Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech Degree S8 (R,S) Exam April 2025 (2019 Scheme)

Course Code: ECT434

Course Name: SECURE COMMUNICATION

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

PART A

Answer all questions, each carries 3 marks. Marks

1 What is meant by security service? Name any three security services. (3)

2 Draw the model of a symmetric cryptosystem. (3)

3 Calculate 5 mod 6, -5 mod 6 and -5 mod -6. (3)

4 What are the elements in Z_4? Find the multiplicative inverse of all the elements in Z_4? (3)

5 Differentiate between block ciphers and stream ciphers with examples. (3)

6 How is S-Box substitution performed in DES encryption? (3)

7 Define Euler's Totient Function $\phi(n)$. Using this, Find ϕ (31) and ϕ (25). (3)

8 What are the key components of a public-key encryption scheme? (3)

9 What are the different types of functions that can be used to produce an authenticator? (3)

10 List out the different applications of Cryptographic Hash Function? (3)

PART B

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

Module I

11 a) Consider the plaintext 'SECURITY'. Using Hill Cipher, encrypt it using the key $K=\begin{bmatrix}2 & 3\\ 1 & 4\end{bmatrix}$ (10)

b) Differentiate between substitution and transposition techniques. (4)

OR

12 a) Explain different active security attacks with diagram. (6)

b) Encrypt the message "RESULT PUBLISHED" using a double Transposition Cipher with the key "3 1 2 4" (8)

Module II

13 a) What is an Abelian group? Check whether the set of integers under multiplication is an abelian group. (8)

b) Find the GCD of 3456 and 876 using the Euclidean algorithm. (6)

OR

14 a) What are the steps involved in the Extended Euclidean algorithm. Using this algorithm, find the multiplicative inverse of 17 mod 26. (7)

b) Determine the GCD of $(x^4 + x^3 + x + 1)$ and $(x^3 + x^2 + x + 1)$ over GF(2). (7)

Module III

15 a) Explain the internal structure of a single round DES encryption algorithm (10)

b) How does the Shift Row Transformation in AES work, and how does it enhance security? Explain with one example. (4)

OR

16 Explain Feistel encryption and decryption with the help of a neat sketch. (14)

Module IV

17 a) With the help of a block diagram, explain public key cryptosystem that can provide both confidentiality and authentication. (7)

b) Explain different methods used for distribution of public keys. (7)

OR

18 a) Alice wants to send a secret message M=2 to Bob using RSA algorithm with p=3, q=11 and e=7. What is the ciphertext C that Alice should send? Also perform decryption. (8)

b) State Fermat's theorem. Using Fermat's theorem, find $5^{37} \bmod 7$. (6)

Module V

19 What are the different ways in which a hash code can be used to provide message authentication? Explain any 3 in detail. (14)

OR

20 a) What are the features of Message Authentication Code (MAC)? (2)

b) Explain how MAC ensures message authentication and confidentiality, differentiating between authentication tied to plaintext and authentication tied to ciphertext. (12)

***