Sarvajanik College of Engineering and Technology

Department of Information Technology

Cryptography and Network Security (3161606)

Practical List

Sr. No.	Practical Statements
1	Implement Ceasar and Hill cipher. Both are substitution cipher. Analyze the strength of the cipher in terms of brute force attack and cryptanalysis attack. Suggest one way to improve and strengthen the cipher and analyze with respect to cryptanalysis attack. Ceasar cipher - Your plaintext is Hello, Welcome. The key used is 3. How Ceaser cipher will work? Test case : A B C D E F Hill Cipher - $\text{Key K} = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ Plaintext = pay Ciphertext = RRL
2	Implement rail Fence and transposition cipher. Both are permutation cipher. Analyze the strength of the cipher in terms of cryptanalysis. Rail fence. Test case : Meetme Ciphertext : MEMETE Transposition Key : 4312567 Plaintext: attackpostponeduntiltwoam Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
3	Implement Playfair Cipher. The plaintext is paired in two characters. Discuss the advantage of polyalphabetic cipher over monoalphabetic cipher.

	Key = MONARCHY Plaintext = ar mu hs ea Ciphertext = RM CM BP IM
4	Write a program to implement Vigenere Cipher.
5	Write a program to implement Vernam Cipher.
6	Implement Euclid algorithm to find GCD. GCD(16,12) = 4 GCD(12,4) = 0 Then 4 is the GCD(16,12)
7	Implement Euler's totient function $\phi(n)$. It is defined as the number of positive integers less than n and relatively prime to n. Find $\phi(35)$ and $\phi(37)$. Observe the value and analyze the behavior of totient function.
8	Implement extended Euclidean Algorithm for finding inverse.
9	Implement RSA algorithm. Take two prime numbers p, q n=pxq Initially take encryption key such that it is relatively prime with ϕ(n). Find out decryption key. Take plaintext message M, Ciphertext C=Me mod n. To get plaintect from ciphertext M=Cd mod n. Test case : Two prime numbers 17,11 Encryption key = 7 Decryption key = 23 M=88 C=11
10	Implement encryption and decryption using Simplified-DES scheme.
11	Implement encryption and decryption using AES scheme.
12	Implement Diffie-Hellman Key Exchange algorithm.
13	Write a program to implement two Digital Signature Algorithms: DSA.
14	Write a program to implement two Digital Signature Algorithms: Elgamal.