TALENTO TECH

# REGIÓN 3
# CAUCA - NARIÑO
# LESSON 4 -UNIT 1

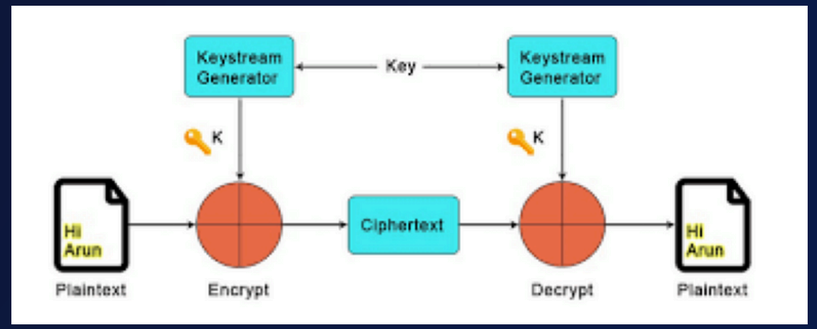
TIC

Universidad Tecnológica de Pereira

faceIT

## LESSON 4. Reading

Stream ciphers




### What Are Stream Ciphers?

Stream ciphers are a type of encryption technique used to secure digital information. Unlike block ciphers, which work with fixed-sized blocks of data, stream ciphers encrypt data bit by bit or byte by byte. This makes stream ciphers particularly useful for encrypting data streams that are continuously transmitted, like audio or video files.

In a stream cipher, a key stream (a sequence of random or pseudorandom bits) is combined with the plaintext (the original data) to produce ciphertext (the encrypted data). This process ensures that even if someone intercepts the data during transmission, they won't be able to understand it without the correct key.

## How Stream Ciphers Work

1. **Key Stream Generation:** A secret key is used to generate a stream of random or pseudorandom bits called the key stream.
2. **Bitwise XOR Operation:** The plaintext is combined with the key stream using an XOR (exclusive OR) operation. XOR is a logical operation that compares bits from both the plaintext and the key stream, returning a 1 when the bits are different and 0 when they are the same.
3. **Encryption and Decryption:** The key stream is combined with the plaintext data to create ciphertext. The same key stream is used to decrypt the ciphertext back into plaintext by applying the XOR operation again.

## Advantages of Stream Ciphers

- Efficiency: Stream ciphers are faster and more efficient than block ciphers when it comes to encrypting large amounts of data or real-time communication like video streaming or voice calls.
- Memory Usage: Stream ciphers use less memory compared to block ciphers, making them ideal for devices with limited processing power or storage, such as embedded systems and mobile devices.
- Real-Time Encryption: Stream ciphers work well in scenarios where data is continuously flowing, such as encrypting data over a network during live communications.

## Disadvantages of Stream Ciphers

- Key Management: Since stream ciphers rely on the key stream, proper management and protection of the key is crucial. If the key stream is reused or guessed by an attacker, the encrypted data can be easily compromised.
- Predictability: Some stream ciphers, like RC4, have vulnerabilities that make them less secure if the key stream is predictable or weak.

## Conclusion

Stream ciphers are a fast and efficient way to secure data, especially for continuous data streams. However, careful attention must be paid to key management and the choice of encryption algorithm to ensure the security of the data. Modern stream ciphers like ChaCha20 have improved security and are commonly used in secure communications today.