B

**1000CST433112401**

Pages: 2

JYOTHI ENGG. COLLEGE LIBRARY THRISSUR EDUCATIONAL TRUST CHERUTHURUTHY

Reg No.:_____ Name:_____

**APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY**

B.Tech Degree S7 (R, S) Examination November 2024 (2019 Scheme)

**Course Code: CST433**

**Course Name: SECURITY IN COMPUTING**

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

**PART A**

***Answer all questions, each carries 3 marks.*** Marks

| | | | |
|---|---|---|---|
| 1 | | Explain the fundamental differences between cryptography and cryptanalysis. How do both play a role in ensuring secure communication? | (3) |
| 2 | | Compare and contrast monoalphabetic and polyalphabetic substitution ciphers. Provide examples of each. | (3) |
| 3 | | What do you mean by Feistel Cipher? Explain its Characteristics. | (3) |
| 4 | | Explain 2DES and discuss its security. | (3) |
| 5 | | Define public key cryptography. Discuss the roles of public and private keys. | (3) |
| 6 | | Illustrate Elgamal Cryptosystem. | (3) |
| 7 | | What are the primary requirements for a secure Message Authentication Code (MAC)? | (3) |
| 8 | | Differentiate between HMAC and CMAC. | (3) |
| 9 | | What are some countermeasures against malicious software threats? | (3) |
| 10 | | Define a virus and give its structure. | (3) |

**PART B**

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

**Module I**

| | | | |
|---|---|---|---|
| 11 | a) | Explain the Security Mechanisms outlined in X.800. | (7) |
| | b) | Show the encryption and Decryption of the Plaintext HELLO using Playfair Cipher with key PLAYFAIREXAMPLE. | (7) |

**OR**

| | | | |
|---|---|---|---|
| 12 | a) | List and explain the different categories of Security attacks. | (7) |
| | b) | Explain the Vigenère cipher and illustrate the encryption and decryption processes for the plaintext "ATTACKATDAWN" using the key "LEMON" | (7) |

**Module II**

| | | | |
|---|---|---|---|
| 13 | a) | Explain single round of DES algorithm with a neat diagram. | (7) |
| | b) | Explain the different modes of operation for block ciphers. | (7) |

**OR**

14 a) Describe the key generation process in DES. (5)

b) Explain the AES encryption process. (9)

**Module III**

15 a) Explain RSA Algorithm. (9)

Using the RSA algorithm, perform the following steps with the given parameters:

Prime Numbers p=17 and q=19

Public Exponent e = 5

i) Verify whether e is a valid choice.
ii) Find the Public Key and Private key.
iii) Encrypt the message m = 12.

b) Explain Man in the middle attack in Diffie Hellman key exchange. (5)

**OR**

16 a) Consider a Diffie–Hellman scheme with a common prime q=17 and a primitive root α=5. (9)

i) Show that 5 is a primitive root of 17.
ii) If User A has public key $Y_A$= 9, what is A's private key $X_A$?
iii) If User B has public key $Y_B$= 3, what is the shared secret key K, shared with A?

b) Explain the key exchange procedure using Elliptic Curves cryptography. (5)

**Module IV**

17 a) Define Hash Function and Explain the Basic uses of Hash Functions. (7)

b) Explain Cipher – Based Message Authentication Code. (7)

**OR**

18 a) Illustrate the working of SHA-512 algorithm with diagrams. (8)

b) Explain the Signing and Verification in Digital Signature Scheme (6)

**Module V**

19 a) Explain secret key distribution with confidentiality and authentication. (8)

b) Briefly explain the four phases, a virus goes through in its lifetime. (6)

**OR**

20 a) What is an audit record? Explain the role and Purpose of Audit records in Intrusion Detection. (8)

b) What are the different password selection strategies? (6)

*****