Symmetric Key-Modern Block Ciphers

Components of a Modern Cipher

- P(D)-Boxes
  - -Straight P-Boxes
  - -Compression P-Boxes
  - -Expansion P-Boxes

- S-Boxes

  An s-box is an m*n substitution unit, where m and n are not necessarily the same.

- Circular Shift
- Swap
- Split and Combine
- Complement

Product Ciphers

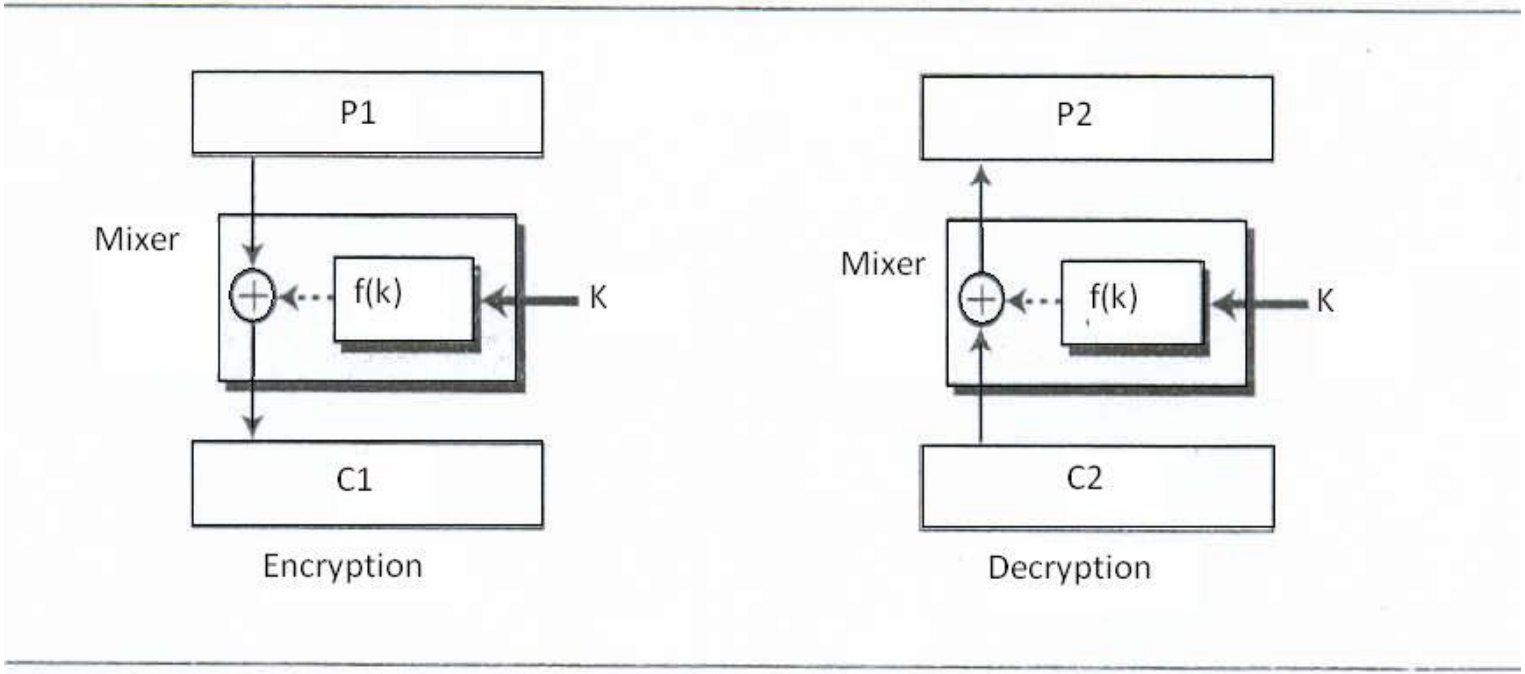
- A product cipher is a complex cipher combing substitution, permutation and other components discussed previously

