Chapter 10.2
Symmetric Encryption and Message Confidentiality

Book Reading: Computer Security Principles and Practice (3ed), 2015, p. 637-668

Symmetric Encryption and Message Confidentiality

- also known as: conventional encryption, secret-key, or single-key encryption
  - only alternative before public-key crypto in 70’s
  - still most widely used alternative
  - has ingredients: plaintext, encryption algorithm, secret key, ciphertext, and decryption algorithm
- generically classified along dimensions of:
  1. type of operations used
  2. number of keys used
  3. way in which the plaintext is processed

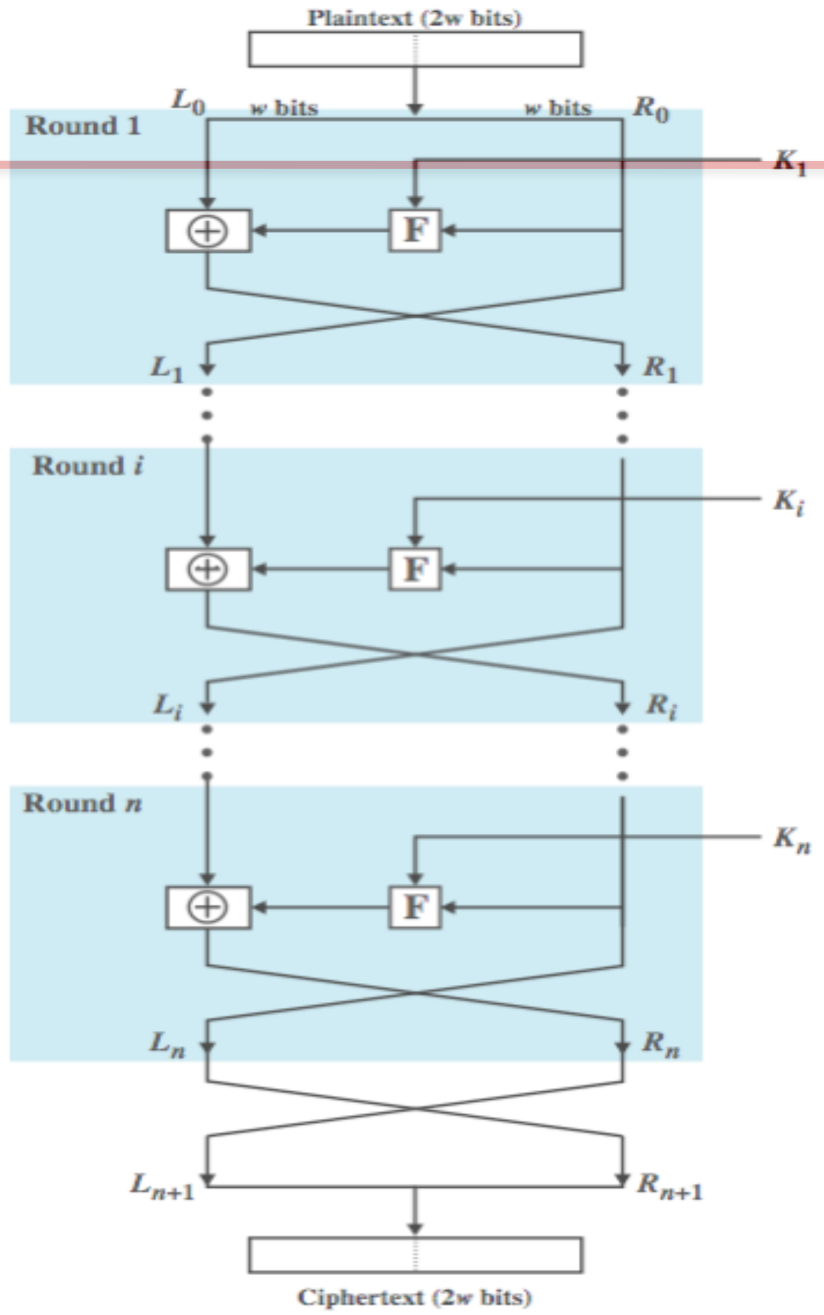
Cryptanalysis

- attacks:
    - ciphertext only - least info, hardest
    - known plaintext - some plain/cipher pairs
    - chosen plaintext - get own plain/cipher pairs
    - chosen ciphertext - rarer
    - chosen text - rarer
- only weak algs fail a ciphertext-only attack
- usually design algs to withstand a known-plaintext attack

Computationally Secure Algs

- encryption is computationally secure if:
  - cost of breaking cipher exceeds info value
  - time required to break cipher exceeds the useful lifetime of the info
- usually very difficult to estimate the amount of effort required to break
- can estimate time/cost of a brute-force attack (see Ch 2)

