Cryptography

Symmetric Encryption – Block Cipher Algorithms

Malay Bhattacharyya

Assistant Professor

Machine Intelligence Unit
and
Centre for Artificial Intelligence and Machine Learning (CAIML)
Indian Statistical Institute, Kolkata

April 10, 2021

1. Introduction
   - What is a block cipher?
   - Working principle of block ciphers
   - Reversible and irreversible mapping
2. Block substitution ciphers
   - Construction of block substitution ciphers
   - Breaking the block substitution ciphers
3. Feistel cipher
   - The idea behind Feistel cipher
   - Feistel structure
   - Breaking the Feistel cipher

What is a block cipher?

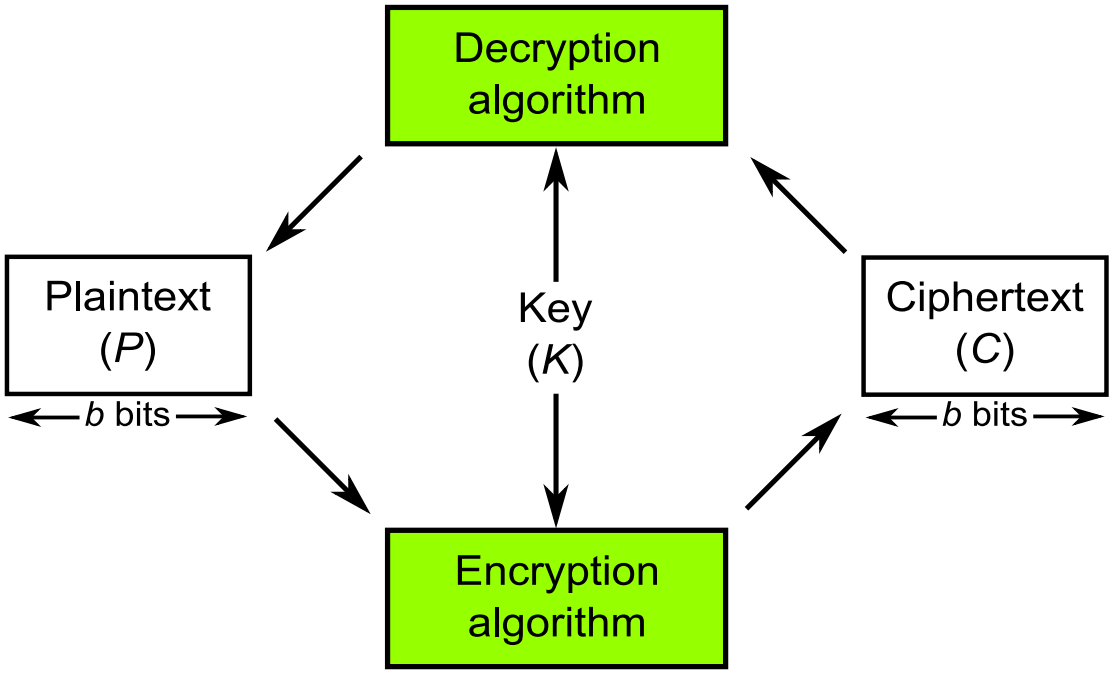
A block cipher is an encryption/decryption scheme in which a block of plaintext/ciphertext is treated as a whole and used to produce a ciphertext/plintext block of equal length.

- Encryption: Ciphertext $C_i = e(P_i, K), \forall i = 1...n$.
- Decryption: Plaintext $P_i = d(C_i, K) = d(e(P_i, K), K), \forall i = 1...n$.

Here, the plaintext $P = P_1 P_2 ... P_n$ and ciphertext $C = C_1 C_2 ... C_n$ are separated into equal-sized blocks.

Note: The block size is generally 64 or 128 bits.

