Unit II. Symmetric Ciphers

Presented By: Er. Kobid Karkee
Himalaya College of Engineering

Concept of Confusion and Diffusion

- The terms diffusion and confusion were introduced by the famous information theorist Claude Shannon to capture the two basic building blocks for any cryptographic system
- According to the Shannon, there are two primitive operations with which strong encryption algorithms can be built
  - Confusion is an encryption operation where the relationship between key and ciphertext is obscured (making unclear and difficult to understand) Example: Substitution table (look-up table)
  - Example:EEC=>FFD

Concept of Confusion and Diffusion

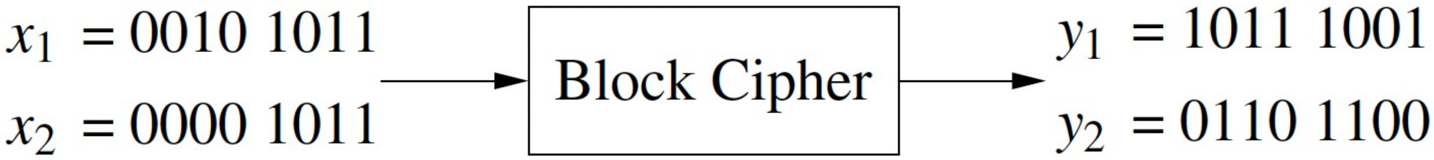
- Diffusion is an encryption operation where the influence of one plaintext symbol is spread over many ciphertext symbols with the goal of hiding statistical properties of the plaintext. Example: Permutation

  ABC=>CAB

- Modern block ciphers possess excellent diffusion properties.
- On a cipher level this means that changing of one bit of plaintext results on average in the change of half the output bits and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change.

Concept of Confusion and Diffusion

- Example : Let's assume a small block cipher with a block length of 8 bits. Encryption of two plaintexts x1 and x2, which differ only by one bit, should roughly result in something as shown in figure below



$x_1 = 0010\ 1011$

$x_2 = 0000\ 1011$

Block Cipher

$y_1 = 1011\ 1001$

$y_2 = 0110\ 1100$

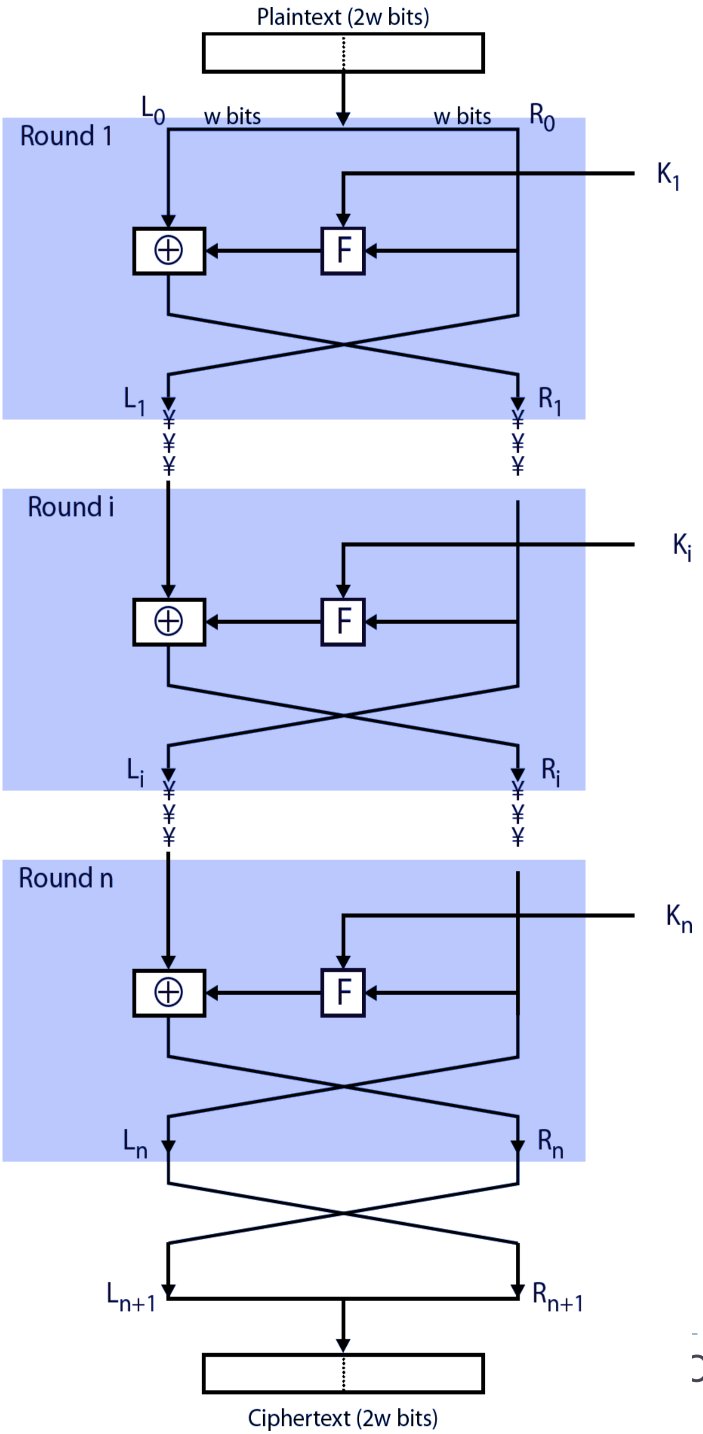
- Strong block cipher can be built by combining confusion and diffusion many times.

