Feistel Mode

In cryptography, a **Feistel cipher** (also known as **Luby–Rackoff block cipher**) is a symmetric structure used in the construction of block ciphers, named after the German-born physicist and cryptographer Horst Feistel, who did pioneering research while working for IBM; it is also commonly known as a **Feistel network**.

A large number of block ciphers use the scheme, including the US Data Encryption Standard, the Soviet/Russian GOST and the more recent Blowfish and Twofish ciphers.

In a Feistel cipher, encryption and decryption are very similar operations, and both consist of iteratively running a function called a "round function" a fixed number of times.

Design

A Feistel network uses a *round function*, a function which takes two inputs – a data block and a subkey – and returns one output of the same size as the data block. In each round, the round function is run on half of the data to be encrypted, and its output is XORed with the other half of the data. This is repeated a fixed number of times, and the final output is the encrypted data.

An important advantage of Feistel networks compared to other cipher designs such as substitution–permutation networks is that the entire operation is guaranteed to be invertible (that is, encrypted data can be decrypted), even if the round function is not itself invertible. The round function can be made arbitrarily complicated, since it does not need to be designed to be invertible.

Furthermore, the encryption and decryption operations are very similar, even identical in some cases, requiring only a reversal of the key schedule. Therefore, the size of the code or circuitry required to implement such a cipher is nearly halved.

Unlike substitution-permutation networks, Feistel networks also do not depend on a substitution box that could cause timing side-channels in software implementations.

Theoretical work

The structure and properties of Feistel ciphers have been extensively analyzed by cryptographers.

Michael Luby and Charles Rackoff analyzed the Feistel cipher construction and proved that if the round function is a cryptographically secure pseudorandom function, with K_i used as the seed,

- then 3 rounds are sufficient to make the block cipher a pseudorandom permutation,
- while 4 rounds are sufficient to make it a "strong" pseudorandom permutation (which means that it remains pseudorandom even to an adversary who gets oracle access to its inverse permutation).

Because of this very important result of Luby and Rackoff, Feistel ciphers are sometimes called Luby–Rackoff block ciphers.

Advantages of using block ciphers

- While they may be tampered with, they generally go undetected and boast strong resistance.

Disadvantages of using block ciphers

- The encryption speed isn't as fast as other methods may be. This is because encryption occurs within entire blocks and multiple bits at a time.
- Small mistakes in even just one symbol may jeopardize the entire block, allowing for errors to spread quickly.

