

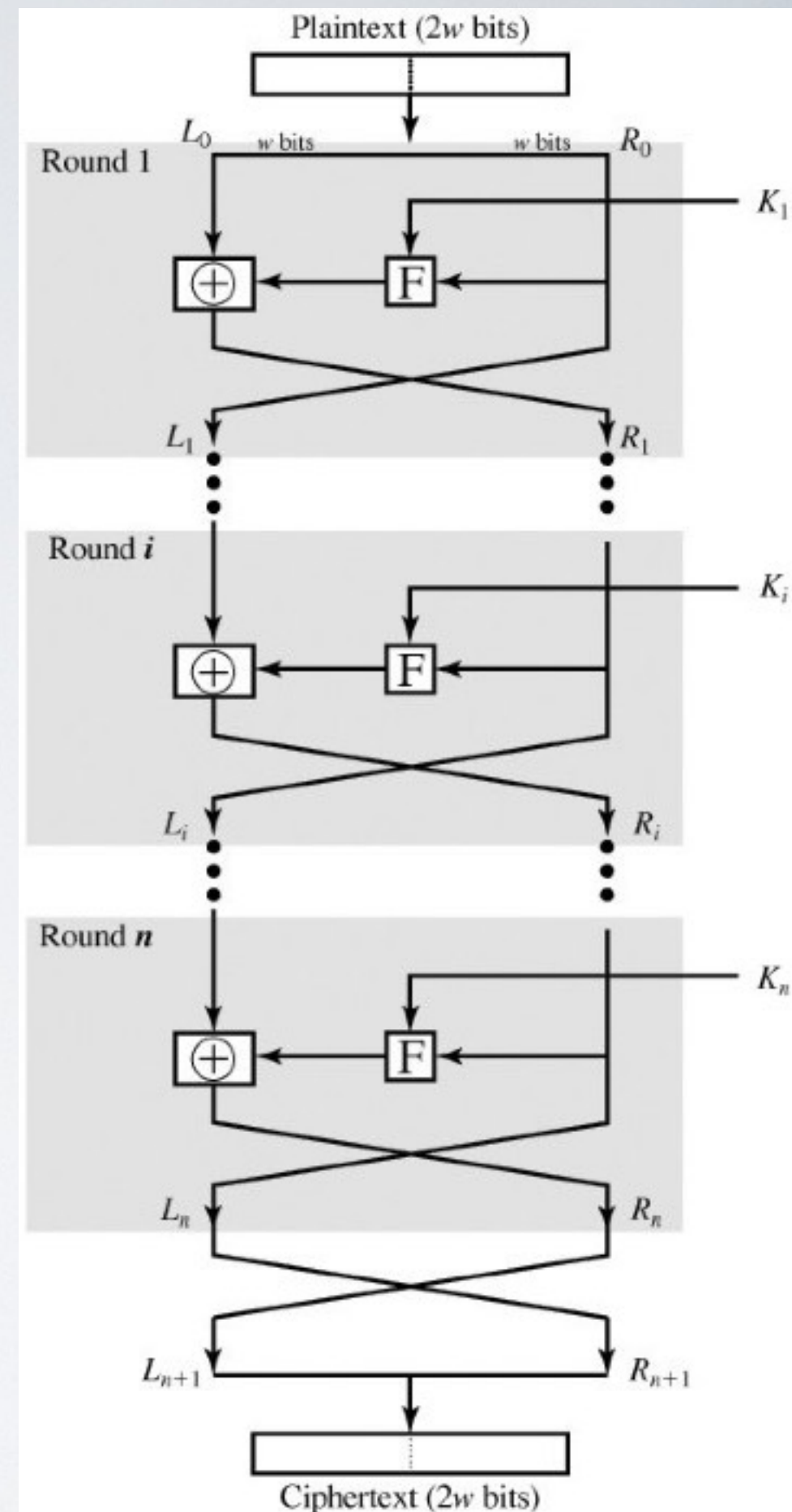
(FYI) Feistel Network

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

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

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 Stallings

Security of DES - DES Challenges (brute force contests)

1998 *Deep Crack*, the EFF's DES cracking machine used 1,856 custom chips

- Speed : matter of days
- Cost : \$250,000

2006 *COPACOBANA*, the Cost-optimized Parallel CodeBreaker used 120 FPGAs

- Speed : less than 24h
- Cost : \$10,000