Unit - 1

Introduction to Cryptography

Cryptography

* Cryptography is used to Secure and Protect data during Communication. It is helpful to Prevent unauthorized person or group of users from accessing any Confidential data. Encryption and decryption are the two essential functionalities of Cryptography.

* It involves using Mathematical algorithms and Protocols to Convert Plain text into an unreadable format Called Cipher text, which can only be reverted to its original form by some Processing the Correct key.

Example

* Cryptography is widely used in applications like online banking, Messaging apps, and Secure email to Protect sensitive data from unauthorized access.

Security Attacks

* An attempt to gain unauthorized access to an information or Services or to Cause harm to damage to information Systems.

* Any action that Compromises the Security of

information owned by an organization.

Types of Security attacks

i) Passive Attacks

ii) Active Attacks

i) Passive Attacks

* Passive attack refers to the attacks where the attacker involves in Monitoring of data transmission.

* Passive attacks are difficult to detect because they do not involve any modification of the data.

* Passive attacks are of two types.

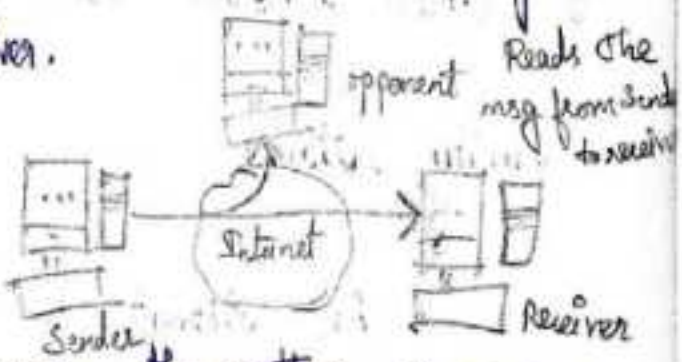
i) Release of Message Contents

ii) Traffic analysis

i) Release of message Contents

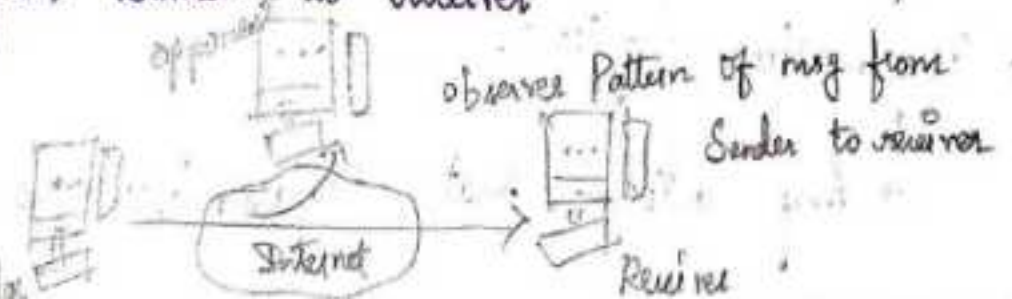
* A telephone conversation, an email Message may have Sensitive Information

* The attacker reads the Content of the Message sent from the Sender to receiver.



