UNIT 1: INTRODUCTION

1. Briefly explain any two active security attacks.
2. Discuss the following terms in brief: brute force attack & cryptography.
3. Explain play - fair cipher substitution technique in detail. Find out cipher text for the following given key and plaintext.

   Key = ENGINEERING

   Plaintext=COMPUTER
4. Write differences between substitution techniques and transposition techniques.
5. Discuss the following terms in brief. Authentication & data integrity.
6. What is symmetric key cryptography? What are the challenges of symmetric key cryptography? List out various symmetric key algorithms and explain Caesar cipher in detail.
7. Explain one-time Pad in detail. What are the practical issues of this algorithm?
8. Write a short note on "Hill Cipher".
9. Given key K = $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ and plaintext ="ney". Find out the ciphertext applying Hill Cipher. Is Hill cipher strong against ciphertext only attack or known plaintext attack? Justify the answer.
10. How cryptanalyst can exploit the regularities of the language? How digrams can solve this problem? Use the key "hidden" and encrypt the message "Message" using playfair cipher.
11. Explain the rail fence cipher. Why a pure transposition cipher is easily recognized?
12. Write a short note on: Cipher text only attack.

****