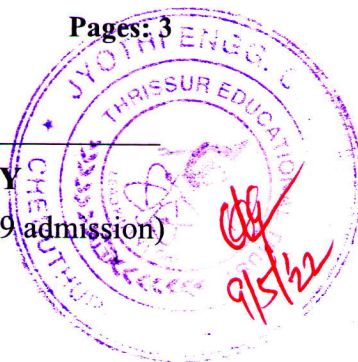


Reg No.: _____

Name: _____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Fifth Semester B.Tech (Hons) Degree Examination December 2021 (2019 admission)

**Course Code: CST393****Course Name: CRYPTOGRAPHIC ALGORITHMS**

Max. Marks: 100

Duration: 3 Hours

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

Marks

- | | | |
|----|---|---|
| 1 | Differentiate between computationally secure cipher and unconditionally secure cipher. | 3 |
| 2 | "Passive attacks are easier to prevent but difficult to detect. On the other hand, active attacks are difficult to prevent but easy to detect". Justify this assertion. | 3 |
| 3 | Illustrate the key expansion procedure of IDEA algorithm. | 3 |
| 4 | Identify the drawbacks of double DES and why do we go for triple DES. | 3 |
| 5 | Explain how knapsack system is cracked. | 3 |
| 6 | Given $p=7$, $q=11$, $e=17$, $M=8$, perform encryption using RSA algorithm. | 3 |
| 7 | List four general categories of schemes for the distribution of public keys. | 3 |
| 8 | Demonstrate how simple secret key distribution is prone to man in the middle attack. | 3 |
| 9 | If the length of the message is 6143 bits, how many padding bits are needed in SHA? | 3 |
| 10 | List out the required properties of a good Hash function. | 3 |

PART B*(Answer one full question from each module; each question carries 14 marks)***Module -1**

- | | | |
|----|--|---|
| 11 | a) Eve has intercepted the ciphertext "UVACLYFZLJBYL". Show how she can use an exhaustive key search to break this Caesar cipher. | 6 |
| | b) What are the different types of cryptanalytic attacks? | 8 |
| 12 | a) The encryption key in a transposition cipher is (3,1,4,5,2). Perform encryption and decryption for the message "meet me after the toga party". Add a bogus character at the end to make the last group the same size as the others. | 6 |
| | b) Explain OSI Security architecture model with suitable diagrams. | 8 |

Module -2

- 13 a) Explain the Key expansion in AES algorithm with a neat sketch. 10
 b) Differentiate between confusion and diffusion. 4
- 14 a) Describe single round of DES algorithm with necessary diagrams. 8
 b) Discuss the stream cipher RC4 in detail. 6

Module -3

- 15 a) Explain RSA algorithm. Prove that the RSA decryption indeed recovers the original plaintext. 8
 b) Consider a Diffie-Hellmann scheme with a prime $q=23$ and a primitive root $\alpha=7$. 6
 Users private key are $X_A=3$ and $X_B=5$.
 i. Find the public keys.
 ii. Find the value of symmetric key.
 iii. Write the algorithm
- 16 a) Discuss the encryption/decryption procedures using Elliptic Curve cryptography. 8
 b) With the following parameters, implement El-Gamal Encryption/ Decryption scheme. 6
- Prime Number, $p=11$
 - Primitive root of $p=g=2$
 - User A's private key, $x=5$
 - Message to be sent by User B to User A, $M=3$
 - Random number chosen by User B for encryption, $k=7$

Determine

- i. Public key y of A
 ii. Ciphertext created by the sender B
 iii. Show how the plaintext is extracted from ciphertext by user A

Module -4

- 17 a) Explain secret key distribution with confidentiality and authentication. 8
 b) What are the key components of a PKI? Briefly describe each component. 6
- 18 a) Define a session key and show how a KDC can create a session key between Alice and Bob. 8

b) Describe the following

i. Backup Keys

ii. Compromised Keys

6

Module -5

19 a) Illustrate the working of SHA-512 algorithm with necessary diagrams. 10

b) Distinguish between HMAC and CMAC. 4

20 a) Discuss message authentication with MAC. 8

b) Describe birthday attack? Explain how it affects the security of hash functions. 6
