Lecture 5

Review

- Strong Encryption Algorithm
  - Confusion
  - Diffusion

Symmetric Block Encryption

Block cipher

- the most commonly used symmetric encryption algorithms
- input: fixed-size blocks (Typically 64, 128 bit blocks), output: equal size blocks
- provide secrecy and/or authentication services
- Data Encryption Standard (DES), triple DES (3DES), and the Advanced Encryption Standard (AES)s
- Usually employ Feistel structure

Feistel Cipher Structure

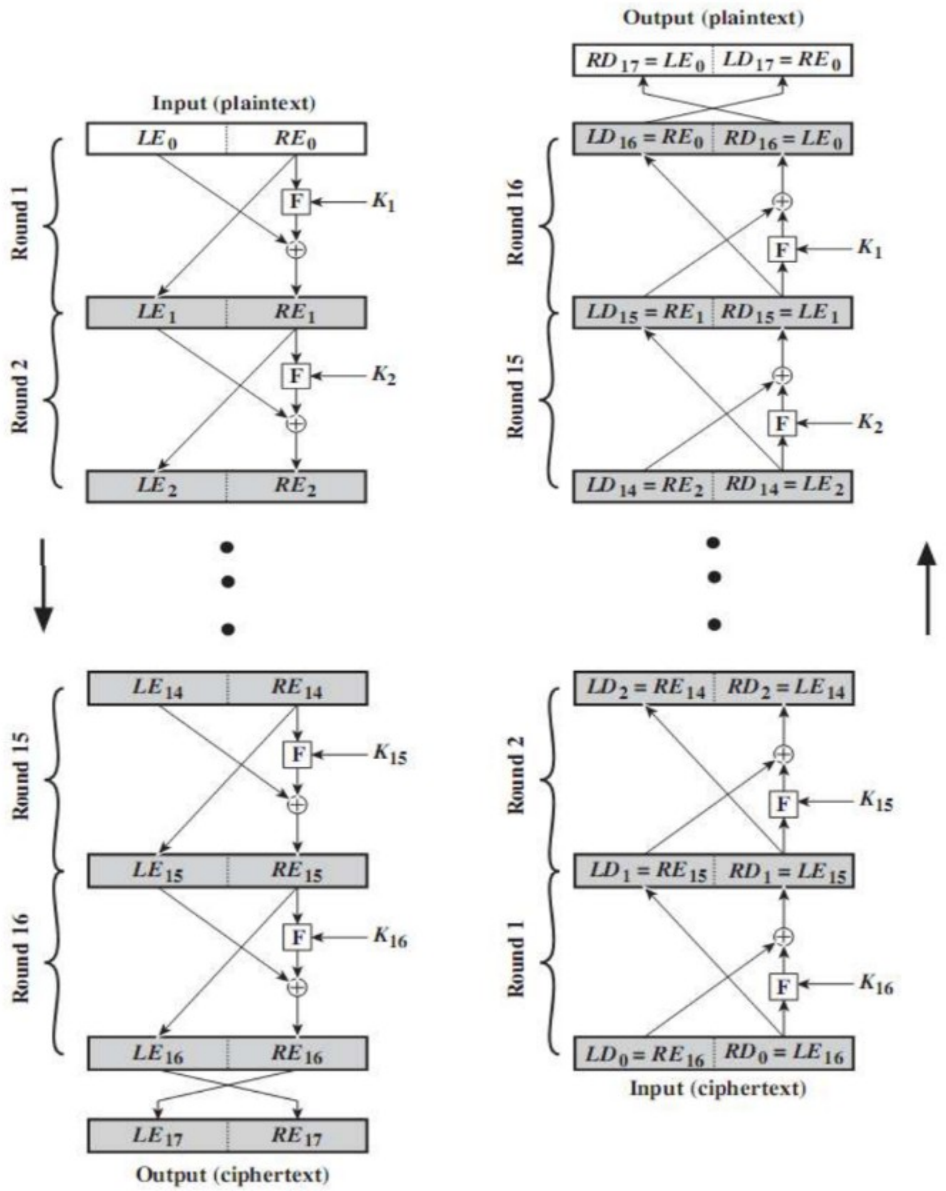
Feistel Cipher Structure

- most symmetric block ciphers are based on a **Feistel Cipher Structure**
- based on the two primitive cryptographic operations
  - *substitution* (S-box)
  - *permutation* (P-box)
- provide *confusion* and *diffusion* of message

Feistel Cipher Structure

- Horst Feistel devised the **feistel cipher** in the 1973
  - based on concept of invertible product cipher
- partitions input block into two halves
  - process through multiple rounds which
    - perform a substitution on left data half
    - based on round function of right half & subkey
    - then have permutation swapping halves
- implements Shannon’s substitution-permutation network concept