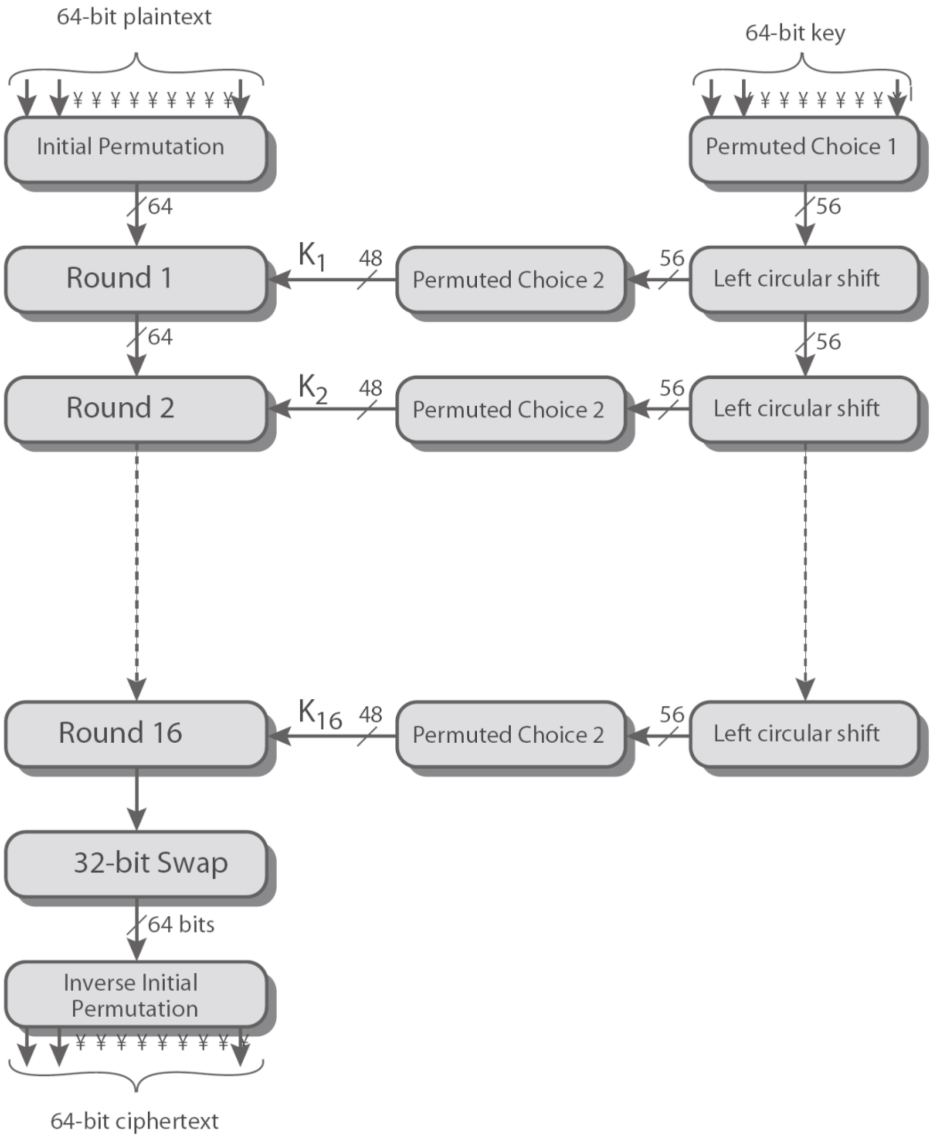
Feistel Cipher Structure



Block Cipher Structure

- have a general iterative block cipher structure
  - with a sequence of rounds
  - with substitutions / permutations controlled by key
- parameters and design features:
  - block size
  - key size
  - number of rounds
  - subkey generation algorithm
  - round function
  - also: fast software en/decrypt, ease of analysis

Data Encryption Standard (DES)



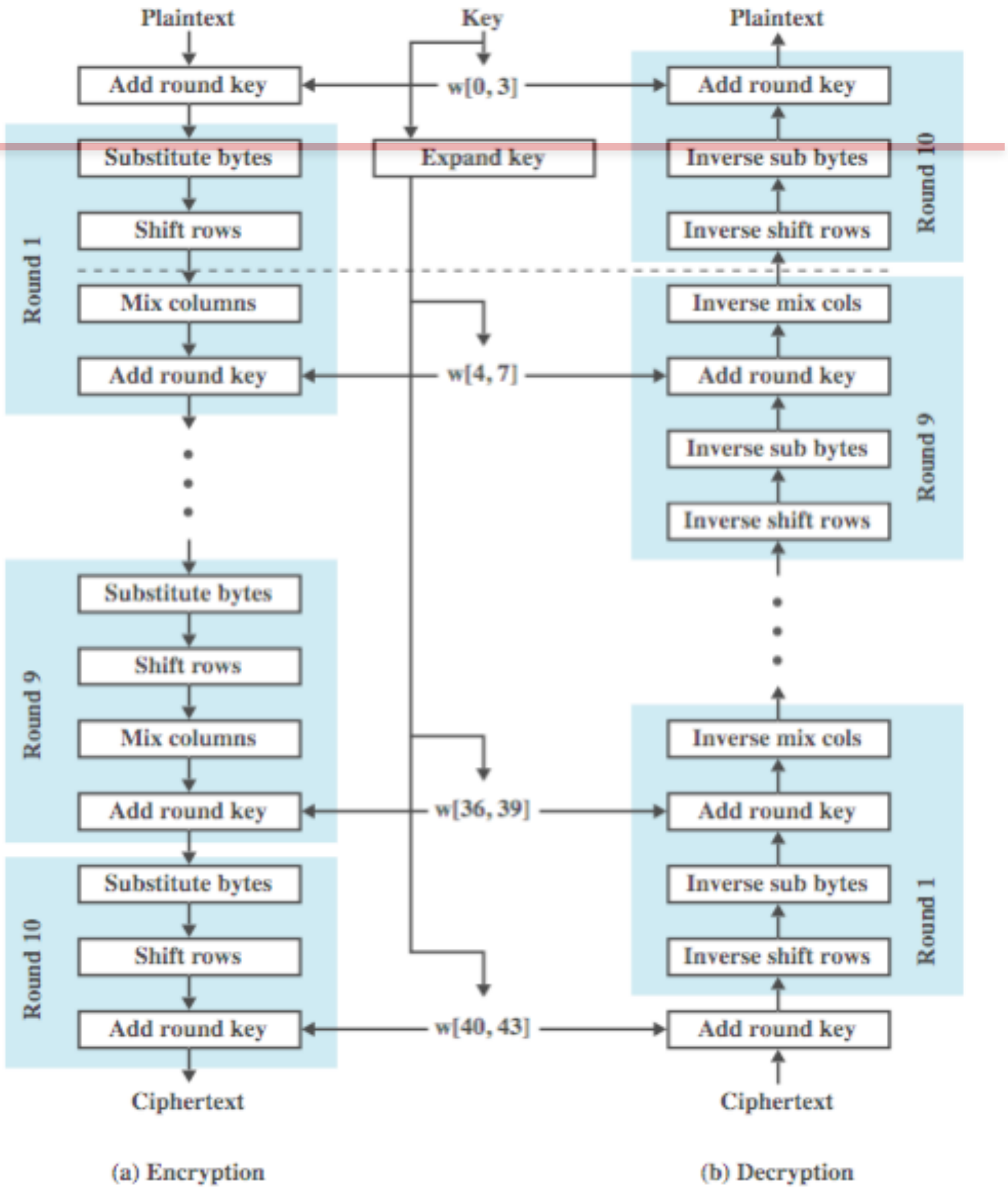
Triple DES (3DES)

