Symmetric Encryption Cipher

Symmetric Key Cipher:

In symmetric key cipher the original massage called Plaintext from Sender called is sent through an insecure channel after encrypting the plain text to a cipher text to the receiver.

To create the cipher text from plain text the sender uses an encryption algorithm using a shared secrete key.

To create the plaintext from received cipher text at receiver end, receiver uses a decryption algorithm with same secrete key used to encrypt the massage.

Here key is the set of values that is used by the encryption or decryption algorithms.

In symmetric key encipherment the same Single secrete key is used for both Encryption and decryption

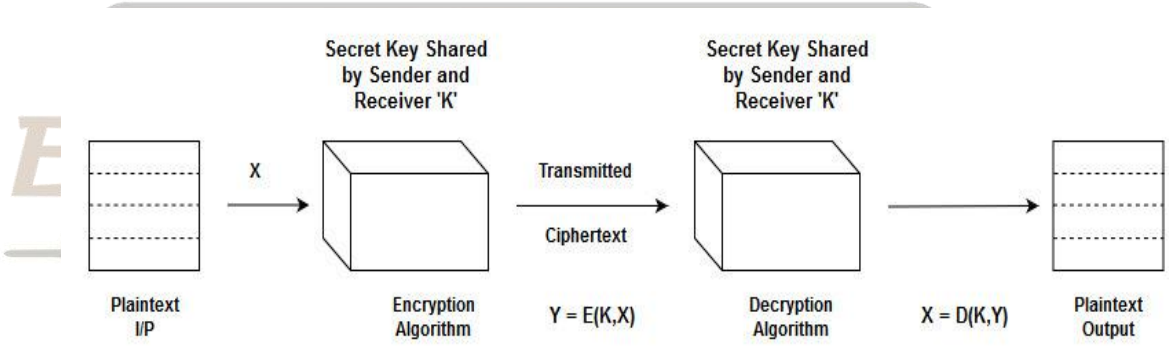
If **P** is the plain text, **C** is the cipher text and **K** is the key then encryption algorithm $\mathbf{E_k}$create the cipher text and decryption algorithm $\mathbf{D_k}$ create the plain text from cipher text.

Encryption: $C = E_k(P)$

Decryption: $P = D_k(C)$

Symmetric cipher model

The process of covering from plaintext to ciphertext is called Encryption, restoring the plaintext from ciphertext is known as Decryption



K= Secret Key
X = Plaintext/Message
Ciphertext Y = E(X,K)
Decrypted/Plaintext X = D(Y,K)

A symmetric encryption scheme has five components:

- **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.

- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.

- **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

- **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Kerckhoff's Principle

A cipher text would be more secure if we can hide both the encryption/decryption algorithm and the secrete key, but according to Kerckhoff principle it is not recommended only the secrecy of the key is enough.

Kerckhoffs's principle is one of the basic principles of modern cryptography. It was formulated in the end of the nineteenth century by Dutch cryptographer Auguste Kerckhoff. The principle states that,

"**A cryptographic system should be secure even if everything about the system, except the key, is public knowledge**."

Cryptanalysis:

Cryptanalysis is the science and art of breaking the security achieved by cryptography. We should study cryptanalysis beside cryptoghraphy to create better and strong secrete code by learning the effectiveness and vulnerability of our cryptosystem, not to break others code.

There are four types of cryptanalysis attack

1. **Ciphertext-Only Attack**

   In cipher text only attack the attacker has access to only the ciphertext. From this the attacker tries to find out the secrete key and the the corresponding plaintext. It is the most probable and common type of attack because the attacker needs only the cipher text for this attack.

Various methods are used for cipher text only attack. Some of them are,

- **Brute-Force Attack**
  It is the exhaustive-key-search method. Attacker tries to use all possible key combination to find the correct one to decrypt the ciphertext, assuming that the attacker knows the algorithm and key domain. Now a days it is not difficult to apply brute-force-attack, as it is very easy to try with all possible key combination using a computer.

