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

MAY-24-0561

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. Q. No.9 is compulsory.

SECTION-A

1. (a) Distinguish between cryptography and steganography.

   (b) Define Euler's theorem and list out its applications. (5+5=10)

2. (a) How is GCD calculated with Euclid's algorithm? Calculate the GCD of (270, 192).

   (b) What is Eulers Totient function? Find it for 37 and 21. (5+5=10)

SECTION-B

3. Write short note on the following:

   (a) Substitution cipher

   (b) Transposition cipher (5+5=10)

4. What is a Feistel Cipher? Explain the structure with neat sketch. Also explain how does it achieve confusion and diffusion? (10)

SECTION-C

5. What is the Digital Signature Standard (DSS)? Explain its purpose and the type of security it provides. (10)

6. Discuss the security of the Merkle-Hellman knapsack. What are some of the weaknesses of the algorithm and how can they be exploited? (10)

SECTION-D

7. Explain the Data Encryption Standard (DES). How it works? Discuss its strengths and weaknesses. (10)

8. Compare and contrast patent law and copyright law in the context of information security. Discuss their similarities, differences, and relevance in protecting intellectual property in the digital age. (10)

SECTION-E (Compulsory)

9. Answer the following questions in brief:

   (a) Use Caesar cipher with key =15 to encrypt the message "Hello".

   (b) Solve the congruence $x^5 \equiv 11 \bmod 17$.

   (c) What are transposition ciphers?

   (d) Find the value of $\phi(100)$ and $\phi(80)$

   (e) Distinguish between diffusion and confusion.

   (f) State Euler's Theorems.

   (g) What are the weaknesses of DES?

   (h) What are the attacks that are possible on RSA?

   (i) What is the Indian IT Act?

   (j) What is Digital Rights Management (DRM)? (10×2=20)