Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech Degree S7 (R,S) Examination November 2025 (2019 Scheme).

Course Code: CST433

Course Name: SECURITY IN COMPUTING

Max. Marks: 100 **Duration: 3 Hours**

PART A

Answer all questions, each carries 3 marks. Marks

1	Differentiate between Passive and Active security attacks with suitable example for each category.	(3)
2	Provide the definitions of the following terms associated with the Security Services of OSI Security Architecture (X.800). **a) Confidentiality** **b) Data Integrity** **c) Non- Repudiation**	(3)
3	Compare stream cipher and block cipher with example.	(3)
4	Suppose the zeroth row of the s-box in DES is initialized with values 0-15 in the increasingly sorted order and subsequent rows are initialized with values from their immediate above row, circularly right shifted 1 position. What will be the output of this s-box, if its 6-bit input is **011101**?	(3)
5	Compute the value of **Φ(100). [**Euler's Totient Function**]**	(3)
6	Define the term primitive root of a cyclic group. Also check whether 2 is a primitive root of $\mathbb{Z}_7^*$.	(3)
7	Think about employing Secure Hash Algorithm-512 for message authentication to create an authenticator for a message M that is **5000** bits long. How many bits of padding will be required?	(3)
8	List and explain two requirements for a Message Authentication Code (MAC) function.	(3)
9	List and explain the different classes of intruders in computer network security.	(3)
10	List and explain three defence techniques against Distributed Denial of Service (DDoS) attacks.	(3)

PART B

Answer any one full question from each module, each carries 14 marks.

Module I

11 a) A plaintext message is encrypted using the **Vigenere Cipher**. The key used for the encryption is **KERALA**. Suppose the ciphertext produced is **WECAJAVED**. What is the corresponding plaintext? (7)

b) A plaintext message is encrypted using the **Playfair Cipher**. The key used for the encryption is **NORMALIZE**. Suppose the ciphertext produced is **HRTBFGMYMTZI**. What is the corresponding plaintext? **[**The filler letter used for pairing the plaintext letters is **X**. Also place the letters **J** and **K** in the same cell of the key matrix. (7)

OR

12 a) A plaintext is encrypted using **Rail Fence Cipher.** The resulting ciphertext is **UIYNIESTNTIDVRIY.** What is the corresponding plaintext? (7)

b) The plaintext **CAT** is encrypted with the **Hill Cipher** using the key matrix $\begin{matrix} 6 & 24 & 1 \\ 13 & 6 & 10 \\ 20 & 17 & 15 \end{matrix}$ **.** What is corresponding ciphertext? (7)

Module II

13 a) Consider the **Add-Round Key operation of a single round of AES (Advanced Encryption Standard).** The round key used for this operation is $\begin{bmatrix} AC & 19 & 28 & 27 \\ 77 & FA & D1 & 5C \\ 66 & DC & 29 & 00 \\ F3 & 21 & 41 & 6A \end{bmatrix}$**.** Suppose the state matrix input to this operation is $\begin{bmatrix} 47 & 40 & A3 & 4C \\ 37 & D4 & 70 & 9F \\ 94 & E4 & 3A & 42 \\ ED & A5 & A6 & BC \end{bmatrix}$, what is the resulting state matrix after the Add-Round-Key operation? (7)

b) Provide a detailed explanation of a single round in the **Data Encryption Standard (DES)** with the help of a clear diagram. (7)

OR

14 a) Provide a detailed explanation of the s-box in the **Data Encryption Standard (DES)** with the help of a clear diagram and an example. (7)

b) Outline the steps involved in **Double DES** and provide an appropriate diagram. Additionally, can you explain how the **Meet in the Middle** attack takes advantage of the vulnerabilities present in Double DES? (7)

Module III

15 a) Alice wants to send the message **M=88** securely to Bob using the RSA cryptosystem. She selects the prime numbers **p=17** and **q=11**, and chooses her private (encryption) key as **7**. Calculate the decryption key and the ciphertext. Additionally, denote C as the computed ciphertext and outline the steps required to recover the plaintext **88** from C. (7)

b) Alice and Bob wish to securely share a key K using the Diffie-Hellman key exchange protocol. What are the computaional steps they perform during this key generation? (7)

OR

16 a) Alice wishes to send the message **M=26** to Bob using the El-Gamal cryptosystem. The public parameters for this encryption are a prime number **q=29** and a primitive root of $\mathbf{Z_{29}}^*$, which is 3. Alice's private key X_A is 5, and Bob's private key X_B is 12. Calculate the encryption and decryption keys, as well as the ciphertext C for this message. (8)

b) Alice wants to securely send a message M to Bob using the RSA algorithm. Outline the computational steps involved in the encryption process carried out by Alice and the decryption process performed by Bob. (6)

Module IV

17 a) Describe the computational procedure used to generate the message schedule of 80, 64-bit words during the processing of a single 1024-bit message block by the **SHA-512** algorithm. (7)

b) Using a block diagram, explain the **DSS** method for generating digital signatures. (7)

OR

18 a) Otline the computational steps involved in the initialization of **8**, **64-**bit hash buffers and **80** round constants in the the processing of a single 1024-bit (6)

message block by the **SHA-512** algorithm.

b) With the help of a diagram, describe the working of **Hash** based **Message Authentication Code (HMAC).** (8)

Module V

19 a) With the help of a diagram explain the steps and different types of messages exchanged in a **symmetric distribution** scenario using **symmetric key encryption** and a **Key Distribution Center**. (7)

b) Explain the various approaches to intrusion detection. (7)

OR

20 a) With the help of a diagram explain the steps and different types of messages exchanged in a **symmetric distribution scenario** using **asymmetric key encryption** that ensures **confidentiality** and **authentication.** (7)

b) Explain the **Reactive Password Checking** and **Proactive Password Checking** strategies. (7)

****