Cryptography and Network Security (TIT-704)
Assignment-01 (Unit-I)

Last Date of Submission: September 30, 2024

1) Define and categorize the different types of security attacks (e.g., passive vs. active attacks). Provide real-world examples for each category.

2) Explain the key security services that are essential for secure communication. Discuss how each service contributes to overall security.

3) What are security mechanisms? Describe at least three mechanisms and their roles in protecting against security attacks.

4) Discuss the importance of cryptography in modern communication. What are the main objectives of cryptographic techniques?

5) Compare symmetric and asymmetric cryptography. Discuss their key differences, advantages, and disadvantages.

6) Describe the conventional encryption model. How does it ensure confidentiality, integrity, and authenticity of data?

7) Differentiate between substitution ciphers and transposition ciphers. Provide examples and discuss their strengths and weaknesses.

8) What is cryptanalysis? Discuss the various techniques used in cryptanalysis to analyze and break conventional encryption schemes.

9) Explain steganography. How does it differ from traditional cryptography, and what are some common methods of steganography?

10) Define stream ciphers and block ciphers. Discuss the main differences between them, including their applications and security implications.

11) Choose a specific block cipher (e.g., AES) and explain its structure, operation, and how it achieves security.

12) Discuss the implications of using weak ciphers in encryption. What are the potential security risks associated with such practices?

13) A substitution cipher replaces each letter with another letter. If the plaintext is "HELLO", and the substitution mapping is: H->K, E->Q, L->M, O->R, what is the ciphertext?

14) Using a transposition cipher with a key of 3, encrypt the message "MEET ME AT NOON". Show the steps involved in the encryption process.

15) If a block cipher encrypts data in blocks of 128 bits, how many 128-bit blocks are needed to encrypt a file of 1 MB (1 megabyte)?

16) Suppose a stream cipher produces a keystream of 8 bits: 10110011. If the plaintext is 11001100, what is the resulting ciphertext using bitwise XOR operation?

17) In a cryptanalysis attack, if an attacker has a 70% success rate in breaking a specific encryption method, what is the probability that the attacker will fail to break the encryption in three consecutive attempts?