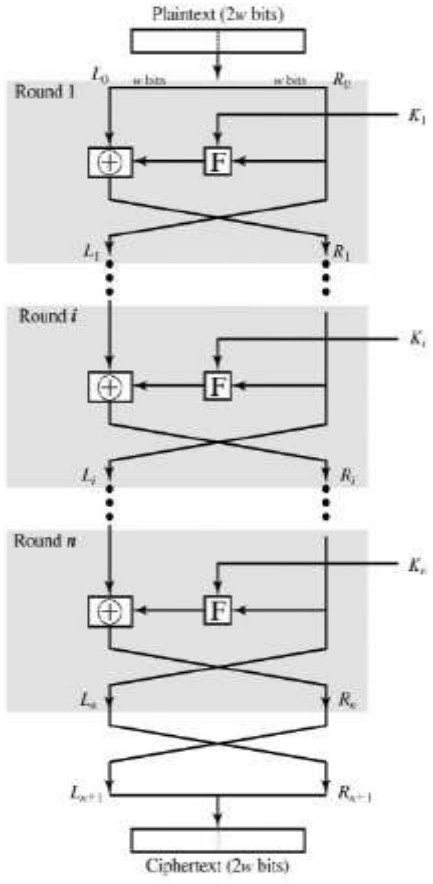
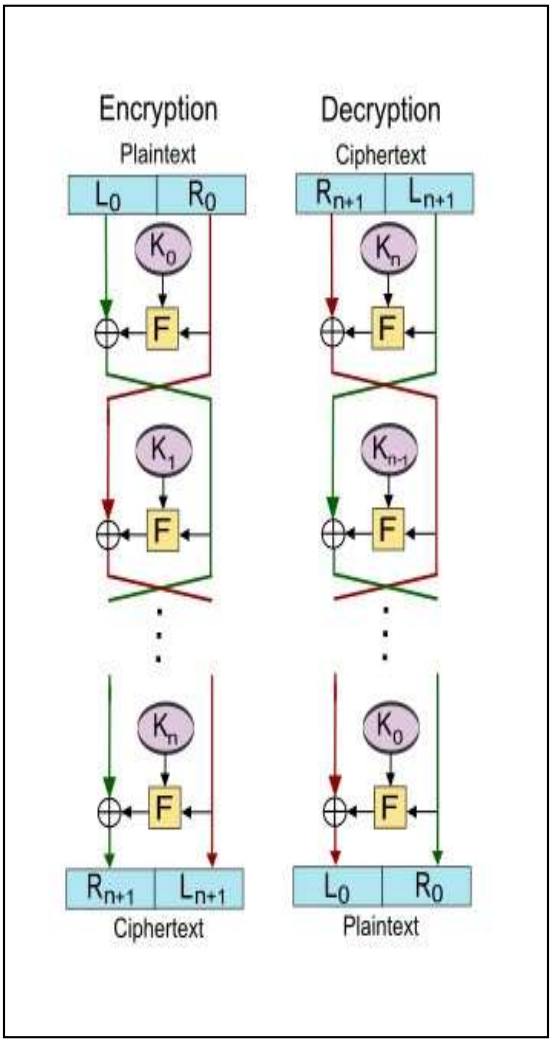


Figure: Feistel Mode



The exact realization of a Feistel network depends on the choice of the following parameters and design features:

- Block size:
  Larger block sizes mean greater security (all other things being equal) but reduced encryption/decryption speed for a given algorithm. The greater security is achieved by greater diffusion Traditionally, a block size of 64 bits has been considered a reasonable tradeoff and was nearly universal in block cipher design. However, the new AES uses a 128-bit block size.

- Key size:
  Larger key size means greater security but may decrease encryption/decryption speed. 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 to be inadequate, and 128 bits has become a common 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:
  Again, greater complexity generally means greater resistance to cryptanalysis.

There are two other considerations in the design of a Feistel cipher:

- Fast software encryption/decryption:
  In many cases, encryption 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:
  Although we would like to make our algorithm as difficult as possible to cryptanalyze, there is great benefit in making the algorithm easy to analyze. That is, 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, for example, does not have an easily analyzed functionality.

Confusion and Diffusion

Successful block cipher designs often integrate the concepts of *confusion* and *diffusion*. These ideas were introduced by Shannon.

Confusion is a measure of the statistical properties of the input with relation to the output. Essentially, looking at the output should give little or no information about the input; in short, the transformation should complicate the input such that the output bears little statistical relationship with the input.

Diffusion, on the other hand, attempts to extend the influence of the input symbols over a wide range of output symbols in order to disguise the tendencies of the input.

It must be noted that is not mandatory for both characteristics to be utilized to achieve secrecy. Indeed, the Vernam stream cipher achieves perfect secrecy with confusion alone. Since each plaintext symbol is combined with completely random data, there is no need to mix adjacent symbols of plaintext to achieve additional randomness.

