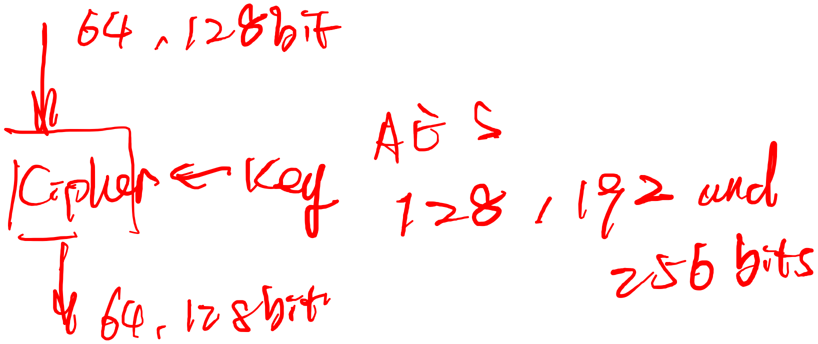
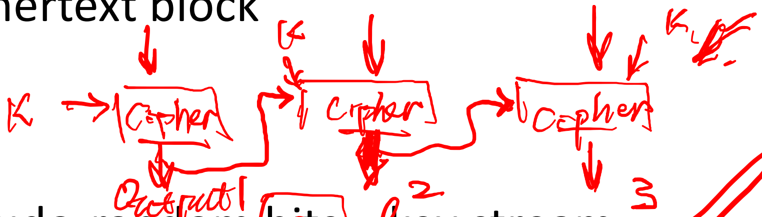
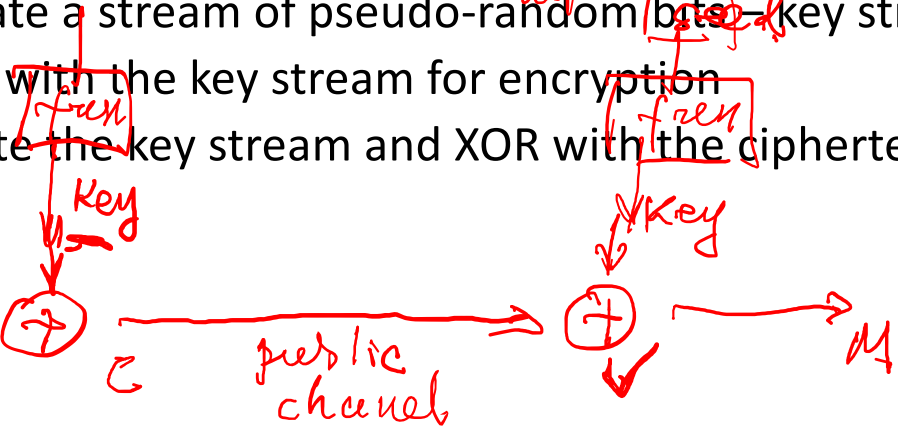
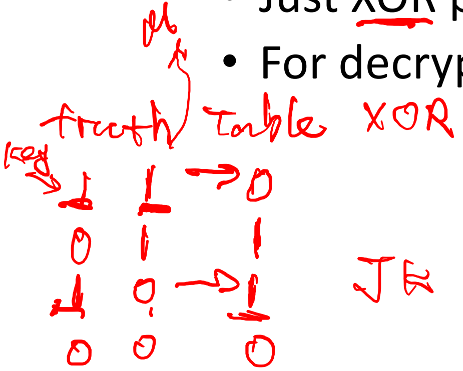
Two basic types

- Block Ciphers
  - Typically 64, 128 bit blocks
  - A k-bit plaintext block maps to a k-bit ciphertext block
  - Usually employ Feistel structure
- Stream Ciphers
  - A key is used to generate a stream of pseudo-random bits – key stream
  - Just XOR plaintext bits with the key stream for encryption
  - For decryption generate the key stream and XOR with the ciphertext!









