B

1000CST433122204

Pages: 2

Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Seventh Semester B.Tech Degree (S, FE) Examination May 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 terms: Cryptography, Cryptanalysis	(3)
2	Alice wishes to send the message "COME EARLY" to Bob, using Playfair cipher. The key to be used is "DOLLARS". Show the process of encryption.	(3)
3	Compare stream cipher and Block cipher with example.	(3)
4	What is the purpose of S Box in DES?	(3)
5	Compare symmetric and asymmetric cryptosystems.	(3)
6	Consider an ElGamal scheme with a common prime q = 71 and a primitive root α = 7. If B has a public key YB = 3 and A chose the random number k = 2, what is the ciphertext of the message M = 30?	(3)
7	Differentiate Message Authentication Code and Hash function.	(3)
8	What are the properties of Digital Signature?	(3)
9	List any two ways in which secret keys can be distributed to two communicating parties.	(3)
10	Mention the phases of operation of a virus.	(3)

PART B

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

Module I

11	a)	What is meant by transposition cipher? Explain rail fence cipher and row transposition ciphers with example.	(7)
	b)	Explain various types of security attacks.	(7)

OR

12	a)	Define Security attacks, security mechanism, security services	(9)
	b)	Differentiate between monoalphabetic ciphers and polyalphabetic ciphers and give one example for each.	(5)

Module II

13 a) Explain the design of DES algorithm. (9)

b) Describe about Counter Mode of operation. (5)

OR

14 a) Explain AES Algorithm in details. (10)

b) How is meet in the middle attack done in 2-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. (8)

b) What are the roles of the public and private key in Public Key Cryptosystem. Explain how we ensure authentication and confidentiality in Public Key Cryptosystem (6)

OR

16 a) Explain Diffie-Hellman Key Exchange algorithm with its merits and demerits. (9)

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

Module IV

17 a) Describe the steps in finding the message digest using SHA-512 algorithm. (10)

b) Describe the digital signature standard DSS. (4)

OR

18 a) Describe about HMAC. (8)

b) Explain three different Arbitrated Digital Signature Techniques. (6)

Module V

19 a) Explain different types of Simple DDoS attack and its countermeasures. (6)

b) Differentiate between statistical anomaly detection and rule-based intrusion detection. (8)

OR

20 a) Explain the types of Intrusion Detection Systems. (8)

b) Explain four techniques used to avoid guessable passwords. (6)

****