C 04000EC468052101 Pages: 2

Reg No.:________________ Name:____________________________

17/8/22

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Eighth Semester B.Tech Degree Examination June 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) Would message integrity on its own ensure that the contents of a message are not changed during transit? Does something more need to be done? (5)

b) Explain the algebraic structures used in cryptography emphasizing the properties to be satisfied in each category. (10)

2 a) Find whether set of natural numbers is an abelian group under addition. Justify your answer. (5)

b) Discuss different types of attack threatening confidentiality and integrity. (10)

3 a) Explain commonly used security mechanisms used in security systems (at least eight). (8)

b) Define linear congruence. Solve $5x \equiv 8 \pmod{6}$ (7)

PART B

Answer any two full questions, each carries 15 marks.

4 a) Encrypt “LET US MEET TODAY” with the key APPLE using playfair cipher. (Ignore the space between words) (10)

b) Explain the terms confusion and diffusion. (5)

5 a) Explain single round in DES and the DES function. (10)

b) Distinguish between a monoalphabetic and a polyalphabetic cipher. (5)

6 a) Use hill cipher to encrypt the message “CORONA” using the key $K = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$ (7)

b) Briefly describe MixColumn Transformation in AES using necessary diagrams. (8)

PART C

Answer any two full questions, each carries 20 marks.

7 a) Explain different methods used for distribution of public keys? (10)

b) Explain the architecture of Distributed Intrusion Detection with neat sketch. (10)

8 a) Given two prime numbers p=7 and q=11 and encryption key e =13. Derive the decryption key d. Let the message be x= 5. Perform encryption and decryption using RSA algorithm (10)

b) Explain the purpose of salt in password protection. Also give various strategies used for password selection. (10)

9 a) Users Alice and Bob use the Diffie-Hellman key exchange technique with common prime q=23 and a primitive root α= 7. If Alice has private key X_A= 3, Find Alice's public key. If Bob has private key X_B= 6, find Bob's public key. Also find the shared secret key (10)

b) Explain Statistical anomaly-based IDS in detail and discuss how it differs from Rule-based anomaly detection (10)

****