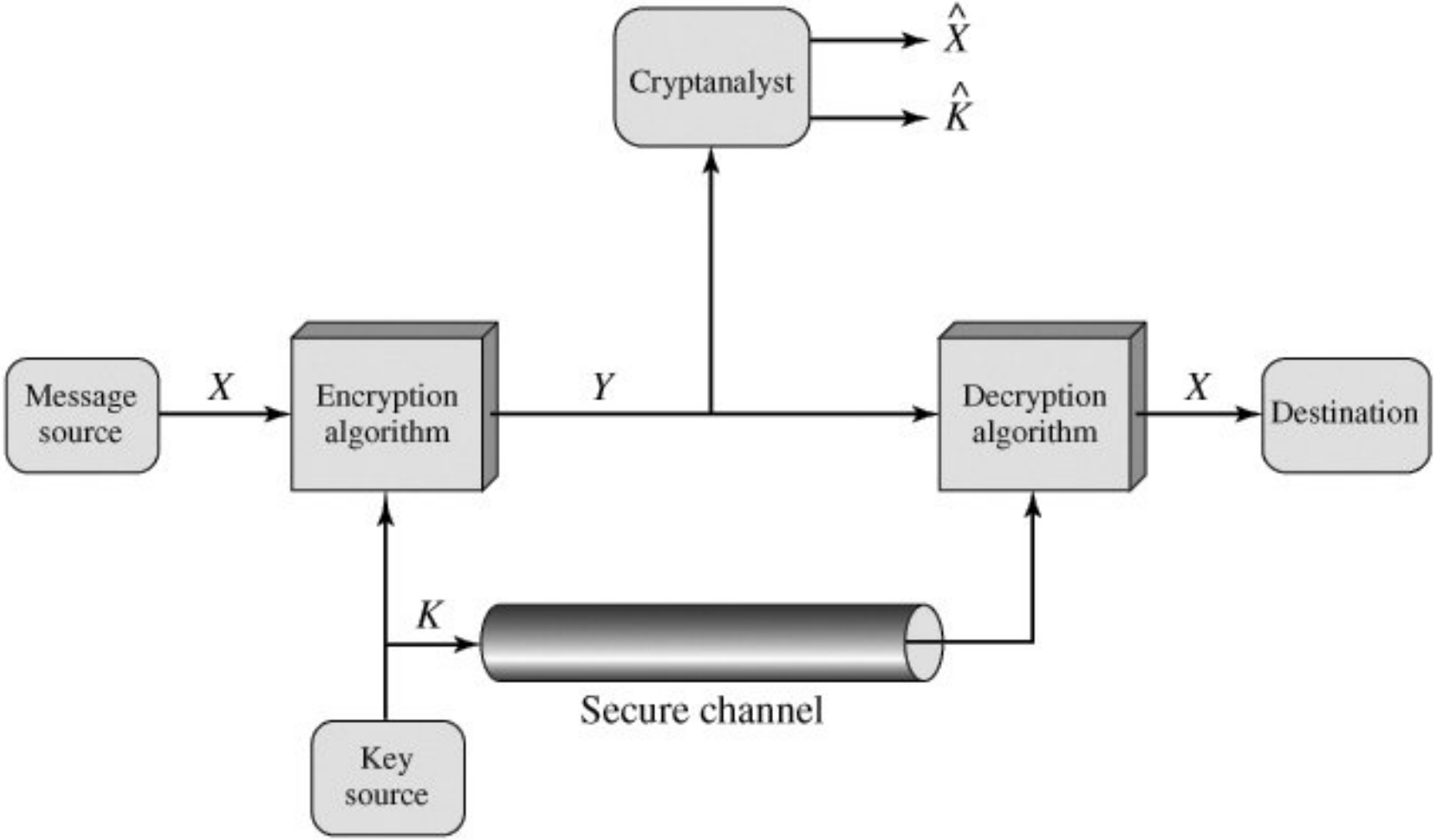
