Code No: G- 5261/N/BL/AICTE

FACULTY OF ENGINEERING

B.E. (CSE) VI Semester (AICTE) (Regular & Backlog) (New) Examination, July/August 2025

Subject: Cryptography and Network Security

Time: 3 Hours **Max. Marks: 70**

Note: (i) First question is compulsory and answer any four questions from the remaining six questions. Each question carries 14 Marks.
(ii) Answer to each question must be written at one place only and in the same order as they occur in the question paper.
(iii) Missing data, if any, may be suitably assumed.

1. a) Define the terms cryptography and steganography.
   b) Differentiate symmetric and asymmetric encryption.
   c) What is Avalanche effect in DES?
   d) Find the value of 7^8 mod 15 using Euler's theorem.
   e) Compare public key and private key.
   f) What are the criterions of cryptography hash function?
   g) Identify the benefits of IP Security.

2. a) Describe the relationship between security services and security mechanisms. Explain how security mechanism is used to implement security services.
   b) Distinguish between Passive and Active security attacks. Name some passive and active attacks.

3. a) Describe the following (i) Message Integrity (ii) Denial of Service (iii) Availability (iv) Authentication
   b) Explain General structure of AES algorithm.

4. a) State the Chinese Remainder Theorem and find X for the given Set of Congruent Equation $X \equiv 2 \bmod 3$, $X \equiv 3 \bmod 5$ & $X \equiv 2 \bmod 7$.
   b) Briefly Explain Elliptic curve cryptosystem.

5. a) Define RSA digital signature scheme and compare it to the RSA cryptosystem.
   b) Briefly Explain SHA-512 cryptographic hash functions.

6. a) What is PGP? Explain how authentication and Confidentiality is maintained in PGP?
   b) In S/MIME, Explain how Bob and Alice exchange the secret key for encrypting messages.

7. a) Give a brief notes X.509 authentication services.
   b) List ISAKMP payload types and the purpose of each type.

****