Modern block ciphers are all product ciphers

- Feistel Ciphers
- Non Feistel Ciphers

Feistel Cipher Design

First design



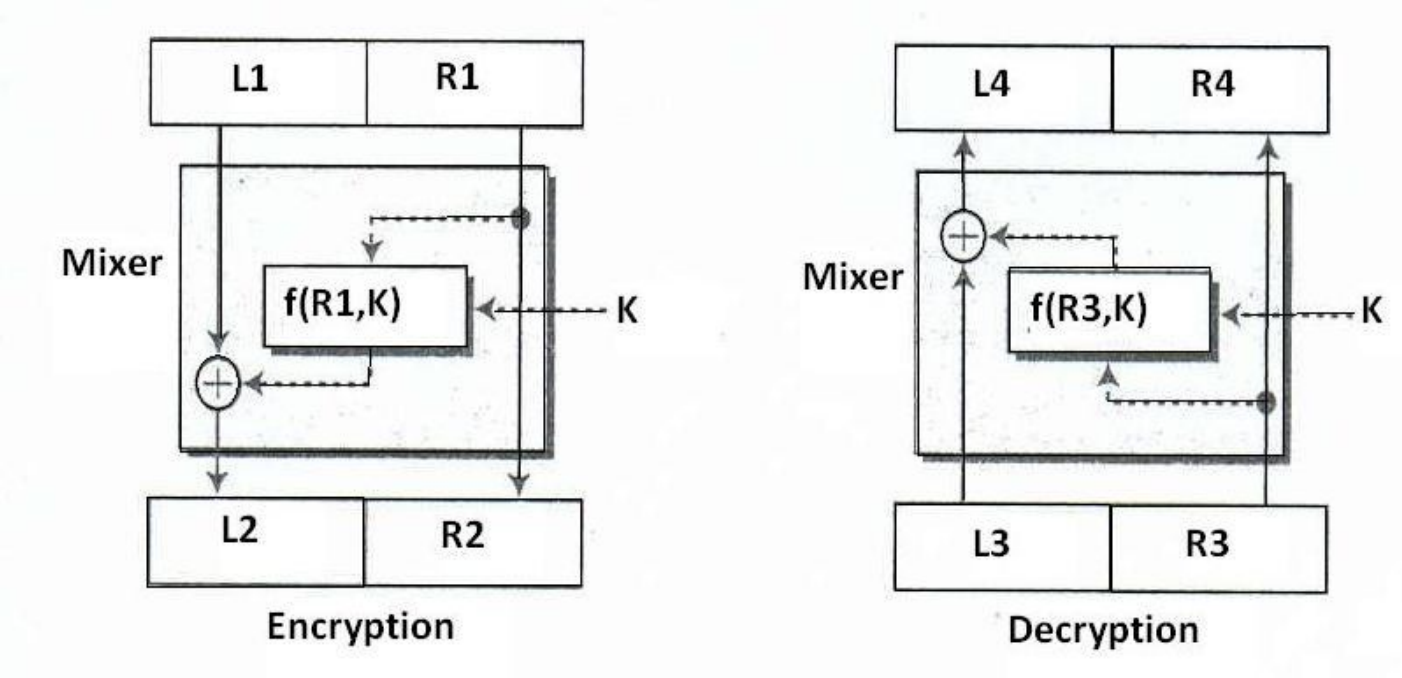
- Encryption: C1=P1 XOR f(k)
- Decryption: P2=C2 XOR f(k)

  =C1 XOR f(k)

  =P1 XOR f(k) XOR f(k)

  =P1 XOR (00…0)=P1

- Improvement of the first Feistel design.



- Assume that L3=L2 and R3=R2(no change in Cipher text during transmission).