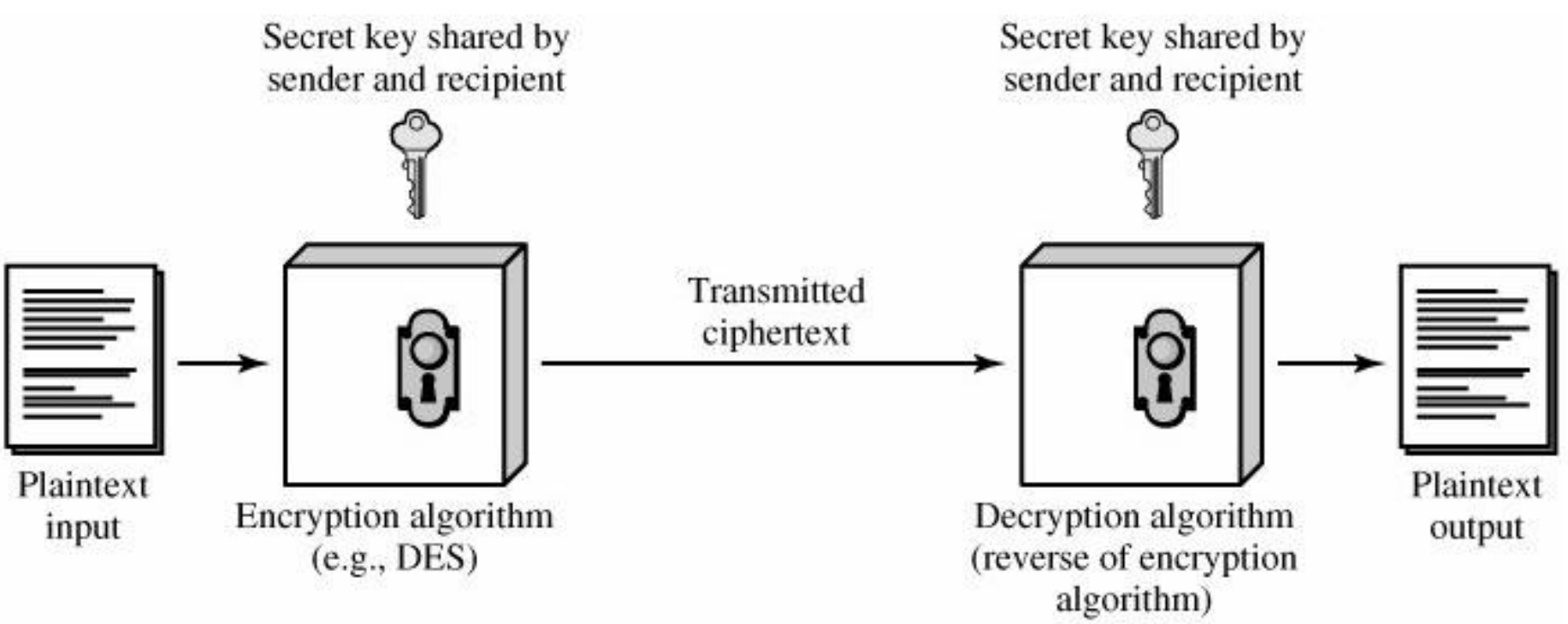
IT 422 Network Security Cryptography 2

