Akhilesh

6E7103

Roll No. 20EMBIT001 [Total No. of Pages : 2

6E7103

B.Tech. VI sem. (Main) Examination, July - 2023
Computer Science and Engg. (Artificial Intelligence)
6CIA4-03 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 suitably be assumed and state clearly. Units of quantities used/calculated must be stated clearly. Use of following supporting material is permitted during examination. (Mentioned in form No.205).

PART - A

(Answer should be given up to 25 words only)

All questions are compulsory. (10×2=20)

1. What are security attacks? Differentiate between active and passive attacks.
2. Write any two difference between Stream and block ciphers.
3. What is avalanche effect?
4. Write any two strengths of DES algorithm.
5. What is public key cryptography?
6. Write any two applications of public key. Cryptography.
7. What is cryptographic hash function? Write its any two properties.
8. What is message authentication code?
9. Write any four general means of authenticating a user's identity.
10. What is HTTPS?

[Contd....

PART - B

(Analytical/Problem solving questions)

Attempt any five questions: **(5×4=20)**

1. Encrypt the message "Code" using the Hill cipher with the key $\begin{bmatrix} 3 & 2 \\ 8 & 5 \end{bmatrix}$ and decrypt the Cipher text to original plaintext.
2. Explain design principles of block cipher.
3. Perform encryption and decryption using RSA algorithm for the following.

   $p = 3, q = 11, e = 7, M = 5$
4. Explain cipher-based message authentication code with suitable diagrams.
5. Explain Elgamal digital signature algorithm.
6. Explain the distribution of public keys. Using public - key certificate scheme.
7. Explain SSL record protocol with suitable diagram.

PART - C

(Descriptive/Analytical/Problem solving/Design questions))

Attempt any three questions. **(3×10=30)**

1. Explain the general structure of AES algorithm. With suitable diagrams.
2. Explain block cipher modes of operations with suitable diagrams.
3. Perform encryption and decryption using Elgamal. Algorithm, for the following

   $q = 71, \alpha = 7, X_A = 3, M = 30, k = 2$
4. Explain SHA-512 algorithm with suitable diagrams.
5. Explain kerberos version 4 protocol with suitable diagram.