Hello everyone! In this video you will learn about various traditional and modern symmetric key ciphers.

The symmetric key cryptography algorithms are of two types based on the unit being encrypted.
The first category is traditional ciphers which are character-oriented ciphers, and the second category is modern ciphers which work based on bits or blocks of bits.

Traditional ciphers are widely categorized as substitution ciphers and transposition ciphers.

In substitution ciphers, the symbols in the plaintext are replaced by another symbol to generate the ciphertext.
The substitution ciphers may be monoalphabetic or polyalphabetic. The relationship between the symbol in the plaintext to the symbol in the ciphertext is always one-to-one in monoalphabetic cipher, while it is one to many in polyalphabetic cipher.

In transposition ciphers, the overall data remains the same, but the positions of the plaintext are changed.
it may be noted here that encryption algorithms are also known as ciphers. Therefore, the encryption algorithm and cipher words will be used unchangeably throughout the videos.

Let us understand some popular traditional ciphers. The additive cipher, a monoalphabetic substitution cipher, is a

traditional cipher in which the letters of the alphabet are shifted a certain number but remain in the same order. The number in which the alphabet is shifted is called a key.
In the given example, the key is 7 modulo 26, which indicates that the plaintext alphabets will be shifted with 7 characters towards the right to get the cipher text using modulo operation while encryption. When decrypted the ciphertext characters will be shifted by 7 characters towards left in the given table using modulo operation.

In polyalphabetic substitution, each occurrence of a character may have a different substitute. The relationship between a character in the plaintext to a character in the cipher text is one to many. For example, “a” could be enciphered as” D” in the beginning of the text, but “N” at the middle.
Autokey Cipher, Playfair cipher, and vigenere cipher are examples.

Here you can see, how the vigenere cipher works. It uses a table of alphabets for encryption and decryption purposes, as shown. During encryption, the plain text is divided among blocks of characters with lengths equal to that of the key. Here the key is FROGFR with a length of 6 characters. To create the cipher text, the intersection points of the column corresponding to the key character and the row corresponding to the plaintext character is considered. Such as the intersection point for S and F is X, for Q and R is H, etc.

In this cipher, each character may have a different substitute, based on the table value.

Another category of symmetric ciphers, Transposition cipher reorders symbols. The overall symbol does not change, only the position changes. It can be keyless or keyed transposition cipher.

The Example here shows a keyless transposition cipher where, the plain text "MEET ME AT NIT" undergoes a Rail fence cipher. Each symbol of the plaintext is placed at first and second row alternately till the end of the plain text input. The final cipher is given by collecting all the symbols from first row followed by the symbols in the second row.

In Example 2, the communicating parties (Alice and Bob) agrees upon the number of column (4). The plaintext is divided into blocks of 4 symbols each till the end of the plaintext. The final cipher is obtained by collecting all symbols from column1 to column 4.

In keyed transposition, the plaintext is divided into predetermined blocks and a permutation key string is used to permute the characters in each block.

The plaintext is divided into blocks of size as 5. Extra padding is done if the block is not completely filled. For ZONE, the block is not completely filled, and Z is padded.

Based on the key, the plaintext ENEMY is permuted. When Key value is 3, the alphabet E(3rd character) is placed at 1st position of the ciphertext. When Key value is 1, the alphabet E(1st character) is placed at 2nd position of the ciphertext. When Key value is 4, the alphabet M(4th character) is placed at 3rd position of the ciphertext. When Key value is 5, the alphabet Y(5th character) is placed at 4th position of the ciphertext. When Key value is 2, the alphabet N(2nd character) is placed at 5th position of the ciphertext. So, for the plaintext "ENEMY", the ciphertext is "EEMYN. Similarly for plaintext block ZONE, the cipher text is NZEZO using keyed transposition cipher.

The traditional symmetric-key ciphers that we have studied so far are character-oriented ciphers. With the advent of the computer, we need bit-oriented ciphers. This is because the information to be encrypted is not just text; it can also consist of numbers, graphics, audio, and video data. It is convenient to convert these types of data into a stream of bits, to encrypt the stream, and then to send the encrypted stream. A modern cipher can be either a block cipher or a stream cipher.

Here is an example of a popularly known cipher DES, the Data Encryption Standard. It is a symmetric key cipher that follows the Feistel Network structure(in which the encryption and decryption algorithms are the same). In

DES, the input plain text size is 64-bits, and the output cipher text size is 64 bits. The key size is 64, Number of rounds is 16, with an F function in each round. The figure shows the structure of the DES algorithm and its rounds.

In 1990's the cracking of DES algorithm became possible. A replacement for DES was needed for modern symmetric-key block cipher. AES or Advanced Encryption Standard algorithm emerged for better security, computational efficiency and flexibility in implementation. It is symmetric block cipher. The inputs are given as blocks of 128 bits. AES supports variable number of rounds. Based on the number of rounds involved, the cipher key size differs. If the number of rounds is 10, the key size is 128 bits. Similarly for 12 and 14 rounds the key sizes are 192 and 256 respectively. The plain text gets transform to ciphertext after passing through the pre-round transformation and all the rounds. In each round, four types are operations are performed Substitute Bytes, Shift Rows, Mix Columns and Add Round Key. The final cipher text is sent to the receiver. The receiver deciphers the plaintext using the same cipher key and the same operations are performed to decipher the cipher text.

To learn more about symmetric key ciphers, follow the books given here.

Thank You…