Code No: E-5901/N/AICTE

FACULTY OF ENGINEERING

B.E. (CSE) VI– Semester (AICTE) (Main) (New) Examinations, September/October 2023

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 questions 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) What do you mean by cryptographic Attacks?
   (b) Define modern Symmetric key ciphers.
   (c) Explain Asymmetric key cryptography.
   (d) Define Fermat's little theorem and explain its application.
   (e) List some features of the Whirlpool cryptographic hash function. What kind of compression function is used in Whirlpool?
   (f) Distinguish between two modes of IPSec.
   (g) Define S/MIME.

2. (a) Explain Network Goals and Network Services.
   (b) Which technique (cryptography or steganography) is used in each of the following cases for confidentiality?
      (i) student writes the answers to a test on a small piece of paper, rolls up the paper, and inserts it in a ball-point pen, and passes the pen to another student.
      (ii) To send a message, a spy replaces each character in the message with a symbol that was agreed upon in advance as the character's replacement.

3. (a) Explain Data Encryption Standard with Block Diagram.
   (b) Explain the difference between symmetric and asymmetric cryptography system.

4. (a) Write an algorithm in pseudocode for the Chinese remainder theorem.
   (b) Define Data integrity and why it is required?

5. (a) Define the elliptic curve digital signature scheme and compare it to the elliptic curve cryptosystem.
   (b) Compare and contrast attacks on digital signatures with attacks on cryptosystems.

6. (a) Explain in detail about PGP PROTOCOL in detail.
   (b) When a session is resumed with a new connection, SSL does not require the full handshaking process. Show the messages that need to be exchanged in a partial handshaking.

7. (a) Define the RSA digital signature scheme and compare it to the RSA cryptosystem.
   (b) Define ISAKMP and List ISAKMP payload types and the purpose of each type.

****