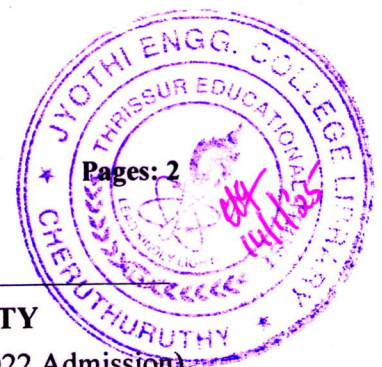


H1

1100CST393122301



Reg No.: \_\_\_\_\_

Name: \_\_\_\_\_

**APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY**

Fifth Semester B.Tech (Hons.) Degree Examination December 2024 (2022 Admission)

**Course Code: CST 393**

**Course Name: CRYPTOGRAPHIC ALGORITHMS**

Max. Marks: 100

Duration: 3 Hours

**PART A**

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

Marks

- |    |                                                                   |   |
|----|-------------------------------------------------------------------|---|
| 1  | What you mean by Integrity of data?                               | 3 |
| 2  | What is Ceaser cipher technique?                                  | 3 |
| 3  | What is differential crypt analysis?                              | 3 |
| 4  | What is the advantage of triple DES?                              | 3 |
| 5  | What are the disadvantages of RSA algorithm?                      | 3 |
| 6  | What are the advantages of Diffie Hellman key exchange algorithm? | 3 |
| 7  | How the key backup is possible in a key distribution environment? | 3 |
| 8  | Discuss about compromised keys in a key distribution system?      | 3 |
| 9  | What is the benefit of using MAC?                                 | 3 |
| 10 | What are the authentication requirements?                         | 3 |

**PART B**

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

**Module -1**

- |    |                                                                                                                                                                              |   |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| 11 | a) Explain Vigenere cipher with example.                                                                                                                                     | 7 |
|    | b) Explain about Playfair cipher. Generate cipher text for the string "instrumentsz" using the keyword "monarchy".                                                           | 7 |
| 12 | a) Explain in detail about cryptanalysis and brute-force attack                                                                                                              | 6 |
|    | b) Encrypt the text "meet me after the toga party" using transposition cipher with the key (3,2,1,4,5). Show decryption of the ciphertext to recover the original text back. | 8 |

**Module -2**

- |    |                                                      |    |
|----|------------------------------------------------------|----|
| 13 | a) Explain in detail about AES.                      | 14 |
| 14 | a) Explain the substitution technique used with DES? | 6  |
|    | b) With suitable diagram explain about RC4           | 8  |

**Module -3**

- 15 a) Explain in detail about RSA algorithm. Given  $p=7$ ,  $q=11$ ,  $e=17$ ,  $M=8$ , encrypt using RSA algorithm. 14
- 16 a) Why we need to use Elgamal cryptographic system? 7
- b) Explain in detail about Diffie Hellman key exchange algorithm. 7

**Module -4**

- 17 a) What is the roll of KDC in generating a session key? 8
- b) Discuss in detail about generating a public key. 6
- 18 a) Explain the concept of symmetric key distribution using symmetric keys 8
- b) Discuss in detail about key transferring in a symmetric key distribution environment. 6

**Module -5**

- 19 a) Explain in detail about MD5 algorithm. 14
- 20 a) Discuss in detail about X.509 authentication services. 8
- b) Explain the security provided by hash functions and MAC in detail. 6

\*\*\*