Types of Ciphers

Erukala Suresh Babu

Digitally signed by Erukala Suresh Babu
DN: cn=Erukala Suresh Babu, o=NITW, ou=CSE, email=esbabu@nitw.ac.in, c=IN
Date: 2019.08.27 06:57:39 +05'30'

Dr. E. Suresh Babu

Assistant Professor

Department of CSE

National Institute of Technology, Warangal

Symmetric Algorithm Works

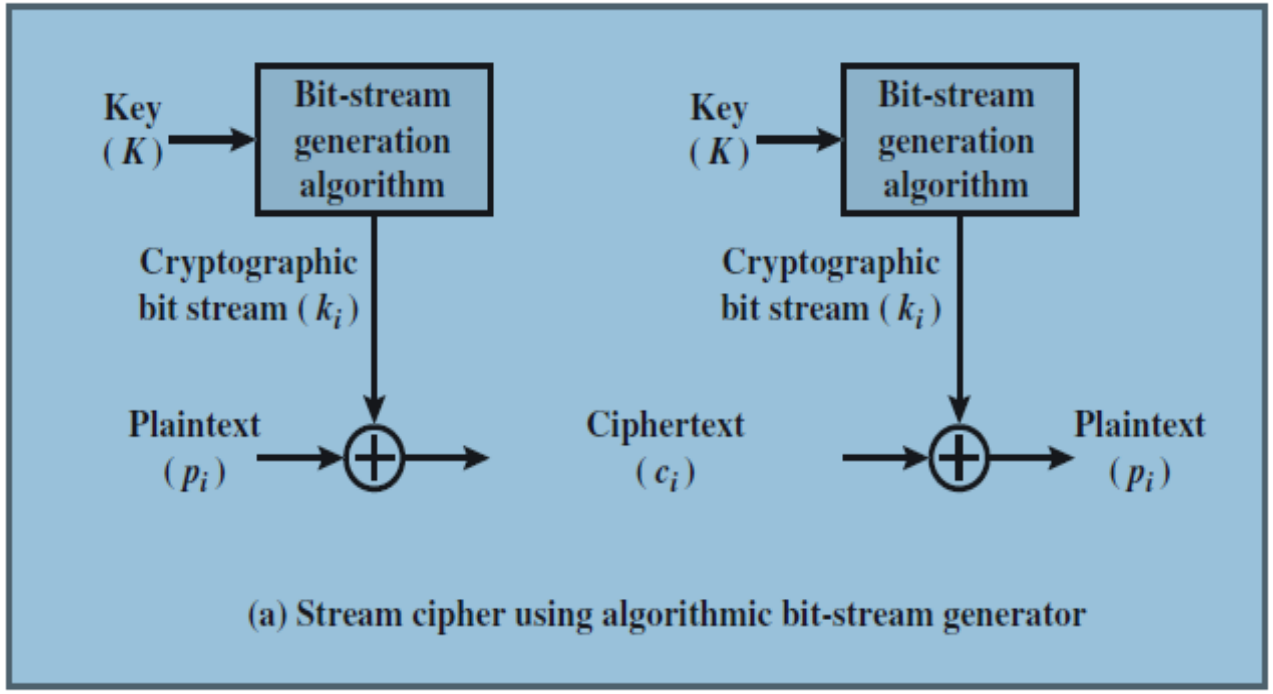
- **Symmetric Algorithms** can be divided into **two categories.**
  - ✓ Some **Symmetric Algorithms** operate on **SINGLE BIT or BYTE**
  - ✓ Some Other **Symmetric Algorithms** operate on **GROUPS OF BITS**.

Stream Cipher

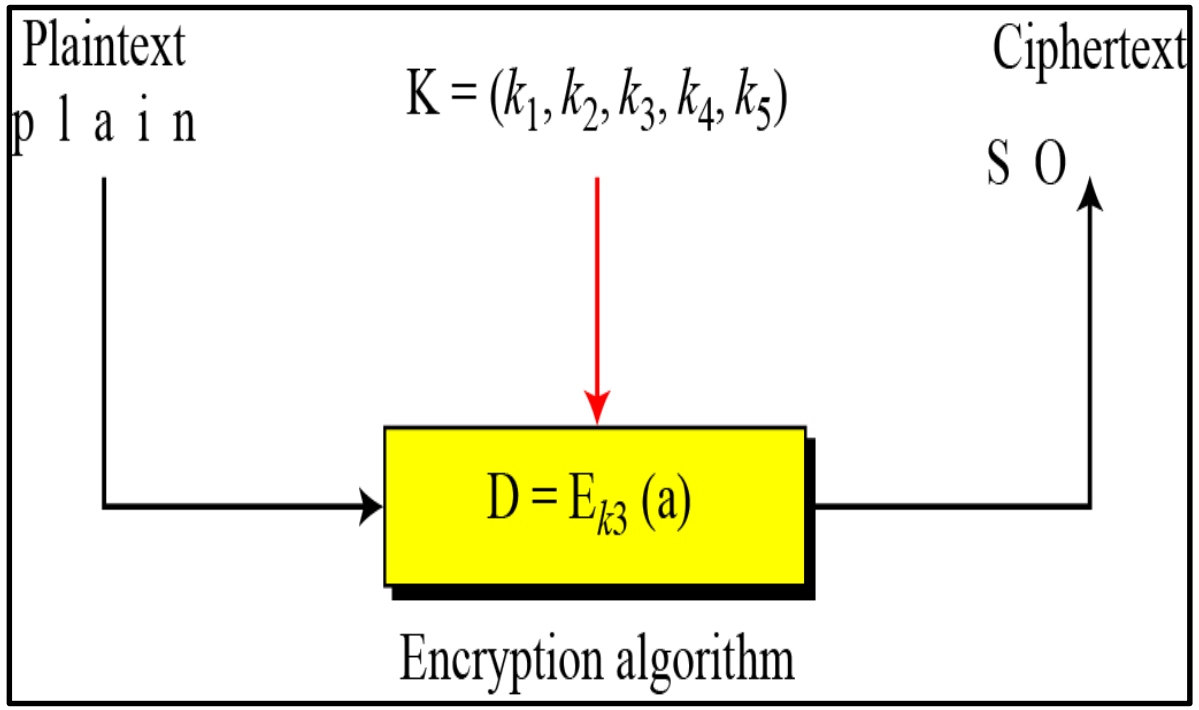
Stream Cipher

- Some **Symmetric Algorithms** operate on the **plaintext** a **SINGLE BIT or BYTE** at a time;
  - ✓ These are called **Stream Algorithms** or **Stream Ciphers**.

