Chapter : Cryptography

Topic: Cipher

Ciphers can be classified into several categories based on different characteristics and properties. Here are the common classifications of ciphers:

1. Symmetric vs. Asymmetric Ciphers:

Ciphers can be classified based on the number of keys used for encryption and decryption:

- Symmetric Ciphers:symmetric ciphers uses a single shared secret key for both encryption and decryption processes. Examples include AES, DES, and Blowfish.

- Asymmetric Ciphers: Also known as public key ciphers, asymmetric ciphers use a pair of mathematically related keys: a public key for encryption and a private key for decryption. RSA and Elliptic Curve Cryptography (ECC) are examples of asymmetric ciphers.

2. Block vs. Stream Ciphers:

Ciphers can be categorized based on how they process the input data:

- Block Ciphers: Block ciphers encrypt fixed-size blocks of data at a time. The plaintext is divided into blocks, and each block is encrypted separately. AES and DES are examples of block ciphers.

- Stream Ciphers: Stream ciphers encrypt data one bit or one byte at a time, usually in a continuous stream. They generate a keystream based on a key, and bitwise operations (such as XOR) are used to encrypt the plaintext. RC4 and Salsa20 are examples of stream ciphers.

3. Substitution vs. Transposition Ciphers:

Ciphers can be classified based on the operations used to transform the plaintext into ciphertext:

- Substitution Ciphers: Substitution ciphers replace characters or groups of characters in the plaintext with different characters or symbols. Examples include Caesar cipher, Vigenère cipher, and monoalphabetic substitution.

- **Transposition Ciphers:** Transposition ciphers rearrange the order of characters or groups of characters in the plaintext without changing the actual characters. Examples include Rail Fence cipher and Columnar Transposition cipher.

4. Classical vs. Modern Ciphers:

Ciphers can be classified based on their historical significance and development:

- **Classical Ciphers:** Classical ciphers are traditional ciphers that were developed and used before the advent of modern computer systems. Examples include Caesar cipher, Vigenère cipher, and Playfair cipher.

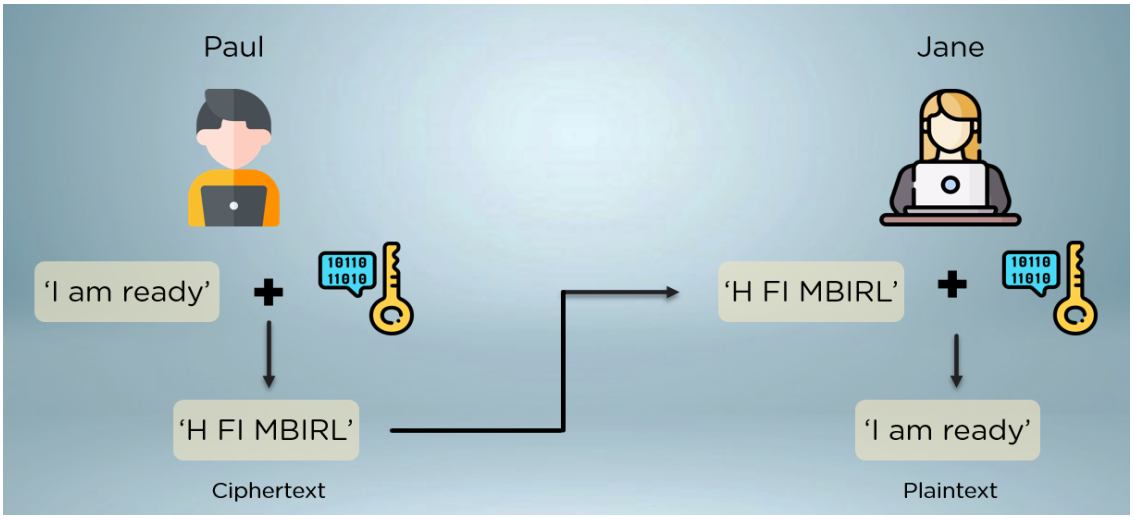
- **Modern Ciphers:** Modern ciphers are cryptographic algorithms that have been developed with modern computational capabilities in mind. Examples include AES, RSA, and ECC.

