# SNS COLLEGE OF ENGINEERING

**Coimbatore-35**
**An Autonomous Institution**

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

Redesigning Common Mind & Business Towards Excellence

1st Indian Institution to Implement & Patent Design Thinking FrameWork

www.snsgroups.com

Build an Entrepreneurial Mindset Through Our Design Thinking FrameWork

# DEPARTMENT OF CSE ( IoT, Cyber Security including Block chain Technology)

## 19SB624 – INFORMATION SECURITY IN IOT

**III YEAR/ V SEMESTER**

## UNIT 2 – Symmetric & Asymmetric key Ciphers

TOPIC 1 –Block Cipher principles & Algorithms (DES, AES)

- Symmetrical Key Cryptography also known as conventional or single-key encryption was the primary method of encryption.

**Techniques Used in Symmetric Key Cryptography**

- Substitution Techniques
- Transposition Techniques

## Substitution Techniques

**Caesar Cipher:** Caesar cipher has their predictability is so complete and no complexity is invested.

**Mono alphabetic Ciphers:** This is where the ciphers use one rule of substitution throughout the message. This may involve replacing letters with numbers, symbols, or another set of letters in another order.

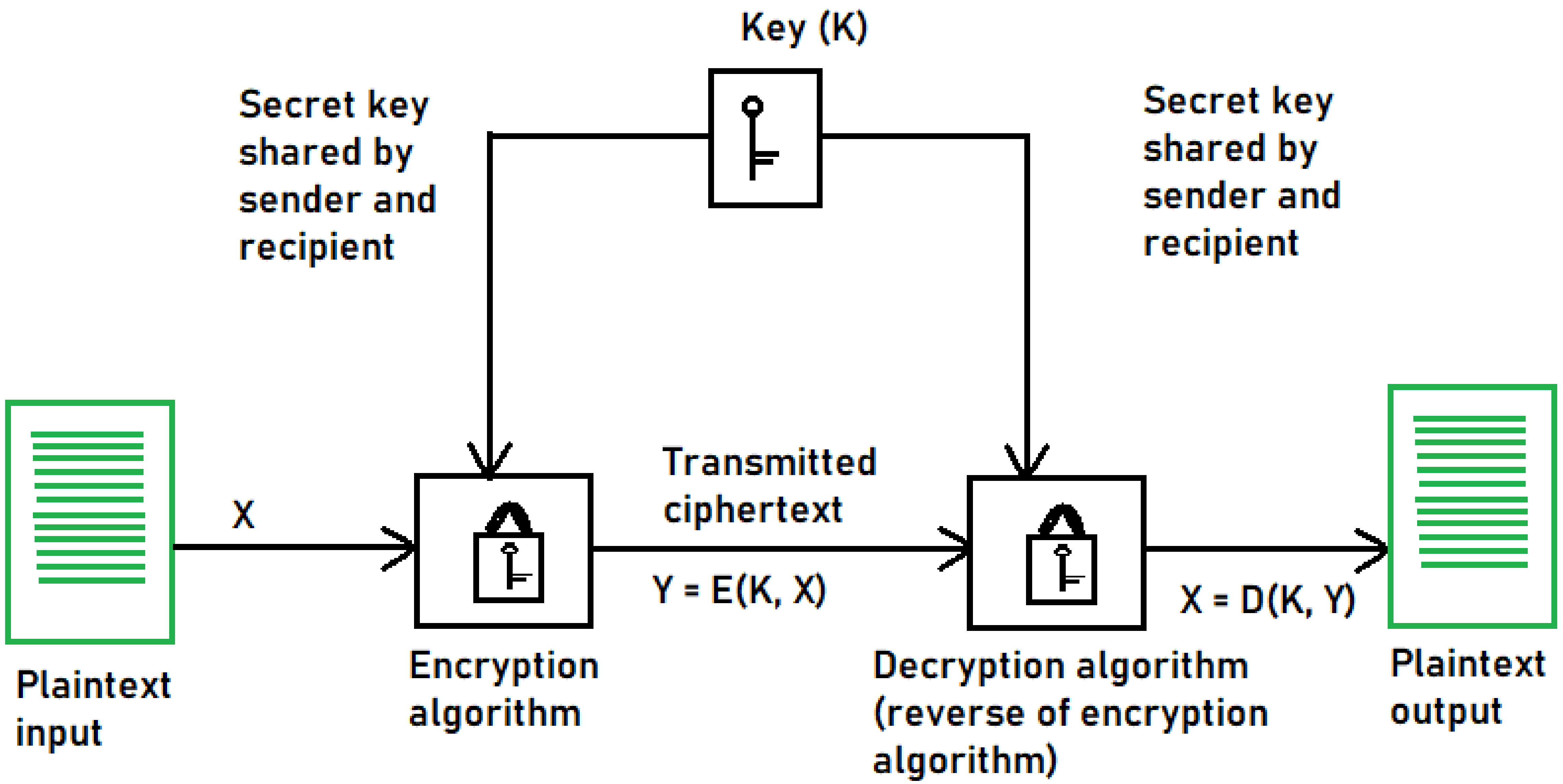
**Play fair Cipher:** Implementation of repeated letters or letter pairs can expose patterns, and cryptanalysis techniques exist to exploit them.