Yasser F. O. Mohammad

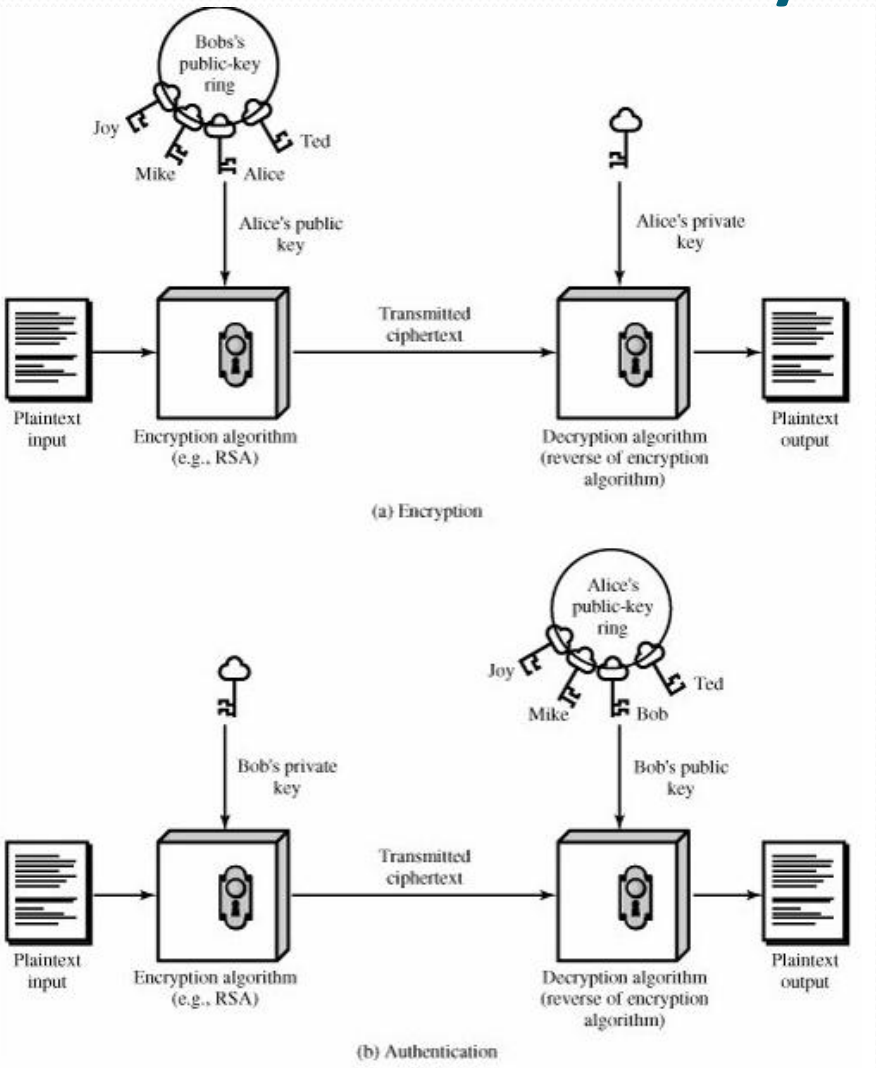
REMINDER 1: Operational of Conventional Cryptosystem



REMINDER 2: Shared Key Encryption



REMINDER 3: Public Key Encryption



REMINDER 4: Classical Cryptosystems

Substitution Techniques

- Caesar Cipher
  - Example
    Plain : meet me after the toga party
    cipher: PHHW PH DIWHU WKH WRJD SDUWB

  - Subtitution Table:
    plain: abcdefghijklmnopqrstuvwxyz
    cipher: DEFGHIJKLMNOPQRSTUVWXYZABC

  - Formula
    $C = E(3, p) = (p + 3) \bmod 26$
    $p = D(k, C) = (C - k) \bmod 26$

How to do cryptanalysis???

One Time Pad

- Ultimate Security Algorithm

$$c_i = k_i \oplus p_i$$

- If *k* is truly random, then the code is unbreakable

- To encipher a text of *n* characters you need to securely distribute a key of *n* characters. Why don't we transfer the original plain text instead?