- first used in financial applications
- in DES FIPS PUB 46-3 standard of 1999
- uses three keys & three DES executions:

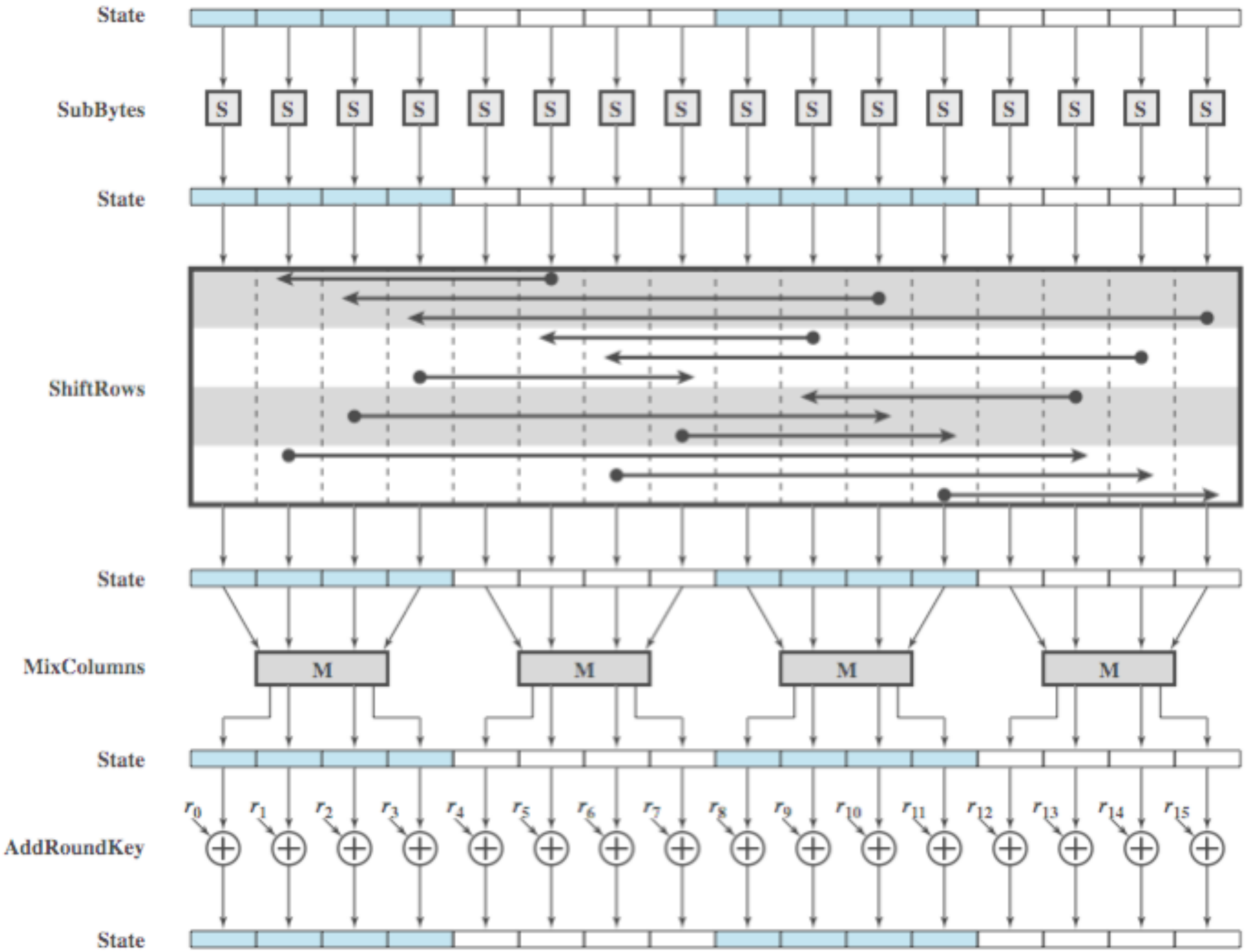
$$C = \mathrm{E}(K_3, \mathrm{D}(K_2, \mathrm{E}(K_1, P)))$$