Feistel Cipher Structure

- Proposed by German-American Cryptographer Horst Feistel in 1973.
- A symmetric structure used in the construction of block ciphers
- A practical application of a proposal by Claude Shannon to develop a product cipher that alternates *confusion* and *diffusion* functions
- Feistel Cipher is not a specific scheme of block cipher.
- It is a design model from which many different block ciphers are derived.
- DES is just one example of a Feistel Cipher.

Feistel Cipher Structure

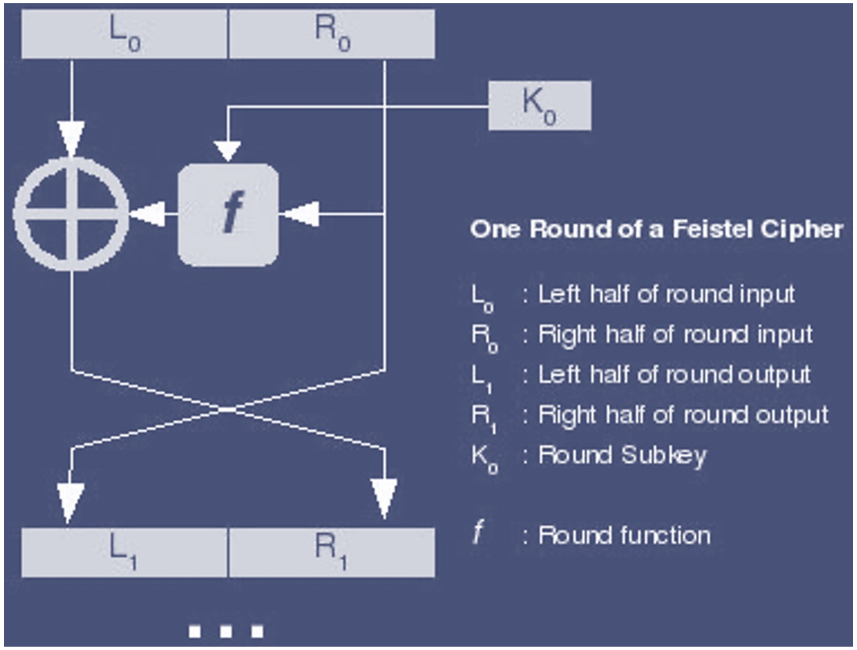
- Feistel cipher alternates substitutions and permutations, where these terms are defined as follows:
  - Substitution: Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.
  - Permutation: A sequence of plaintext elements is replaced by a permutation of that sequence. That is, no elements added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed.
- A cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption.



Fiestel Cipher Structure

The figure alongside shows the Fiestel cipher encryption model consisting of n number of rounds.

Feistel Cipher Encryption



One Round of a Feistel Cipher

L_0 : Left half of round input
R_0 : Right half of round input
L_1 : Left half of round output
R_1 : Right half of round output
K_0 : Round Subkey
f : Round function

One Round of a Feistel Structure

- The encryption process uses the Feistel structure consisting multiple rounds of processing of the plaintext, each round consisting of a “substitution” step followed by a permutation step.

