Block Cipher

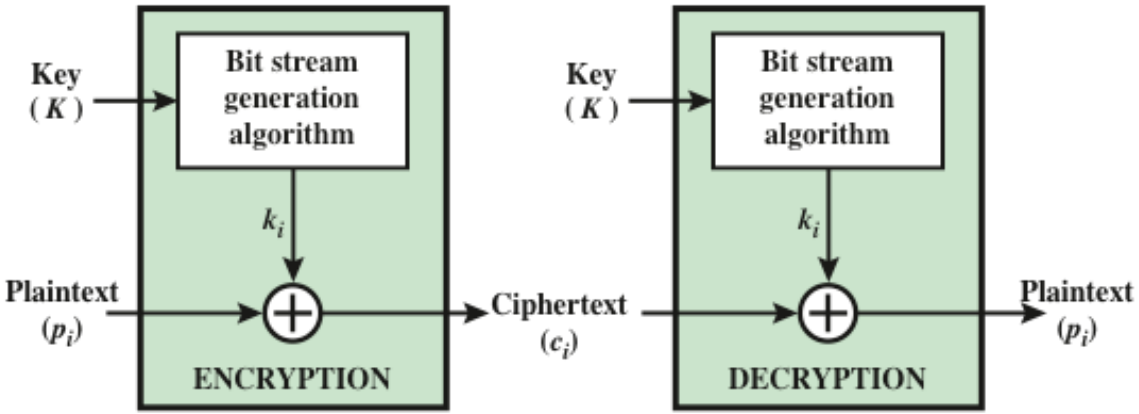
Dr. Mana Khatua
Assistant Professor
Dept. of CSE, IIT Guwahati
Email: manaskhatua@iitg.ac.in

Stream Cipher vs Block Cipher

Stream Cipher:

Encrypts a digital data stream **one bit or one byte at a time**

e.g. RC4, Autokeyed Vigenere Cipher, Vernam Cipher



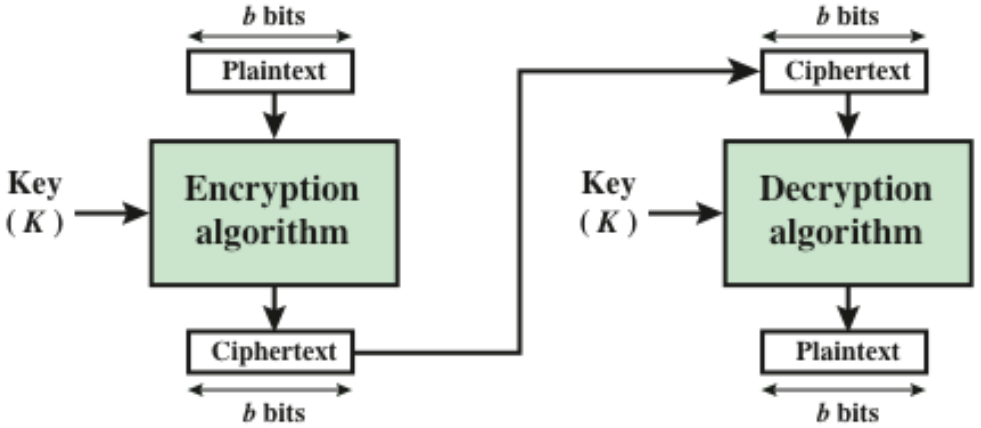
If the cryptographic keystream (k_i) is random, stream cipher is unbreakable!

Issue: keystream must be provided to both users in advance via independent and secure channel.

Block Cipher:

A block of plaintext is treated as a whole and used to produce a ciphertext block of equal length

e.g. DES, AES



Typically a block size of 64 or 128 bits is used.

Majority of network-based symmetric cryptographic applications use block ciphers.

Reversible or Nonsingular Mapping

Reversible Mapping	
Plaintext	**Ciphertext**
00	11
01	10
10	00
11	01

Irreversible Mapping	
Plaintext	**Ciphertext**
00	11
01	10
10	01
11	01

Let, a block cipher operates on a plaintext block of *n* bits to produce a ciphertext block of *n* bits.