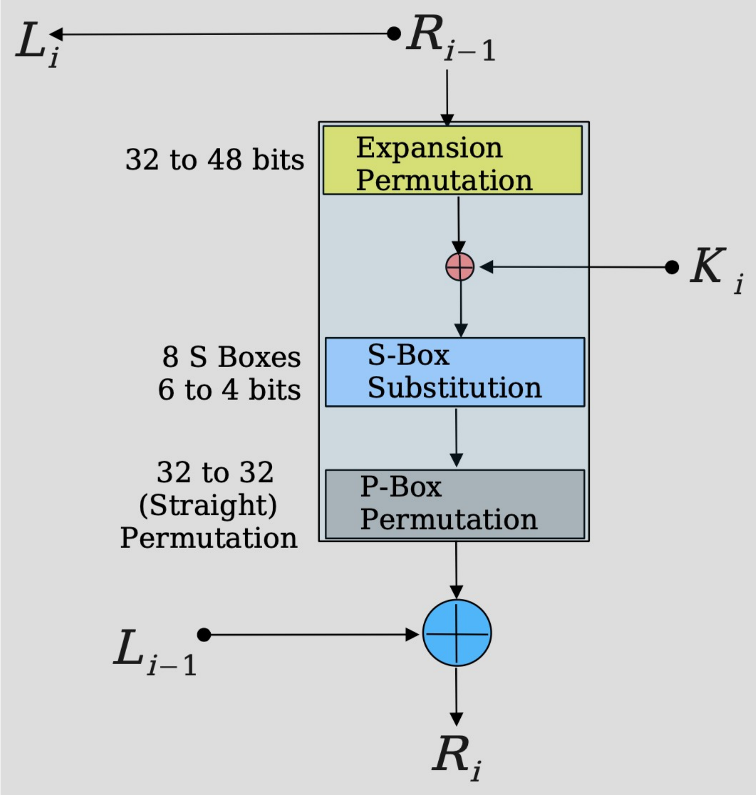
Feistel Encryption and Decryption



Encryption

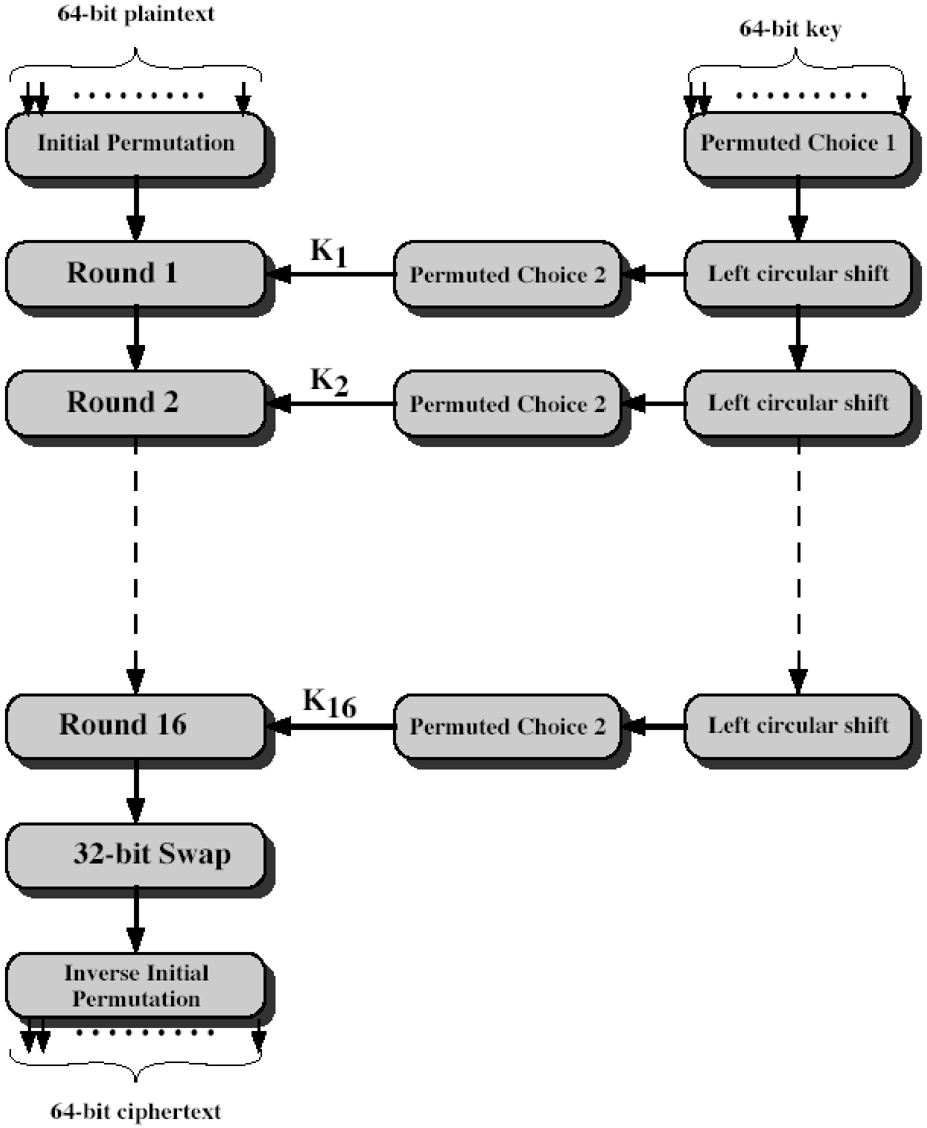
$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$



DES encryption

- 64 bits plaintext
- 56 bits effective key length


64-bit plaintext
64-bit key
Initial Permutation
Permuted Choice 1
Round 1
K1
Permuted Choice 2
Left circular shift
Round 2
K2
Permuted Choice 2
Left circular shift
Round 16
K16
Permuted Choice 2
Left circular shift
32-bit Swap
Inverse Initial Permutation
64-bit ciphertext