Working principle of block ciphers



The encryption and decryption scheme for block ciphers

Reversible and irreversible mapping

Reversible (or nonsingular) mappings are one-to-one

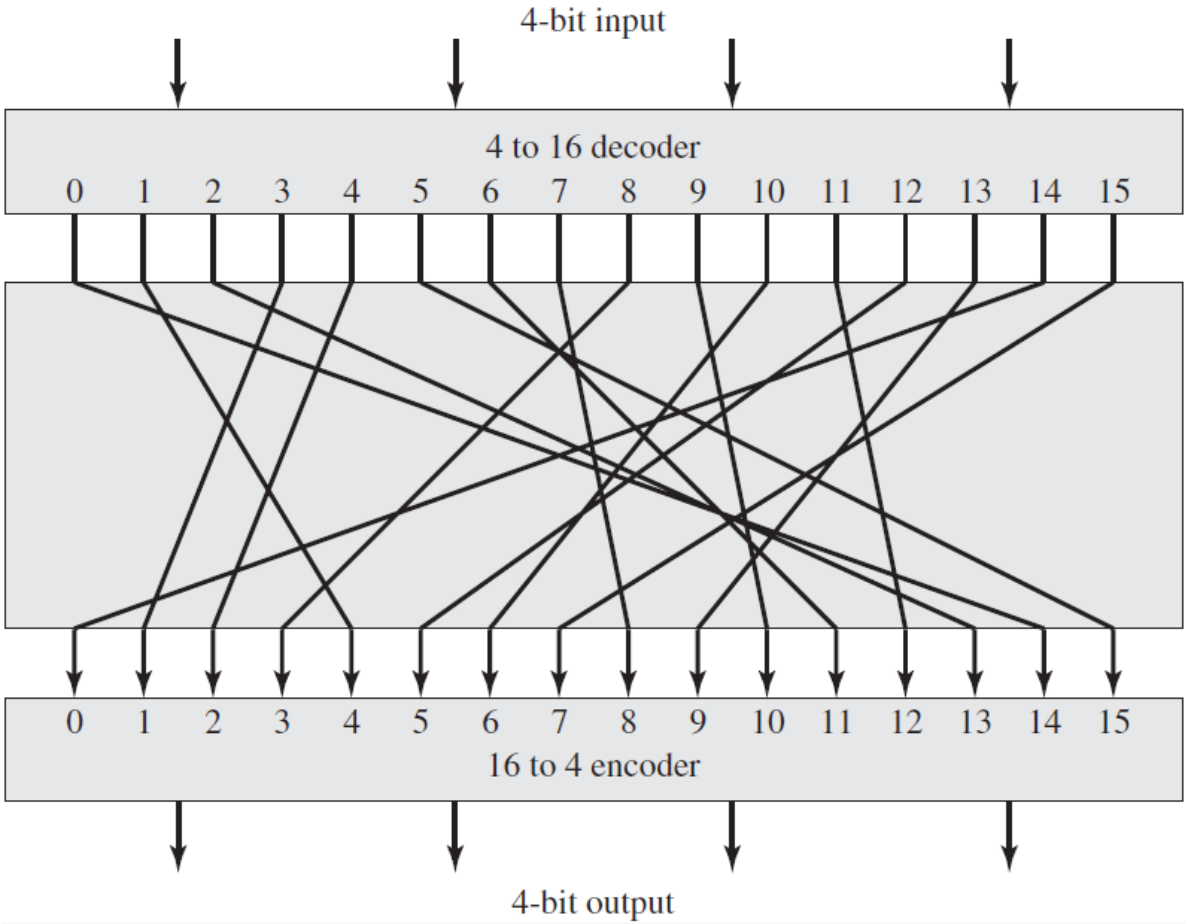
Plaintext	**Ciphertext**
00	01
01	10
10	11
11	00

Irreversible (or singular) mappings are one-to-many

Plaintext	**Ciphertext**
00	01
01	10
10	10
11	00

Note: We do not prefer singular mappings as its decryption is impossible.

Construction of block substitution ciphers



An n-bit-n-bit (for n = 4) block substitution cipher

Breaking the block substitution ciphers

If a small block size is used then the system is equivalent to a classical substitution ciphers. Such systems, as we have seen, are vulnerable to a statistical analysis of the plaintext.

This weakness is not inherent in the use of a substitution cipher but rather results from the use of a small block size.

If is sufficiently large and an arbitrary reversible substitution between plaintext and ciphertext is allowed, then the statistical characteristics of the source plaintext are masked to such an extent that breaking this becomes infeasible.

The idea behind Feistel cipher

Feistel showed that we can approximate the ideal block cipher by utilizing the concept of a product cipher, which is the execution of two or more simple ciphers in sequence in such a way that the final result or product is cryptographically stronger than any of the component ciphers.