- decryption same with keys reversed
- use of decryption in second stage gives compatibility with original DES users
- effective 168-bit key length, slow, secure
- AES will eventually replace 3DES

Advanced Encryption Standard (AES)



AES Round Structure



Substitute Bytes

- a simple table lookup in S-box
  - a 16🎞16 matrix of byte values
  - mapping old byte to a new value
    - e.g. {95} maps to {2A}
  - a permutation of all possible 256 8-bit values
- constructed using finite field properties
  - designed to be resistant to known cryptanalytic attacks
- decrypt uses inverse of S-box

Shift Rows

- on encrypt left rotate each row of State by 0,1,2,3 bytes respectively
- decrypt does reverse
- to move individual bytes from one column to another and spread bytes over columns

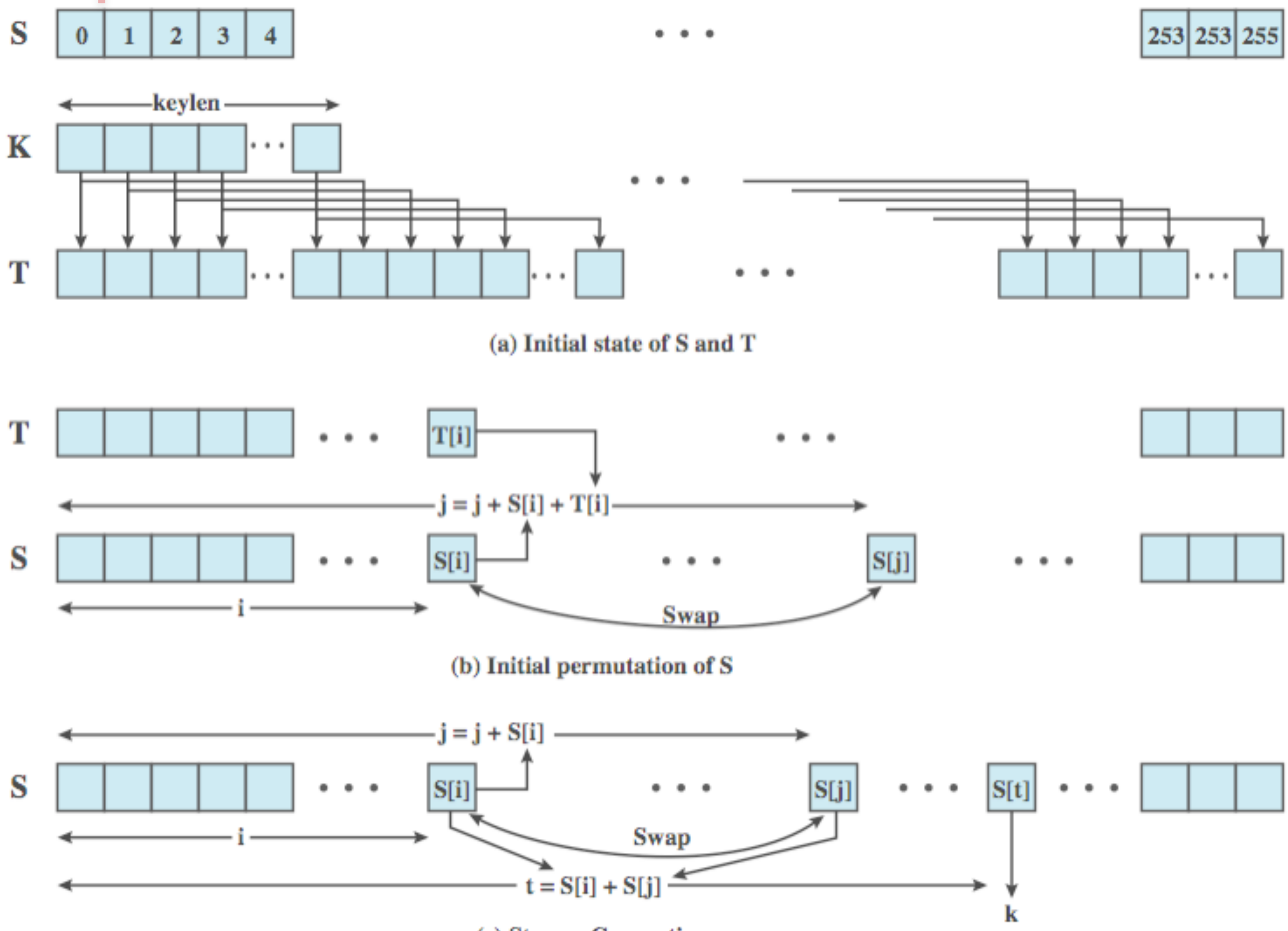
Mix Columns & Add Key

- Mix Columns
  - operates on each column individually
  - mapping each byte to a new value that is a function of all four bytes in the column
  - use of equations over finite fields
  - to provide good mixing of bytes in column
- Add Round Key
  - simply XOR State with bits of expanded key
  - security from complexity of round key expansion and other stages of AES

