SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with ‘A’ Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(IoT and Cybersecurity Including BCT)

COURSE NAME : FUNDAMENTALS OF CRYPTOGRAPHY 19CS301

II YEAR / III SEMESTER

Unit II-

Topic : CLASSICAL CRYPTOGRAPHIC TECHNIQUES

CLASSICAL CRYPTOGRAPIC TECHNIQUES

Classical cryptographic techniques are methods of secure communication and data protection that were developed before the advent of modern computers and advanced encryption algorithms. These techniques rely on mathematical principles and various methods to transform plaintext (unencrypted data) into ciphertext (encrypted data) in order to keep the information confidential and secure. Here are some of the most well-known classical cryptographic techniques:

Caesar Cipher: Named after Julius Caesar, this technique involves shifting each letter in the plaintext by a fixed number of positions down the alphabet. For example, with a shift of 3, "HELLO" becomes "KHOOR".

Substitution Cipher: In this method, each letter in the plaintext is replaced with another letter according to a predetermined key. The key defines the substitution pattern, which can be a simple one-to-one mapping or a more complex arrangement.

Vigenère Cipher: This is an extension of the Caesar cipher where a keyword is used to determine the shift for each letter in the plaintext. The keyword is repeated to match the length of the plaintext.

Transposition Cipher: This technique involves rearranging the letters or blocks of letters in the plaintext according to a specific system, often involving a keyword. This changes the order of the characters in the ciphertext.

Playfair Cipher: This method uses a 5x5 grid of letters to encrypt pairs of letters in the plaintext. The positions of the letters in the grid determine the substitutions.

Hill Cipher: A more complex technique that uses matrix multiplication to encrypt and decrypt messages. The matrix key determines the transformation of the plaintext into ciphertext and vice versa.

Polyalphabetic Cipher: Similar to the Vigenère cipher, this technique uses multiple substitution alphabets to encrypt different parts of the plaintext, making the encryption more secure.

It's important to note that classical cryptographic techniques are generally not considered secure for modern applications due to their vulnerabilities. Many of these techniques can be broken using frequency analysis, pattern recognition, and other mathematical methods. As a result, modern encryption methods, which are based on complex mathematical algorithms and require strong keys, are used to secure digital communications and data.

Any Query????

Thank you……