Feistel Cipher Encryption

- The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.
- In each round, the right half of the block, R, goes through unchanged.
- But the left half, L, goes through an operation that depends on R and the encryption key.
- First, we apply an encrypting function ‘f’ that takes two input – the key K and R.
- The function produces the output f(R,K). Then, we XOR the output of the mathematical function with L.
- The permutation step at the end of each round swaps the modified L and unmodified R.

Feistel Cipher Encryption

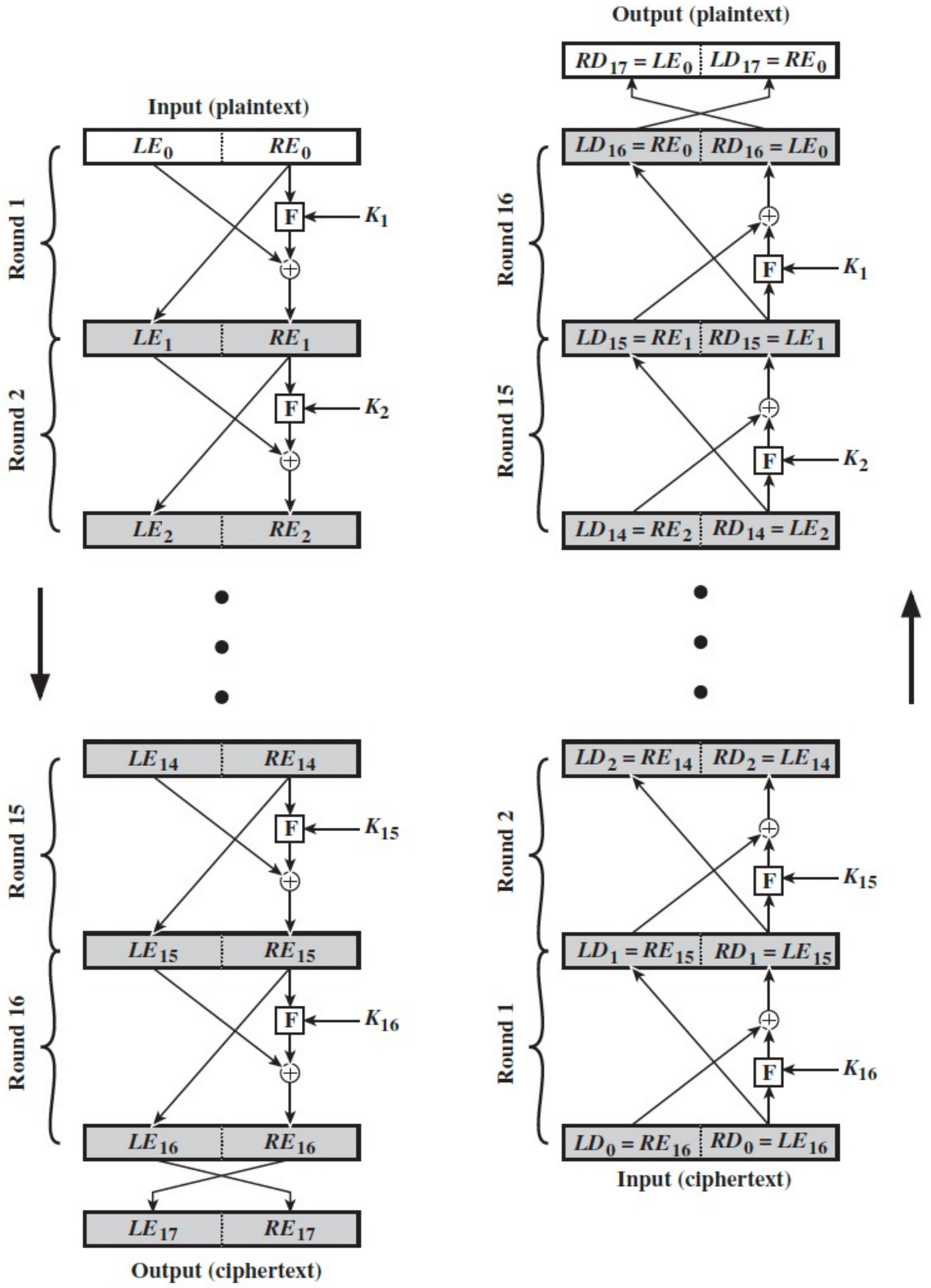
- Therefore, the L for the next round would be R of the current round. And R for the next round be the output L of the current round.
- Above substitution and permutation steps form a ‘round’. The total number of rounds ‘n’ are specified by the algorithm design.
- The round function has the same general structure for each round but is parameterized by the round subkey K_i.
- Once the last round is completed then the two sub blocks, ‘R’ and ‘L’ are concatenated in this order to form the ciphertext block.

