B 1000CST433122205 Pages: 2

Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Seventh Semester B.Tech Degree (S, FE) Examination May 2023 (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 Use Playfair Cipher with key COMPUTER to encrypt the message “CRYPTOGRAPHY”. (3)

2 Differentiate between passive attack and active attack. (3)

3 What is avalanche effect? (3)

4 What is the purpose of S Box in DES? (3)

5 In RSA, given p=11, q=7, public key(e)=11, find n, ϕ(n) and private key(d). (3)

6 Illustrate man in the middle attack on Diffie Hellman key exchange algorithm. (3)

7 Give the requirements of MAC function. (3)

8 What do you mean by one way property in hash function? (3)

9 List any two ways in which secret keys can be distributed to two communicating parties. (3)

10 List three different classes of intruders. (3)

PART B

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

Module I

11 a) Explain transposition technique. Convert plain text to Cipher text using Rail Fence technique “COMPUTER ENGINEERING”. (7)

b) Explain about OSI Security architecture model with neat diagram. (7)

OR

12 a) Convert “MEET ME” using Hill cipher with the key matrix .Explain how decryption can be performed. (8)

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

b) What are the two ways of attacking conventional encryption scheme? Explain (6)

Module II

13 a) Summarize the primitive operations of RC4 algorithm. (9)

b) Explain construction of S Box in AES (5)

OR

14 a) Illustrate AES encryption in detail. (10)

b) How is round key generated in DES? (4)

Module III

15 a) Explain RSA cryptosystem. In an RSA cryptosystem a participant A uses two prime numbers p=13 and q=17 to generate public key and private key. The public key of A is 35. Find the private key of A. (7)

b) Explain in detail about elliptic curve cryptography. (7)

OR

16 a) Consider a Diffie–Hellman scheme with a common prime q=11 and a primitive root α=2. (8)

i) Show that 2 is a primitive root of 11.
ii) If User A has public key YA= 9, what is A's private key XA?
iii) If User B has public key YB= 3, what is the shared secret key K, shared with A?

b) Illustrate ElGamal cryptosystem. (6)

Module IV

17 a) Describe about Hash Function. How its algorithm is designed? Explain its features & properties? (10)

b) How signing and verification is done in Digital Signature algorithm? (4)

OR

18 a) Explain Cipher – Based Message Authentication Code. (8)

b) Describe the digital signature schemes DSS. (6)

Module V

19 a) Explain secret key distribution with confidentiality and authentication. (7)

b) Explain about viruses in detail. (7)

OR

20 a) Explain about Malicious Software. (9)

b) Explain decentralized key control. (5)

****