Semester : VI Subject : CSS Academic Year: 2023-2024

Monoalphabetic Cipher:-

* In monoalphabetic cipher, a character (or a symbol) in the plaintext is always replaced by the same character (or a symbol) in the ciphertext irrespective of its position in the plaintext.
* The relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.
* For example, if the algorithm says that letter A in the plaintext is replaced by letter D in the ciphertext, then every letter A is replaced by the letter D.

Polyalphabetic Ciphers:-

* In polyalphabetic substitution, each occurance of a character may have a different substitution character.
* 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 $K = (K_1, K_2, K_3 \ldots)$ in which K_i is used to encipher the i^{th} character in the plaintext to create i^{th} character in the ciphertext.