Feistel Cipher Design Principles

- **block size**
  - increasing size improves security, but slows cipher
- **key size**
  - increasing size improves security, makes exhaustive key searching harder, but may slow cipher
- **number of rounds**
  - increasing number improves security, but slows cipher
- **subkey generation**
  - greater complexity can make analysis harder, but slows cipher
- **round function**
  - greater complexity can make analysis harder, but slows cipher
- **fast software en/decryption & ease of analysis**
  - are more recent concerns for practical use and testing

Feistel Cipher Decryption

- The process of decryption with a Feistel cipher is essentially the same as the encryption process.
- The rule is as follows:
  - Use the ciphertext as input to the algorithm, but use the subkeys K_i in reverse order, i.e., use K_n in the first round, $K_{n\text{-}1}$ in the second round, and so on until K_1 is used in the last round.
- This is a nice feature because it means we need not implement two different algorithms, one for encryption and one for decryption.



Feistel Cipher Decryption

Alongside figure shows the encryption and decryption process in Fiestel Structure with 16 rounds.

The encryption process going down the left-hand side and the decryption process going up the right-hand side of the figure for a 16-round algorithm.

Feistel Cipher Decryption

- For ith iteration of the encryption algorithm,

$$\begin{aligned} LE_i &= RE_{i-1} \\ RE_i &= LE_{i-1} \oplus \mathrm{F}(RE_{i-1}, K_i) \end{aligned}$$

Rearranging terms:

$$\begin{aligned} RE_{i-1} &= LE_i \\ LE_{i-1} &= RE_i \oplus \mathrm{F}(RE_{i-1}, K_i) = RE_i \oplus \mathrm{F}(LE_i, K_i) \end{aligned}$$

- Feistel structure really only encrypts (decrypts) half of the input bits per each round, namely the left half of the input. The right half is copied to the next round unchanged.

Substitution-Permutation Networks

- An SP-network, or substitution–permutation network (SPN), is a series of linked mathematical operations used in block cipher algorithms such as AES.
- Such a network takes a block of the plaintext and the key as inputs and applies several alternating "rounds" or "layers" of substitution boxes (S-boxes) and permutation boxes (P-boxes) to produce the ciphertext block.
- The S-boxes and P-boxes transform (sub-)blocks of input bits into output bits. It is common for these transformations to be operations that are efficient to perform in hardware, such as exclusive or (XOR) and bitwise rotation.

Substitution-Permutation Networks

- The key is introduced in each round, usually in the form of "round keys" derived from it.
- Decryption is done by simply reversing the process (using the inverses of the S-boxes and P-boxes and applying the round keys in reversed order).
- An S-box substitutes a small block of bits (the input of the S-box) by another block of bits (the output of the S-box).
- This substitution should be one-to-one, to ensure invertibility (hence decryption).

Substitution-Permutation Networks

- In particular, the length of the output should be the same as the length of the input (the picture below has S-boxes with 4 input and 4 output bits), which is different from S-boxes in general that could also change the length, as in DES (Data Encryption Standard), for example.
- Rather, a good S-box will have the property that changing one input bit will change about half of the output bits (or an avalanche effect).
- It will also have the property that each output bit will depend on every input bit.

Substitution-Permutation Networks

- A P-box is a permutation of all the bits: it takes the outputs of all the S-boxes of one round, permutes the bits, and feeds them into the S-boxes of the next round.
- A good P-box has the property that the output bits of any S-box are distributed to as many S-box inputs as possible.
- At each round, the round key (obtained from the key with some simple operations, for instance, using S-boxes and P-boxes) is combined using some group operation, typically XOR.

