Reg No.:_______________ Name:______________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Eighth Semester B.Tech Degree Regular Examination June 2023 (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 With examples explain the different classification of security attacks. (3)

2 What are the important criteria that should be considered by a programmer who is developing an encryption algorithm? (3)

3 Define the inverse element for any operation in a group (3)

4 Perform the following operations (3)

a. Add 17 to 27 in Z14

b. Subtract 43 from 12 in Z_{13}

5 What is Avalanche effect in cryptography? (3)

6 Explain how an Expansion Permutation is used in DES Encryption algorithm (3)

7 State and prove Euler's theorem (3)

8 Compare and Contrast between Conventional Encryption and Public Key Encryption algorithms (3)

9 What are the different attacks that can be addressed using message authentication? (3)

10 What are the different applications of Cryptographic Hash Functions? (3)

PART B

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

Module I

11 a) How is monoalphabetic substitution cipher stronger than Ceaser Cipher. Discuss the advantages and disadvantages of monoalphabetic cipher (6)

A message is encrypted using monoalphabetic substitution cipher using the following key. Decrypt the message.

Key: CFJNSXADHLORVZEKPUBGMWITQY
Cipher: KUCJGHJS VCOSB VCZ KSUXSJG

b) With a block diagram, explain the model of a symmetric cryptosystem. Discuss the broad classification of cryptosystem based on the three independent dimensions of cryptography (8)

OR

12 a) Explain in detail the different types of attacks on Encrypted messages based on the information available for Cryptanalysis (8)

b) Encrypt the text "HOW ARE YOU" using the key "GYBNQKURP", taking one word of the message at a time (6)

Module II

13 a) Consider the set S=[a,b] with addition and multiplication defined by the following tables (9)

+	a	b
a	a	b
b	b	a

×	a	b
a	a	a
b	a	b

Is S a ring? Justify your answer

b) Determine the GCD of 4655 and 12075. Check whether these numbers are relatively prime (5)

OR

14 a) Check whether a multiplicative inverse exist for 27 in Z_{100} and if so, Find the multiplicative inverse of 27 in Z_{100} (7)

b) What is an Abelian group? Find whether the set of integers is an abelian group under addition. Justify (7)

Module III

15 a) With the help of appropriate diagrams explain the Feistel Encryption and Decryption in detail (14)

OR

16 a) Describe in detail the key expansion logic used in AES Encryption (7)

b) Describe the internal structure of a single round of DES Encryption algorithm (7)

Module IV

17 a) With the help of a block diagram, explain the architecture of a public key cryptosystem that can provide both confidentiality and authentication (8)

b) In a public key cryptosystem using RSA algorithm, a person intercept the Cipher text sent to a user whose public key is e=5 and n=35. The intercepted ciphertext is 10. Find out the plaintext? (6)

OR

18 a) What is the driving principle behind Diffie-Hellman algorithm for key exchange. Elaborate on the algorithm with an example using a prime number 19 and its primitive root 3. (10)

b) Using Fermats theorem, calculate 25^8 mod7 (4)

Module V

19 a) With the help of appropriate diagrams, explain the different types of message authentication using hash function and their applications (14)

OR

20 a) List out the different mechanisms possible to generate a message authenticator. (4)

b) Explain in detail how MAC can be used for message authentication (10)

****