Simple Transposition Cipher

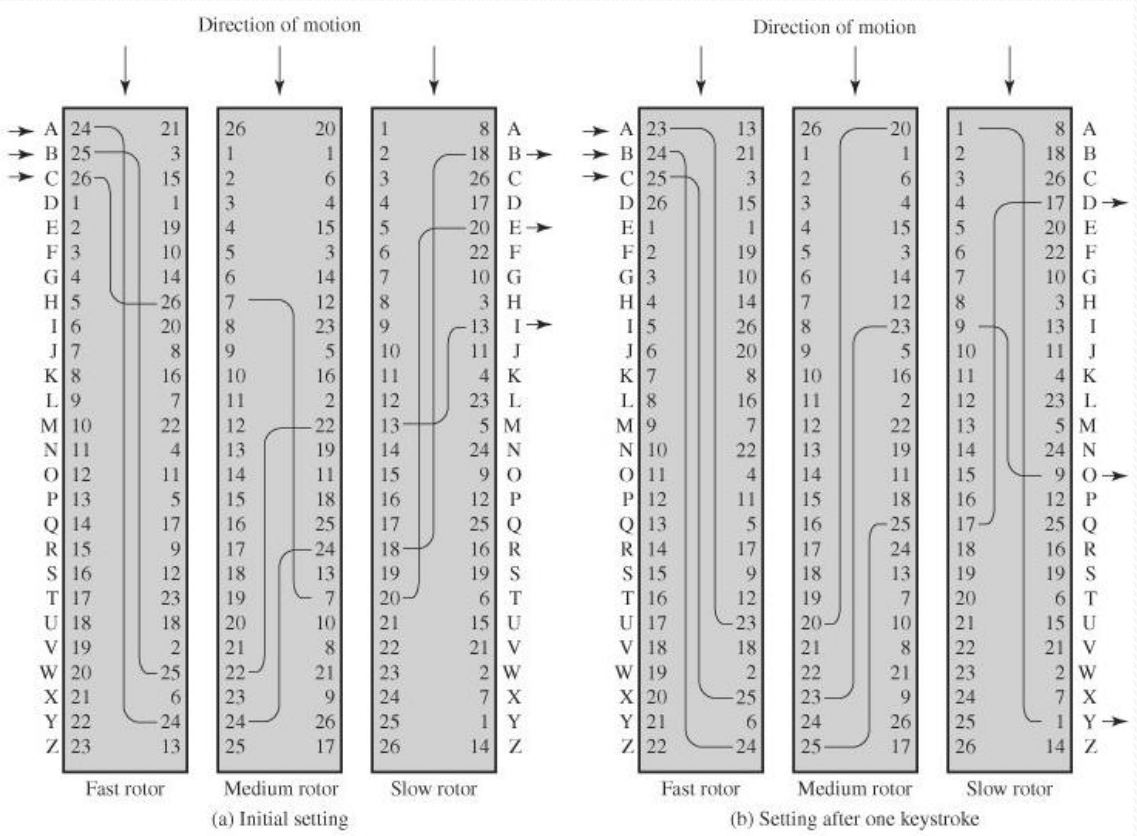
- Put data in rows and read them in columns of arbitrary order

- Key: 4 3 1 2 5 6 7
- Input: t t n a a p t
  m t s u o a o
  d w c o i x k
  n l y p e t z