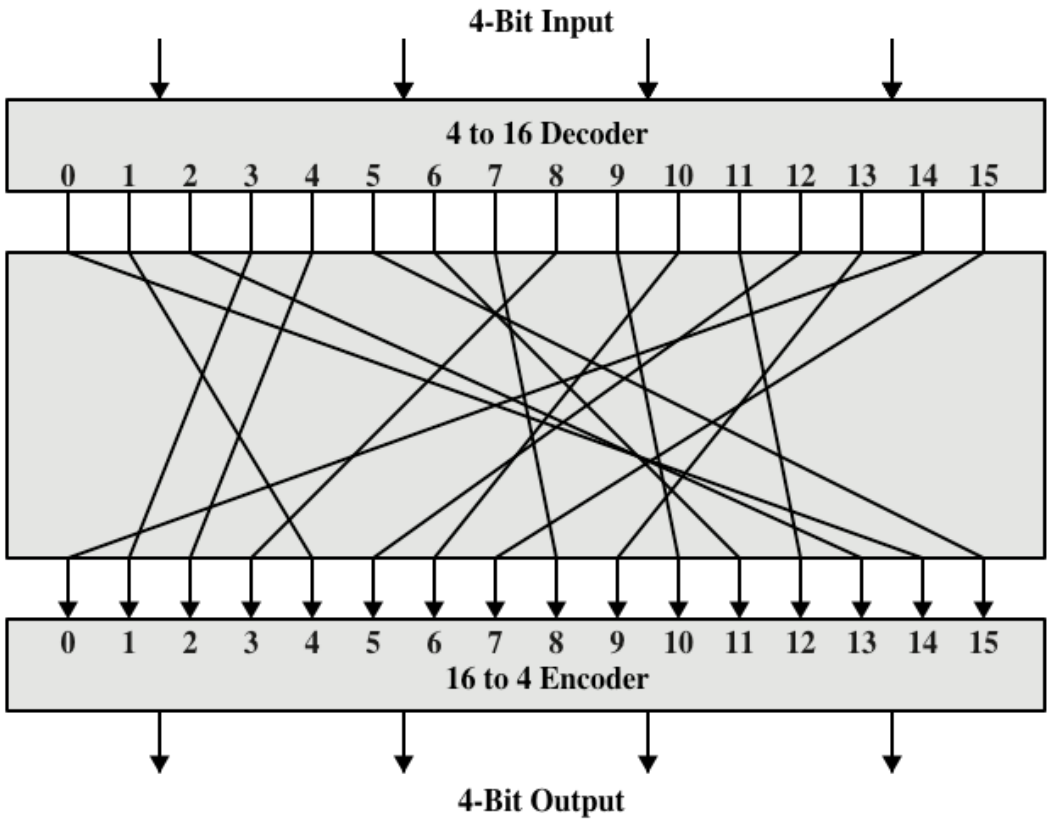
There are 2^n possible different plaintext blocks.

For the encryption to be **reversible** (i.e., for decryption to be possible), **each must produce a unique ciphertext block.**

So, if we limit ourselves to reversible mappings, the number of different transformations is $(2^n!)$.

Points to Ponder: Prove the above statement

Ideal Block Cipher



General *n*-bit-*n*-bit Block Substitution (for *n* = 4)

Ideal Block Cipher: allows for the maximum number of possible reversible encryption mappings from the plaintext block.

This is most general form of block cipher following substitution method. It can be used to define any reversible mapping between plaintext and ciphertext.

A snapshot of Encryption & Decryption Tables:

Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111

Ciphertext	Plaintext
0000	1110
0001	0011
0010	0100
0011	1000
0100	0001
0101	1100

Issue: Vulnerable to a statistical analysis of the plaintext if the block size is small.

Impracticality of Ideal Block Cipher

Small block size is vulnerable to attack.

Very large block size is impractical from the implementation and performance point of view!

For such a transformation, mapping itself constitutes the key.

