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

 ****

**Presidency University**

**Bengaluru**

**Ph.D. Course Work End Term Examinations – JAN-FEB 2025**

**Date**: 06-02-2025

**Time**: 9.30 AMTO 12.30 PM

**Max Marks**: 100

**Weightage**: 50%

**Semester**:

**Course Code**: CSE859

**Course Name**: Cryptography and Network Security

**School**:SOCSE

 **Instructions:**

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

**PART A**

**Answer all the Questions. Each question carries 10 marks. (6Qx 10M= 60M)**

|  |  |
| --- | --- |
| **1.** | Discuss the functionality of single round Data Encryption Standard with neat diagram. **. [10 Marks]** |
| **2.** | Construct a Play fair 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 Marks]**  |
| **3.** | Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 11 and a primitive root ɑ = 2.1. If Bob has a public key YB = 3, what is Bob’s private key XB?
2. If Alice has a public key YA = 9, what is Alice’s private key XA?
3. What is the shared key K with Bob**? [10 Marks]**
 |
| **4.** | 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 Marks]** |
| **5.** | How can the signed data entity of S/MIME be prepared**? [4 Marks]**Draw the flow diagram for Handshake protocol and its functionality in web client server application. **[6 Marks]**  |
| **6.** | What are the actual services provided by PGP?  **[4 Marks]**Discuss security Association (SA) is uniquely identified by three parameters in IP security policy. [6 Marks] |

**PART B**

**Answer all the Questions. Each question carries 20 marks. (2Qx 20M= 40M)**

|  |  |
| --- | --- |
| **7.** | **a)** A Box contains gold coins. If the coins are equally divided among three friends, two coins are left over 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 the conditions, how many coins are there? (Hint: Use Chinese Remainder Theorem)**. [10 Marks]****b)** Compute the corresponding Ciphertext for the message “ATTACK” using the Hill cipher with the key.  $\begin{matrix}17&17&5\\21&18&21\\2&2&19\end{matrix}$ **[10 Marks]** |
| **8.** | **a)** Discuss the roles of the different servers in Kerberos protocol. How does the user get authenticated to the different servers**? [10 Marks]****b)** Discuss the importance of Digital Signature in Information Security? Explain how it is created at the sender end and retrieved at receiver end differentiate digital signature from digital certificate**. [10 Marks]** |