Topic: Cryptography:

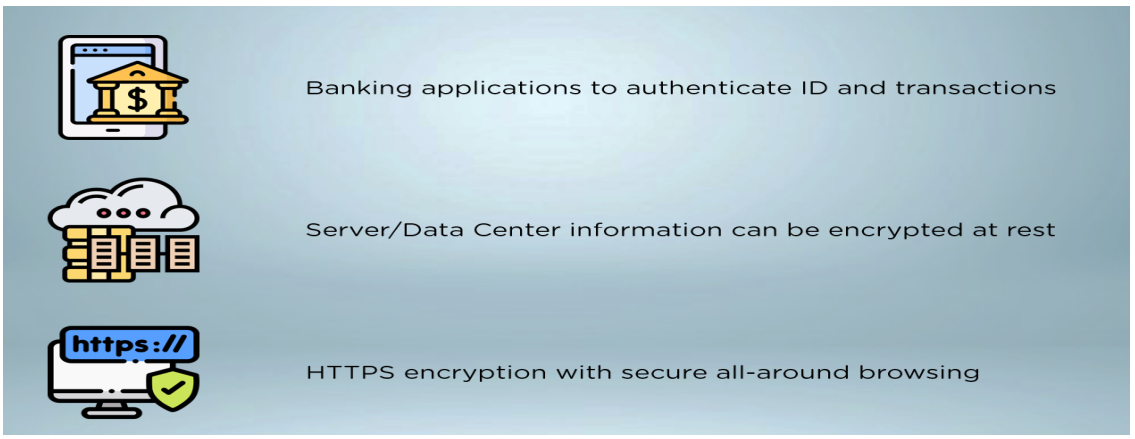
Cryptography: Cryptography is the practice of securing information by transforming it into an unreadable format.

Here are the main classifications of cryptography:

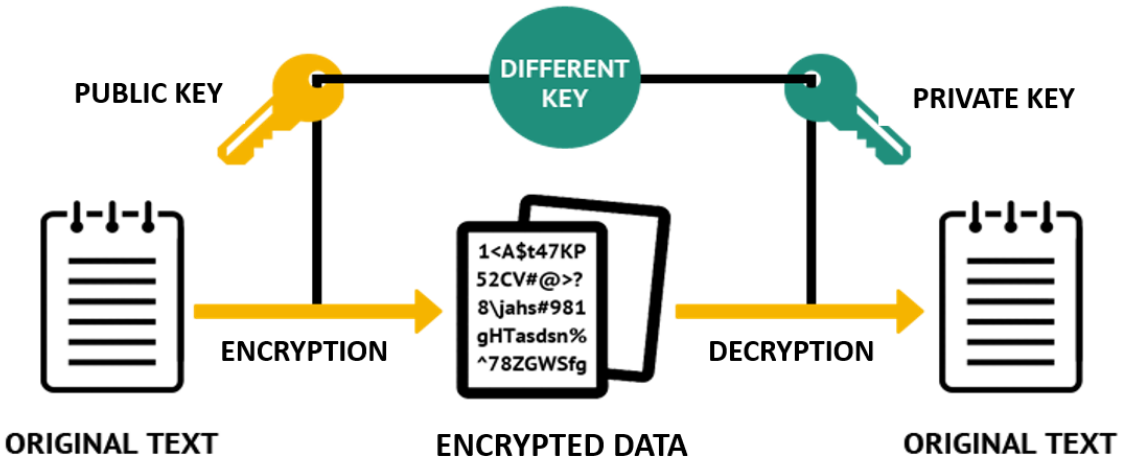
1.Symmetric Key Cryptography (Secret Key Cryptography): Symmetric key cryptography uses a single shared secret key for both encryption and decryption processes.same key is used by both the sender and the recipient to encrypt and decrypt the message



Applications of symmetric cryptography:



2.Asymmetric key cryptography: Asymmetric key cryptography use two different keys for encryption and decryption. The key used for encryption is the public key, and the key used for decryption is the private key. Both the keys must belong to the receiver.