R4=R3=R2=R1

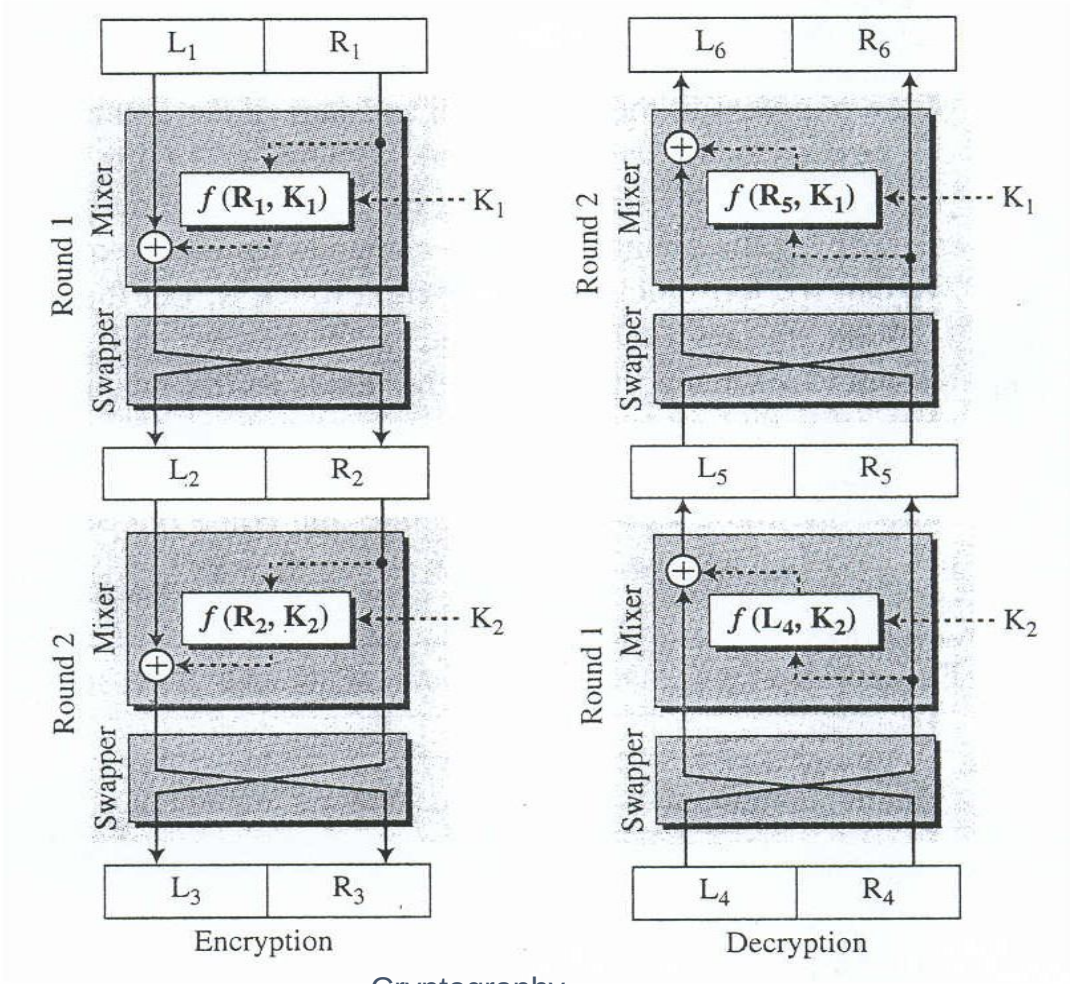
L4=L3 XOR f(R3,k)

=L2 XOR f(R2,k)

=L1 XOR f(R1,K) XOR f(R1,k)

=L1

- Final Design



- Here the encryption and decryptions are inverses of each other.
- We can prove this fact using relationship between the left and right sections in each cipher.

Proof for the equality for the middle text:

L5=R4 XOR f(L4,k2)

=R3 XOR f(R2,k2)

=L2 XOR f(R2,k2) XOR f(R2,k2)

=L2

R5=L4=L3=R2

L6=R5 XOR f(L5,k1)

=R2 XOR f(L2,k1)

=L1 XOR f(R1,k1) XOR f(R1,k1)

=L1

R6=L5=L2=R1