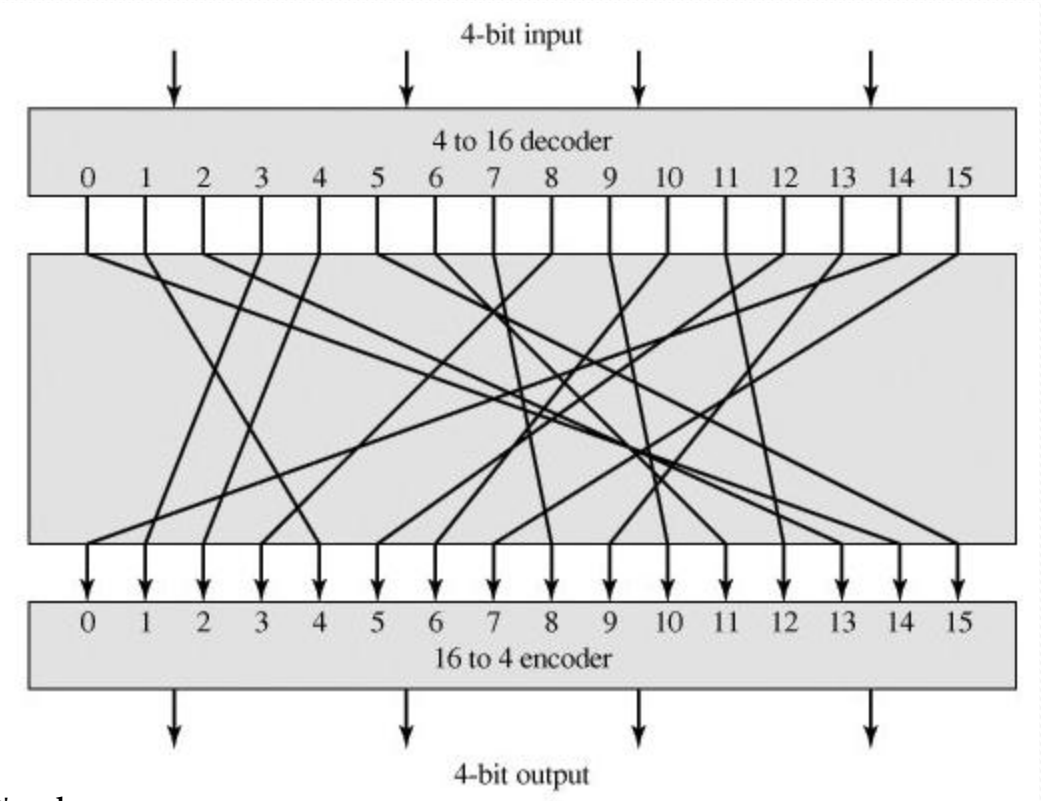
Output: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

Rotor Machines

- Used by German (Engema) and Japanes (Purple) in WW II and was broken by Turing and others



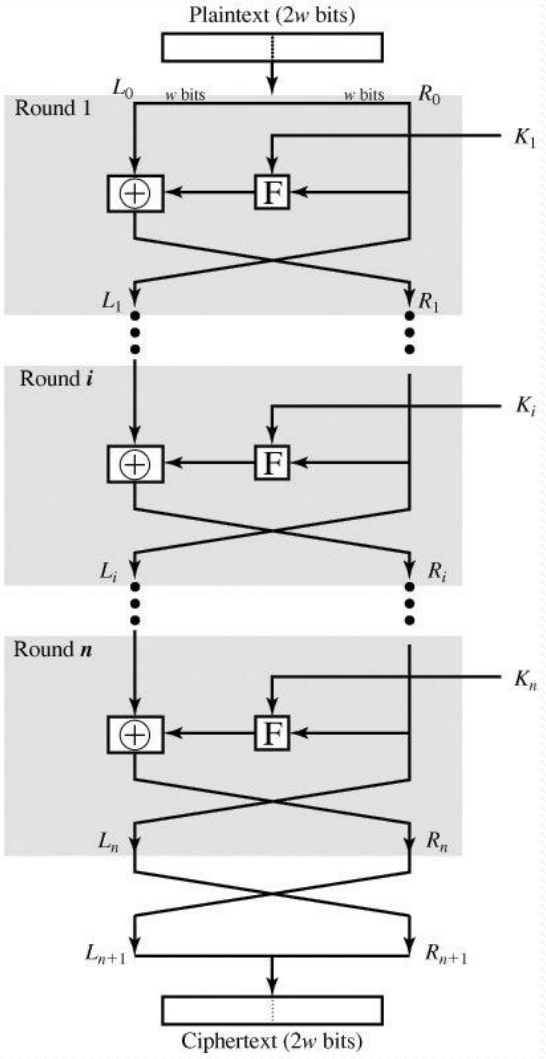
Ideal Block Cipher



- Needs $n*2^n$ key
- Short Block → Easily breakable
- Long Block → Difficult to implement (storing the key)

Fiestel Network

- Each round consists of:
  - Substitution on left half of text
  - Permutation of the two halves
- The substitution is controlled by the key of every round
- Factors of Security:
  - Block size
  - Key size
  - N. rounds
  - Subkey generation
  - Round Function
- Decryption = Encryption with reversed subkey order