ii) Traffic Analysis

* The attacker observes the pattern of messages Sent from sender to receiver



ii) Active Attacks

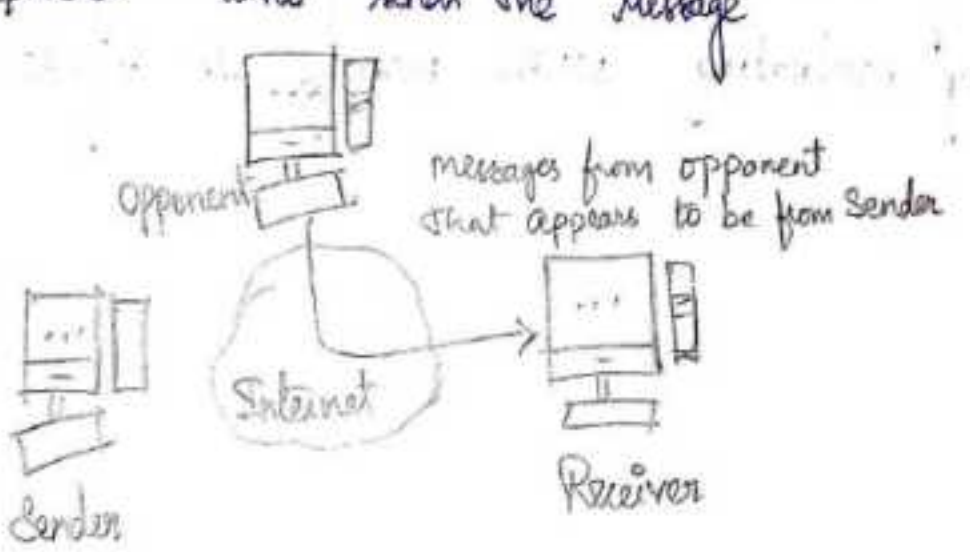
* Active attacks refers to the attacks where the attacker involves some modification of the data or Creation of false data. Monitoring & Modification

* Active attacks are of four types.

i) Masquerade
ii) Replay
iii) Modification of Message
iv) Denial of Services.

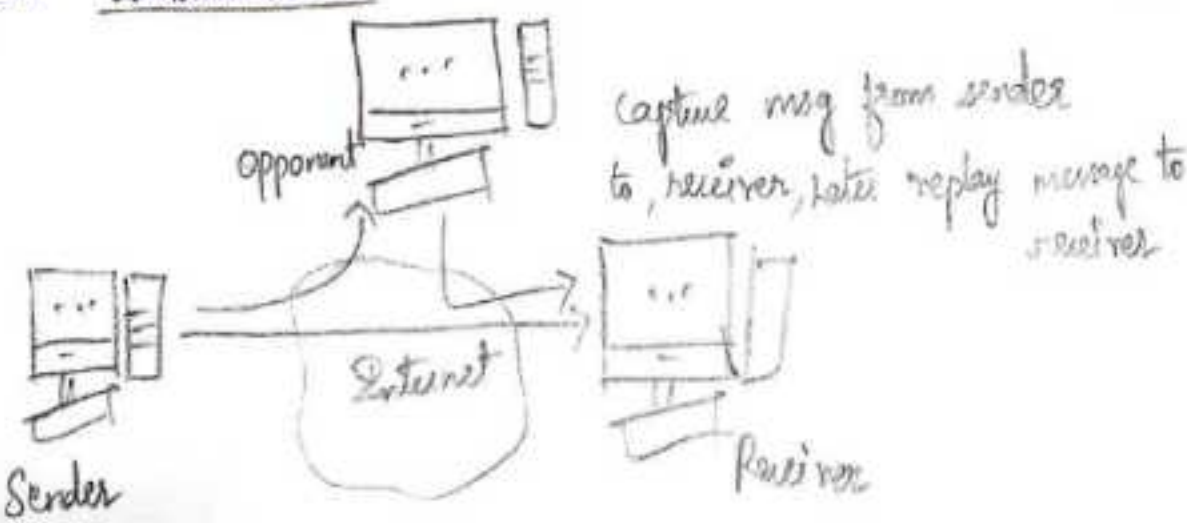
i) Masquerade

* It takes place when the attacker pretends to be the Sender who sends the Message