Feistel proposed the use of a cipher that alternates substitutions and permutations, where these terms are defined as follows:

- **Substitution:** Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.
- **Permutation:** A sequence of plaintext elements is replaced by a permutation of that sequence. That is, no elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed.

The concept of diffusion and confusion

- **Diffusion:** It tries to dissipate the statistical structure of the plaintext into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext characters/digits.
- **Confusion:** It tries to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible.

These two conceptual schemas suggested long back by Shannon leads to the development of Feistel ciphers.

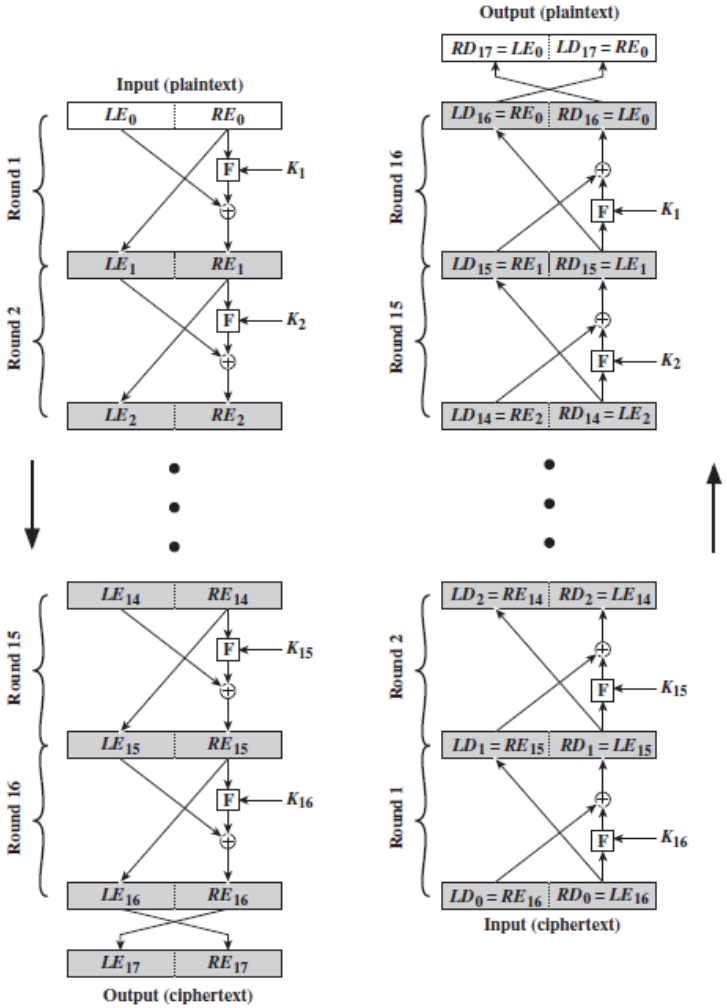
The Avalanche effect

A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the ciphertext.

The Avalanche effect particularly claims that a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext.

If the change were small, this might provide a way to reduce the size of the plaintext or key space to be searched.

Feistel structure



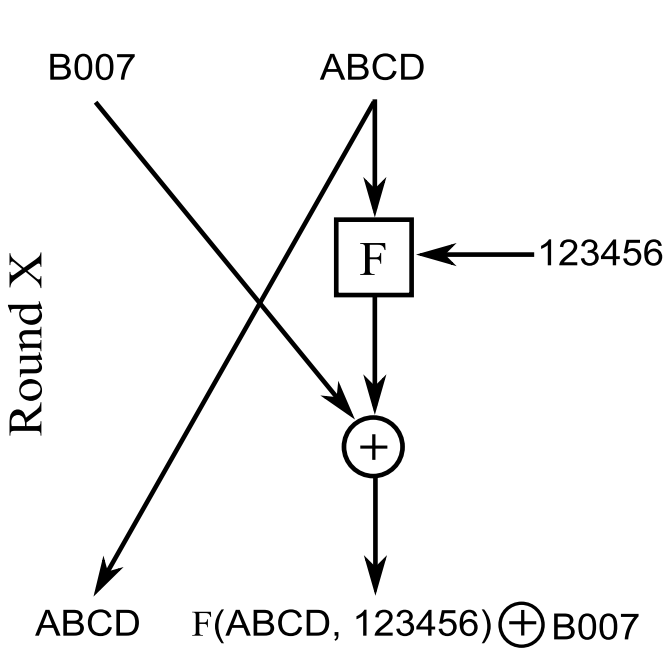
Feistel Encryption and Decryption (16 rounds)

