

A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering **Data Science**



Subject : CSS

Academic Year: 2023-2024

Monoalphabetic Cipher:-

*In monoalphabetic clipher, a character (or a symbol) in the plainless is always replaced by the same character (or a symbol) in the ciphertent irrespective of Ils position in the plaintent

* The relationship between a symbol in the plaintent 10 a

symbol in the aphertent is always one-to-one.

* For example, if the algorithm says that letter A in the plaintent is replaced by letter D in the ciphertext, then every letter A is replaced by the letter D.

Volyalphabetic Ciphers:

* In polyalphabetic substitution, each occurance substitution of a character may have a different charader.

* The relationship between a character in the plaintext to a character in the ciphertext is one-to-many. For example, "A" could be enciphered as 'B' in the beginning of the text, but as 'D' at the middle.

* In polyalphabetic cipher, we need to have a key stream K= (K1, K2, K3....) in which K1 is used to encipher the ith character in the plaintent to create ith character in the uphertext.

Subject Incharge: Prof. Sarala Mary Page No. 1

Department of CSE-Data Science | APSIT