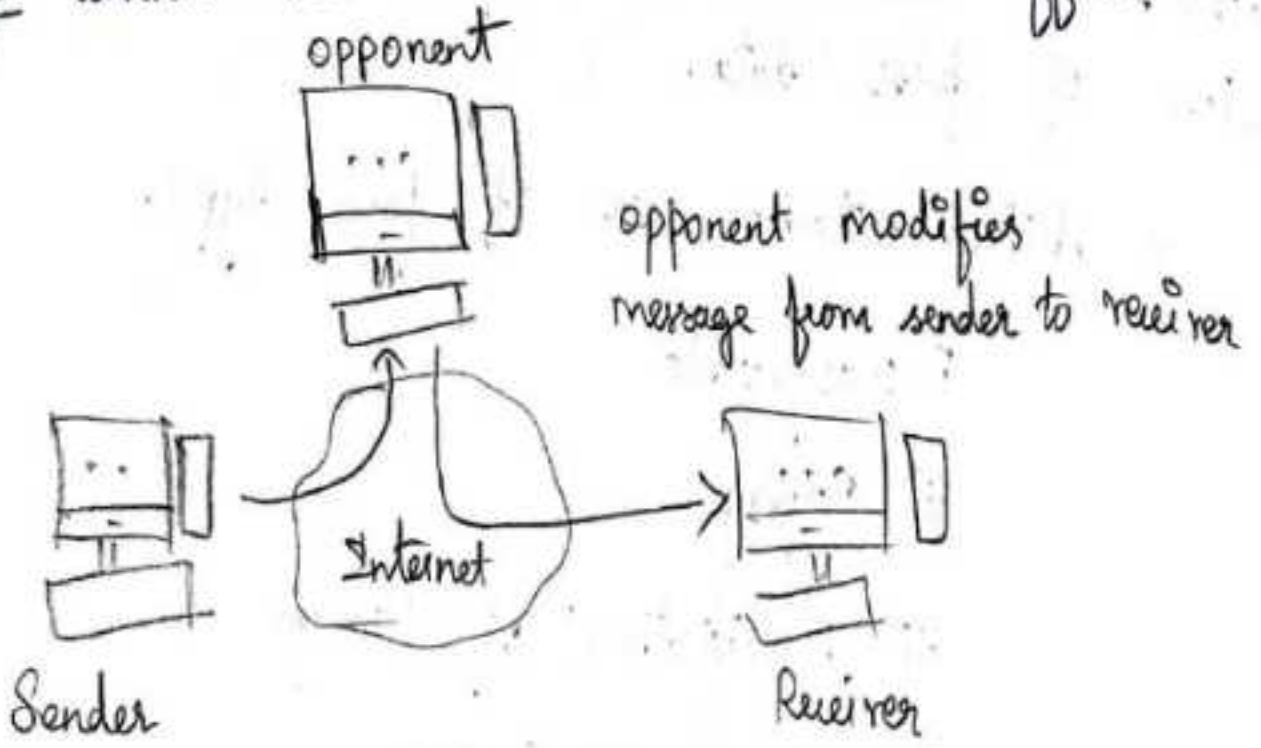
ii) Replay

* It involves the Passive Capture of data and its subsequent retransmission to Produces an unauthorized effect.