Feistel structure

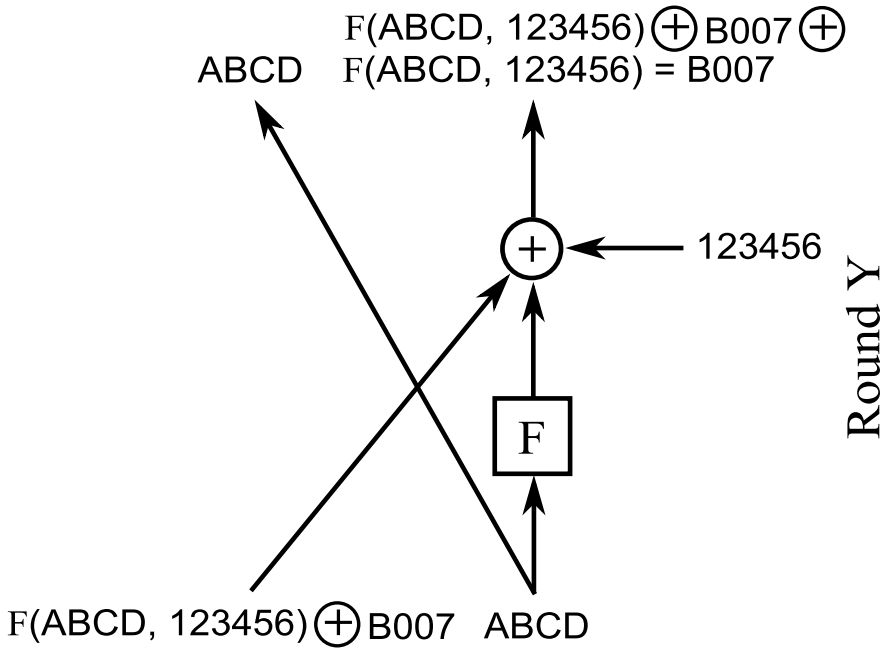
The inputs to the encryption algorithm are a plaintext block of length $2w$ bits and a key K. The plaintext block is divided into two halves, L_0 and R_0. The two halves of the data pass through n rounds of processing and then combine to produce the ciphertext block. Each round i has as inputs L_{i-1} and R_{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 and from each other.

A substitution is performed on the left half of the data. This is done 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. A permutation is performed that consists of the interchange of the two halves of the data.

Feistel structure – An example



Encryption round



Decryption round

Balanced and unbalanced Feistel ciphers

The Feistel ciphers designed over the conventional Feistel structures is balanced. However, an unbalanced Feistel cipher breaks the plaintext blocks into two halves (L_i and R_i) of unequal sizes.

Lucifer is an example of balanced Feistel cipher, whereas the Skipjack cipher is unbalanced.

Note: The Thorp shuffle is an extreme case of an unbalanced Feistel cipher in which one side is a single bit.

The key factors in Feistel structure

- **Block size:** Larger block sizes mean greater security (all other things being equal) but reduced encryption/decryption speed for a given algorithm.
- **Key size:** Larger key size means greater security but may decrease encryption/decryption speed.
- **Number of rounds:** A single round offers inadequate security but that multiple rounds offer increasing security.
- **Subkey generation algorithm:** Greater complexity in subkey generation should lead to greater difficulty of cryptanalysis.
- **Round function F:** Using a complex round function helps to achieve greater resistance from the possibility of breaking.

Breaking the Feistel cipher

Luby and Rackoff have shown in 1988 that a balanced Feistel scheme with only 4 rounds is perfectly secure as long as the round functions are random enough. Maurer and Pietrzak, and then Patarin, later showed that with more rounds, one can get more security.

Breaking a general Feistel cipher might involve the generation of as much as $2^n!$ possible mappings, which makes it really hard to break.