JK Flip-Flop

$C_1 = M_1 \oplus K$

$C_2 = M_2 \oplus K$

$C_1 \oplus C_2 =$

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

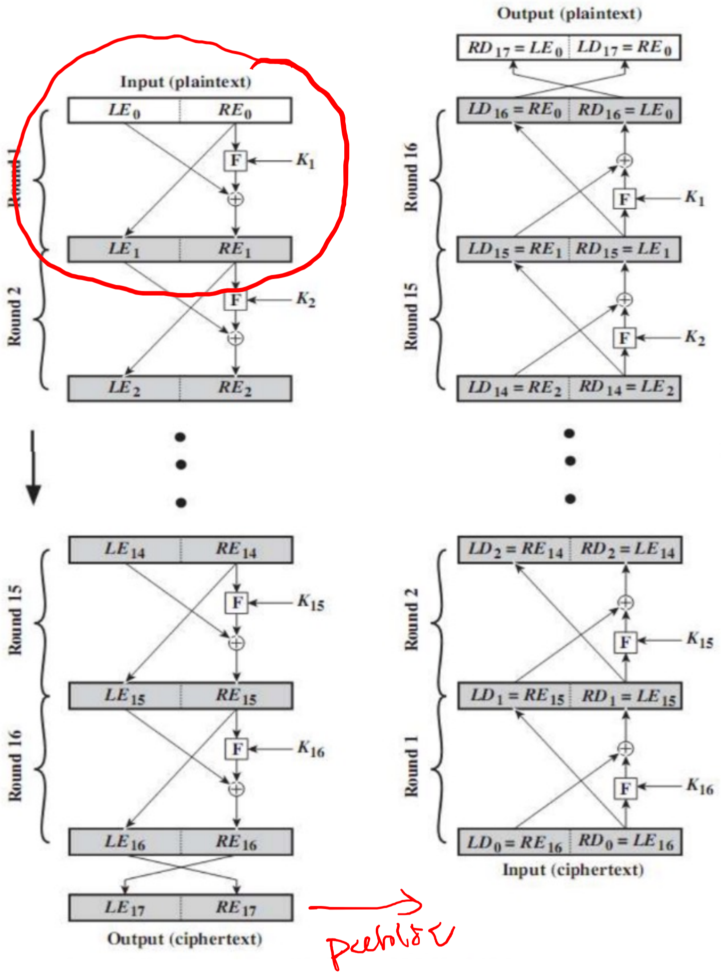
- most symmetric block ciphers are based on a **Feistel Cipher Structure**
- based on the two primitive cryptographic operations
  - *substitution* (S-box)
  - *permutation* (P-box)
- provide *confusion* and *diffusion* of message

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

64 bit 128

Feistel Encryption and Decryption



[illegible]

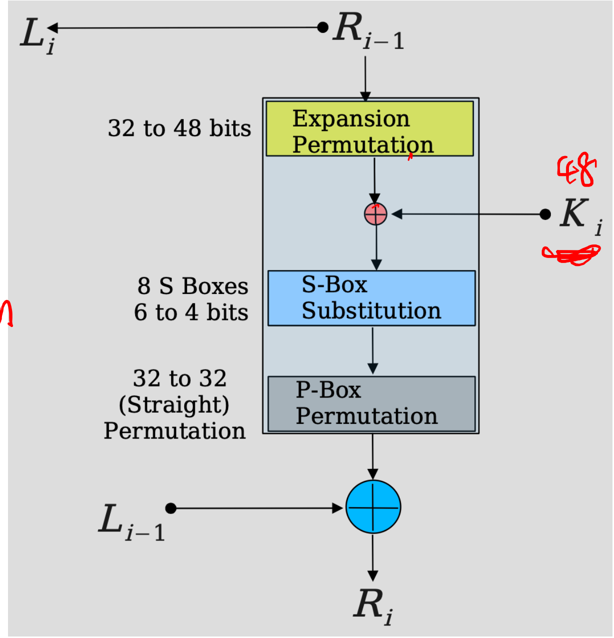
Encryption

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

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

decrypt

32 bits



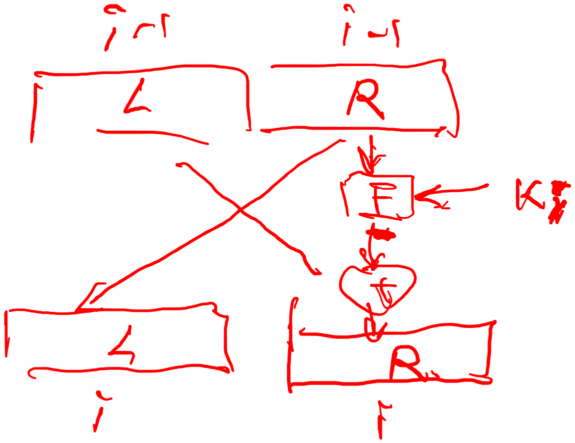
operation

k

$[\ ]$ $[\ ]$

$n \times m$ $m \times k$

$\|$ $n \times k$



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

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

No class on Wednesday (Sept 17)

- The Engineering Job Fair will be held in-person on **Tuesday, September 16, 2025 and Wednesday, September 17, 2025** at the **Lubbock Memorial Civic Center**.
- https://www.depts.ttu.edu/coe/careers/students/jobfair.php