For one particular reversible mapping from plaintext to ciphertext when n = 4, the required key length is (4 bits) x (16 rows) = 64 bits.

Points to Ponder: Prove the above statement

So, for an *n*-bit ideal block cipher, the length of the key defined in this fashion is ($n \times 2^n$) bits!

If n=64 bit, the key length is $\approx 10^{21}$ bits !!

Encryption

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

Decryption

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

Cont...

To make its implementation tractable, confine ourselves to a subset of the $2^n!$ possible reversible mappings.

Let, we define the mapping in terms of a set of linear equations.

$$y_1 = k_{11}x_1 + k_{12}x_2 + k_{13}x_3 + k_{14}x_4$$
$$y_2 = k_{21}x_1 + k_{22}x_2 + k_{23}x_3 + k_{24}x_4$$
$$y_3 = k_{31}x_1 + k_{32}x_2 + k_{33}x_3 + k_{34}x_4$$
$$y_4 = k_{41}x_1 + k_{42}x_2 + k_{43}x_3 + k_{44}x_4$$

Where,

- x_i are the four binary digits of the plaintext block
- y_i are the four binary digits of the ciphertext block
- k_{ij} are the binary coefficients
- arithmetic is Mod 2

Now, the key size is just n^2.

Issue: vulnerable to cryptanalysis by an attacker that is aware of the structure of the algorithm.

Feistel Cipher

Feistel proposed the use of a cipher that alternates substitutions and permutations

Substitutions
- Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements

Permutation
- No elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed

- It is a practical application of a proposal by Claude Shannon in 1945 to develop a product cipher that alternates *diffusion* and *confusion* functions.
- It is the structure used by many significant symmetric block ciphers currently in use.
  e.g. Triple Data Encryption Algorithm (TDEA)

Shannon's concern was to thwart cryptanalysis based on statistical analysis

Diffusion

The statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext

This is achieved by having each plaintext digit affect the value of many ciphertext digits.

e.g. $y_n = \left(\sum_{i=1}^{k} m_{n+i}\right) \bmod 26$

In a binary block cipher, bits from different positions in the original plaintext contribute to a single bit of ciphertext

Confusion

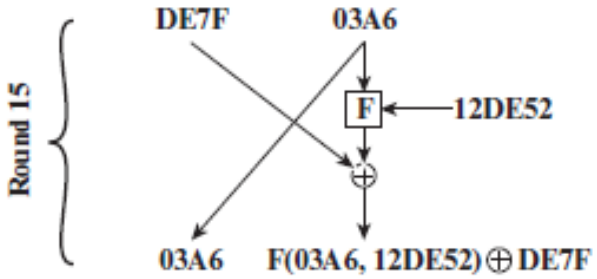
Seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible

This is achieved by the use of a complex substitution algorithm, but not a simple linear substitution.

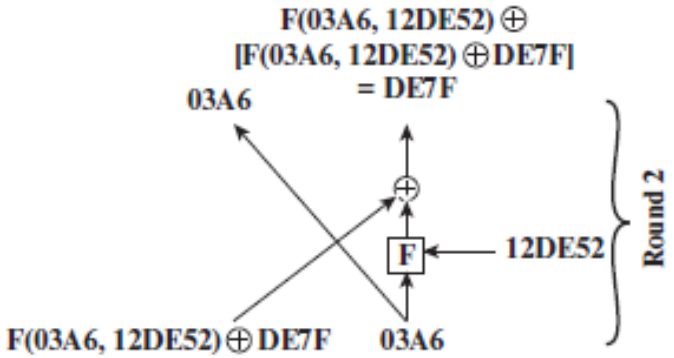
Feistel Cipher Structure

We will start with an example in one round:

Encryption round



Decryption round



Point to Ponder:

- Encryption and Decryption are just reversible design
- Design does not require that F be a reversible function

Prove this statement

Substitution:

- by applying a *round function F* to the right half of the data and then taking the *exclusive-OR* of the output of that function and the left half of the data.