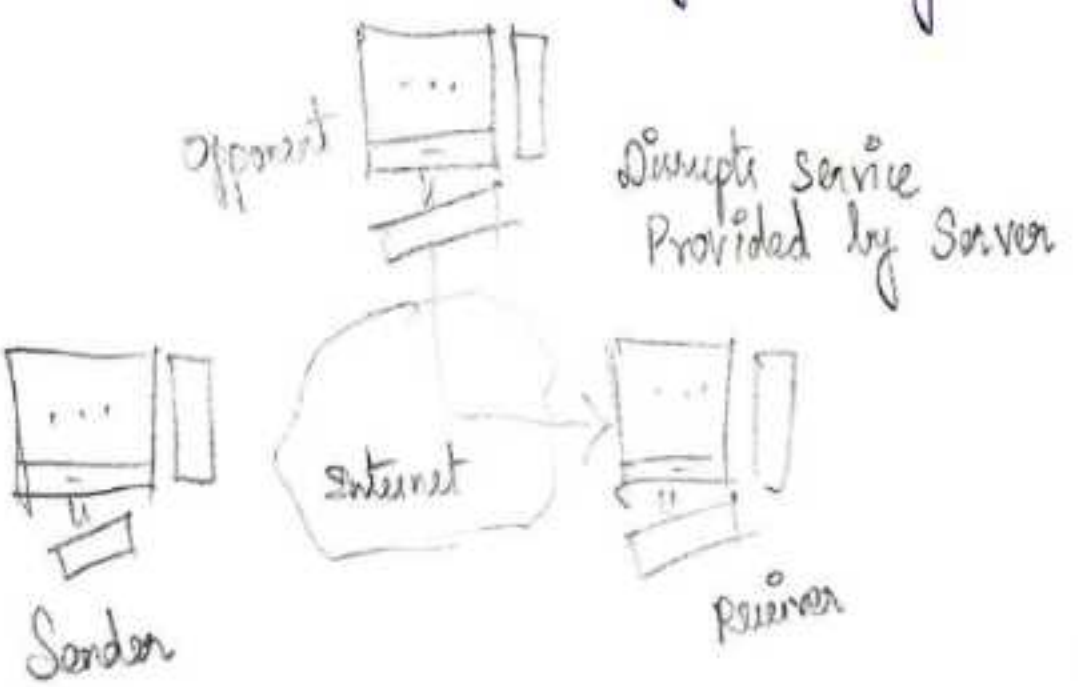
iii) Modification of Message

* It involves some change to the original message which Produces an unauthorized effect.



iv) Denial of Service

* The attacker disrupts the Service Provided by the Server, either by disabling the network or by overloading with message to degrade its Performance



Security Services

* Security Services refers to the Services Provided by a Protocol layer, which ensure adequate Security of data transfers or Systems.

* The Services are intended to counter Security attacks, and they make use of one or more Security Mechanisms to provide the Service.

* X.800 (Security Architecture for OSI) divides these services into many categories and Specific Services.

* Types of Security Services

i) Authentication
ii) Access Control
iii) Data Confidentiality
iv) Data integrity
v) Non-repudiation
vi) Availability

i) Authentication

* Authentication is the process of determining whether the person access the data is, who it is declared to be.

* Authentication is commonly done through the use of login and Passwords.

* It is of two types

i) Peer Entity authentication

ii) Data Origin Authentication

↳ Peer entity Authentication

* It is used in association with a logical connection to Provide Confidence in the identity of the entities connected.

↳ Data Origin authentication

* It ensures the recipient to verify that the message have not been modified in transit and they originally from the expected sender.

2) Access Control

* It is the ability to limit and Control access to the host systems and application via communication links.

* This service controls who have access to a resource.

3) Data Confidentiality

* Confidentiality refers to the Protection of transmitted data from Passive attacks.

* It is of four types

Connection Confidentiality, Connectionless Confidentiality Selective field Confidentiality, Traffic flow Confidentiality

i) Connection Confidentiality - The Protection of all user data on a Connection.

ii) Connectionless Confidentiality - The protection of all users data on a single data block.

iii) Selective field Confidentiality - The Confidentiality of selected fields within the user data on a Connection or in a single data block.

iv) Traffic flow Confidentiality - The Protection of the information that might be derived from the observation of traffic flows.

4) Data Integrity

* Data Integrity refers to the accuracy, Completeness and Consistency of the data.

* It ensures that the data is not Modified, deleted or altered without authorization.

* It involves Quality and validity of data by Preventing unauthorized changes.

