SVKM's NMIMS
MPSTME
Electronics and Telecommunication Engineering Department
Subject: Data Encryption and Network Security **Programme: B.Tech/BTI**
Sem: VIII/X **ACAY: 2020-21**

EXPERIMENT NO. 2

Aim:	To implement Cryptanalysis on traditional cipher
Software	Python
Theory	Cryptography is the science and art of creating secret codes, whereas cryptanalysis is the science and art of breaking those codes. We need to learn cryptanalysis techniques to understand the vulnerability of our cryptosystem which enables us to strengthen it. The common cryptanalysis attacks are: *ciphertext-only, known-plaintext, chosen-plaintext, chosen-ciphertext.* In ciphertext-only attack, the attacker has access to only some cipher text. The attacker tries to find the corresponding key and plain text. The assumption is that the attacker knows the algorithm and can intercept the cipher text. The various methods used for ciphertext-only attack are: B*rute-Force Attack, Statistical Attack and Pattern Attack.* In Brute-Force Attack or exhaustive-key-search method, the attacker tries to use all the possible keys. We assume that the algorithm and the key domain (the list of all possible keys) are known to the attacker. Using the intercepted cipher, the attacker decrypts the cipher text with every possible key until the plain text makes sense. To prevent this attack, the number of possible keys must be very large.
Algorithm	**Caesar Cipher Encryption** 1. Enter the plain text, P 2. Enter the key, $K = 3$ 3. Enter modulus, n. 4. Obtain cipher text as follows. $C = (P + K) mod\ n$ **Brute Force Attack on Caesar Cipher** 1. Enter the cipher text C 2. Obtain deciphered text as follows for all the possible values of the key K $DC = (C - K) mod\ n$ 3. The key corresponding to the intelligible deciphered text would be the key used to encrypt the plain text. **Reverse Cipher**

	1. Enter the plain text 2. Enter the positions(key) by which the text has to be transposed 3. Apply the circular shift logic to obtain the Transposition Cipher. **Brute Force Attack on Reverse Cipher** 1. Enter the cipher text C 2. Apply the circular shift logic for all the different keys in the key domain. 3. The key corresponding to the intelligible deciphered text would be the key used to encrypt the plain text.
Program and Output	To be attached.
Conclusion	To be written by the student
References	1. William Stallings, Cryptography and Network Security, Pearson Education Asia Publication, 5th edition, 2013. 2. Behrouz A. Forouzan and Debdeep Mukhopadhyay, Cryptography and Network Security, Mc Graw Hill, 2nd edition, 2013.

Student Submission

Name	
Roll No.	
Program/Semester	
Subject	
Expt Title	