**Hill Cipher:** This cipher operates on blocks of letters (typically bigrams or trigrams) using a matrix multiplication approach. The Hill ciphers have a limitation on key size and susceptibility towards cryptanalysis for larger key sizes.

**Polyalphabetic Ciphers:** This is the type of cipher where any one of the letters in the plaintext is substituted by a different letter to keep frequency analysis challenging.

**One-Time Pad (OTP):** It is a theoretically impossible cipher where the key is a random string of characters that is exactly as long as the message itself. The key is used for a single encryption and then discarded.

# Symmetric Key Cryptography


Key (K)
Secret key shared by sender and recipient
Secret key shared by sender and recipient
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

## Transposition Techniques

Transposition techniques rearrange the order of elements in the plaintext message without changing the elements themselves.

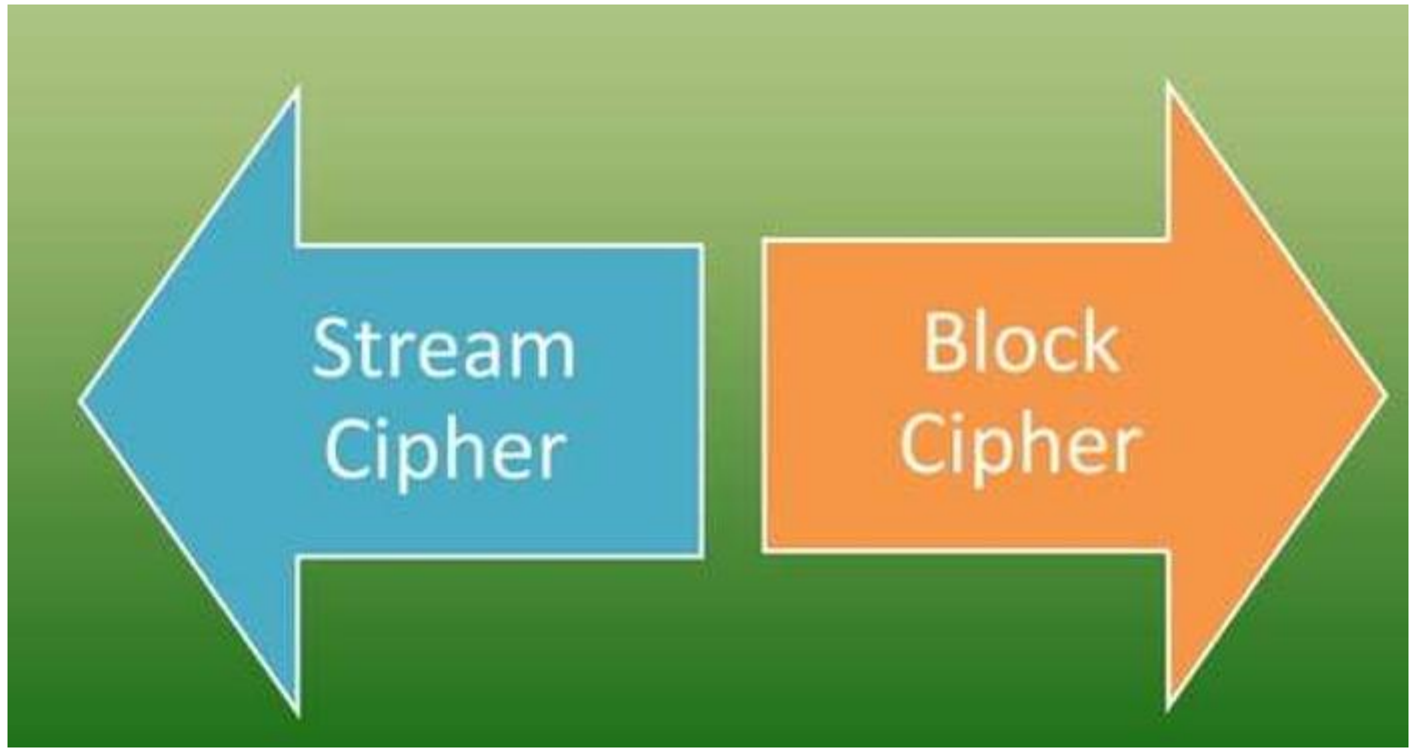
**Rail Fence Cipher:** This is a simple cipher that rearranges the elements by writing the plaintext message in a zigzag pattern, with the different components written in rows (rails) of an imaginary fence and then reading through the columns in a standard order. The key to this is the number of rails used.

