Today Contents:

1. What is Cryptanalysis?

2. What is Steganography?

   * Steganography Examples

3. Stream and Block Ciphers

   * Stream Ciphers

   * Types of Stream Cipher

   * Stream cipher with examples

   * Block Ciphers

   * Block cipher with examples

4. Key Differences between Stream Cipher vs Block Cipher

5. Comparison Table of Stream Cipher vs Block Cipher

What is Cryptanalysis?

Cryptanalysis is the art of trying to decrypt the encrypted messages without the use of the key that was used to encrypt the messages**.** Cryptanalysis uses mathematical analysis & algorithms to decipher the ciphers. The success of cryptanalysis attacks depends

- Amount of time available
- Computing power available
- Storage capacity available

The following is a list of the commonly used Cryptanalysis attacks;

- **Brute force attack**– this type of attack uses algorithms that try to guess all the possible logical combinations of the plaintext which are then ciphered and compared against the original cipher.
- **Dictionary attack**– this type of attack uses a wordlist in order to find a match of either the plaintext or key. It is mostly used when trying to crack encrypted passwords.
- **Rainbow table attack**– this type of attack compares the cipher text against pre-computed hashes to find matches.

What is Steganography?

Steganography is the art of concealing information. In computer science, it refers to hiding data within a message or file. It serves a similar purpose to cryptography, but instead of encrypting data, steganography simply hides it from the user.

Invisible ink is an example of steganography that is unrelated to computers. A person can write a message with clear or "invisible" ink that can only be seen when another ink or liquid is applied to the paper. Similarly, in digital steganography, the goal is to hide information from users except those who are meant to see or hear it.

Steganography Examples

Since steganography is more of an art than a science, there is no limit to the ways steganography can be used. Below are a few examples:

1. Playing an audio track backwards to reveal a secret message
2. Playing a video at a faster frame rate (FPS) to reveal a hidden image
3. Embedding a message in the red, green, or blue channel of an RGB image
4. Hiding information within a file header or metadata
5. Embedding an image or message within a photo through the addition of digital noise.

Stream and Block Ciphers:

A **stream cipher** is a symmetric key **cipher** where plaintext digits are combined with a pseudorandom **cipher** digit **stream** (keystream). ... **Stream ciphers** represent a different approach to symmetric encryption from **block ciphers**. **Block ciphers** operate on large **blocks** of digits with a fixed, unvarying transformation.

Stream Cipher

A stream cipher is a symmetric key cipher (method of encryption) where plaintext digits are combined with a pseudorandom cipher digit stream. A stream cipher encrypts plaintext with a key and algorithm applied to every binary digit (one and zeros) for every bit in the data stream. The pseudorandom cipher digits are generated through a number of random seed values that use digit shift registers.

In a stream cipher, text is divided into small blocks, one bit or one byte long and each block is encoded depending on many previous blocks.

Types of Stream Cipher

1. **Synchronous Stream Ciphers**: A synchronous stream cipher generates a Keystream based on internal states not related to the plaintext or ciphertext. Encryption and

decryption require that the synchronous state cipher be in the same state, otherwise the message cannot be decrypted.

2. **Self-Synchronising Stream Ciphers:** A self-synchronizing Stream Cipher, also known as an asynchronous stream cipher or ciphertext autokey (CTAK), is a stream Cipher which uses the previous *N* digits in order to compute the keystream used for the next *N* characters.

What is a stream cipher with examples?

RC4 is an **example** of a modern symmetric-key **stream cipher**. ... RC2, RC5, and RC6 are symmetric-key block **ciphers**. RC4 does not generate its keystream by using a LFSR. For RC4, **stream** combinations are done on byte-length strings of plaintext. 256 bytes of memory are required for the state array.

Block Cipher

A block cipher is an encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text, rather than encrypting one bit at a time as in stream ciphers. In block cipher, text is divided in relatively large blocks, typically 64 0r 128 bytes long and that each block is encoded separately. Plaintext is used during the encryption and the resulting encrypted text is referred to as a ciphertext.

Block cipher algorithm is symmetric in that, during encryption, it uses the shared key to transform its plaintext input into a cyphertext (encrypted text). During decryption, it uses the same key to transform the ciphertext back to the original plaintext. The length of the output is the same as the input.

What is a block cipher with examples?

A **block cipher** is an encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a **block** of text, rather than encrypting one bit at a time as in stream **ciphers**. For **example**, a common **block cipher**, AES, encrypts 128 bit blocks with a key of predetermined length: 128, 192, or 256 bits.

Key Differences between Stream Cipher vs Block Cipher

1. In stream cipher, the encryption is done bit by bit whereas, in block cipher, it is done block by block.
2. In stream cipher, the decryption is also done by bit by bit whereas in block cipher it is done by block by block.
3. Stream cipher relies on substitution techniques like Caesar cipher, modified Caesar cipher, monoalphabetic cipher, homophonic cipher, polygram substitution cipher, polyalphabetic cipher, Playfair cipher, and hill cipher.
4. Block cipher relies on transposition techniques like rail-fence technique, columnar transposition technique, Vernam cipher, and book cipher.
5. Stream cipher uses confusion to ensure that it doesn't give clues about plain text whereas block cipher uses both confusion and diffusion.
6. A stream cipher is faster than block cipher whereas block cipher is slower.
7. In a stream cipher, one key is used for one time whereas in block cipher key can be reused.
8. Stream cipher requires s less code than block cipher.
9. Stream Cipher doesn't consist of a complex algorithm or process as a Block Ciphers.
10. It is simple to implement Stream cipher in Hardware than that of Block cipher.
11. Redundancy is less in stream cipher whereas block cipher increases the redundancy. A stream cipher is used for SSL secure connection for web whereas block cipher is used for database, file encryption.
12. Encryption can be implemented bit by bit in stream ciphers and instantly when new data is available for processing, so an incoming bit will automatically generate an outgoing bit without buffering the input. On the other hand, block ciphers require a complete data block by applying a padding scheme to be collected before the first output bit can be generated.

Comparison Table of Stream Cipher vs Block Cipher

Basis of Comparison between Stream Cipher vs Block Cipher	**Stream Cipher**	**Block Cipher**
Encryption Process	It encrypts one bit of plain text at a time.	It encrypts one block of plain text at a time.
Decryption Process	It decrypts a bit of plain text at a time.	It decrypts one block of plain text at a time.
Confusion and Diffusion	Stream cipher uses only confusion.	Block cipher uses both Confusion and diffusion.
Techniques Used	It uses substitution techniques	It uses transposition techniques.
Speed	It is faster than block cipher.	It is slower than stream cipher.
Scope of Redundancy	There are no chances of Redundancy.	It increases the redundancy of plain text.
Source of Code	It requires less code.	It requires more code.
Algorithm Modes	It uses Electronic Code Block (ECB) and Cipher Block Chaining (CBC).	It uses Cipher Feedback (CFB) and Output Feedback (OFB).
Use of Key	One key is used only one time.	One key can be used multiple times.
Implementation	It is widely used for hardware implementation.	It is suitable for software implementation.
Example	OTP (One Time Pad).	DES (Data Encryption Standard).