- **Statistical Attack**
  In this method cryptanalyst or attacker uses some statistical information or characteristic of the plain text to assume the corresponding ciphertext and launch the attack. For example, Statistics state that 'E' is the most frequently used letter in English text. Thus the attacker find the most frequently used letter in cipher text and replace it by 'E' thus after finding some pair attacker can find the key and using it they can decrypt the ciphertext to corresponding plaintext.

- **Pattern Attack**
  I Some ciphertext there was some common pattern of text. The attacker uses this common patterns of the languages to find the corresponding plaintext and guessing the key to decrypt the cipher key. This method is called pattern attack.

2. **Known-Plaintext Attack**
   In this method of attack the attacker has access to some earlier plain text-cipher text pair other than the cipher text they want to break. The attacker analyze the relationship between previous known plaintext-ciphertext pair to find the key to break the next secret massage assuming that the sender uses the same key to encrypt every massage.

3. **Chosen-Plaintext Attack**
   This method is like known plain text attack but here the plaintext-ciphertext pair have been chosen by the attacker from various previous plain text stored in the sender's computer. It is possible only if the attacker has access to the sender's computer.

4. **Chosen-Ciphertext Attack**
   This method is like chosen plain text attack where the attacker has access to the receiver's computer. The attacker chose a previous cipher text from receiver's computer and decrypt to plain text to find the key. This key used to break the secret massage.

Categories Of Traditional Ciphers:

Symmetric key ciphers can be classified into two broad categories, substitution cipher and transposition cipher. In substitution cipher we replace one symbol in the plain text with another symbol in the cipher text. And in case of transposition cipher the cipher text is created be reordering of the character of the plain text.

Substitution Ciphers

Substitution cipher replace every symbol of plaintext by one corresponding symbol. For example Letter A can be replaced by letter 'E', letter 'B' can be replaced by letter 'F' and so on. It can by classified into two type, monoalphabetic cipher and polyalphabetic cipher.

Substitution Cipher replaces one symbol with another.

Monoalphabetic Cipher

Monoalphabetic substitution replaces all the occurrence of a particular character in the plain text with a same symbol in the ciphertext.

In monoalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-one.

Additive Cipher

The simplest mono-alphabetic cipher is additive cipher. As the name suggests, 'addition' operation is performed on the plain-text to obtain a cipher-text. It is also referred to as '**Shift Cipher**' or '**Caesar Cipher**'.

If the plain text is consist of integer numbers then the key value is added to the integer of plain text to find the corresponding integer of the cipher text.

If the plaintext consist of Alphabets the 'addition modulo 26' operation is used to find the cipher text.

At sender side if the plaintext is 'P' cipher text is 'C' and key is 'k' then the cipher text can be calculated from plain text as $C = (P + k) \bmod 26$. and at the receiver end the cipher text cab be decrypted as $P = (C - k) \bmod 26$.

Additive cipher is vulnerable to cipher-text-only attacks using exhaustive key searches (brute-force attack) because the key domain of the additive cipher very small. For the plain text containing alphabet there are only 25 keys (26 -1 as zero is useless for additive cipher).

Multiplicative Cipher

Multiplicative cipher is just like additive cipher except the multiplication operation with key value is used to calculate cipher text from plain text. And multiplication with inverse of key value is used for decryption purpose.

Affine Cipher

Affine cipher is the combination of multiplicative cipher and additive cipher used one after another. In this method two keys are used, the 1st one is used with multiplicative cipher and the 2nd one is for additive cipher.

In affine cipher the encryption and decryption operations are as follows,

$$C = (P * k_1 + k_2) \bmod 26$$
$$P = ((C - k_2) * k_1^{-1}) \bmod 26$$

Where C = Cipher text
P = Plain text
k_1 = Key used for multiplicative cipher
k_2 = Key used for additive cipher
k_1^{-1} = multiplicative inverse of k1

Polyalphabetic Cipher

Polyalphabetic substitution replaces each occurrence of a particular character in the plain text may have a different symbols in the ciphertext. Here we use a stream of sub-keys as key for encryption and decryption operations. Each sub-key is depends on the positions of the character in the plain text and used to encrypt or decrypt the corresponding character.

For example if the key stream is $\mathbf{k = (k_1, k_2, k_3, \ldots)}$, then the i^{th} character in the plain text is enciphered by i^{th} key to create i^{th} cipher text.

In polyalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the ciphertext is always one-to-many.

Autokey Cipher

Auto key cipher is the simplest polyalphabetic cipher where the key stream consist of sub keys depending on plain text, 1^{st} key is a predetermined value secretly agreed upon by sender and receiver, the second sub-key is the value of the first plain text the third sub-key is the 2^{nd} character of the plaintext and so on.

The encryption and decryption operation are as follows,

$$C_i = (P_i + k_i) \bmod 26$$
$$P_i = (C_i - k_i) \bmod 26$$

Where P = Plaintext ($P_1P_2P_3\ldots$)
C = Cipher text ($C_1C_2C_3\ldots$)
k = Key stream ($k_1, P_1, P_2, \ldots$)

Playfair Cipher

Playfair cipher method is used at the time of 1^{st} world war. The secret key for this cipher is made of 25 alphabets arranged in 5*5 matrix taking 'I' and 'J' in the same position. Different arrangement of key in the matrix can create many different secret key. This matrix is used to encrypt a massage. In playfair cipher the encryption is done by the following steps,

I. The plaintext is split into pairs of two letters. If two letter in a pair are same a bogus letter is inserted to separate them. After that if there is an odd number of letters, another bogus letter is added at end.

II. If two letters in a pair are located in the same row of the key matrix the corresponding encrypted letter is the next letter to the right in the same row (with warping to the beginning of he same row).

III. If two letters in a pair are located in the same column of the key matrix the corresponding encrypted letter is the letter bellow, in the same column (with warping to the beginning of he same column).

IV. If the tow letters in a pair are not in the same row or column of the key matrix. The corresponding cipher character for each letter is a letter that is in its own row but in the same column as the other letter.

Vigenere Cipher

In Vigenere Cipher the key stream is the repetition of an initial key stream of length ***m****(1 <= m <= 26)*. It takes each key from initial key stream one by one for corresponding plain text characters. When the key stream exhaust after encryption of ***m*** plain text character the same key stream repeated again from first.

One-Time Pad

In One-Time pad technique the secrecy is achieved by randomize the key value for encryption operation. In this cipher the key stream has same length as the length of plain text. The sender change the key randomly each time a massage is to e send. Cipher text only attack or any other type of attack are impossible. And it is not possible to implement commercially because of the randomize nature of the key selection.

Transposition Ciphers:

It is the reordering of the symbols. In transposition cipher the position of each letter in the plaintext changes the location to create the ciphertext. It is the permutation of the characters present in the text. It doesn't substitute each letter with another. For example the symbol in th 1st position of plain text appear in the 8th position an may symbol from 3rd position appears in 1st place and so on.

Key-less Transposition Cipher

Key less transposition is the method used for transposition cipher for which there is no need of any key. Two type of key less transposition is possible.

In the 1st type, the text of the massage is written in a table, column by column and then transmitted row by row.

In the 2nd type we arrange the massage row by row in a table, and transmit column by column.

Keyed Transposition Cipher

Keyed transposition cipher uses keys to encrypt and decrypt the messages. It shares the same secret key among the senders and the receivers. Key is used as position finder for the cipher text. For example,

Suppose the plaintext is- "I am Indian".

The cipher text will be calculated as follows, by the keys presented below,

As the length of the key is 3, The plain text is partitioned in 3 characters groups,

Partitioned Plain Text : I a m | I n d | i a n

Keys :

3	1	2
1	2	3

Cipher Text (encryption) : m I a | d I n | n i a

Plain Text (Decryption) : I a m | I n d | i a n

Here for encryption the 3rd character 'm' is placed at 1stposition, 1st character in the plain text 'I' is at 2nd position, and the 2nd character 'a' is at 3rd position to get the cipher text from the given key taking down-word. And for the other group the same method is applied.

For decryption operation the same method is applied with the key taking up-word.

Recently Transposition cipher combine key less and keyed transposition approaches to achieve better scrambling.

Transposition cipher are vulnerable to several kinds of ciphrtext-only attacks, like

Statistical Attack,
Brute-Force Attack,
Pattern Attack