Stream Ciphers

- processes input elements continuously
- key input to a pseudorandom bit generator
  - produces stream of random like numbers
  - unpredictable without knowing input key
  - XOR keystream output with plaintext bytes
- are faster and use far less code
- design considerations:
  - encryption sequence should have a large period
  - keystream approximates random number properties
  - uses a sufficiently long key

RC4



(a) Initial state of S and T

(b) Initial permutation of S

(c) Stream Generation

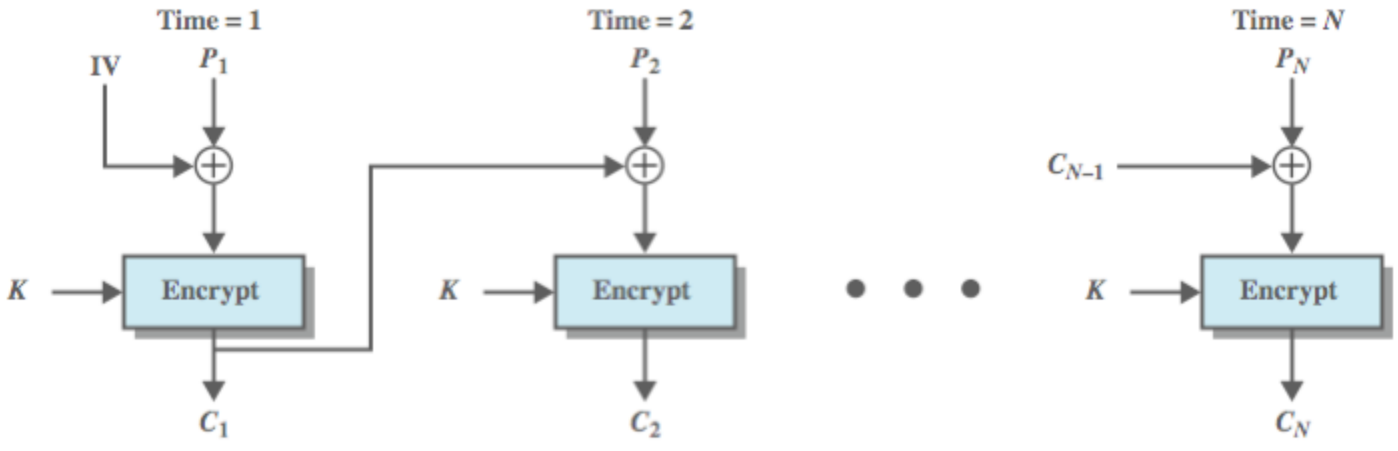
Modes of Operation

- block ciphers process data in blocks
  - e.g. 64-bits (DES, 3DES) or 128-bits (AES)
- for longer messages must break up
  - and possibly pad end to blocksize multiple
- have 5 five **modes of operation** for this
  - defined in NIST SP 800-38A
  - modes are: ECB, CBC, CFB, OFB, CTR

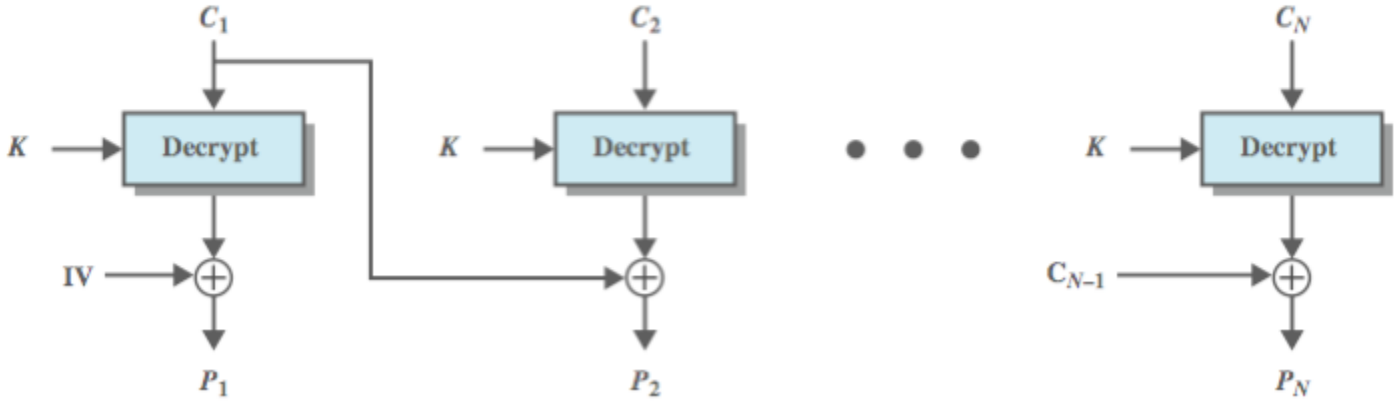
Electronic Codebook (ECB)

- simplest mode
- split plaintext into blocks
- encrypt each block using the same key
- “codebook” because have unique ciphertext value for each plaintext block
  - not secure for long messages since repeated plaintext is seen in repeated ciphertext

Cipher Block Chaining (CBC)