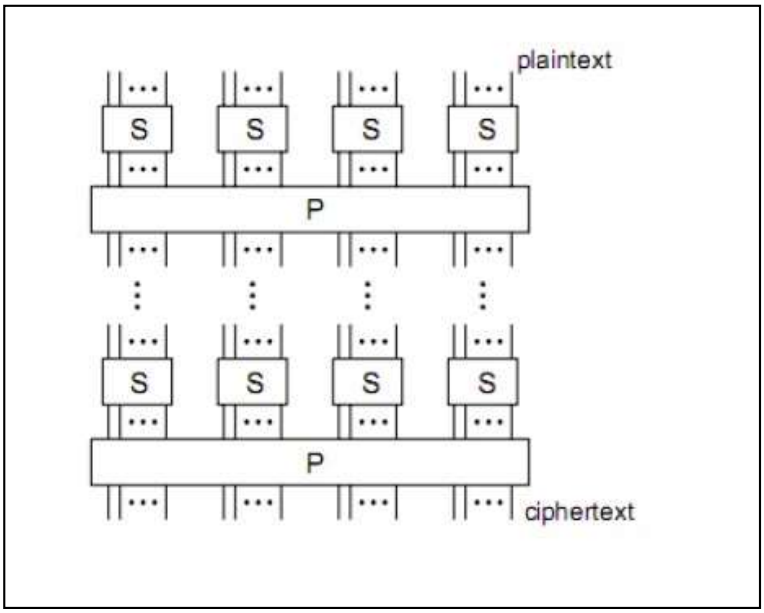
Unlike stream ciphers, block cipher design depends heavily on both principles of confusion and diffusion. Since the symbol length of a typical block cipher (64 bits) is often longer than the corresponding symbol in a stream cipher (8 or 32 bits), there

are more possible bits positions, which necessitate and assist diffusion. A successful diffusion is one in which each plaintext bit and each key bit affects each and every ciphertext bit (in the case of encryption).

This diffusion can be applied using a permutation which exchanges individual bit locations or sequential algebraic functions which combine and spread the influence of the inputs. A well diffused cipher will satisfy the strict avalanche criteria whereby if a single bit changes in the input, then half of the output bits will change in a random manner.

Definition : A product cipher combines two more transformations in manner intending that the resulting cipher is more secure than the individual components.

Definition : A substitution-permutation (SP) network is a product cipher composed of a number of stages each involving substitutions and permutations .



Substitution Operation a binary word is replaced by some other binary word the whole substitution function forms the key if use n bit words, the key is 2^(n)!bits, grows rapidly

can also think of this as a large lookup table, with n address lines (hence 2^(n) addresses), each n bits wide being the output value will call them S-boxes

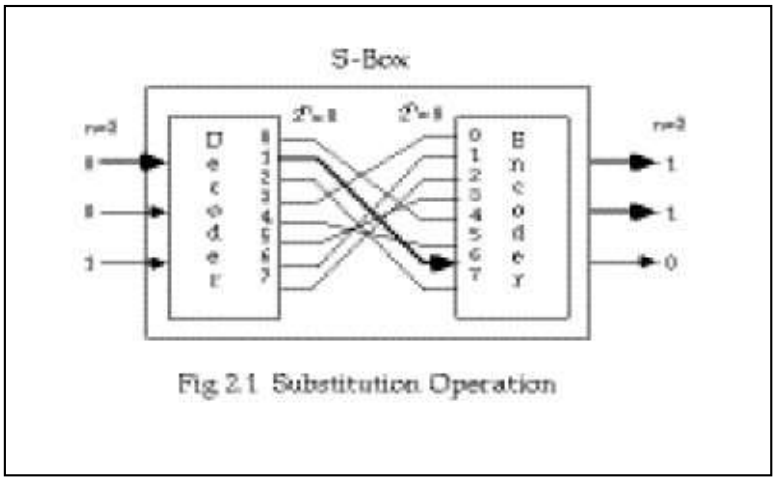
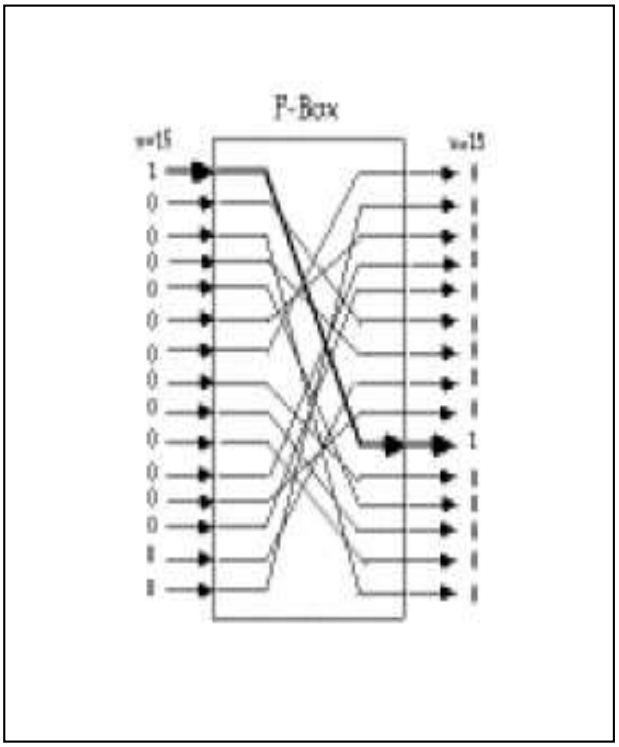