* It is a five types

i) Connection integrity with recovery

ii) Connection integrity without recovery

iii) Selective field Connection integrity,

iv) Connectionless integrity

iv Selective field Connectionless integrity

i) Connection integrity with recovery

Provides integrity for all user data on a Connection with recovery attempted

ii) Connection integrity without recovery

Provides only integrity without recovery.

iii) Selective field Connection integrity

It Provides integrity for selected fields within the user data on a Connection

iv) Connectionless integrity

It Provides integrity for a single Connectionless data block

v) Selective field Connectionless Integrity

It Provides integrity for selected fields of user data in a single data block

5. Non - Repudiation

* Non repudiation prevents either sender or receiver from denying a transmitted Message.
* When a message is sent, the receiver can Prove that the alleged sender in fact sent the Message.

* When a Message is received, the Sender can Prove that the alleged receiver in fact received the Message.

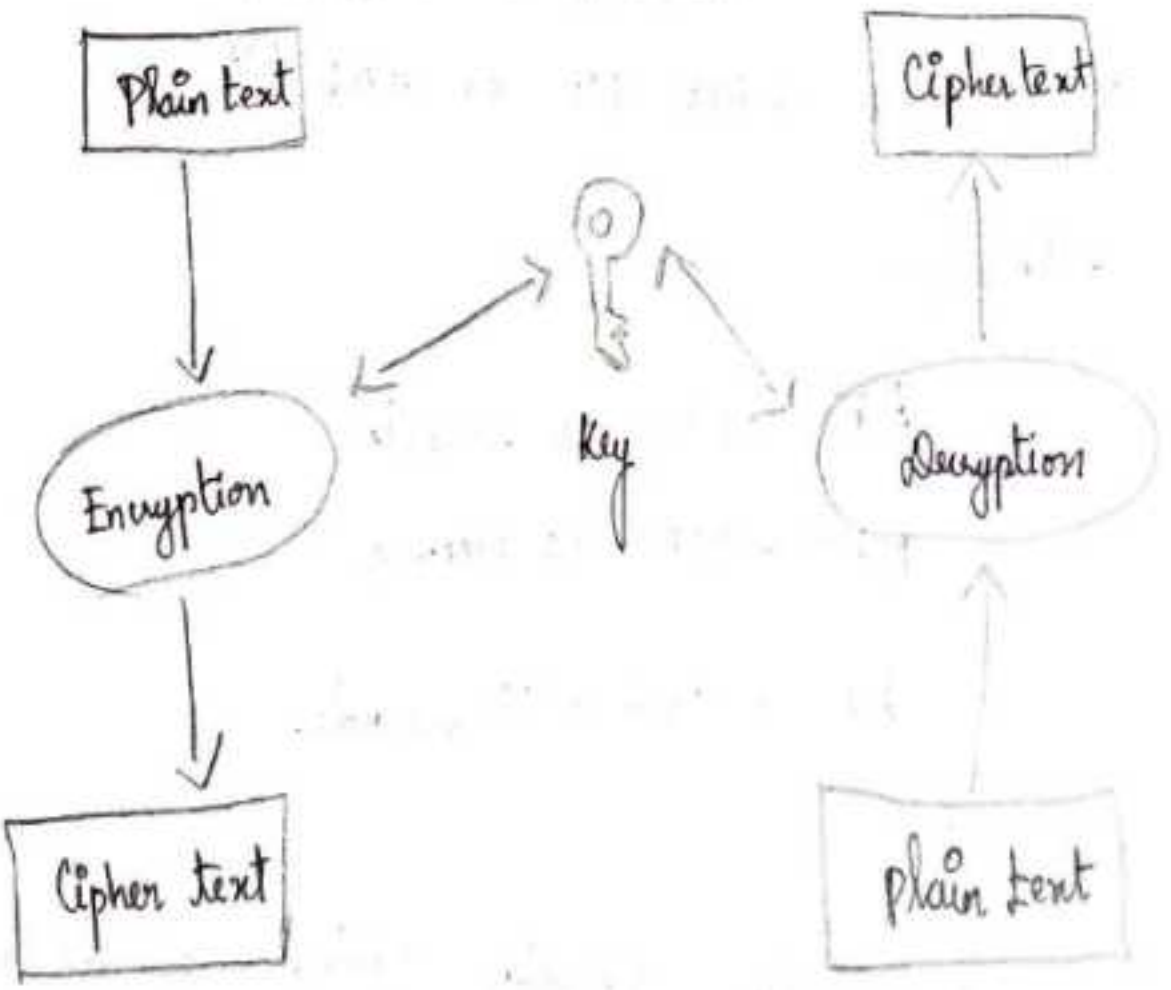
Cryptographic Algorithms

* A Cryptographic algorithm is a set of steps that can be used to Convert plain text into Cipher text.