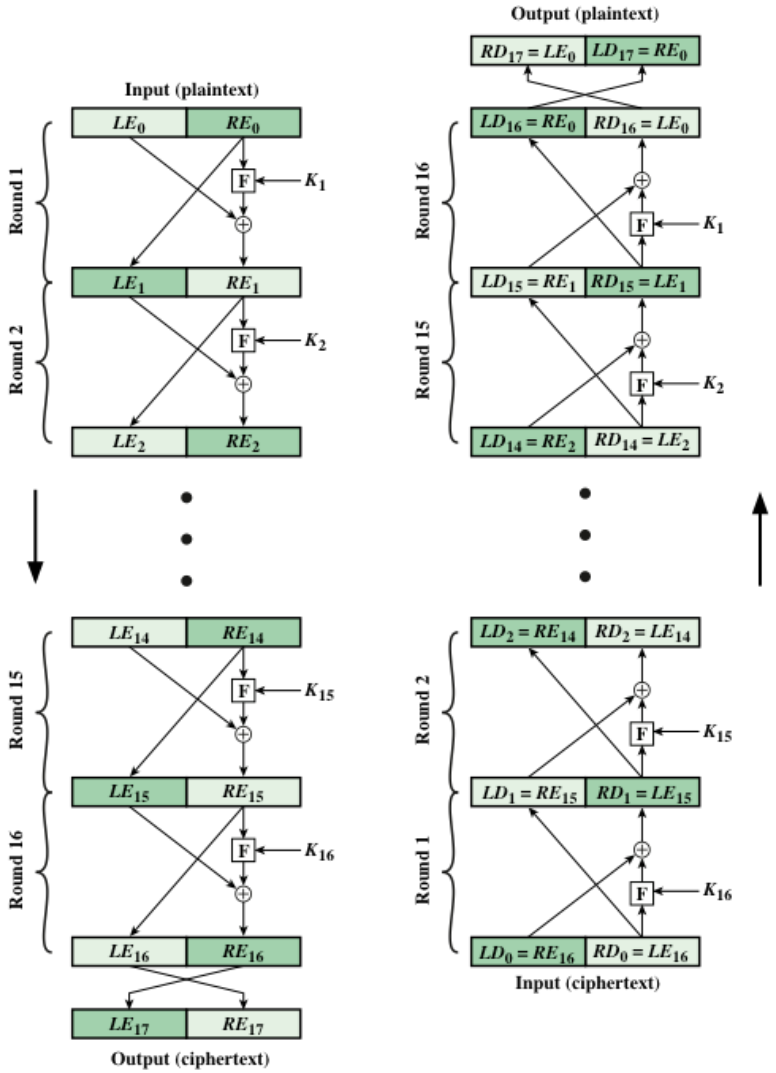
Permutation:

- interchange of the two halves of the Data

The XOR has the following properties:

