CRYPTOGRAPHY & NETWORK SECURITY

SYMMETRIC CIPHERS

Block Ciphers

Vijesh Nair

Symmetric ciphers can also be classified in another way.

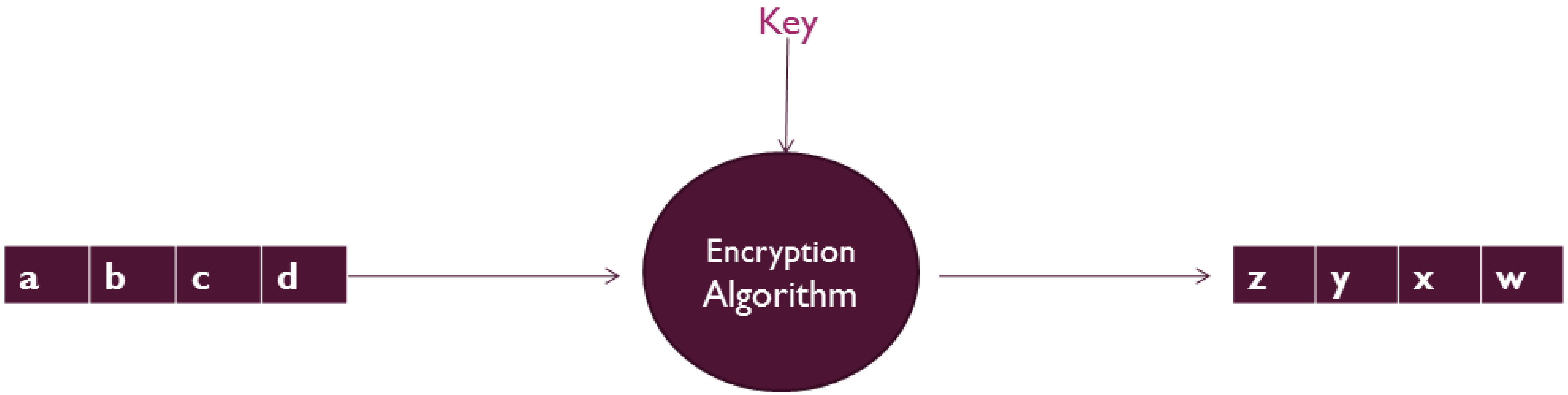
1. Block cipher.
2. Stream cipher.

- Block cipher encrypts & decrypts a block of data at a time.

- Stream cipher encrypts & decrypts a single unit of data at a time.

BLOCK CIPHERS

- A block of plaintext is encrypted to produce a block of cipher text of equal length.
- Uses a single symmetric key for encryption.



Key

a b c d

Encryption Algorithm

z y x w

BLOCK CIPHERS

- The plain text is divided into fixed sized blocks.
- And each block is encrypted.
- The size of the block is preferably large and a multiple of 8.
- If the plain text is not a multiple of block size, padding schemes can be applied.

BLOCK CIPHERS

- The plain text is divided into fixed sized blocks.
- And each block is encrypted.
- The size of the block is preferably large and a multiple of 8.
- If the plain text is not a multiple of block size, padding schemes can be applied.

- Let P = DONTGIVEMONEY
- Let block size be 4;

D	O	N	T	G	I	V	E	M	O	N	E	Y			

BLOCK CIPHERS

- The ciphertext of previous block is applied to the next block.
- Thus even identical blocks will produce different cipher text.

BLOCK CIPHERS

- The ciphertext of previous block is applied to the next block.
- Thus even identical blocks will produce different cipher text.

- 2 identical blocks : ABCD ABCD

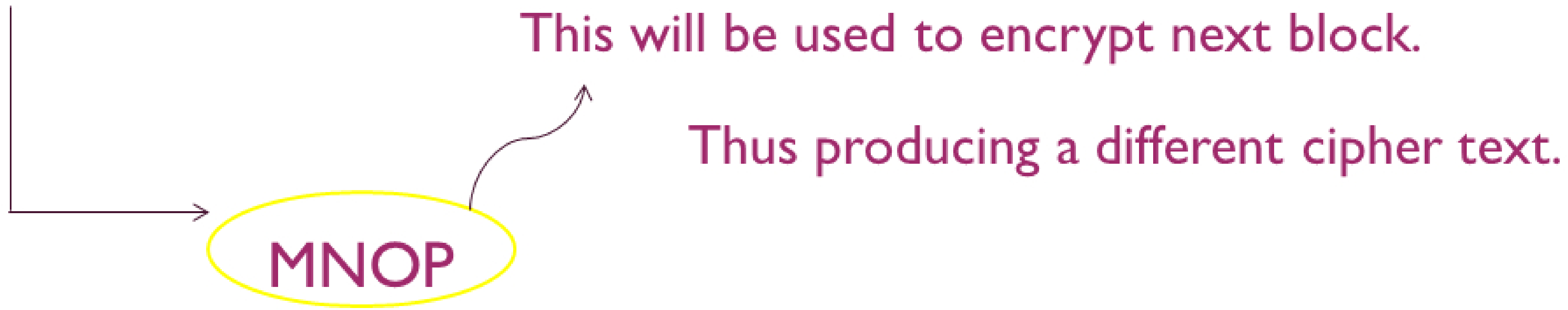
- ABCD ABCD

BLOCK CIPHERS

- The ciphertext of previous block is applied to the next block.
- Thus even identical blocks will produce different cipher text.