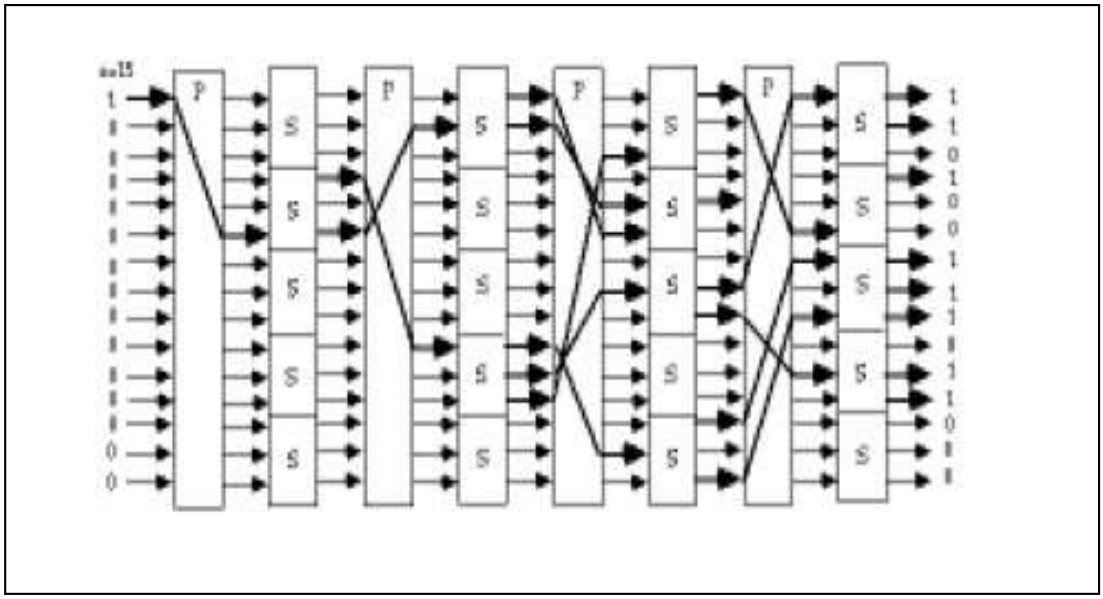
Fig 2.1 Substitution Operation

Permutation Operation a binary word has its bits reordered (permuted) the re-ordering forms the key if use n bit words, the key is n!bits, which grows more slowly, and hence is less secure than substitution

this is equivalent to a wire-crossing in practice (though is much harder to do in software) will call these P-boxes



Substitution-Permutation Network Shannon combined these two primitives he called these mixing transformations



Shannons mixing transformations are a special form of product ciphers where

- **S-Boxes**

provide confusion of input bits

- **P-Boxes**

Feistel networks and similar constructions are product ciphers, and so combine multiple rounds of repeated operations, such as:

- **Bit-shuffling** (often called permutation boxes or P-boxes)
- **Simple non-linear functions** (often called substitution boxes or S-boxes)
- **Linear mixing** (in the sense of modular algebra) using XOR to produce a function with large amounts of what Claude Shannon described as "confusion and diffusion". Bit shuffling creates the diffusion effect, while substitution is used for confusion.