CSE / AIML

(T) Roll No. .....

PAPER ID—11450

B. Tech, EXAMINATION, 2026

(Sixth Semester)

COMPUTER SCIENCE AND ENGINEERING

Professional Elective Course-III

Network Security and Cryptography

Time : 3 *Hours* *Maximum Marks* : 70

Before answering the question-paper candidates should ensure that they have been supplied to correct and complete question-paper. No complaint, in this regard, will be entertained after the examination.

Note : Attempt *Five* questions in all, selecting *one* question from each Unit. Q. No. **1** is compulsory. All questions carry equal marks.

used authentication
ecure network
in the architecture
e of the Kerberos
7

) allows users to
ns using a single
ss. Explain the
and discuss its
ty challenges. 7

540

1. (a) If a message 'HELLO' becomes 'KHOOR' after encryption, identify the type of cipher technique used.

(b) Suppose a message is encrypted to protect confidential information during transmission. What is the main purpose of encryption here ?

(c) A secure messaging system requires an encryption method that uses 128-bit, 192-bit, or 256-bit keys. Identify the algorithm used.

(d) In RSA, if a message is encrypted using a public key, which key is required to decrypt it ?

(e) Write any *two* differences between SSL and TLS.

(f) What is the purpose of Secure Hyper Text Transfer Protocol (SHTTP) ?

(g) Give any *two* examples of biometric authentication techniques. 7×2=14

Unit I

2. (a) Classical encryption methods are often used to demonstrate the basic working of cryptography. Describe the substitution technique and explain, how it differs from a transposition technique with suitable examples. 7

(b) Many secure systems today rely on the use of two different keys for encryption and decryption. Explain the concept of asymmetric key cryptography and describe, how it improves security compared to symmetric methods. 7

3. (a) Consider a scenario where an organization needs to protect sensitive data during storage and transmission. Explain the role of cryptography in maintaining confidentiality and data security. 7

(b) Plain text and cipher text are fundamental concepts in cryptography. Explain these terms and describe how information is transformed during secure communication. 7

Unit II

4. (a) Using the RSA algorithm, consider two prime numbers $p = 3$ and $q = 11$. Calculate n, $\phi(n)$ and determine the public and private keys if $e = 3$. Encrypt the message M = 4. 7

(b) Cryptographic algorithms can operate in different modes of operation to enhance security and efficiency. Explain the concept of block cipher modes and discuss why they are important in symmetric encryption systems. 7

5. (a) In modern security systems, symmetric and asymmetric cryptography are often used together. Explain, how these two cryptographic approaches complement each other in practical communication systems. 7

(b) Advanced Encryption Standard (AES) is currently one of the most widely used encryption algorithms. Explain the features of AES and discuss, why it is considered more secure and efficient than earlier symmetric algorithms ? 7

Unit III

6. (a) Internet security protocols are essential for protecting communication over public networks. Explain the basic concepts of Internet security protocols and discuss their role in ensuring secure data transmission. 7

(b) Secure Hyper Text Transfer Protocol (SHTTP) was developed to enhance the security of HTTP communication. Explain the concept and functioning of SHTTP and discuss its role in secure web communication. 7

7. (a) Electronic Money (e-Money) is widely used in modern digital payment systems. Explain the concept of electronic money and discuss the security requirements associated with digital payments. 7

(b) Secure communication protocols play a crucial role in e-Commerce and online services. Discuss the applications and importance of Internet security protocols in modern digital networks. 7

Unit IV

8. (a) Authentication tokens are widely used in modern security systems for verifying user identity. Explain the concept of authentication tokens and discuss their role in improving security in authentication processes. 7

(b) The Key Distribution Center (KDC) plays an important role in the Kerberos authentication process. Explain the functions of KDC and describe how it helps in establishing secure communication between users and services. 7