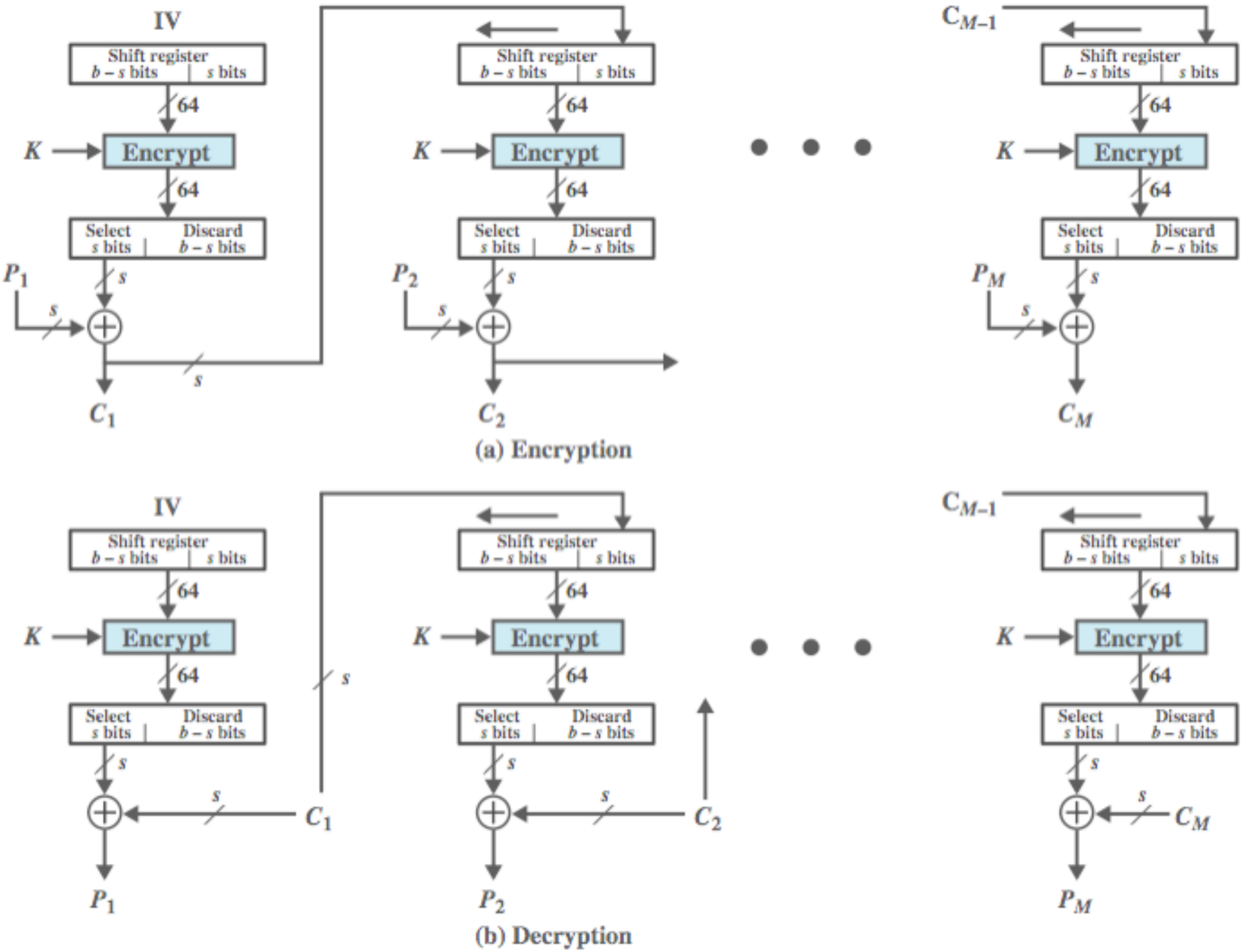


(a) Encryption

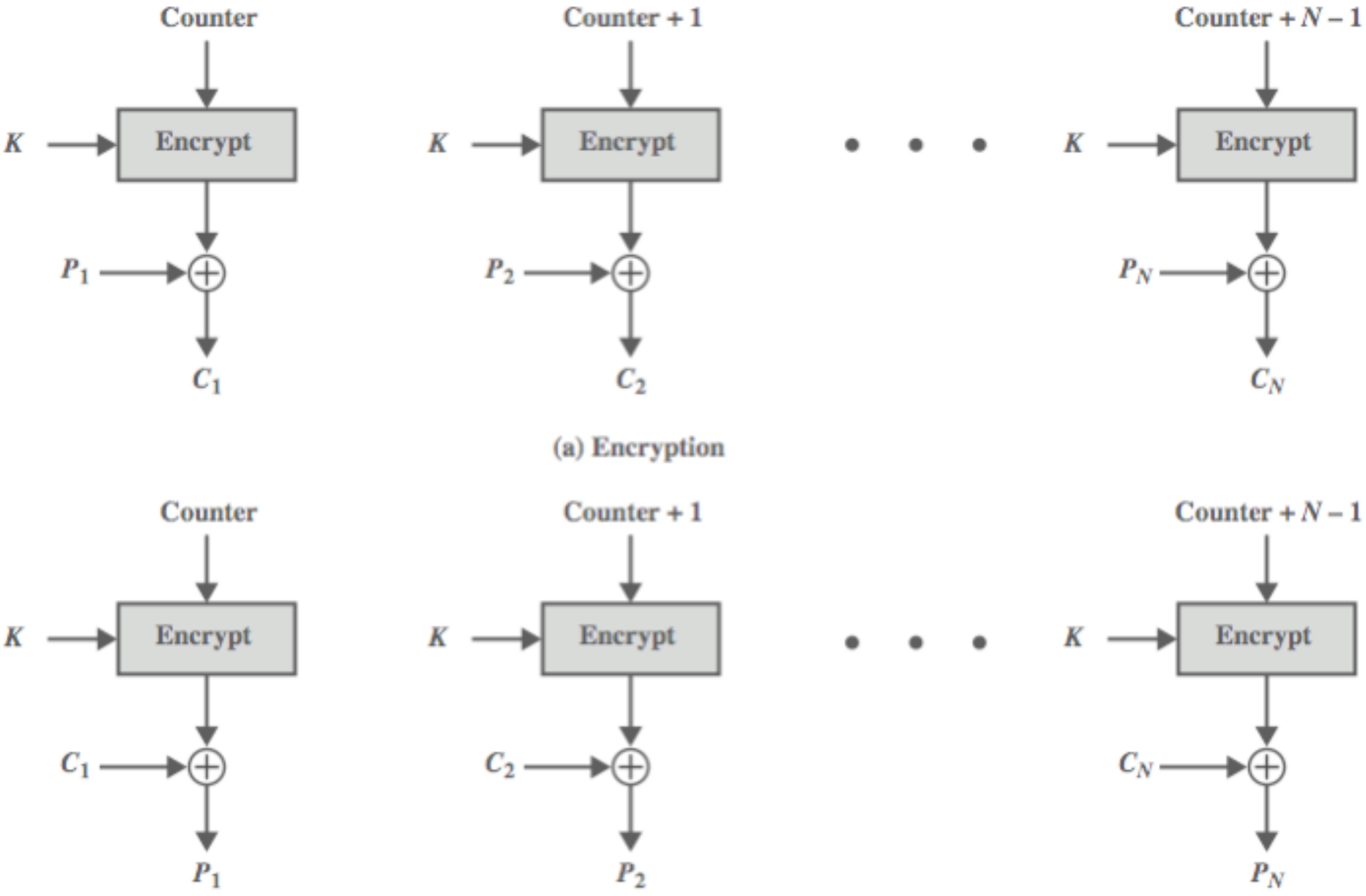


