symmetric-key cipher

symmetric-key cipher

In a **symmetric-key cipher**, both participants[1] in a communication share the same **key**. In other words, if a message is encrypted using a particular **key**, the same **key** is required for decrypting the message.

OR
Symmetric ciphers use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. They are faster than asymmetric ciphers.(**Asymmetric ciphers are also referred to as ciphers with public and private keys. They use two keys, one for encryption of messages and the other one during decryption.)**

Some examples of symmetric encryption algorithms include or Examples of symmetric ciphers are:

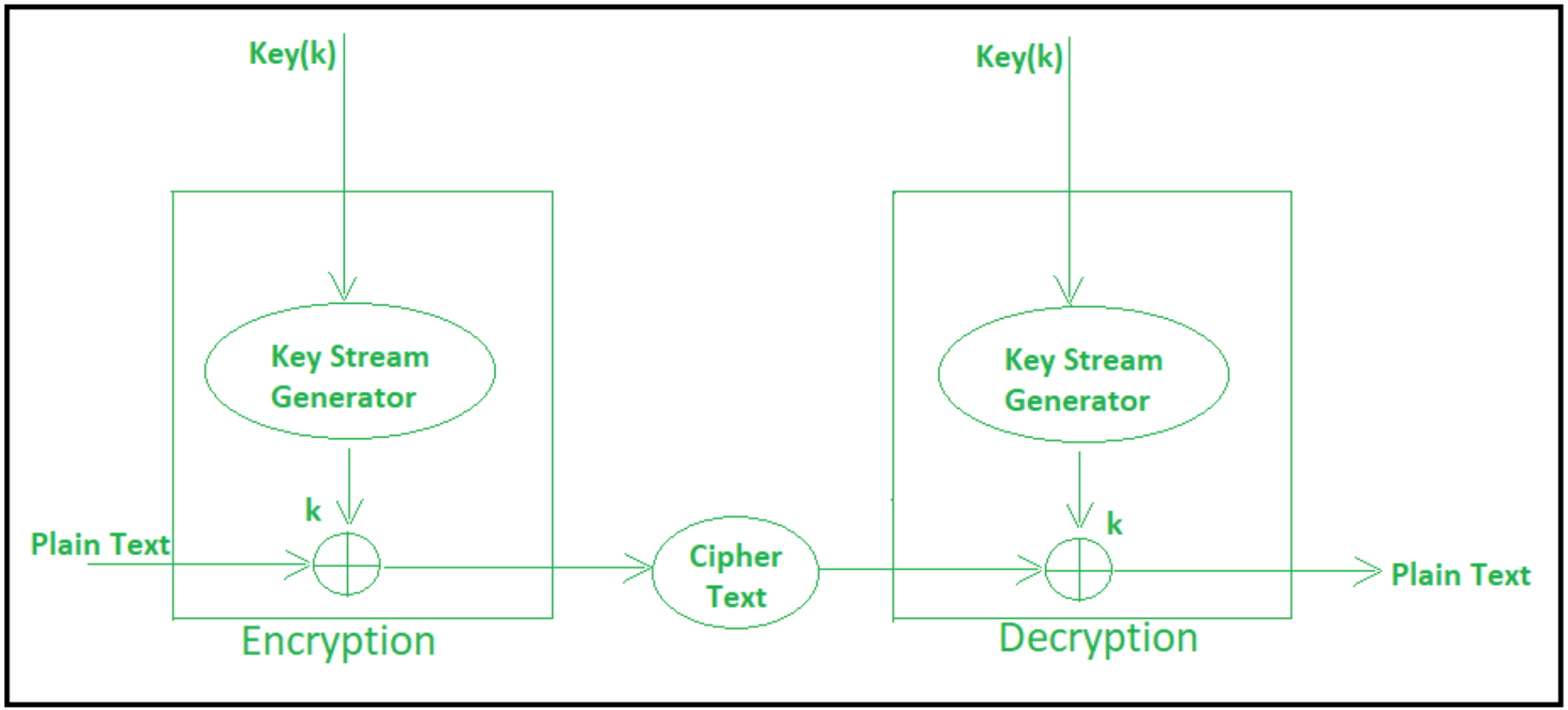
Advanced Encryption Standard (AES),
Data Encryption Standard (DES),
Blowfish
International Data Encryption Algorithm (IDEA).