* A Cryptographic algorithm is also known as an Encryption Algorithm

* A Cryptographic algorithm uses an encryption key to hide the information and Convert it into an unreadable format.

* Similarly, a decryption key can be used to Convert it back into plain-readable text.



Types

1) AES -> Advanced Encrypted Standard

2) DES - Data -> Data Encryption Standard

3) RSA -> Rivest, Shamir, Adleman

4) SHA -> Secure Hash Algorithm

1) Advanced Encryption Standard (AES)

* AES is a widely used Symmetric block cipher algorithm that encrypts and decrypts data using the same key.

* It replaced the older DES algorithm and is considered highly secure.

* Block Sizes : 128, 192 or 256 bits

* Key Sizes : 128, 192 or 256 bits

* Rounds :

AES - 128 = 10 rounds

AES - 192 = 12 rounds

AES - 256 = 14 rounds.

Characteristics

* Strongly security against the modern

threats.

* used in both hardware and software
* Widely adopted in applications like cloud Services Social media and Password managers.
* The higher the number of rounds, the stronger the encryption.

2) Data Encryption Standard (DES)

* DES is an older Symmetric encryption algorithm that converts 64-bit plaintext into encrypted ciphertext using the same key for both Processes.

Block Size : 64 bits
Key size : 56 bits (effective)

Charactiristics :-

* Symmetric key usage for both encryption and decryption.
* Designed for hardware efficiency
* Employs both transposition and substitution cipher techniques.
* Now considered less secure but foundational for learning and for building newer algorithms

3. RSA Algorithm (Rivest - Shamir - Adleman)

* RSA is a foundational asymmetric cryptographic algorithm, using a pair of keys ; a public key for encryption and a Private key for decryption.

Key & Types : Public and Private

Characteristics :

* High Security for data transmisson.

* Enables Secure Key exchange without transmitting the Private Key.

* Widely used for digital digital signature and Secure communications.

* Allows fast implementation for Cryptographic needs.

4. Secure Hash Algorithms (SHA)

* SHA algorithms generate unique, fixed - length digital fingerprints (hashes) of input data, ensuring data integrity and ... authenticity

Popular Versions : SHA - 2, SHA-3

Characteristics :-

* One way hashing : irreversible Process, ideal for Password storage
* Avalanche effect : A Minor input change drastically alters the hash.
* Variable input length, but fixed output length (eg., SHA-256 produces a 256-bit hash)
* Resistant Collision attacks (Two different inputs Providing the same hash)

Block Cipher

* A block Cipher is a cryptographic algorithm that encrypts data in a fixed-size blocks (128 bit) using a Symmetric key.
* It Processes each block through Multiple rounds of Substitution, permutation, and mixing, often using expanded Subkeys for each round.
* This design ensures strong security by applying both confusion (making the relationship between key and Ciphertext complex) and diffusion (Spreading plaintext changes

across the Ciphertext)

How it Works :-

Encryption → The plaintext is divided into fixed-size blocks.
↳ Each block is transformed into Ciphertext using the key and several rounds of operations.

Decryption → The process is reversed, applying the inverse operations to recover the original Plaintext.