Stream Cipher



(a) Stream cipher using algorithmic bit-stream generator

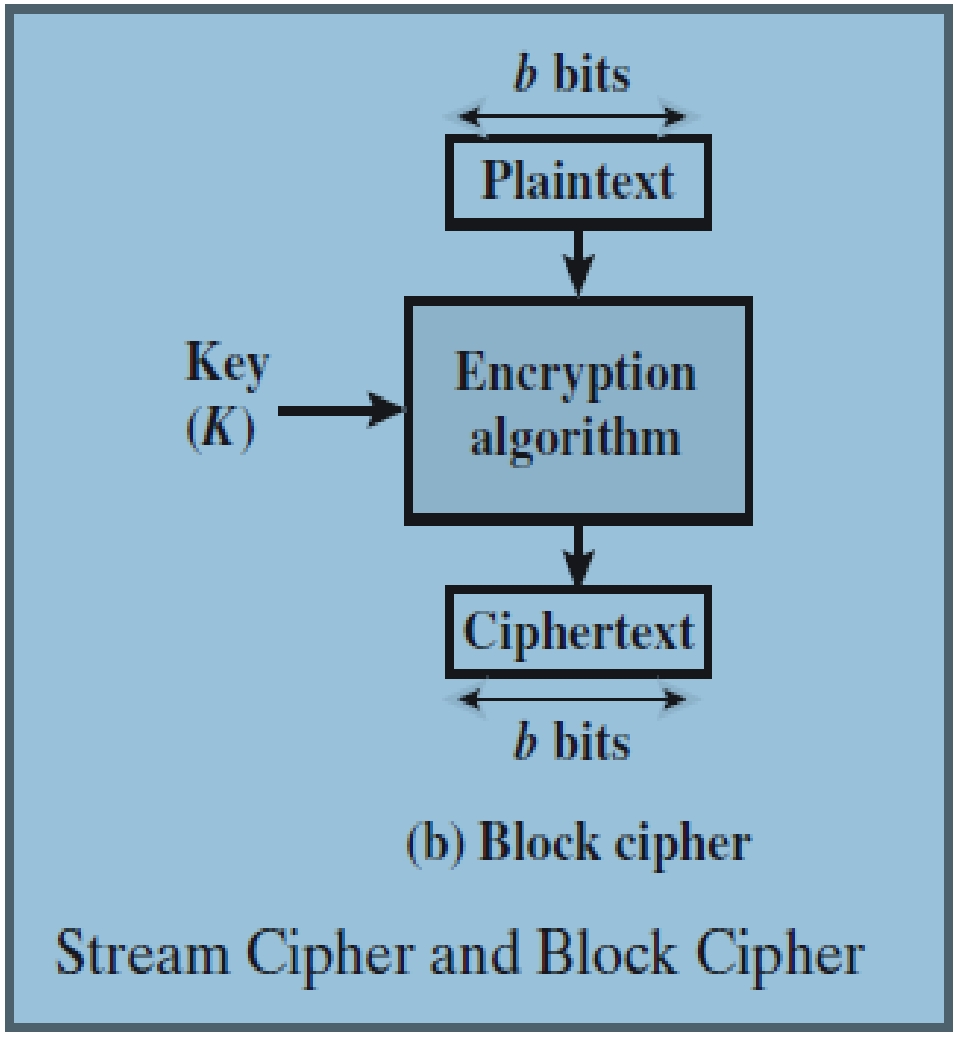


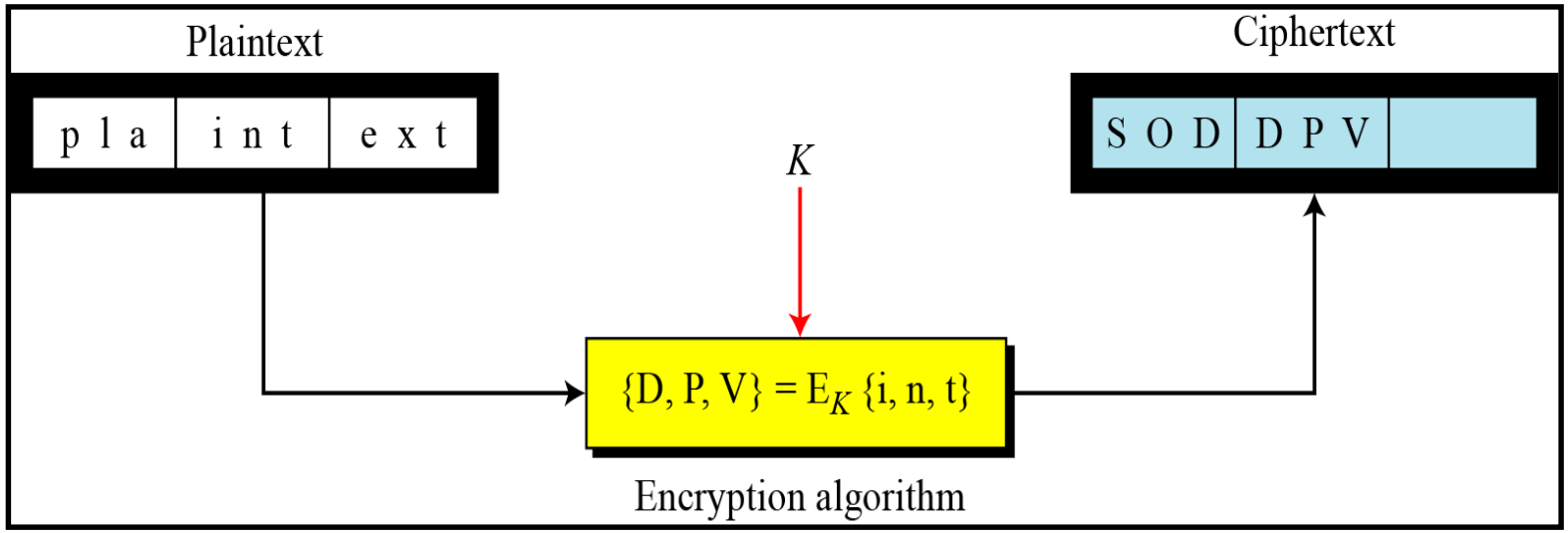
Blocks Ciphers

Blocks Ciphers

- Some Other Symmetric Algorithms operate on the plaintext in GROUPS OF BITS
  - ✓ The groups of bits are called BLOCKS, and the algorithms are called Block Algorithms or Block Ciphers.
  - ✓ Modern Computer Algorithms, works on typical Blocks