There are two kinds of symmetric ciphers:

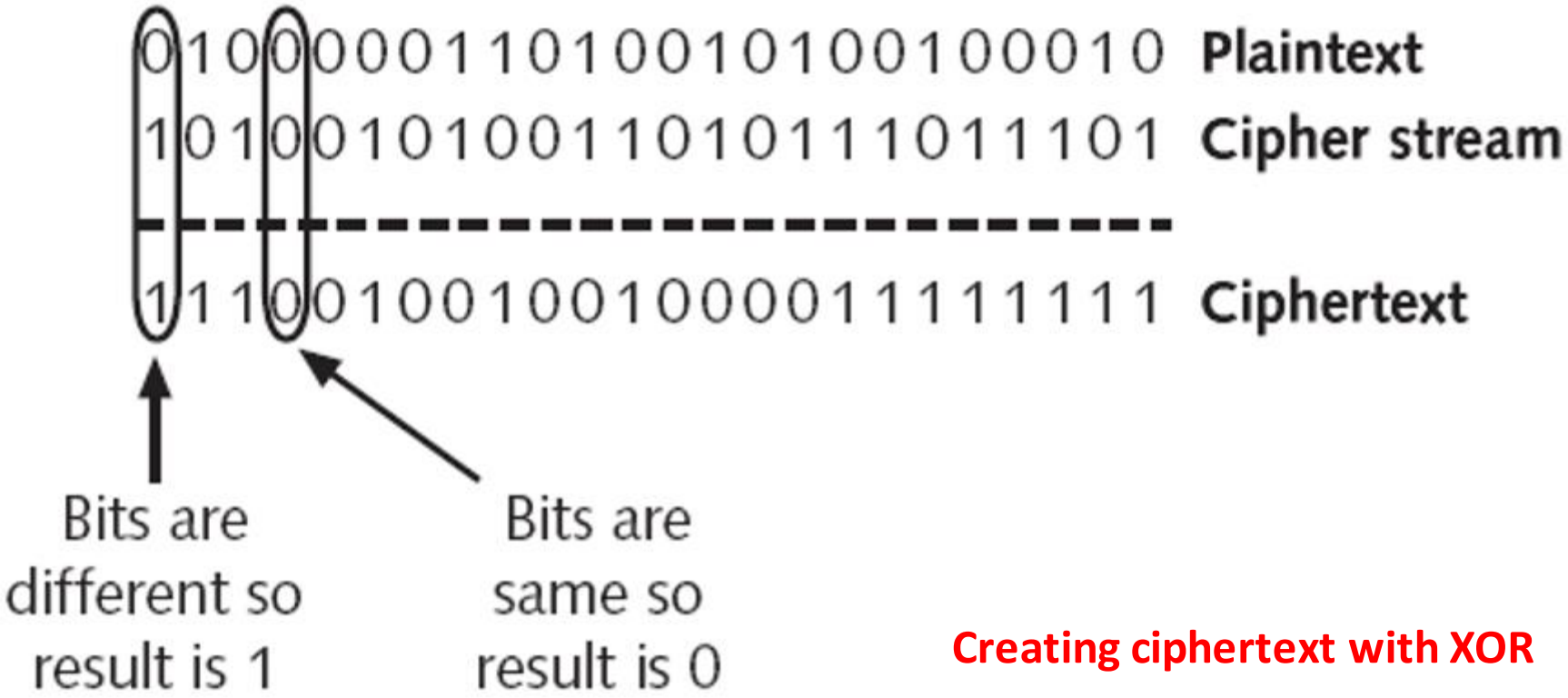
1. **stream ciphers**
2. **block ciphers**

Stream Symmetric Ciphers

A stream cipher is a method of encrypting text (to produce ciphertext) in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time. This method is not much used in modern cryptography. The main alternative method is the block cipher in which a key and algorithm are applied to blocks of data rather than individual bits in a stream.



Stream cipher example:



Creating ciphertext with XOR

The XOR logic is simple to understand. XOR produces an output of 1 when one input is 0, and the other is 1. The output is 0 if either both the inputs are 0 or both the inputs are 1.

Example –

Plain Text : 10011001
Keystream : 11000011
``````````````````````

Cipher Text : 01011010

**Encryption :**
For Encryption,
•Plain Text and Keystream produces Cipher Text (Same keystream will be used for decryption.).
•The Plaintext will undergo XOR operation with keystream bit-by-bit and produces the Cipher Text.

**Decryption :**
For Decryption,
•Cipher Text and Keystream gives the original Plain Text (Same keystream will be used for encryption.).
•The Ciphertext will undergo XOR operation with keystream bit-by-bit and produces the actual Plain Text.

Example –

Cipher Text : 01011010
Keystream : 11000011
``````````````````````

