B 0400ECT434052301 Pages: 3

Reg No.:_______________ Name:___________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Eighth Semester B.Tech Degree Supplementary Examination October 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 What are the three key objectives of computer security. In these objectives, which one is affected by the attack - modification of messages? (3)

2 List the five ingredients of a symmetric cipher model. (3)

3 Find the GCD of 63 and 24 using Euclidean algorithm. (3)

4 Prove the following relationship. (3)

(a mod n + b mod n) mod n = (a + b) mod n

5 What is the Avalanche effect? Explain (3)

6 Differentiate stream cipher and block cipher. Give one example of each. (3)

7 State Euler's theorem. How is it related to Fermat's theorem? (3)

8 Explain simple secrete key distribution. (3)

9 Explain how a document is digitally signed using cryptographic methods. (3)

10 List any three applications of Hash functions. (3)

PART B

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

Module I

11 a) Explain different types of passive and active security attacks. (7)

b) Define security service. Explain the following security services. (7)

i) Authentication

ii) Data confidentiality

OR

12 a) Consider the plain text 'secure communication'. Encrypt it using Hill algorithm (9)

where the key, $\boldsymbol{K} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 20 & 0 & 17 \end{pmatrix}$

b) Illustrate the double transposition cipher algorithm using the following inputs. (5)

K = 4 3 1 2 5 6 1

Plain text = A secret message

Module II

13 a) Define abelian group. Check whether the set of non-zero real numbers under multiplication is an abelian group. (7)

b) Given that the numbers A and B are relatively prime. What does it mean? Prove that the number 11 has a multiplicative inverse in Z26. (7)

OR

14 a) Find The multiplicative inverse of $(x^7 + x + 1)\ mod\ x^8 + x^4 + x^3 + x + 1$. (7)

b) Let Z_n is defined as the set of nonnegative integers less than n. Find the additive and multiplicative inverse of each member in the set Z_4 if it exists. (7)

Module III

15 a) Explain the encryption and decryption blocks of Feistel cipher. (10)

b) Show that the output of first stage decryption of Feistel cipher is equal to the 32-bit swap of input to the sixteenth round of encryption process. (4)

OR

16 a) Sketch the general block diagram of DES algorithm and explain the details of a single round. (12)

b) What are the four functions in each round of AES algorithm? (2)

Module IV

17 a) Explain different methods used for distribution of public keys. (8)

b) Give the details of a public key encryption system which ensures both authentication and secrecy. (6)

OR

18 a) Illustrate RSA algorithm using the following inputs. (10)

Plain text M = 88, p = 17, q = 11 and e = 7.

Perform both encryption and decryption.

b) What is man in middle attack in simple secrete key distribution? (4)

Module V

19 a) What are the requirements of message authentication? Explain. (6)

b) Explain how authentication is ensured using message authentication code. (8)

OR

20 a) What is Hash function? Describe the different ways in which it can be used to provide message authentication. (10)

b) What are the three different groups of authentication functions. What is the authenticator in each case? (4)

****