Substitution-Permutation Networks

- A single typical S-box or a single P-box alone does not have much cryptographic strength: an S-box could be thought of as a substitution cipher, while a P-box could be thought of as a transposition cipher.
- However, a well-designed SP network with several alternating rounds of S- and P-boxes already satisfies Shannon's confusion and diffusion properties.
- The reason for diffusion is the following: If one changes one bit of the plaintext, then it is fed into an S-box, whose output will change at several bits, then all these changes are distributed by the P-box among several S-boxes, hence the outputs of all of these S-boxes are again changed at several bits, and so on.

Substitution-Permutation Networks

- Doing several rounds, each bit changes several times back and forth, therefore, by the end, the ciphertext has changed completely, in a pseudorandom manner.
- In particular, for a randomly chosen input block, if one flips the i-th bit, then the probability that the j-th output bit will change is approximately a half, for any i and j, which is the Strict Avalanche Criterion.
- Vice versa, if one changes one bit of the ciphertext, then attempts to decrypt it, the result is a message completely different from the original plaintext— SP ciphers are not easily malleable.

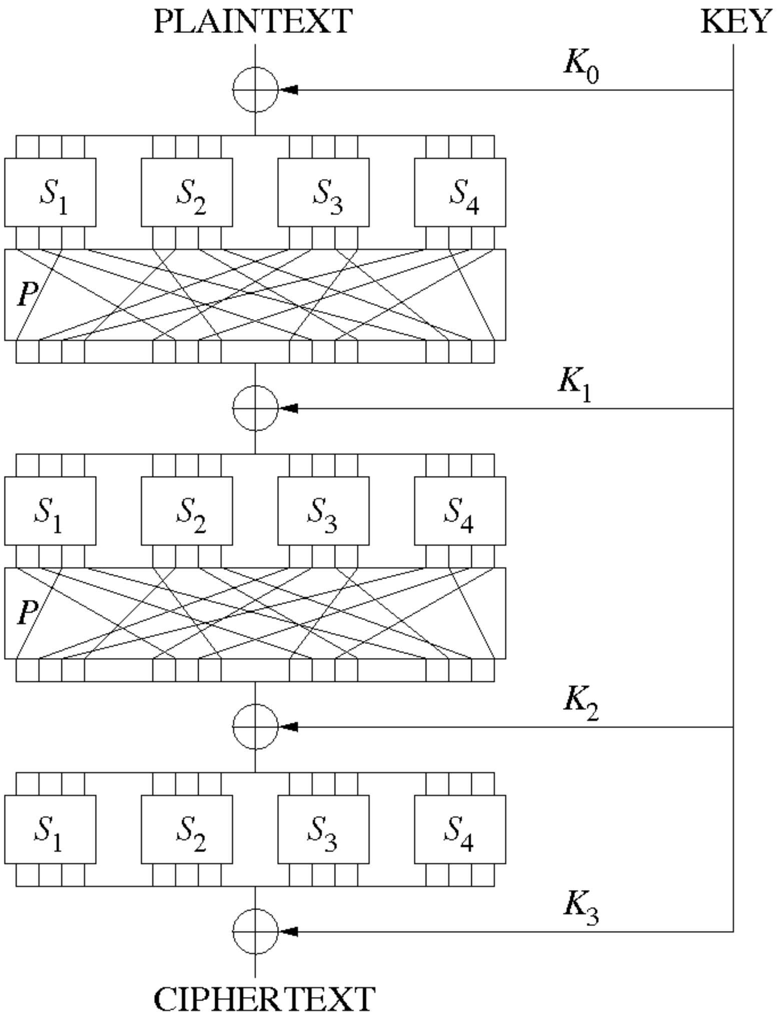
Substitution-Permutation Networks

- The reason for confusion is exactly the same as for diffusion: changing one bit of the key changes several of the round keys, and every change in every round key diffuses over all the bits, changing the ciphertext in a very complex manner.
- Even if an attacker somehow obtains one plaintext corresponding to one ciphertext—a known- plaintext attack, or worse, a chosen plaintext or chosen-ciphertext attack—the confusion and diffusion make it difficult for the attacker to recover the key.

Substitution-Permutation Networks

A sketch of a substitution–permutation network with 3 rounds, encrypting a plaintext block of 16 bits into a ciphertext block of 16 bits.

The S-boxes are the S_i, the P-boxes are the same P, and the round keys are the K_i.


PLAINTEXT
KEY
K_0
S_1
S_2
S_3
S_4
P
K_1
S_1
S_2
S_3
S_4
P
K_2
S_1
S_2
S_3
S_4
K_3
CIPHERTEXT