C **16000EC468062303** **Pages: 2**

Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech Degree S8 (S, FE) / S8 (PT) (S, FE) Examination January 2024 (2015 Scheme)

Course Code: EC468

Course Name: SECURE COMMUNICATION

Max. Marks: 100 Duration: 3 Hours

PART A

Answer any two full questions, each carries 15 marks. Marks

1 a) What is a denial-of-service attack, and how does it work? (5)

b) Differentiate between privacy, integrity and authentication in security services. (5)

c) Define five security services to prevent security attacks. (5)

2 a) What are the different types of security attacks on confidentiality & integrity? (8)

b) List out the different algebraic structures used in cryptography. Define each of them with examples. (7)

3 a) Find the result of the following operations. (4)

i. 27 mod 5 ii. -18 mod 14

b) Find whether the set of integers under addition is an Abelian group or not. Give proper justification to your answer. (5)

c) Find the GCD(2740,1760) using Euclidean algorithm. (6)

PART B

Answer any two full questions, each carries 15 marks.

4 a) What are the components of a symmetric cipher model? (5)

b) What is the basic principle behind substitution techniques in symmetric cipher? How do transposition techniques differ from substitution techniques? (5)

c) Distinguish between monoalphabetic and polyalphabetic ciphers. Give one example for each. (5)

5 a) Encrypt the plain text **CRYPTO IS TOO EASY** with key as **INFOSEC** using play fair cipher. (7)

b) What are the different types of transformations used in the Advanced Encryption Standard (AES) algorithm and how do they contribute to the overall security and effectiveness of the encryption process? (8)

6 a) What are the steps involved in DES algorithm. Illustrate the general structure of DES with a neat diagram. (10)

b) Distinguish between the terms Confusion and Diffusion in cryptography. (5)

PART C

Answer any two full questions, each carries 20 marks.

7 a) What is public key cryptography? How can we achieve confidentiality and authentication through public key cryptography? (10)

b) Perform encryption and decryption using RSA algorithm for the parameters p=3, q=11, e=7 and M=31. (10)

8 a) What is the role of a Public Key Authority (PKA) in a public key distribution scenario? Illustrate with a neat diagram. (10)

b) How statistical and rule-based anomaly detection systems work? (10)

9 a) Illustrate the architecture of Distributed Intrusion Detection System with a neat diagram. (10)

b) How does the password management system work in UNIX-based operating systems? (10)

****