Blocks Ciphers





Observation

- Many Symmetric Block Encryption Algorithms are based on a Feistel block cipher structure

Feistel Block Ciphers

Introduction

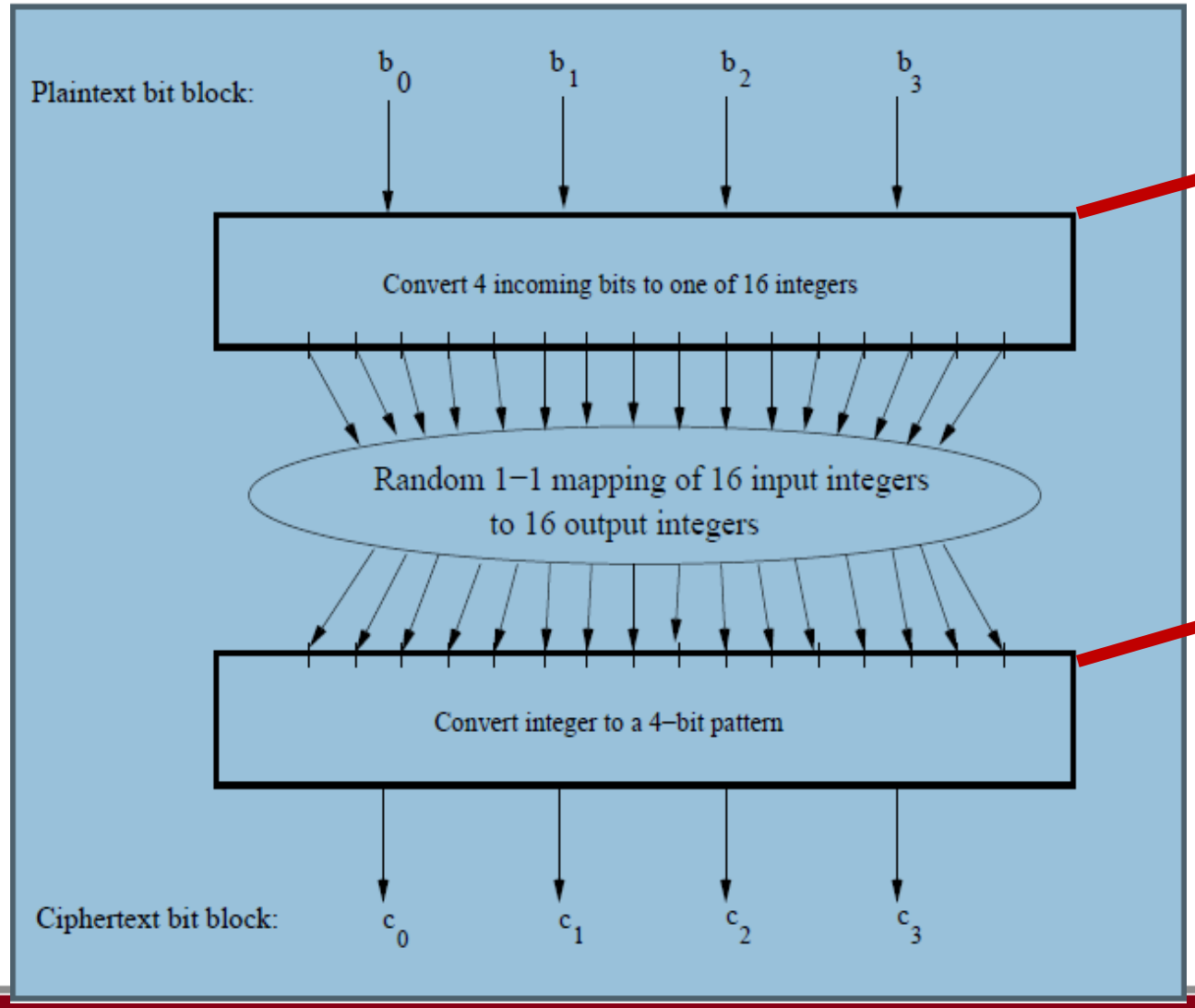
- We begin with the motivation for the Ideal block cipher. Finally, we discuss about Feistel block cipher structure.

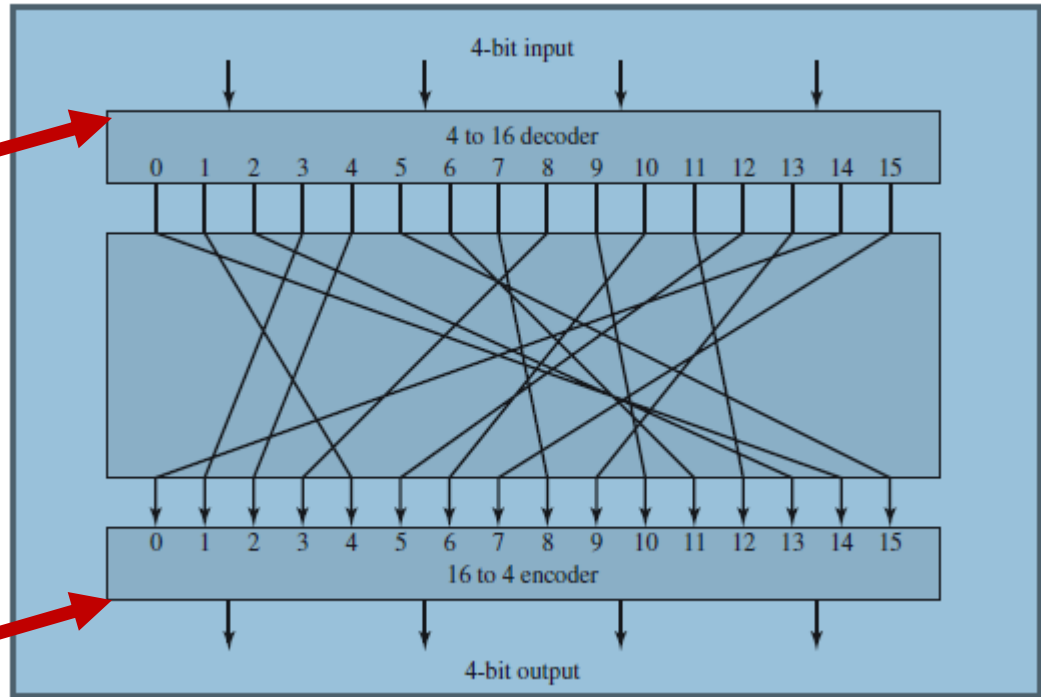
Ideal Cipher Structure

Ideal Cipher Structure

- The logic of a **general substitution cipher** for **n=4**
  - ✓ A 4-bit input produces one of 16 possible input states, which is mapped by the substitution cipher into a unique one of 16 possible output states, each of which is represented by 4 cipher text bits

Ideal Cipher Structure (n=4)





Ideal Cipher Structure

- To understand Figure , Note that there are **16 different possible**

4-bit patterns.

Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Ciphertext	Plaintext
0000	1110
0001	0011
0010	0100
0011	1000
0100	0001
0101	1100
0110	1010
0111	1111
1000	0111
1001	1101
1010	1001
1011	0110
1100	1011
1101	0010
1110	0000
1111	0101

Ideal Cipher Structure

- In an Ideal Block Cipher, the relationship between the input blocks and the output block is completely random. But it must be **invertible for decryption** to work.
- Ideal Block Cipher will have one-to- one,
  - ✓ Each input block is mapped to a **unique output block.**
  - ✓ The mapping itself constitutes the key

Ideal Cipher Structure

- The Encryption Key for the ideal block cipher is the **codebook itself,** meaning the table that shows the relationship between the input blocks and the output blocks.

The Size of the Encryption Key for the Ideal Block Cipher (n=4)

- The key that determines the specific mapping from among all possible mappings.
- In this case, using this straightforward method of defining the key, the required key length is **(4 Key) X (16 Rows) = 64 bits.**

Observation

- In general, for an n-bit ideal block cipher, the length of the key defined as **n X 2^n bits.**
- For a 64-bit block, which is a desirable length to thwart statistical attacks, the required key length is **$64 * 2^{64} = 2^{70} \approx 10^{21}$bits.**
- That implies that the **encryption key for the ideal block cipher** using **64-bit blocks** will be of **size 10^{21}.**

Limitation of Ideal Block Cipher

- The **size of the encryption key** would make the **ideal block cipher** an **impractical idea.**
  - ✓ Think of the **logistical issues** related to the **transmission, storage,** and **processing** of such **LARGE KEYS.**

Feistel Block Ciphers:
Feistel Cipher Structure

Motivation for the Feistel Cipher Structure

- In a **Modern Block Cipher** (but still using a **Classical Encryption Method),**
  - ✓ we replace a **block of N bits** from the **plaintext** with a **block of N bits** from the **cipher text.**
  - ✓ There are possible different **2^n plaintext blocks**

Feistel Cipher Structure

- Feistel Cipher named after the IBM cryptographer Horst Feistel and first implemented in the **Lucifer cipher** by **Horst Feistel and Don Coppersmith.**
- A Cryptographic System based on Feistel structure uses the same basic algorithm for both **Encryption** and **Decryption.**

Observations on Feistel Cipher

- In particular, **Feistel proposed** the **use of a cipher** that alternates both
  - ✓ **Substitutions and**
  - ✓ **Permutations**,

Claude Shannon: Substitution-Permutation Ciphers

Claude Shannon : Substitution-Permutation Ciphers

- Claude Shannon's [1949 paper] has the key ideas that led to the development of modern block ciphers.
- S-P Networks are based on the Two Primitive Cryptographic Operations:
  - ✓ **Substitution (S-box)**
  - ✓ **Permutation (P-box)**

S-Box and P-Box Ciphers

- Claude Shannon Principle was groups of S-boxes separated by a larger P-box to form the S-P network,

1. **Substitution(S-box) :** S-box is a Keyless fixed Substitution Cipher
2. **Permutation(P-box) :** P-box is a Keyless fixed Transposition Cipher

Feistel Cipher Uses Proposal of Shannon Principle

Feistel Cipher Uses Proposal of Shannon Principle

- Shannon ideas of introducing the confusion and diffusion, notionally provided by **S-boxes** and **P-boxes.**
  - ✓ **S-Box** uses **Confusion**
  - ✓ **P-Box** uses **Diffusion**
- Shannon was concern to frustrate cryptanalysis based on **statistical analysis**.

Diffusion Operation

Diffusion Operation

- **Diffusion** hides the relationship between the plain text and cipher text.
- The mechanism of diffusion seeks to make the statistical relationship between the plaintext and ciphertext as complex as possible in order to Hacker, who make the attempts to deduce the key

Diffusion (P) Boxes

❖ Straight Boxes

Example

24X24 Box

01	15	02	13	06	17	03	19	09	04	21	11
14	05	12	16	18	07	24	10	23	08	22	20

❖ Expansion Boxes

Example

12X24 Box

01	03	02	01	06	17	03	07	09	04	09	11
02	05	12	04	06	07	12	10	11	08	10	08

❖ Compression Boxes

Example

24X12 Box

01	15	02	13	06	17	03	19	09	04	21	11

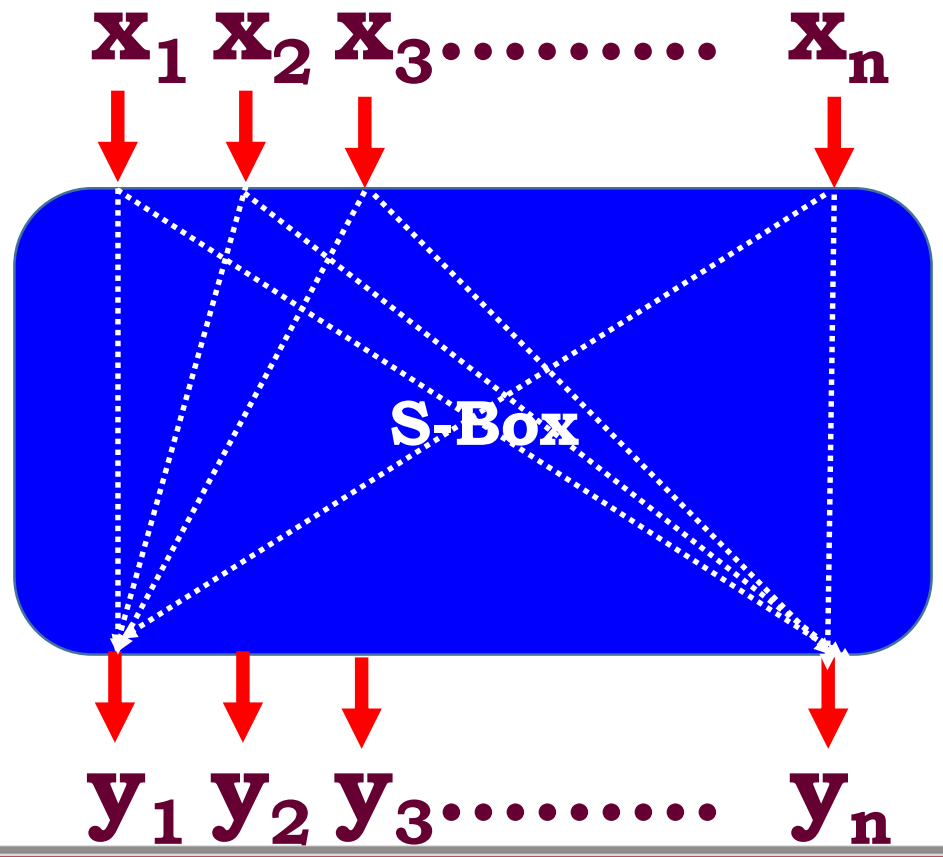
Confusion Operation

- **Confusion** hides the relationship between the cipher text and Key
- The mechanism of **Confusion** seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again(Hacker) in order to make the attempts to discover the key.

