6E7103

Total No. of Questions : 22 Total No. of Pages : 04

Roll No. : .....

6E7103

B.Tech. VI-Sem. (Main/Back) Exam., May-2025

COMPUTER SCIENCE AND ENGINEERING (ARTIFICIAL INTELLIGENCE & DATA SCIENCE)

6CAI4-03/Information Security Systems

CS, IT, AID, CAI, CIT, CCS, CDS

Time : 3 Hours **Maximum Marks : 70**

Instructions to Candidates :

Attempt all ten questions from Part-A, five questions out of seven questions from Part-B and three questions out of five questions from Part-C.

Schematic diagrams must be shown wherever necessary. Any data you feel missing suitably be assumed and stated clearly. Units of quantities used / calculated must be stated clearly.

Use of following supporting material is permitted during examination. (Mentioned in Form No. 205)

1. ..... 2. .....

PART-A [10x2=20]

(Answer should be given up to 25 words only)

All questions are compulsory

Q.1. What is difference between Cryptography and Cryptanalysis?

Q.2. What is difference between stream and block ciphers?

Q.3. What are Confusion and Diffusion in Cryptography?

Q.4. What are strength of DES algorithm?

Q.5. What is difference between public key and private key cryptosystems?

Q.6. Write any two applications of public key cryptography.

Q.7. What is cryptographic hash function? Write its any two properties.

Q.8. What are the requirements of Message Authentication Codes?

Q.9. Write any four general means of authenticating a user's identity.

Q.10. What is HTTPS?

PART-B [5x4=20]

(Analytical/Problem solving questions)

Attempt any five questions

Q.1. Encrypt the message "Code" using the Hill cipher with the key $\begin{bmatrix} 3 & 2 \\ 8 & 5 \end{bmatrix}$ and also decrypt the ciphertext to original plaintext.

Q.2 Explain AES key expansion algorithm with suitable diagram.

Q.3. Perform encryption and decryption using the elgamal algorithm for the following:

$q = 19; \alpha = 13, X_A = 5; M = 15; k = 6$

Q.4. Explain Cipher-Based Message Authentication Code (CMAC) with suitable diagram.

Q 5. Explain SSL Record Protocol with suitable diagram.

Q.6. Explain the Electronic Code Book (ECB) block cipher mode of operation.

Q.7. Explain the application of cryptographic hash function for digital signature.

PART-C [3x10=30]

(Descriptive/Analytical/Problem Solving/Design questions)

Attempt any three questions

Q.1. What are security attacks? Explain different types of security attacks.

Q.2. Explain the internal structure of single round of DES algorithm.

Q.3. Explain the RSA algorithm and using this algorithm perform the encryption and decryption for the following :

$p = 5; q = 31; e = 13; M = 5$

Q.4. Explain the digital signature algorithm with the diagrams showing functions of signing and verifying.

Q. 5. Explain the Public-key certificates technique for distribution of public keys.

----- × -----