CS 465

Feistel Model

Last Updated: Aug 27, 2013

Feistel Cipher Structure

- Described by Horst Feistel (IBM) in 1973
- Many symmetric encryption algorithms use this structure
  - DES, IDEA, Blowfish, RC6, MARS, Twofish
  - Not AES
    - Substitution-permutation network
- Block cipher
- Features – block size, key size, number of rounds, sub-key generation algorithm, round function
- Decryption is essentially the same as encryption
  - Input: ciphertext
  - Use sub-keys in reverse order
- Sources
  - Stallings NSE Fig 2.2 (next slide)
  - Wikipedie: Feistel Cipher

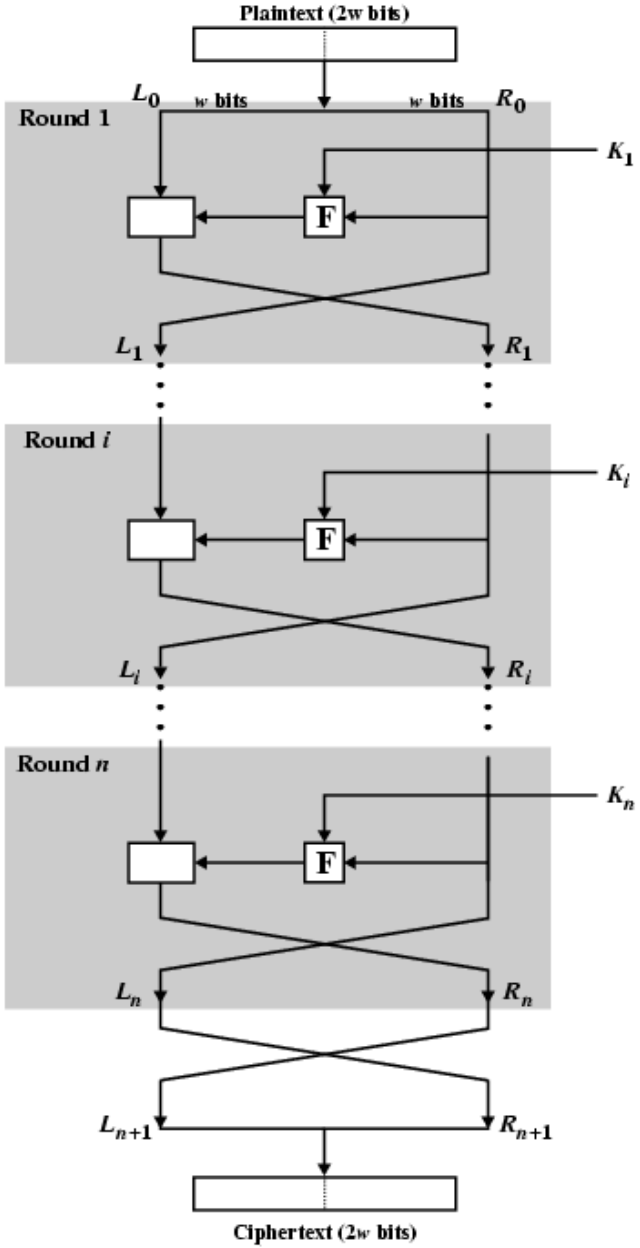

Figure 2.2 Classical Feistel Network

Source: Network Security Essentials (Stallings)

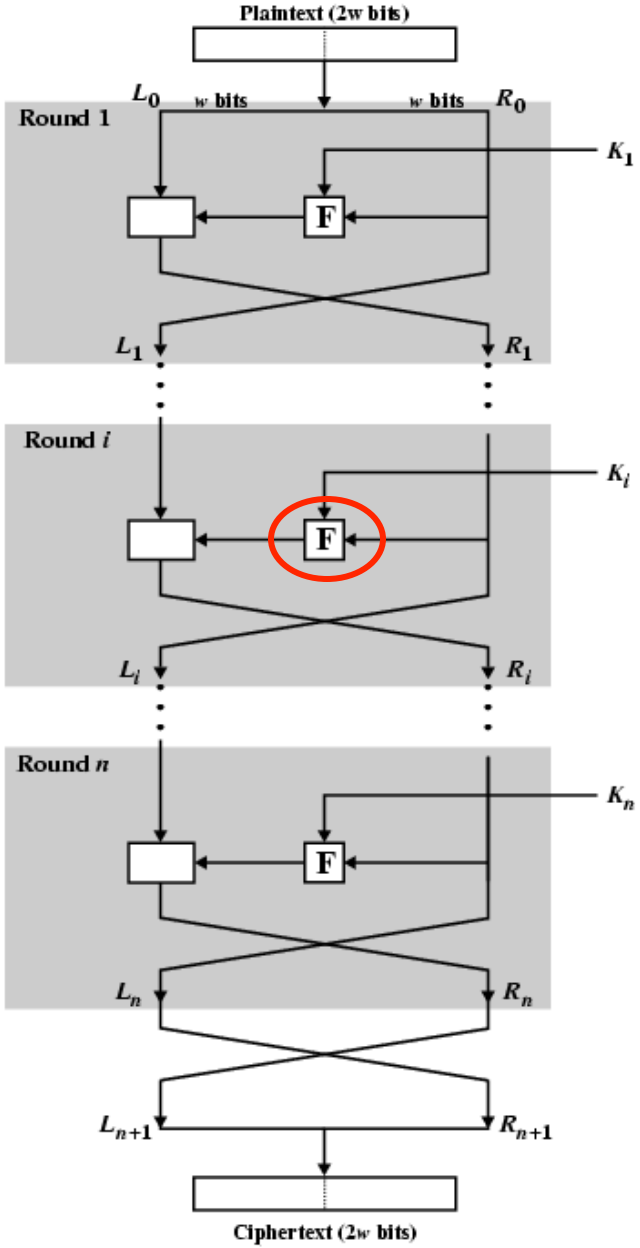

Figure 2.2 Classical Feistel Network

Source: Network Security Essentials (Stallings)

The Feistel Network Round Function (F)

- The Feistel network is guaranteed to be reversible if we can reconstruct its inputs, which are derived from the key
- It doesn't matter how complicated or simple F is or if it can be inverted

Proof of Feistel Network

- On the board

- What is the disadvantage of a 1-round Feistel network?