6E7103

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

Roll No. : .....

6E7103

B.Tech. VI-Sem. (Main/Back) Exam. - 2024

COMPUTER SC. AND ENGG. (ARTIFICIAL INTELLIGENCE)

6CAI4-03 Information Security Systems

CS,IT, AID,CAI

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 may 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. Differentiate between active and passive attacks.

Q.2. Differentiate between stream and block ciphers.

Q.3. What is avalanche effect ?

Q.4. Write advantages of multiple encryption and triple DES.

Q.5. Differentiate between private key and public key cryptography.

Q.6. Write disadvantages of public key cryptography.

Q.7. What is cryptographic hash function ?

Q.8. What is message authentication code ?

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

Q.10. What is HTTPS ?

PART-B

[5x4=20]

(Analytical/Problem Solving questions)

Attempt any five questions

Q.1. Construct a Play fair matrix with the key "occurrence" and encrypt the message "Jaipur".

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

Q.3. Explain the design principles of block cipher.

Q.4. Perform encryption and decryption using the EIG amal algorithm, for the following :

$q = 71;\ \alpha = 7;\ X_A = 3;\ M = 30;\ k = 2$

Q.5. Explain the security requirements for cryptographic hash functions.

Q.6. Explain Cipher-based Message Authentication Code (CMAC).

Q.7. Explain the public-key certificate technique for the distribution of public keys.

PART-C **[3x10=30]**

(Descriptive/Analytical/Problem Solving Design/Questions)

Attempt any three questions

Q.1. Explain the Data Encryption Standard (DES) algorithm with suitable diagrams.

Q.2. Explain the Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes of block cipher operations.

Q.3. Explain the SHA-512 algorithm using suitable diagrams.

Q.4. Explain the digital signature algorithm.

Q.5. Explain the SSL architecture and protocols with suitable diagrams.

------X------