Example Block Ciphers

- DES (Data Encryption Standard)≈DEA
  - 1977 and cracked in 1998 with 250,000$ in 3 days
  - 64 bits block and 56 bits key
- 3DES
  - C=E(k3,D(k2(E(k1,M))), M=D(k1,E(k2(D(k3,C)))
  - Key length=56, 112, 168
  - Not suitable for software
- AES (Advanced Encryption Standard)
  - 128 bits block and 128,192,256 blocks key
  - Not a Feistel structure

Other Examples of Block Ciphers

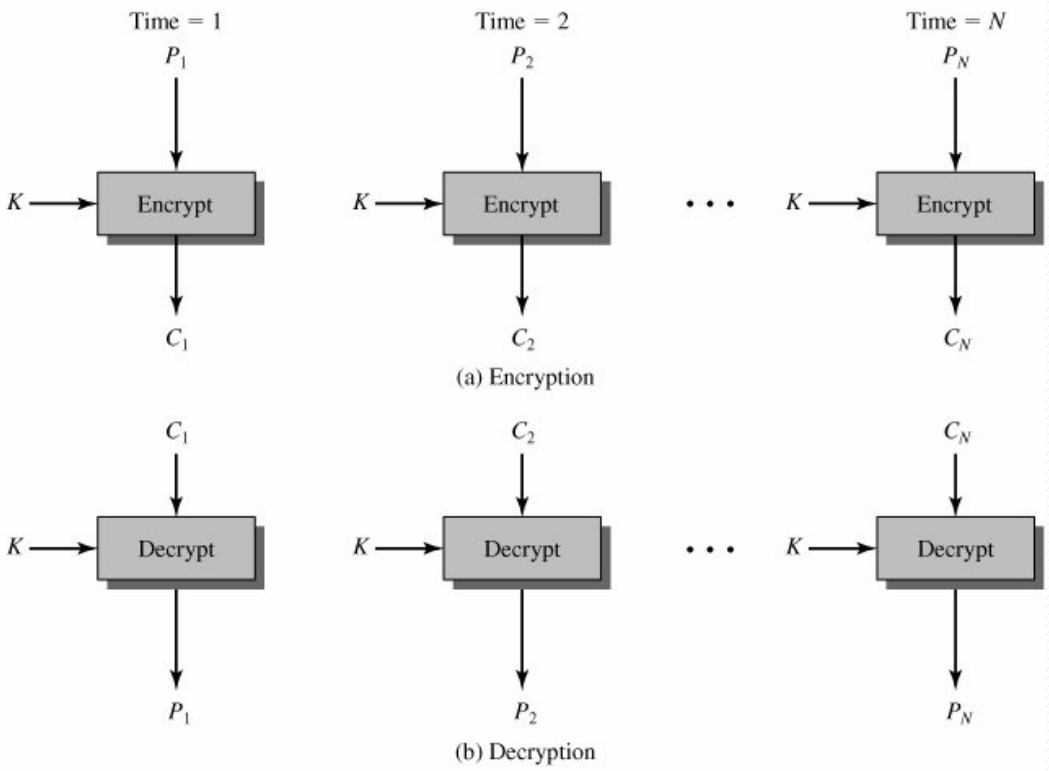
- IDEA (International Data Encryption Algorithm)
  - 128 bit key
  - Uses XOR, binary addition and multiplication
- Blowfish
  - 1993 by Bruce Schneier
  - Fast and easy to implement
  - Variable S-boxes
- RC5
  - 1994 By Ron Rivest
  - Suitable for hardware and software
  - Used by RSA security Inc.

