Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Eighth Semester B.Tech Degree Supplementary Examination October 2022 (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) List and briefly define categories of security mechanisms. (8)

b) Differentiate between group, ring and field emphasising the properties required to be satisfied in each category. Also give example for each. (7)

2 a) Consider an automated cash deposit machine in which users provide a card or an account number to deposit cash. Give examples of confidentiality, integrity, and availability requirements associated with the system. (6)

b) Solve the equation $5x \equiv 3 (\text{mod} 11)$. (5)

c) State Lagrange's theorem. Mention its applications. (4)

3 a) Discuss Extended Euclidean algorithm. (5)

b) In GF(2^8), find the inverse of (x^5) modulo ($x^8+x^4+x^3+x+1$) using Extended Euclidean Algorithm (10)

PART B

Answer any two full questions, each carries 15 marks.

4 a) What are the design parameters of Feistel Cipher network? (3)

b) Using the key 'Guidance' encrypt the message 'This is the final exam' using Playfair cipher. (7)

c) Discuss about any two monoalphabetic ciphers with example. (5)

5 a) Explain AES-128 with necessary diagrams. (15)

6 a) Explain the encryption and decryption of Hill cipher with an example. (7)

b) Write notes on different types of cryptanalytic attacks. (4)

c) What does it mean by Confusion and Diffusion in Cryptography? (4)

PART C

Answer any two full questions, each carries 20 marks.

7 a) Explain the steps of RSA Algorithm and perform encryption and decryption using RSA Algorithm for the following P=7; q=11; e=17; M=8. (15)

b) What are the differences between symmetric key encryption and asymmetric key encryption? (5)

8 a) Write notes on public key certificates and distribution of secret keys. (8)

b) What are two common techniques used to protect a password file? (6)

c) What is the difference between rule-based anomaly detection and rule-based penetration identification? (6)

9 a) What are audit records? Discuss two types of audit records. (6)

b) What metrics are useful for profile-based intrusion detection? (6)

c) List and briefly define four techniques used to avoid guessable passwords. (8)

****