[Total No. of Questions - 9] [Total No. of Printed Pages - 2]

Dec.-23-0561

CS-703 (Information Security)

B.Tech. 7th (CBCS)

Time : 3 Hours **Max. Marks : 60**

The candidates shall limit their answers precisely within the answer-book (40 pages) issued to them and no supplementary/continuation sheet will be issued.

Note : Attempt five questions in all, selecting one question each from section A, B, C and D. Question no. 9 is compulsory.

SECTION - A

1. Explain the following three security goals: confidentiality, integrity, and availability. Also discuss the possible attacks on each of these three security goals. (10)

2. Briefly define the monoalphabetic cipher. What is the difference between a monoalphabetic cipher and a polyalphabetic cipher? (10)

SECTION - B

3. (a) Use Vigenere Cipher with key HEALTH to encrypt the message "Life is full of surprises". (5)

   (b) Discuss any four Substitution Technique and list their merits and demerits. (5)

4. Describe the Affine Cipher and explain how it works. Discuss at least two cryptanalysis techniques that can be used to break the Affine Cipher and explain how they work. (10)

SECTION - C

5. What is a digital signature? What are different types of attacks possible on digital signature? Explain. (10)

6. Perform the encryption of message 111 using RSA algorithm with p=3, q=11, and e=7. Also show decryption process to get back the original message. (10)

SECTION - D

7. Give the structure of AES. Explain how Encryption/Decryption is done in AES. (10)

8. Describe the key provisions of the Indian IT Act, including its objectives, scope, and penalties for offenses related to computer systems, data, and digital signatures. (10)

SECTION - E (Compulsory)

9. Answer the following questions in brief:

   (a) What is meant by cryptography?

   (b) List few examples for transposition cipher.

   (c) State and describe Fermat's theorem.

   (d) Applications of Fermat Theorem.

   (e) What is a block cipher?

   (f) List the properties of Euler's theorem.

   (g) What is public key encryption system?

   (h) What are the disadvantages of double DES?

   (i) Explain the concept of patent infringement.

   (j) Explain the concept of Personally Identifiable Information (PII). (10×2=20)