cryptographic techniques are used to create a digital signature? | **2 Marks** | **L1** | **CO3** |
| **8** | What is the role of the Security Association (SA) in IPSec? | **2 Marks** | **L1** | **CO4** |
| **9** | What is a TLS handshake? | **2 Marks** | **L1** | **CO4** |
| **10** | Name two key features provided by S/MIME. | **2 Marks** | **L1** | **CO4** |

**Part B**

|  |
| --- |
| **Answer the Questions Total 80 Marks.** |
| **11.** | **a.** | **i.** Discuss in detail about the network security model with neat diagram. **(5 Marks)****ii.** Apply Columnar Transposition Technique to encrypt the given plaintext "plan postponed until further order". Key : 4312567 **(5 Marks)** | **10 Marks** | **L2** | **CO1** |
| **b.** | When the PT-109 American patrol boat, under the command of Lieutenant John F. Kennedy, was sunk by a Japanese destroyer, a message was received at an Australian wireless station in Playfair code:KXJEY UREBE ZWEHE WRYTU HEYFS KREHE GOYFI WTTTU OLKSY CAJPO BOTEI ZONTX BYBNT GONEY CUZWR GDSON SXBOU YWRHE BAAHY USEDQ The key used was "royal new zealand navy". Find the plaintext for given ciphertext. (**Note**: Translate TT into tt) | **10 Marks** | **L3** | **CO1** |
| **Or** |
| **12.** | **a.** | **i.** Compute the determinant of  \begin{bmatrix} 21 &12 &25 \\ 5&7 &18 \\ 3&14 &12 \end{bmatrix} mod 26 **(5 Marks)****ii**. Using the Vigenère cipher, encrypt the word “cryptographic” using the key “eng” **(5 Marks)** | **10 Marks** | **L3** | **CO1** |
| **b.** | Compute the corresponding ciphertext for the message “SECRET” using the Hill cipher with the key $\begin{matrix}17&17&5\\21&18&21\\2&2&19\end{matrix}$ matrix. | **10 Marks** | **L3** | **CO1** |
|  |  |  |  |  |  |
| **13.** | **a.** | Given the plaintext {0F0E0D0C0B0A09080706050403020100} and the key {03030303 03030303 03030303 03030303} for Advanced Encryption Standard.a. Show the original contents of State, displayed as a 4 \* 4 matrix.b. Show the value of State after initial AddRoundKey.c. Show the value of State after SubBytes. | **10 Marks** | **L3** | **CO2** |
| **b.** | Discuss the functionality of single round Data Encryption Standard with neat diagram. | **10 Marks** | **L2** | **CO2** |
| **Or** |
| **14.** | **a.** | i. Using the extended Euclidean algorithm, find the multiplicative inverse of 550 mod 1759. **(6 Marks)**ii. Determine gcd(72345, 43215) **(4 Marks)** | **10 Marks** | **L3** | **CO2** |
| **b.** | State Chinese Remainder theorem and compute the value of X for the given set of congruent equations using CRT. Justify the given equation by applying X value.X ≡ 1(mod 5)X ≡ 2(mod 7)X ≡ 3(mod 9)X ≡ 4(mod 11) | **10 Marks** | **L3** | **CO2** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **15.** | **a.** | Describe the public key cryptography system and discuss about complexity of security and its limitations. | **10 Marks** | **L2** | **CO3** |
| **b.** | Generate keys for encryption and decryption using the given data: p = 3, q = 7 and also compute ciphertext using RSA for given plaintext M=10. | **10 Marks** | **L3** | **CO3** |
| **Or** |
| **16.** | **a.** | 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. | **10 Marks** | **L2** | **CO3** |
| **b.** | Alice and Bob use the Diffie-Hellman key exchange technique with a Common prime q = 11 and a primitive root ɑ = 2.a. If Bob has a public key YB = 3, what is Bob’s private key XB?b. If Alice has a public key YA = 9, what is Alice’s private key XA?c. what is the shared key K with Bob? | **10 Marks** | **L3** | **CO3** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **17.** | **a.** | Explain the operational description of PGP cryptographic functions in detail with suitable block diagrams. | **10 Marks** | **L2** | **CO4** |
| **b.** | Discuss the roles of the different servers in Kerberos protocol. How does the user get authenticated to the different servers? | **10 Marks** | **L2** | **CO4** |
| **Or** |
| **18.** | **a.** | Illustrate the Encapsulating Security Payload (ESP) security services and functionality with neat diagram in IPsec. | **10 Marks** | **L2** | **CO4** |
| **b.** | Draw the flow diagram for Handshake protocol and its functionality in web client server application. | **10 Marks** | **L2** | **CO4** |

**\*\*\*\*\* BEST WISHES \*\*\*\*\***