3.Hash Functions: There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

Two types of ciphers can be used in symmetric algorithms. These two types are:

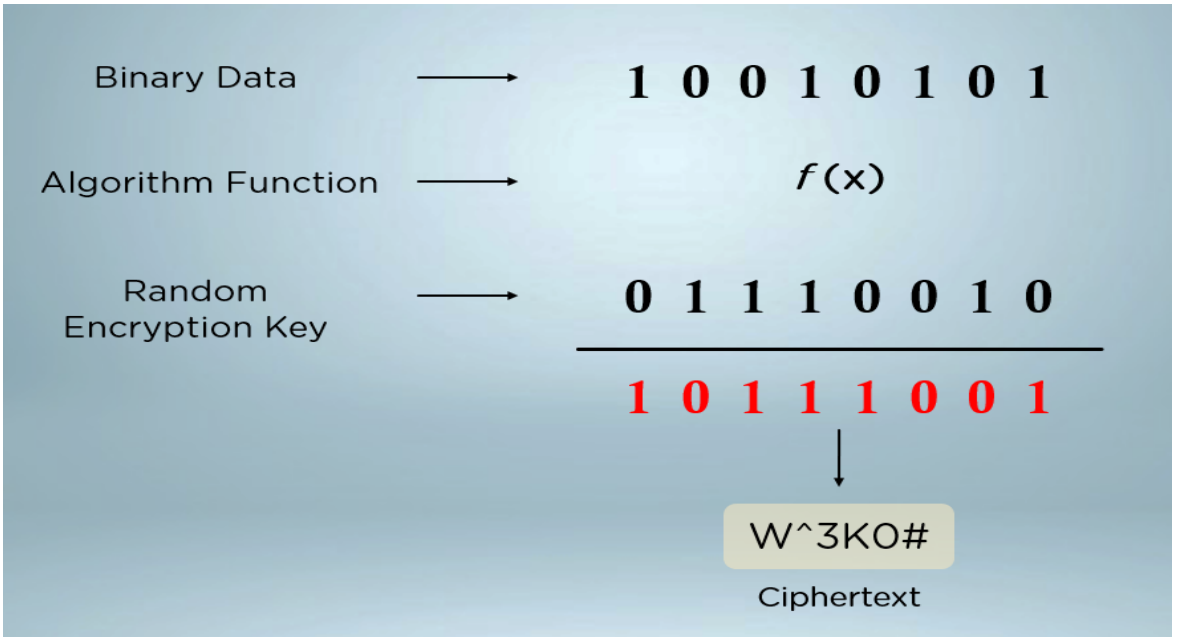
- **Stream Ciphers**
- **Block Ciphers**

1. Stream Ciphers

Stream ciphers are the algorithms that encrypt basic information, one byte/bit at a time. You use a bitstream generation algorithm to create a binary key and encrypt the plaintext.

The process for encryption and decryption using stream ciphers are as follows :