- [A ⊕B] ⊕C = A ⊕[B ⊕C]
- D⊕D = 0
- E⊕0 = E

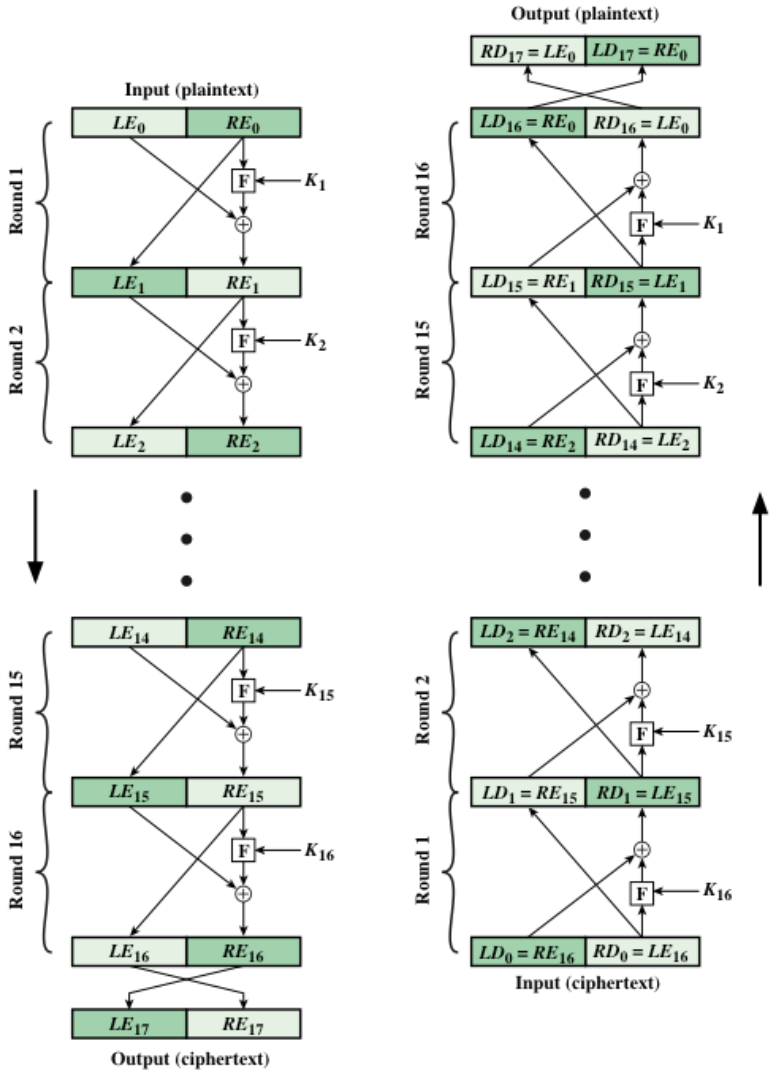
Feistel Cipher Structure



Structural rules for Encryption:

- Inputs are a plaintext block of length *2w* bits and a key *K*.
- The plaintext block is divided into two equal halves, LE_0 and RE_0.
- The two halves of the data pass through *n* rounds of processing and then combine to produce the ciphertext block as final output
- Each round *i* has as inputs LE_{i-1} and RE_{i-1} derived from the previous round, as well as a subkey K_i derived from the overall *K*.
- In general, the subkeys K_i are different from *K* and from each other.
- All rounds have the same structure.
- In each round, substitution and permutation are performed as mentioned before.
- In substitution, a *function F* is applied on the right-half block of *w* bits and a subkey of *y* bits, which produces an output value of length *w* bits: $F(RE_i, K_{i+1})$.

Feistel Cipher Structure



Structural rules for Decryption:

- Use the ciphertext as input to the algorithm
- use the *subkeys* K_i in reverse order, i.e. use K_n in the first round, K_{n-1} in the second round, and so on, until K_1 is used in the last round.
- Note that, at every round, the intermediate value of the decryption process is equal to the corresponding value of the encryption process with the two halves of the value swapped.
  - let the output of the i^{th} encryption round be $LE_i \,||\, RE_i$ (LE_i concatenated with RE_i). Then the corresponding output of the $(16-i)^{th}$ decryption round is $Re_i \,||\, LE_i$ or, equivalently, $LD_{16-i} \,||\, RD_{16-i}$.

Points to Ponder: Prove the above statement

Feistel Cipher Design Features

- Block size
  - Larger block sizes mean greater security but reduced encryption/decryption speed for a given algorithm
  - A block size of 64 bit is reasonably good
- Key size
  - Larger key size means greater security but may decrease encryption/decryption speeds
  - 128 bit key size has become the standard size
- 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
- Subkey generation algorithm
  - Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis
- Round function F
  - Greater complexity generally means greater resistance to cryptanalysis
- Fast software encryption/decryption
  - In many cases, encrypting is embedded in applications or utility functions in such a way as to preclude a hardware implementation; accordingly, the speed of execution of the algorithm becomes a concern
- Ease of analysis
  - If the algorithm can be concisely and clearly explained, it is easier to analyze that algorithm for cryptanalytic vulnerabilities and therefore develop a higher level of assurance as to its strength

DES and Block Cipher Design Principle

Note:

See the hand-written notes for these topics.


Thank
You