(b) Decryption

Cipher Feedback (CFB)



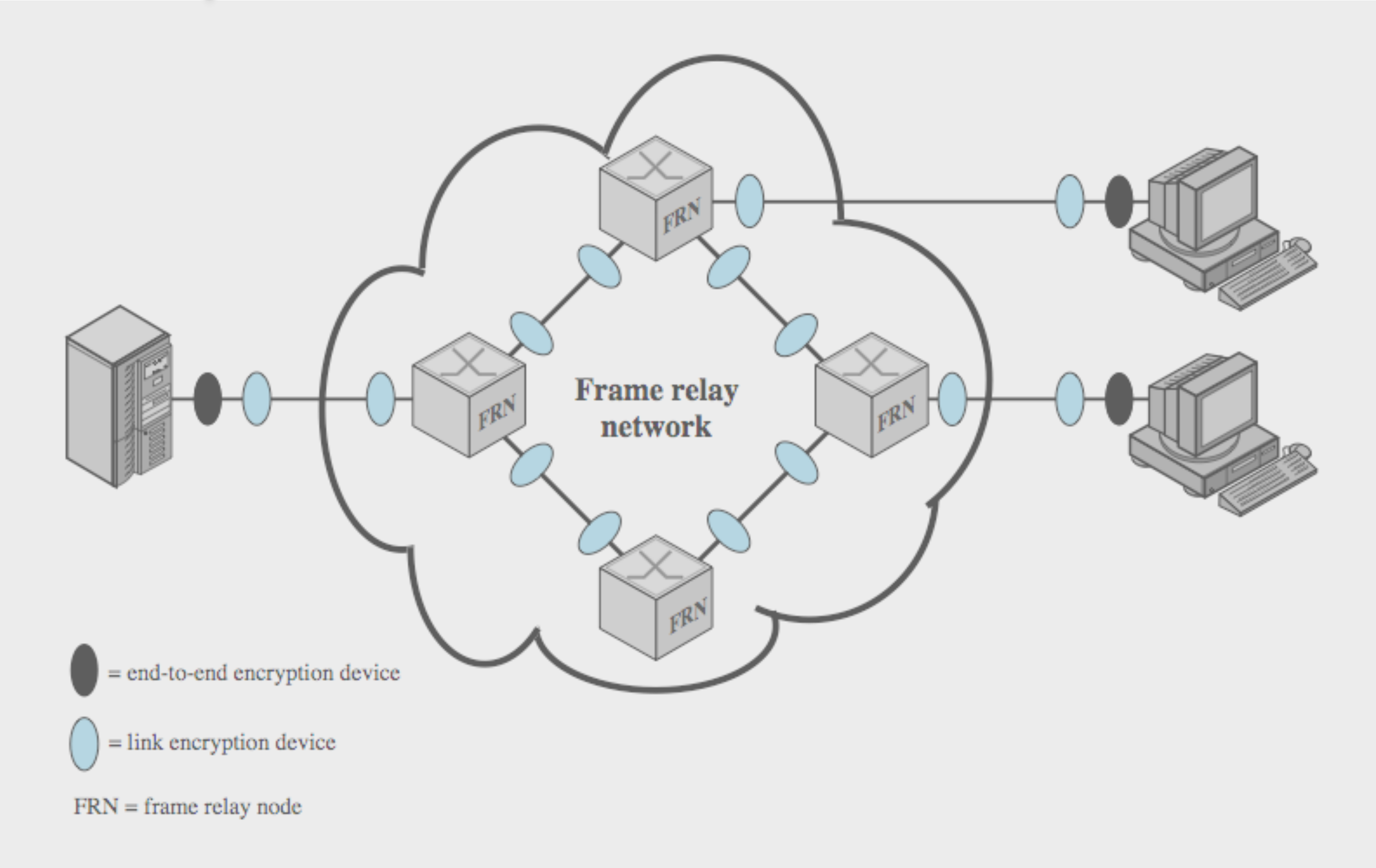
Counter (CTR)