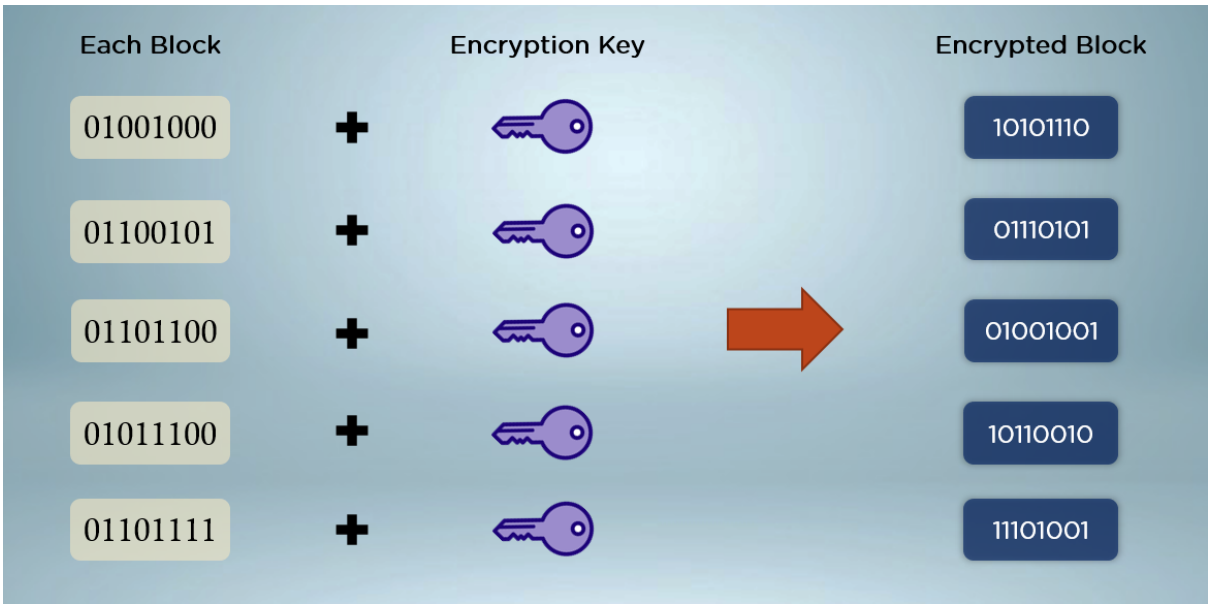
- Get the plaintext to be encrypted.
- Create a binary key using the bitstream generation algorithm.
- Perform XOR operation on the plaintext using the generated binary key.
- The output becomes the ciphertext.
- Perform XOR operations on the ciphertext using the same key to get back the plaintext.