- 2 identical blocks : ABCD ABCD

- ABCD ABCD



MNOP

This will be used to encrypt next block.

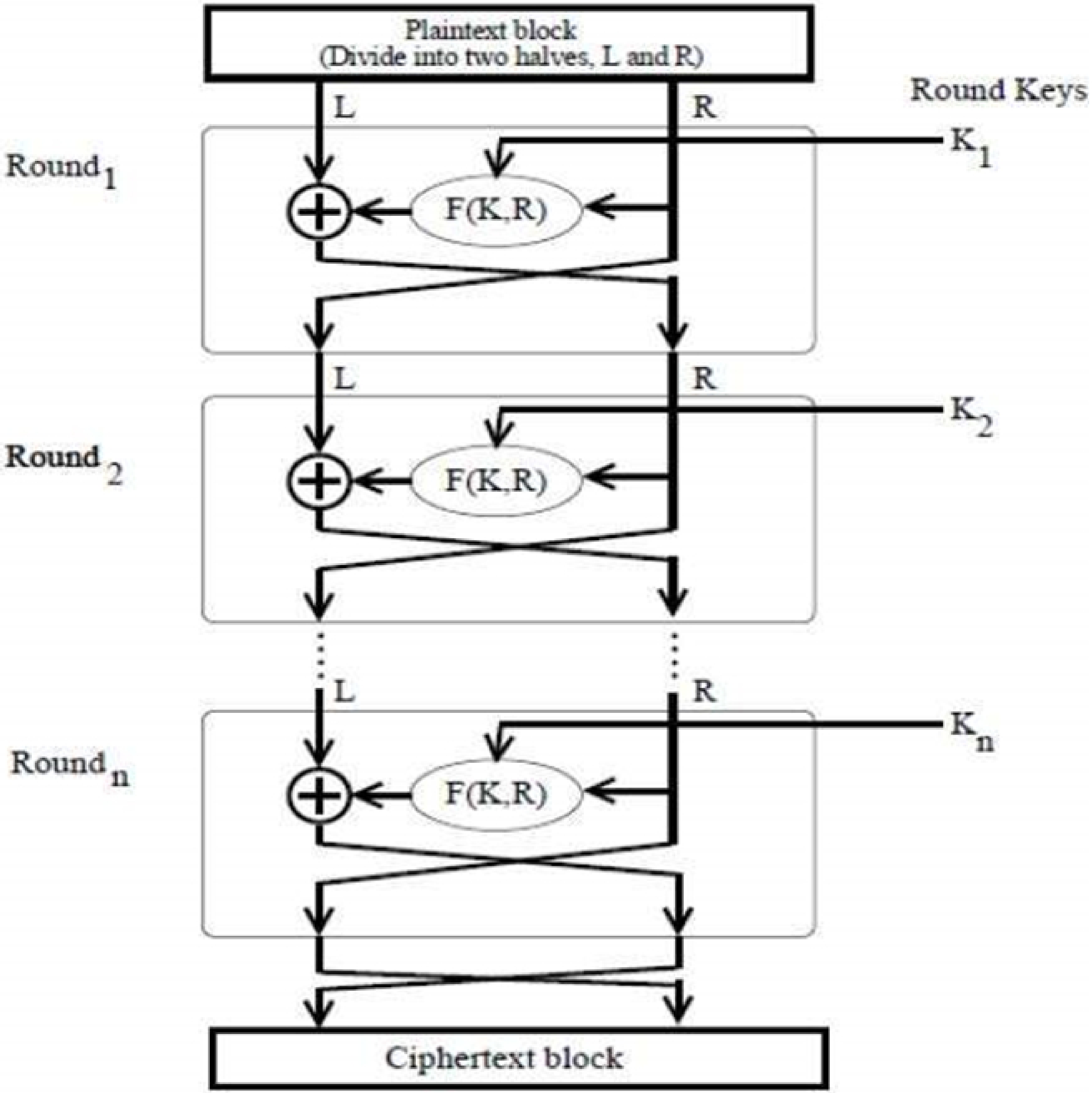
Thus producing a different cipher text.

BLOCK CIPHERS - EXAMPLES

- Data Encryption Standard - DES
- Advanced Encryption Standard - AES
- International Data Encryption Algorithm - IDEA
- Triple DES
- RC5 - Rivest Cipher 5 or Ron's Code 5
- Blowfish Algorithm
- Twofish Algorithm, etc.

FEISTEL STRUCTURE

- A symmetric structure used to construct block ciphers.
- eg:- DES, Triple DES, RC5 etc.
- A number of encryption rounds.
- A round function F.
- A number of sub keys.



Vijesh Nair

THANK YOU

Vijesh Nair