**Columnar Transposition:** In the case of a plaintext message written in columns and then the columns rearranged according to a permutation determined by the key, this cipher is known as columnar transposition.

It is still vulnerable to cryptanalysis techniques that exploit the statistical properties of the language.

# Types of Symmetric Key Cryptography

- Stream Ciphers
- Block Ciphers



## Stream Ciphers

- The encryption process begins with the stream cipher's algorithm generating a pseudo-random keystream made up of the encryption key and the unique randomly generated number known as the nonce.
- The result is a random stream of bits corresponding to the length of the ordinary plaintext. Then, the ordinary plaintext is also deciphered into single bits.

- These bits are then joined one by one to the key stream bits, gradually converting the ordinary plaintext into the ciphertext using the XOR bitwise operations.
- When the recipient wants to decrypt the encrypted plaintext, they must generate a new key stream made during the encryption.
- The encrypted plaintext is then deciphered one by one to derive the encrypted plaintext at the recipient's end.

## Stream cipher algorithms

**Rivest Cipher 4 (RC4)**

**Strengths:** The initial appeal of RC4 came from its efficient design and capability to handle variable-length data streams.

**Salsa20**

**Strengths:** It's fast and efficient, with a simple and elegant design. Most importantly, the security it offers against known attacks is robust. Apart from that, Salsa20 serves as a building block for other cryptographic protocols, exhibiting its versatility.

## Grain-128

**Strengths of Grain-128 include** efficiency, lightweight implementation, and the ability to perform well with limited processing power and memory, making it ideal for RFID tags and sensor networks. Importantly, Grain-128 still provides strong security with such simplicity.

## Block Cipher

- The result of a block cipher is a sequence of blocks that are then encrypted with the key. The output is a sequence of blocks of encrypted data in a specific order.
- When the cipher btext travels to its endpoint, the receiver uses the same cryptographic key to decrypt the ciphertext block chain to the plaintext message.

## Block cipher algorithms

### Advanced Encryption Standard (AES)

- It has support for three-length keys: 128 bits, 192 bits, or 256 bits, the most commonly used one is a 128-bit key.
- It includes secure communication, data encryption in storage devices, digital rights management (DRM), and so on.

### Data Encryption Standard (DES)

- In DES, the 64-bit blocks of plaintext are encrypted using a 56-bit key.
- This weakness caused by the small key size led to the development of a more secure algorithm, called AES.

# Triple Data Encryption Algorithm (Triple DES)

- The development of the Triple DES, also called Triple-DES or TDEA, was triggered by the weak security resulting from the small key size in the DES.
- Triple DES denotes a method of three times applying the DES algorithm sequentially (encrypt-decrypt-encrypt) on every plaintext block.

# Advantages of Symmetric Key Cryptography

- Speed and efficiency
- Scalability
- Simplicity

# THANK YOU