

B

1000CST433122201

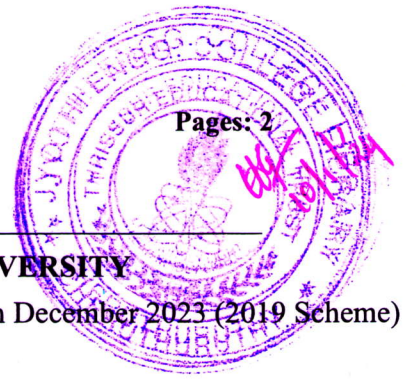
Pages: 2

Reg No.: _____

Name: _____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Seventh Semester B.Tech Degree Regular and Supplementary Examination December 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 | What is the difference between passive and active security attacks? | (3) |
| 2 | Distinguish between Security Mechanisms and Security Services? | (3) |
| 3 | Compare block and stream ciphers with example. | (3) |
| 4 | Define Avalanche effect in DES? | (3) |
| 5 | List the three applications of Public-Key Cryptosystems. | (3) |
| 6 | What are the main properties of Elliptic Curves that make them useful for Cryptographic Applications. | (3) |
| 7 | List the requirements of Hash functions. | (3) |
| 8 | State the need for Digital Signatures. | (3) |
| 9 | List and briefly define three classes of Intruders | (3) |
| 10 | In general terms, how does a virus propagate? | (3) |

PART B

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

Module I

- 11 a) Differentiate between substitution and transposition ciphers with examples for each. (7)
- b) Use the Play-fair cipher to decipher the message "MANAGE". The secret key is the word "BRAZIL". (The characters 'J and K' should occupy same slot). (7)

OR

- 12 a) Use Hill cipher to encipher the message "secure world" with the following key: $\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$. [Use filler letter as "x"] (7)
- b) Encrypt the message "this is an exercise" using each of the following ciphers given below. Ignore the space between words. Decrypt the message to get the original plaintext. (7)

- i. Additive(Shift) cipher with key = 20
- ii. Affine cipher with key = (15, 20)

Module II

- 13 a) Explain with figure the operations in a single round of DES algorithm (10)
- b) Illustrate the working of Triple DES algorithm. (4)

OR

- 14 a) Briefly describe sub-key generation in AES Cipher? (10)
- b) Compare Electronic Codebook (ECB) and Cipher Block Chaining (CBC) modes of block ciphers (4)

Module III

- 15 a) Users A and B use the Diffie-Hellman key exchange technique with a common prime $q=71$ and a primitive root $\alpha=7$ (7)
 - a. If user A has private key $X_A=5$ what is A's public key ?
 - b. If user B has private key $X_B=12$ what is B's public key ?
 - c. What is the shared secret key?
- b) Perform encryption using RSA algorithm for message $M=8$, given prime numbers $p=7$, $q=11$ and public key $e=17$. (7)

OR

- 16 a) Explain the El-Gamal cryptosystem with an example (7)
- b) Illustrate the steps in key exchange using Elliptic Curve Cryptography (ECC)? (7)

Module IV

- 17 a) With diagrams, briefly describe the working of SHA-512 algorithm. (10)
- b) Explain Cipher based Message Authentication code (CMAC) (4)

OR

- 18 a) Explain El-Gamal Digital Signature Scheme with example. (7)
- b) What are the properties a digital signature should have? Explain the two categories of digital signatures. (7)

Module V

- 19 a) Describe the different intrusion detection techniques. (7)
- b) What is Distributed denial of service (DDoS) attack? How can it be prevented? (7)

OR

- 20 a) What are the different password selection strategies? (7)
- b) Briefly explain the four phases, a virus goes through in its lifetime. (7)