(a) Encryption

(b) Decryption

Location of Encryption

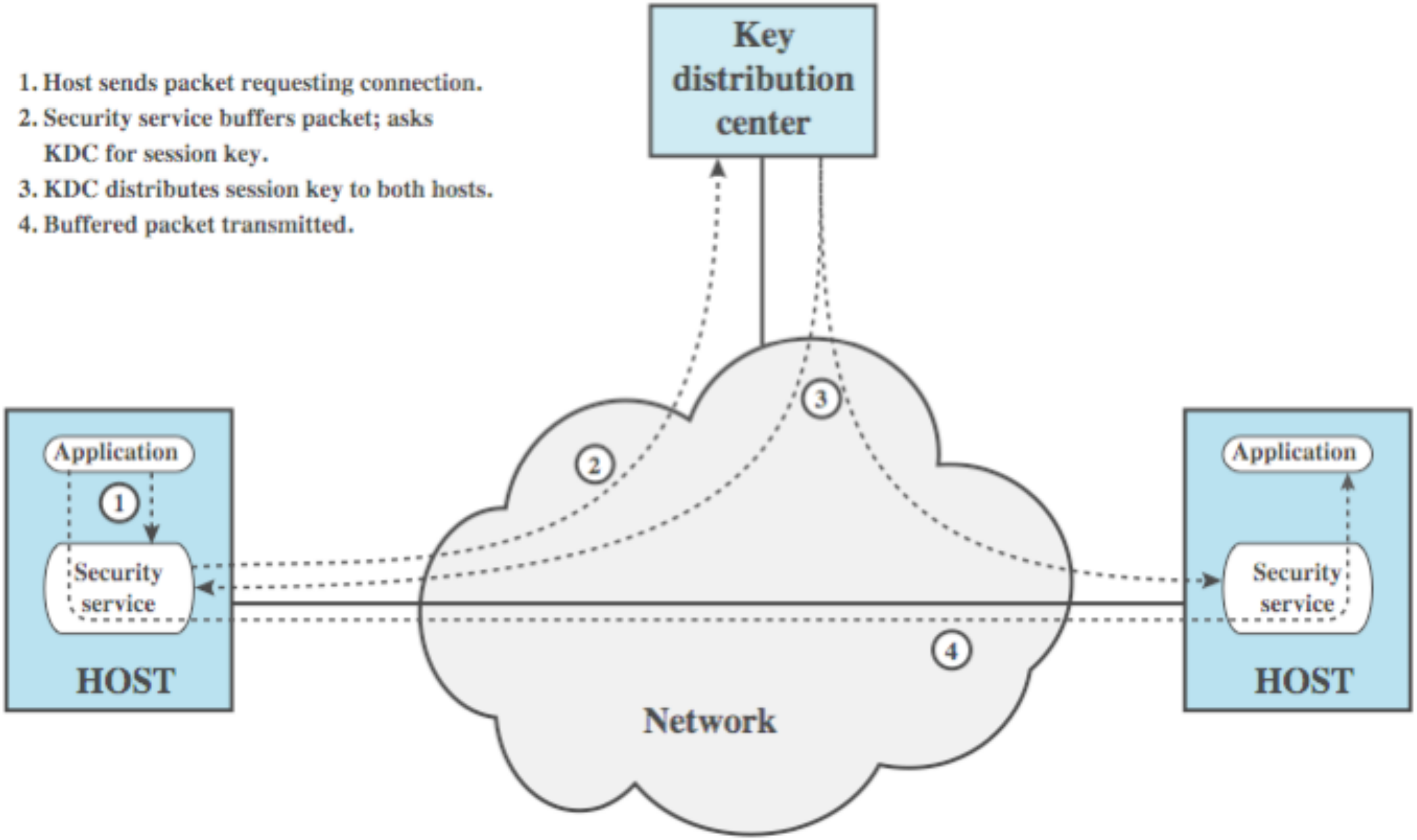


Key Distribution

- symmetric crypto needs a shared key:
- two parties A & B can achieve this by:
  - A selects key, physically delivers to B
  - 3rd party select keys, physically delivers to A, B
    - reasonable for link crypto, bad for large no's users
  - A selects new key, sends encrypted using previous old key to B
    - good for either, but security fails if any key discovered
  - 3rd party C selects key, sends encrypted to each of A & B using existing key with each
    - best for end-to-end encryption

Key Distribution

1. Host sends packet requesting connection.
2. Security service buffers packet; asks KDC for session key.
3. KDC distributes session key to both hosts.
4. Buffered packet transmitted.



Summary

- introduced symmetric encryption basics
- DES, 3DES and AES
- stream ciphers and RC4
- modes of operation
- location of encryption
- key distribution