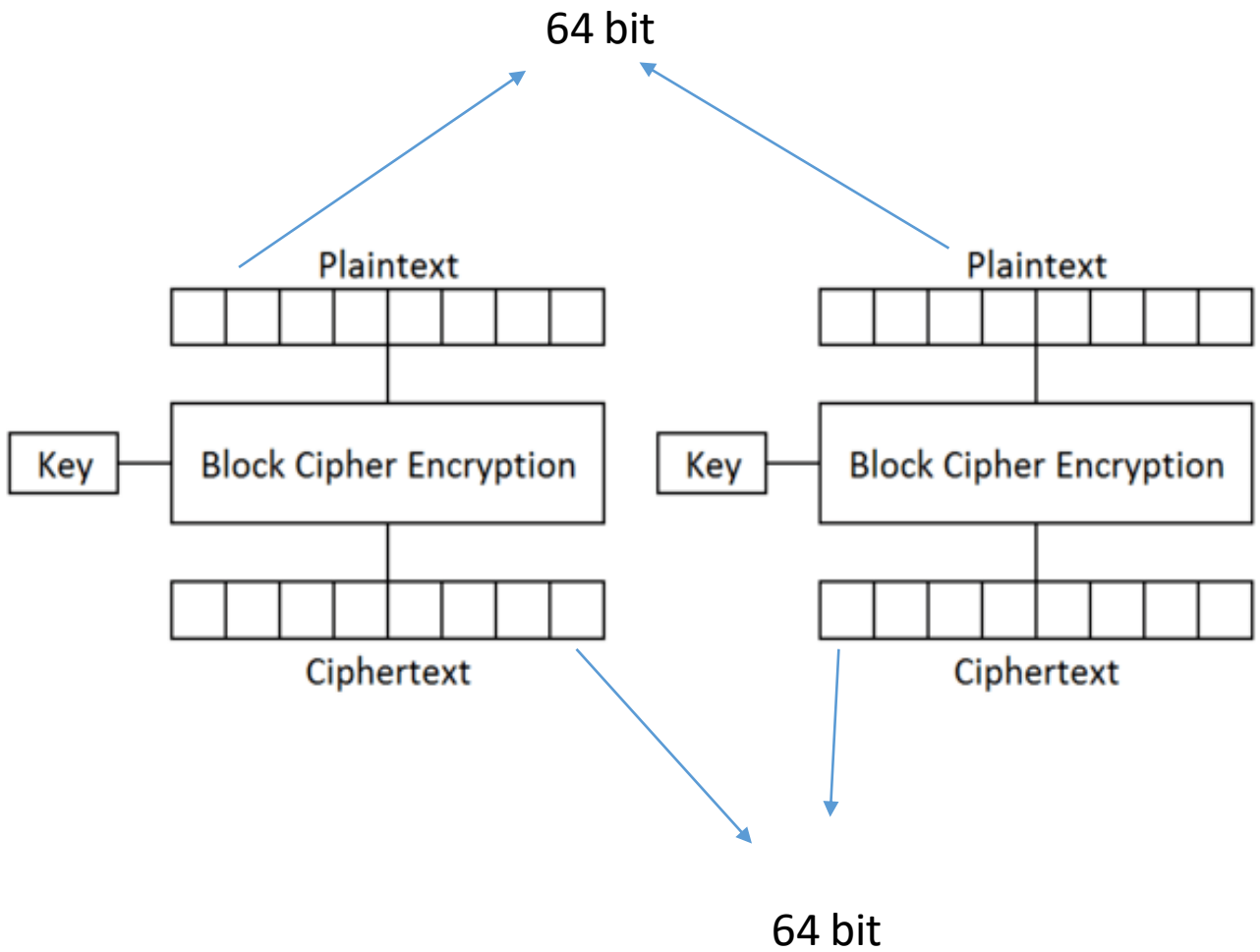
Plain Text : 10011001

NOTE: Decryption is just the reverse process of Encryption i.e. performing XOR with Cipher Text.

Block cipher

Block cipher is an encryption and decryption method which operates on the **blocks** of plain text, instead of operating on each bit of plain text separately.
Each block is of equal size and has fixed no of bits.
The generated ciphertext has blocks equal to the number of blocks in plaintext and also has the same number of bits in each block as of plain text.
Block cipher uses the same key for encryption and decryption

Well-known implementations of the block cipher algorithm are the Data Encryption Standard (DES), TripleDES and the Advanced Encryption standard (AES).


64 bit
Plaintext
Plaintext
Key
Block Cipher Encryption
Key
Block Cipher Encryption
Ciphertext
Ciphertext
64 bit

STREAM CIPHER

VERSUS

BLOCK CIPHER

STREAM CIPHER	BLOCK CIPHER
Type of symmetric key cipher that converts the plain text to cipher text by converting one byte of plain text at a time	Type of symmetric key cipher that converts the plain text into cipher text by converting plaintext block wise at a time
Involves in dividing the plain text to bytes to convert it into cipher text	Involves in dividing the plain text to large blocks to convert it into cipher text
Complex than block cipher	Simpler than stream cipher
Uses 8 bits at a time	Uses 64 bit or more at a time
It is easier to reverse the encrypted text to plain text	It is difficult to reverse the encrypted text to plain text

Conclusion

Block Cipher and Stream Cipher differ in the way in which plain text is **encrypted and decrypted**.

The idea behind **block cipher** is to divide the plain text into blocks further encrypt those blocks.

While **stream cipher** converts plain text bit by bit similar to stream.