D 1100CCT307112402 Pages: 2

Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech Degree S5 (R,S) Examination November 2025 (2019 Scheme).

Course Code: CCT307

Course Name: APPLIED CRYPTOGRAPHY

Max. Marks: 100 **Duration: 3 Hours**

PART A

(Answer all questions; each question carries 3 marks) Marks

1 Give a scenario that explains non-repudiation. 3

2 What is the difference between computationally secure and unconditionally secure cipher? 3

3 Briefly describe Avalanche effect in the context of cryptography. 3

4 What are the five modes of operation used with block ciphers? 3

5 What are the primary uses of MD5 algorithm? 3

6 What is the role of X.509 in authentication? 3

7 What is the role of a Certificate Authority (CA) in Public Key Infrastructure (PKI)? 3

8 Define biometric authentication and discuss its advantages over traditional methods. 3

9 Describe side-channel attacks and their potential impact on cryptographic systems. 3

10 What is quantum-safe cryptography, and why is it important? 3

PART B

(Answer one full question from each module, each question carries 14 marks)

Module -1

11 a) With the help of a neat block diagram, describe how asymmetric key cryptography can be used for both confidentiality and authenticity. 8

b) Describe brute-force attack on the cipher "DWWDFNDWGDZQ" assuming that the encryption algorithm is Caesar cipher 6

12 a) Explain the various techniques of steganography used for hiding data. 8

b) Write short notes on 6

a) Brute Force Attack

b) Linear Cryptanalysis

c) Differential cryptanalysis

Module -2

13 a) Demonstrate RSA encryption and decryption algorithm for the parameters 8

p = 3, q = 11, e = 7, and M = 5

b) What are the advantages of elliptic curve cryptography (ECC) over traditional cryptographic algorithms? 6

14 a) With block diagrams, explain the concept of double DES and triple DES. 8

b) Explain how diffusion and confusion are achieved in encryption algorithms. 6

Module -3

15 a) Explain the concept of Hash-based Message Authentication Code (HMAC) and its advantages over simple MACs. 8

b) List any four requirements a cryptographic Hash Function must satisfy to be considered for use. 6

16 a) Describe the role of X.509 certificates in public key infrastructure (PKI) and their significance in secure communications. 8

b) Security of HMAC relies heavily on effective key management. How it is achieved? 6

Module -4

17 a) Explain the Kerberos authentication protocol and its significance in network security. 8

b) What is biometric authentication, and how does it enhance security? 6

18 a) Explain Multi-Factor Authentication (MFA) and its role in enhancing security measures across various applications. 8

b) Discuss any three cryptographic protocols used in securing communications and their significance in trust establishment. 6

Module -5

19 a) Explain the concept of user authentication and its importance in secure online banking. 8

b) Describe the challenge-response authentication method and its advantages over traditional password-based systems. 6

20 a) Explain how blockchain technology supports digital cash applications and its implications for secure transactions. 8

b) Discuss the challenges posed by quantum computing on traditional cryptographic algorithms and potential solutions through quantum-resistant cryptography 6

***