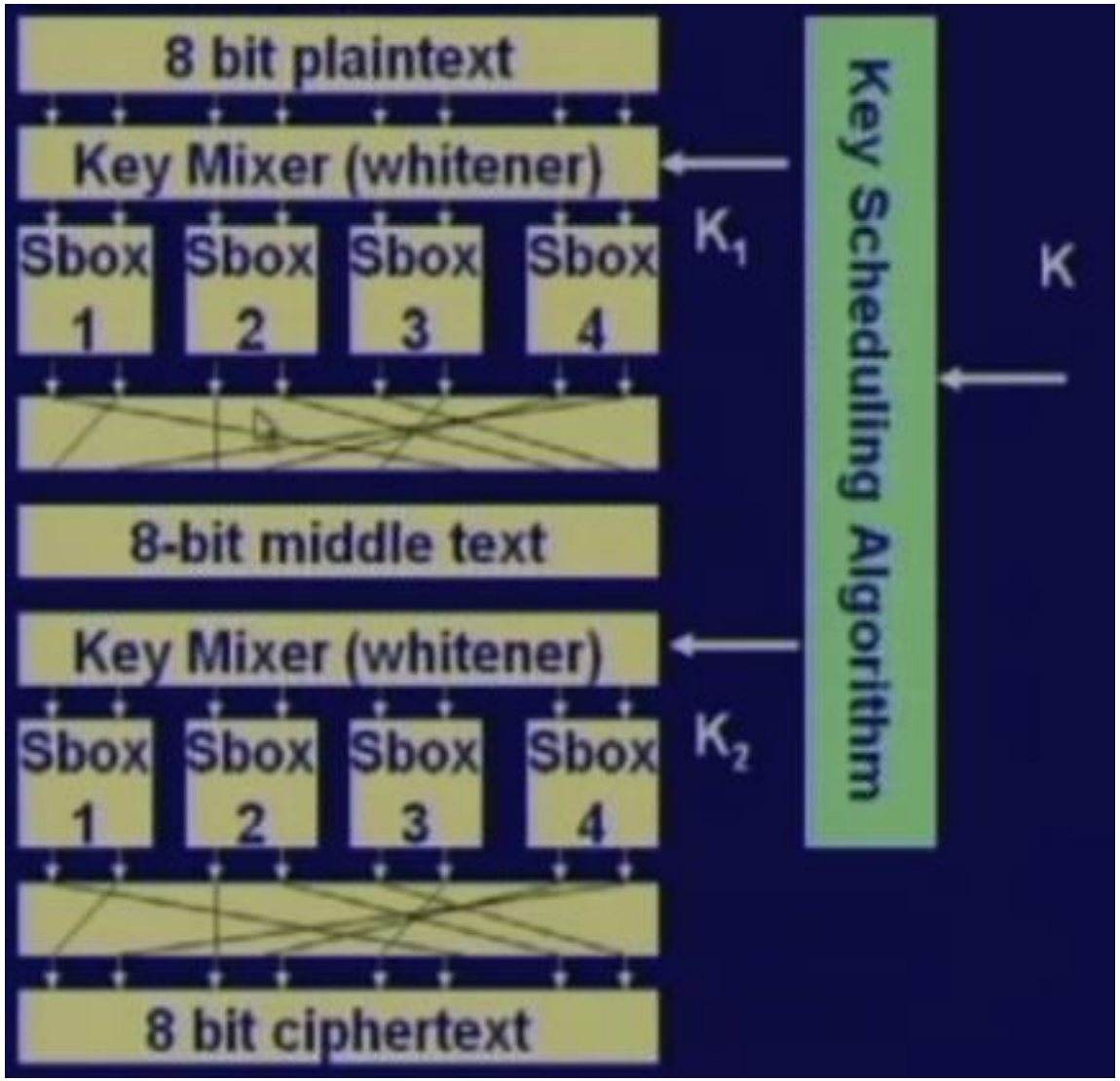
Confusion (S-Box) Operation

- An **S-Box (Substitution Box)** is a **m X n Matrix** where **m,n are not necessary same**