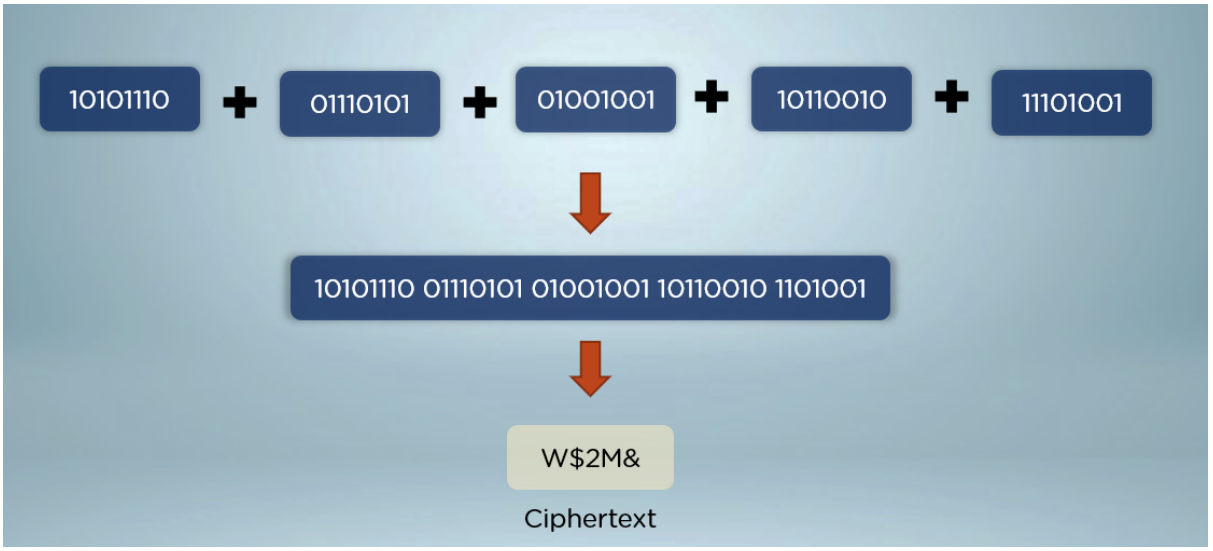


**** The most well-known stream ciphers are RC-4, SALSA and PANAMA.**

2. Block Ciphers

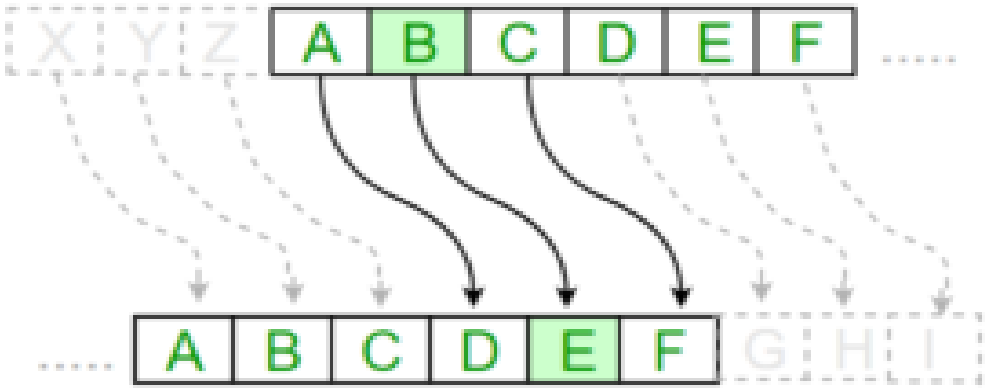
On the other hand, block ciphers dissect the raw information into chunks of data of a fixed size. The size depends on the exact cipher being used. A 128-bit block cipher will break the plaintext into blocks of 128-bit each and encrypt those blocks instead of a single digit. These ciphers are slower but much more tamper-proof and are used in some of the most common algorithms being employed today.





**** Today, the most popular symmetric-key algorithms like AES, DES, and 3DES are block cipher methodology subsets.**

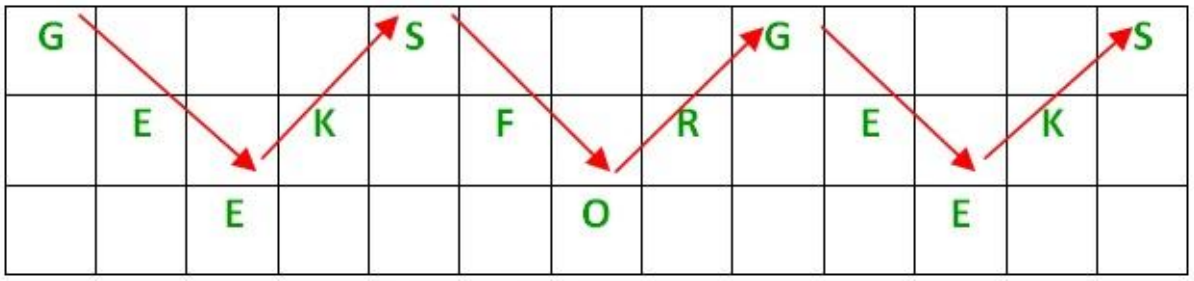
 # Substitution Cypher: In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key. For example with a shift of 1, A would be replaced by B, B would become C, and so on.



#Transpositional Cipher :A transpositional cipher is a type of cipher that rearranges the positions of characters or groups of characters in the plaintext to obtain the ciphertext. Unlike substitution ciphers that replace characters with different characters, transpositional ciphers only change the order of the characters while keeping the characters themselves unchanged.

some common types of transpositional ciphers include:

> **Rail Fence Cipher:** The Rail Fence cipher involves writing the plaintext diagonally on successive "rails" or lines, and then reading off the characters row by row to obtain the ciphertext. The number of rails used determines the depth of the zigzag pattern.



Columnar Transposition Cipher: The Columnar Transposition cipher involves writing the plaintext in a grid with a fixed number of columns. The ciphertext is then obtained by reading off the characters column by column according to a specific rule, typically dictated by a keyword or key phrase.

Encryption

Given text = Geeks for Geeks
Keyword = HACK **Length of Keyword** = 4 (no of rows) **Order of Alphabets in HACK** = 3124

H	A	C	K
3	1	2	4
G	e	e	k
s	_	f	o
r	_	G	e
e	k	s	_

Print Characters of column 1,2,3,4
Encrypted Text = e kefGsGsrekoe_