DES - Data Encryption Standard

Block size	64 bits
Key Size	56 bits
Speed	~ 50 cycles per byte
Algorithm	Feistel Network

Timeline

- **1972** NBS call for proposals
- **1974** IBM Lucifer proposal
  analyzed by DOD and enhanced by NSA
- **1976** adopted as standard
- **2004** NIST withdraws the standard

(FYI) Feistel Network

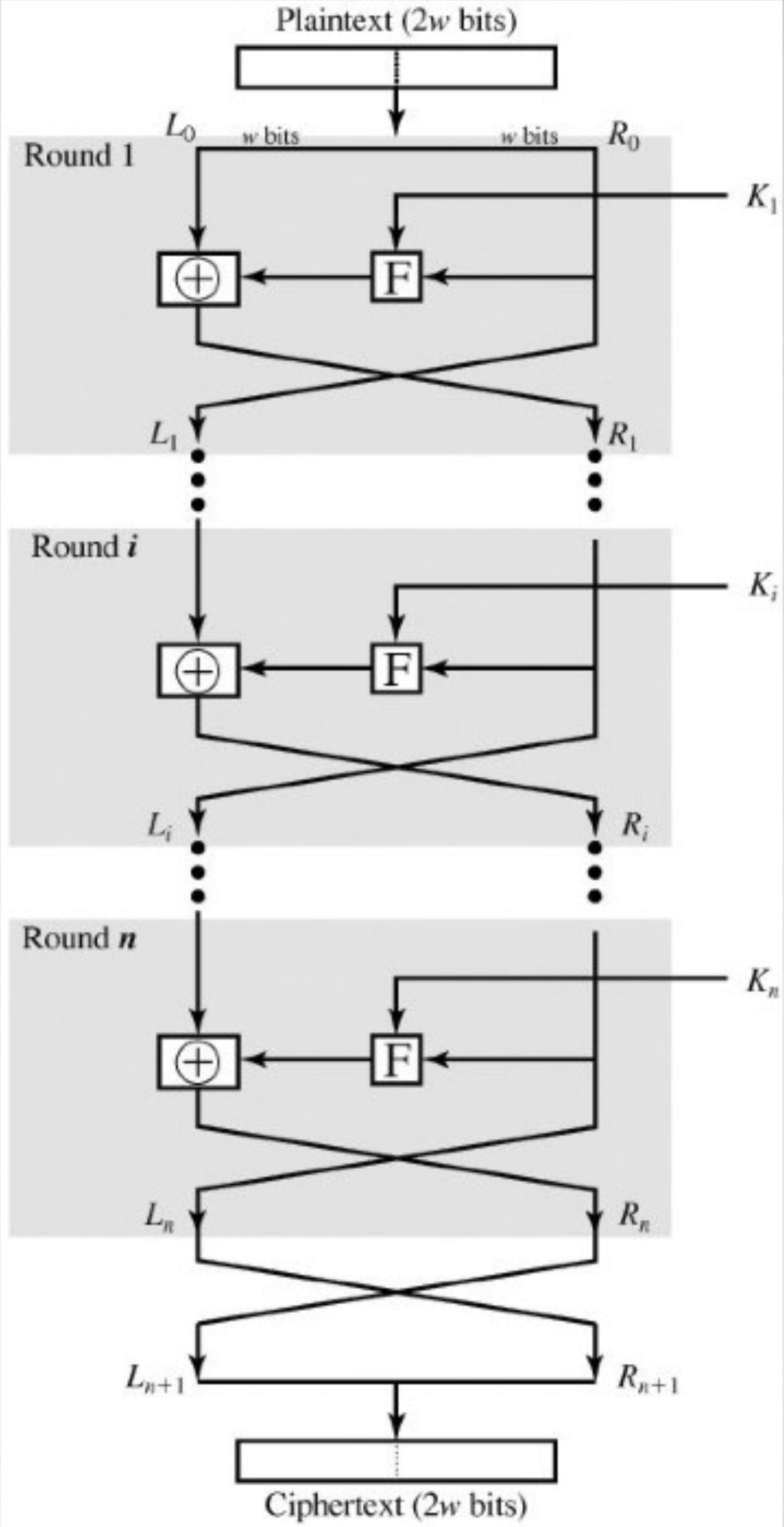
$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus F_i(R_{i-1},k_i)$

Properties:

- F is an arbitrary function that scrambles the input based on a key
- F is not necessary invertible
- A Feistel Network is invertible

➡ Achieves confusion and diffusion



"Cryptography and Network Security" by *William Stalllings*