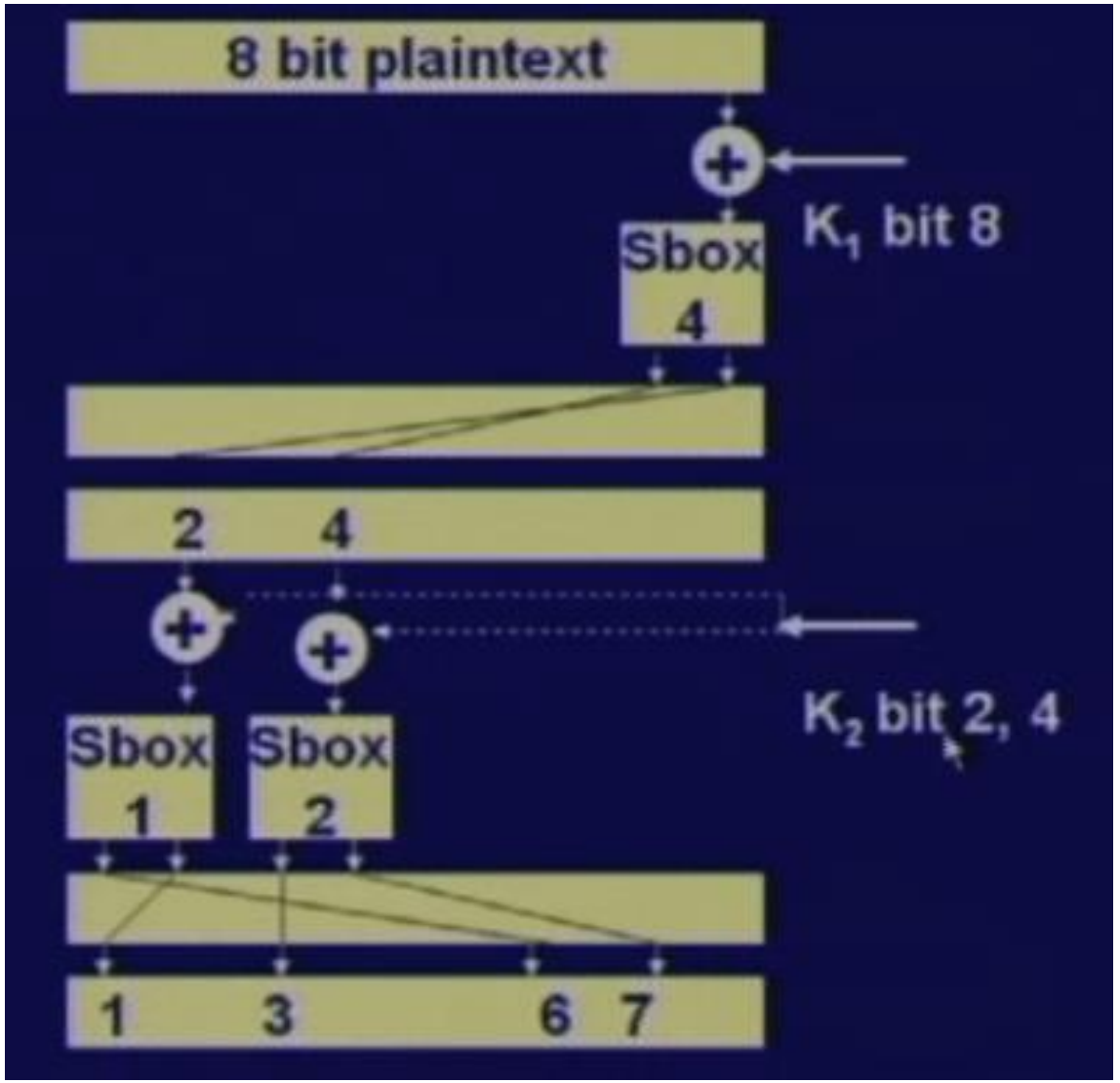
$$
\begin{aligned}
y_1 &= f_1\,(x_1, x_2, x_3 \ldots\ldots\ldots x_n)\\
y_2 &= f_2\,(x_1, x_2, x_3 \ldots\ldots\ldots x_n)\\
y_3 &= f_3\,(x_1, x_2, x_3 \ldots\ldots\ldots x_n)\\
&\vdots\\
y_m &= f_m\,(x_1, x_2, x_3 \ldots\ldots\ldots x_n)
\end{aligned}
$$



