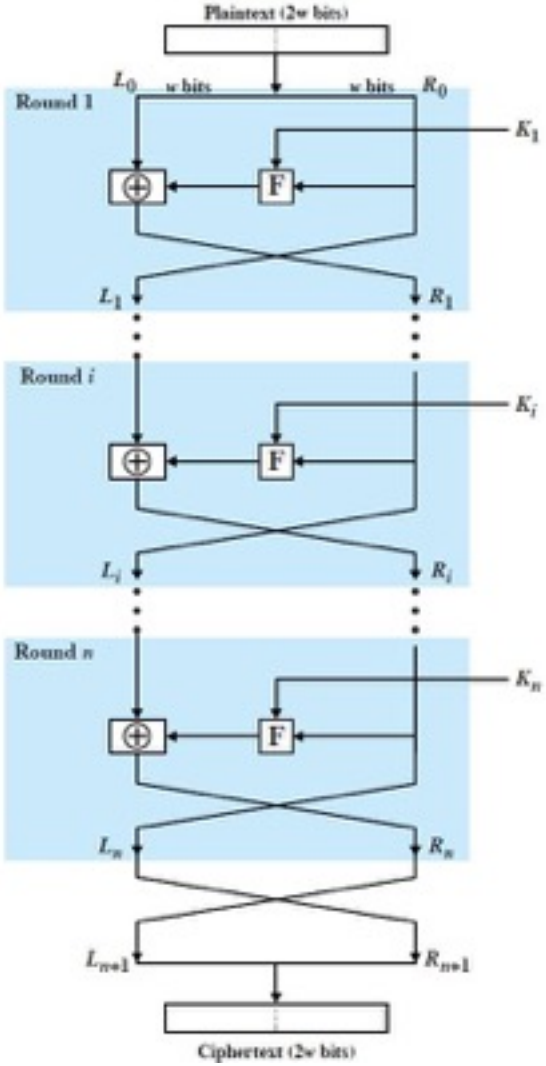
Week 4
Feistel Cipher

Now I Believe…

- You understand how the same key can be used for encryption and decryption in the secret-key-based cryptography
- However, the previous examples are too weak for real crypto systems
  - The transformation methods can be made much more secure by sophisticated mathematical algorithms
  - In a real crypto system, we must use multiple rounds of substitution and transposition as depicted in the following Feistel cipher structure

Feistel Cipher Structure (1973)



- Each round *i* has inputs L_{i-1} (left half of the data) and R_{i-1} (right half of the data), derived from the previous round, and a subkey K_i, derived from *K*
- All rounds have the same structure
- A substitution is conducted on L_i via *XOR* (exclusive OR) with the output of *F* (round function)
- Many symmetric block cipher algorithms, including DES, are based on this structure

SYRACUSE UNIVERSITY
SUOS
CULTORES
SCIENTIA
CORONAT