Key Features

Block size : Typically 64 or 128 bits per block

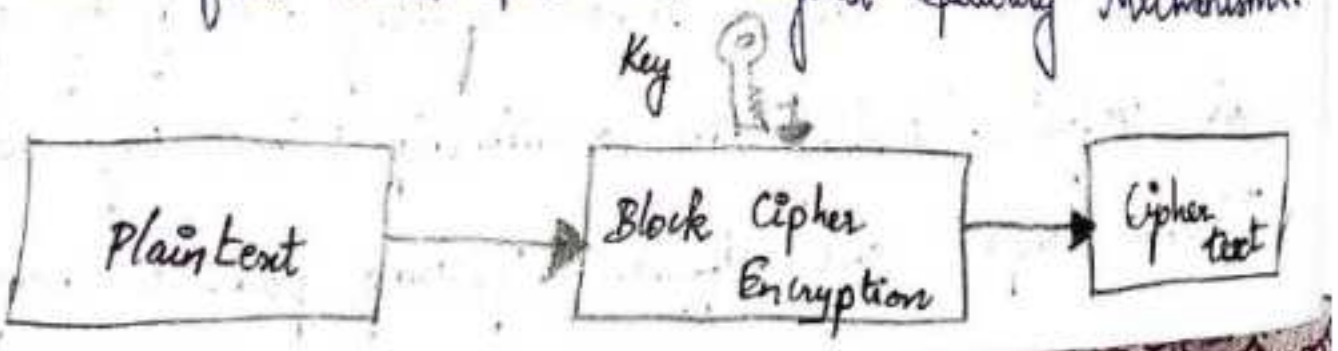
Key expansion : The main key is expanded into subkeys for each round.

Modes of operations]→ Common Modes includes ECB(Electronic Code Book) and CBC(Cipher Block Chaining)

Security → Resistant to cryptanalytic attacks due to its structure and multiple transformation rounds

Use Cases → Ideal for encrypting data at rest, such as files or secure communications

* Block Ciphers are foundational in modern cryptography providing robust protection for various applications due to their fixed block size and layered security Mechanisms.



Stream Cipher

* A stream cipher is a Symmetric encryption algorithm that encrypts data one bit or byte at a time, producing a continuous stream of ciphertext.

* It uses a key to generate a pseudorandom keystream, which is then combined with the plaintext to create the cipher text.

Key Features

Keystream generation -> A key is input into a pseudorandom bit-generator to Produce a keystream, which is as long as the message.

Encryption / Decryption -> Each plaintext bit or byte is XORed with the corresponding keystream bit or byte. The same keystream is used for decryption by XORing again

Speed and efficiency -> Stream ciphers are fast and suitable for realtime applications like video streaming or online gaming

Security -> using a long, unique keystream for each Message, increases resistance to cryptanalysis & brute force attacks.

Error Handling -> Errors affect only the corresponding bit or byte not the whole Message

Exeple

* plaintext - 10011001
* Keystream - 11000011
* Ciphatext - 01011010 (result of XOR operation).

* Stream Ciphers are valued for their Simplicity, Speed and efficiency, making them ideal for encrypting data in real-time scenarios.

NO.	Aspect	Block Cipher	Stream Cipher
1.	Operation	Encrypts data in fixed-size blocks	Encrypts data one bit or byte at a time
2.	Speed	Generally slower	Generally faster
3.	Complexity	Simpler algorithmic structure	More complex due to Continuous Processing
4.	Confusion/Diffusion	Uses both Confusion & diffusion	Uses only Confusion
5.	Error Propagation	Errors affect the whole block	Errors affect only the Corresponding bit/byte
6.	Modes of Operation	ECB, CBC, etc..	CFB, OFB, etc...
7.	Techniques	Based on transposition	Based on Substitution
8.	Padding	Requires Padding for non-block sized data	Does not requires padding.
9.	Security (Key Reuse)	More Secure with repeated key use	less Secure with repeated key use
10.	Use Cases	Best for data at rest (file storage internet Comms)	Best for data in transit (real-time, streaming)