Product Cipher with Two Round Keys



Diffusion and Confusion

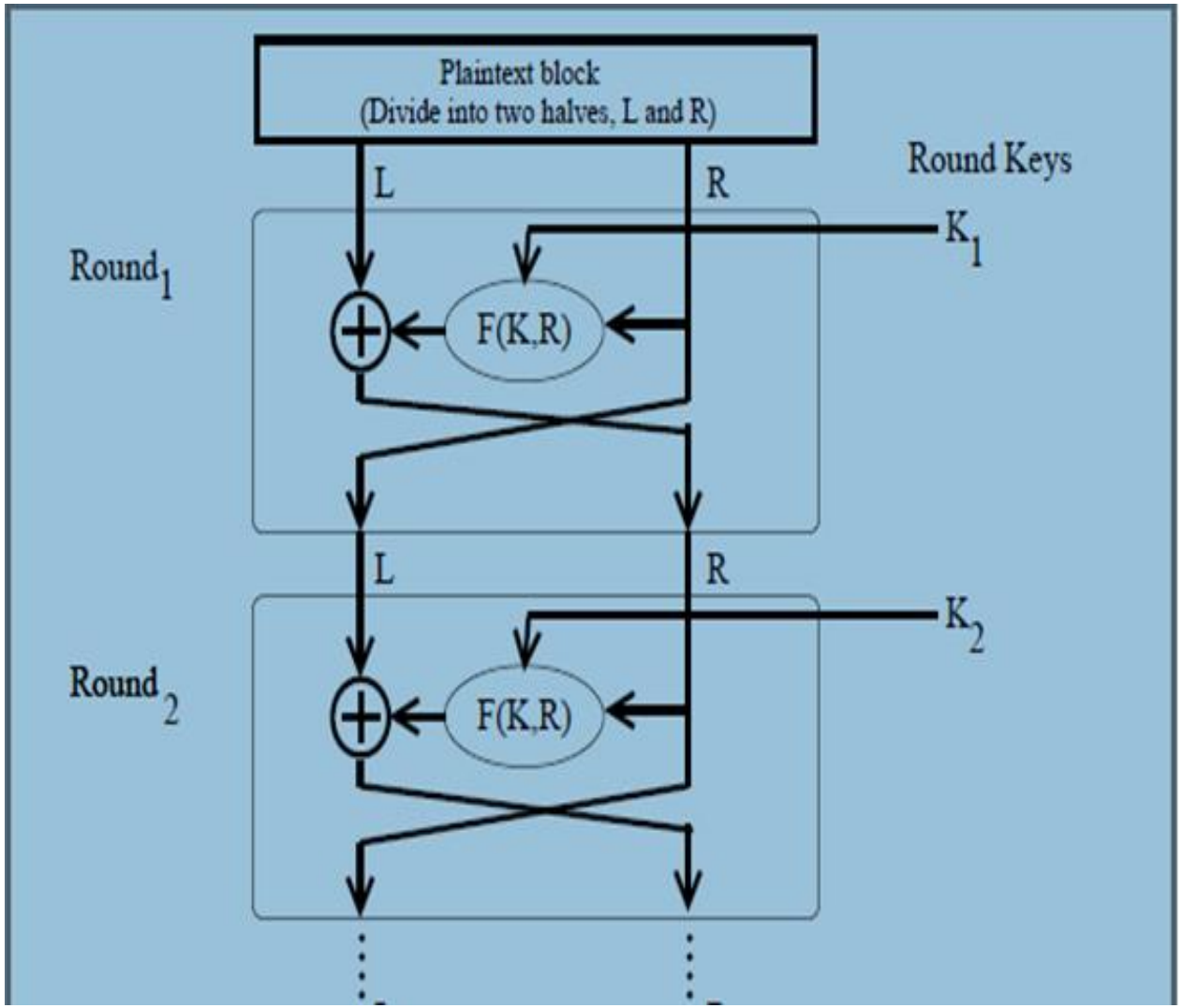


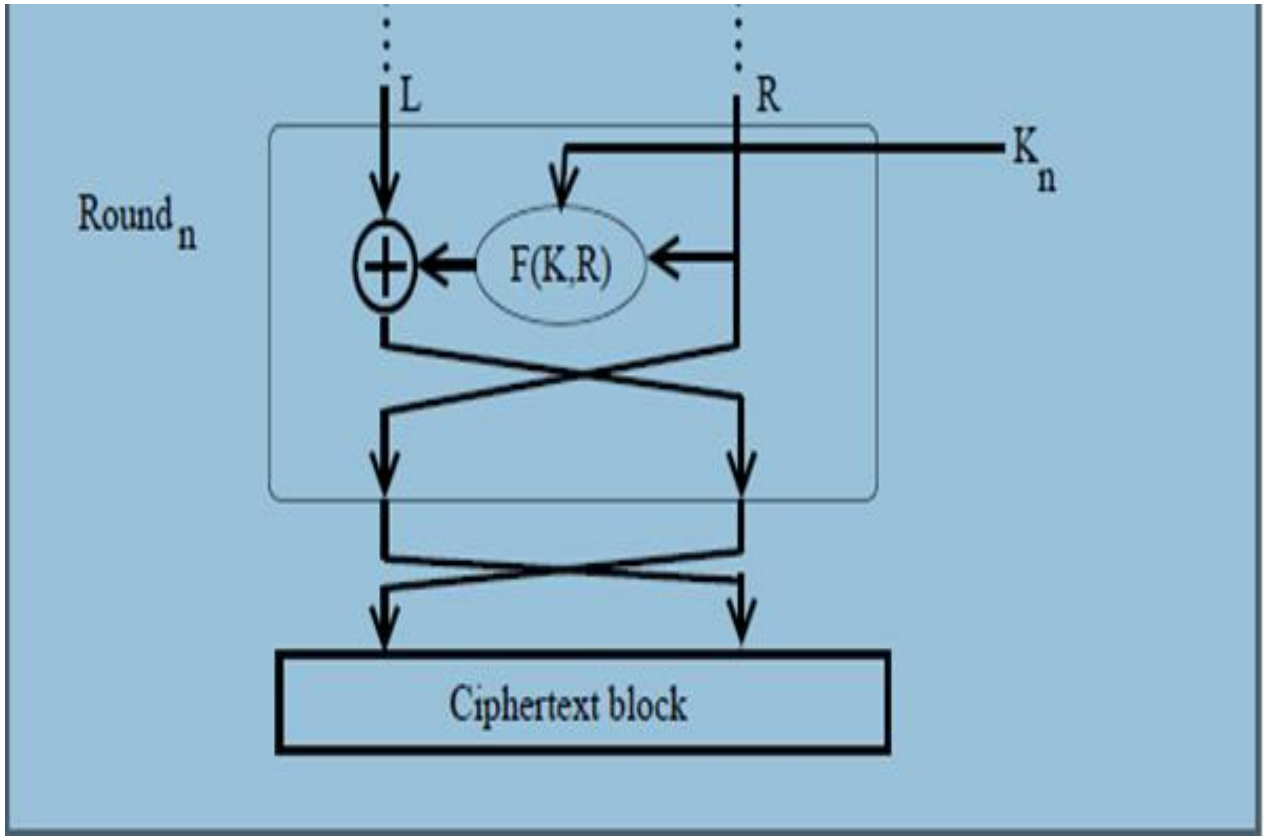
Feistel Cipher Structure

Feistel Cipher Structure

- **Horst Feistel** invented the feistel cipher based on concept of invertible product cipher
- The Feistel structure consists of multiple rounds of processing of the plaintext,
  - ✓ Each round consisting of a "substitution" step followed by a permutation step.

Feistel Cipher Structure





Feistel Cipher Design Parameters

Feistel Cipher Design Parameters

❖ **Feistel Cipher** depends on the choice of the **following parameters** and **design features:**

- ✓ **Block size**
- ✓ **Key size**
- ✓ **Number of rounds**
- ✓ **Sub key generation algorithm**
- ✓ **Round function F**

Parameters : Block size

- **Larger block sizes** mean greater security
  - ✓ The greater security is achieved by greater diffusion.
  - ✓ Traditionally, a block size of 64 bits in block cipher design.
  - ✓ The new AES uses a 128-bit block size.
- But reduces encryption/decryption speed for a given algorithm.

Parameters : Key Size

- **Larger key** size means greater security
  - ✓ The greater security is achieved by greater resistance to brute-force attacks and greater confusion.
  - ✓ Key sizes of 64 bits or less are now widely considered
  - ✓ Later,128 bits has become a common size.
- Decrease encryption/decryption speed due to Larger key

Parameters : Number of Rounds

- The essence of the **Feistel cipher** is that
  - ✓ A single round offers inadequate security but that multiple rounds offer increasing security.
  - ✓ A typical size is **16 rounds.**

Parameters : Sub key generation algorithm

- **Greater complexity** in this algorithm should lead to **greater difficulty of cryptanalysis.**

Parameters : Round Function

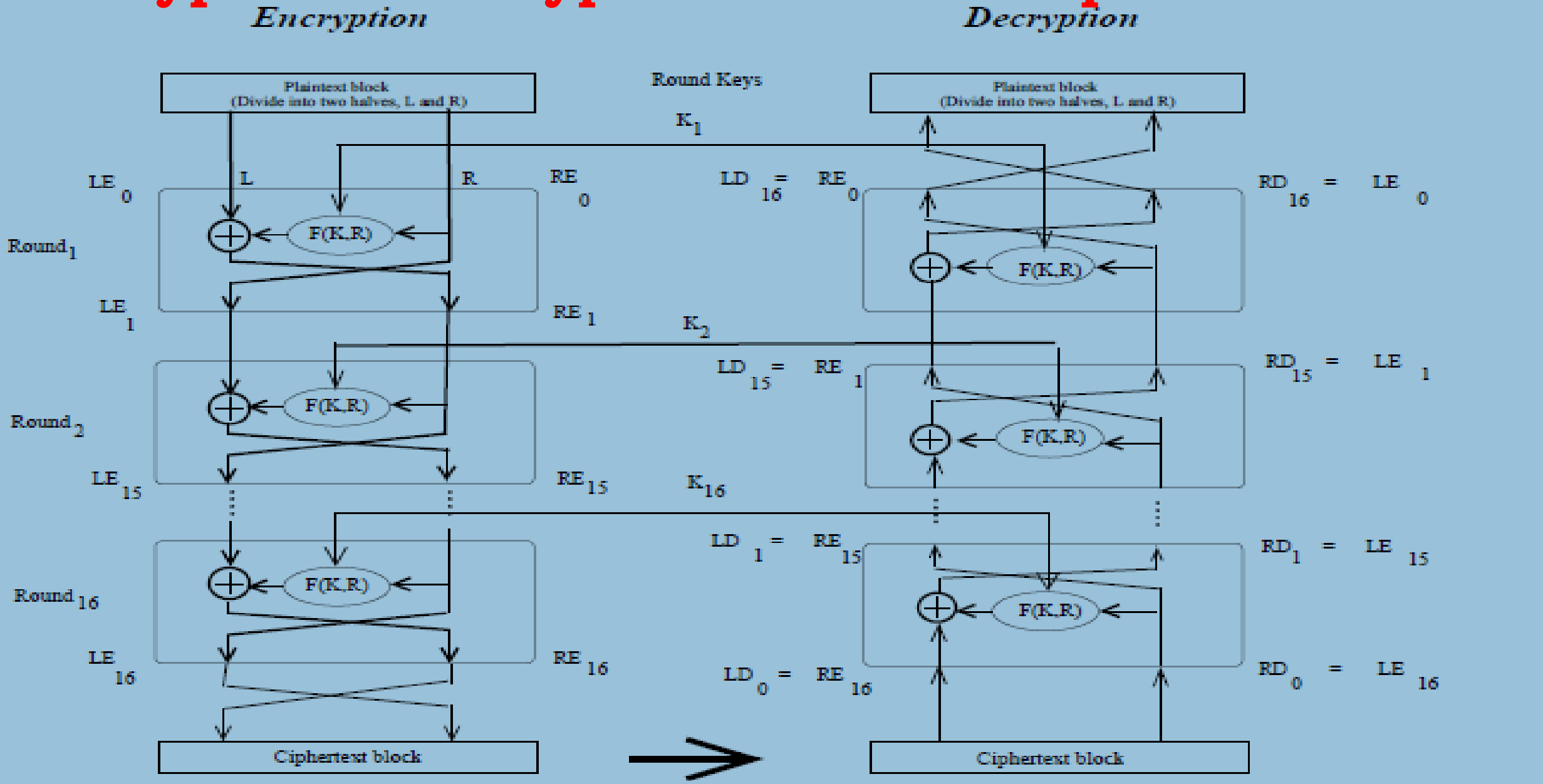
- **Greater complexity** generally means **greater resistance** to **cryptanalysis.**

Decryption of Feistel Cipher

Decryption in Ciphers Based on the Feistel Structure

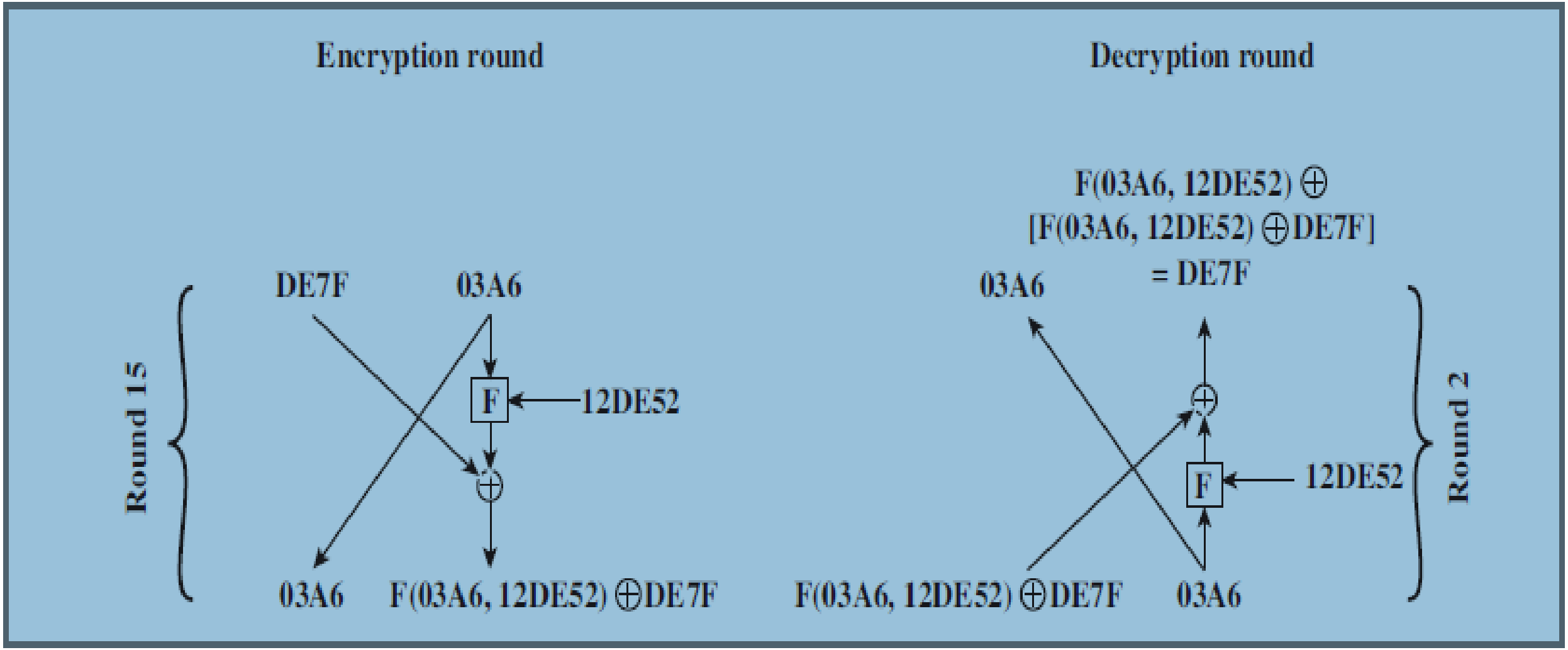
- As shown in Figure, the **Decryption Algorithm** is exactly the same as the **Encryption Algorithm** with the only difference that the **Round Keys** are used in the **reverse order** $\{k_n, k_{n-1}, k_{n-2} \ldots k_1\}$.

Encryption & Decryption of Feistel Ciphers Structure



Example : Feistel Cipher

Feistel Example



Thank U