Uses of Shared-Key Ciphers

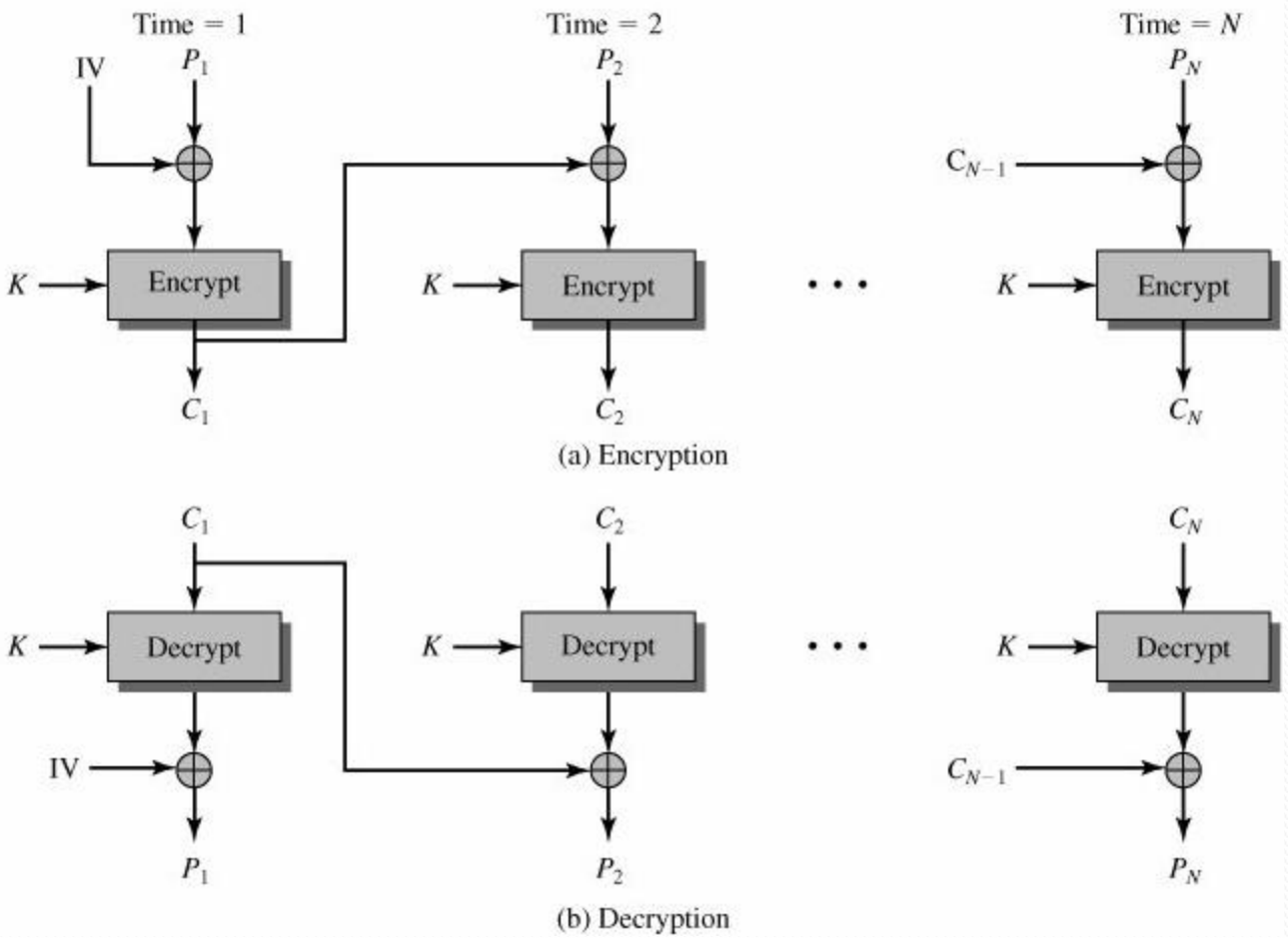
Algorithm	Key Size (bits)	Block Size (bits)	Number of Rounds	Applications
DES	56	64	16	SET, Kerberos
Triple DES	112 or 168	64	48	Financial key management, PGP, S/MIME
AES	128, 192, or 256	128	10, 12, or 14	Intended to replace DES and 3DES
IDEA	128	64	8	PGP
Blowfish	Variable to 448	64	16	Various software packages
RC5	Variable to 2048	64	Variable to 255	Various software packages

ECB (Electronic Codebook)

- Just apply it to every block in succession
- Every plain text block has the same corresponding cipher

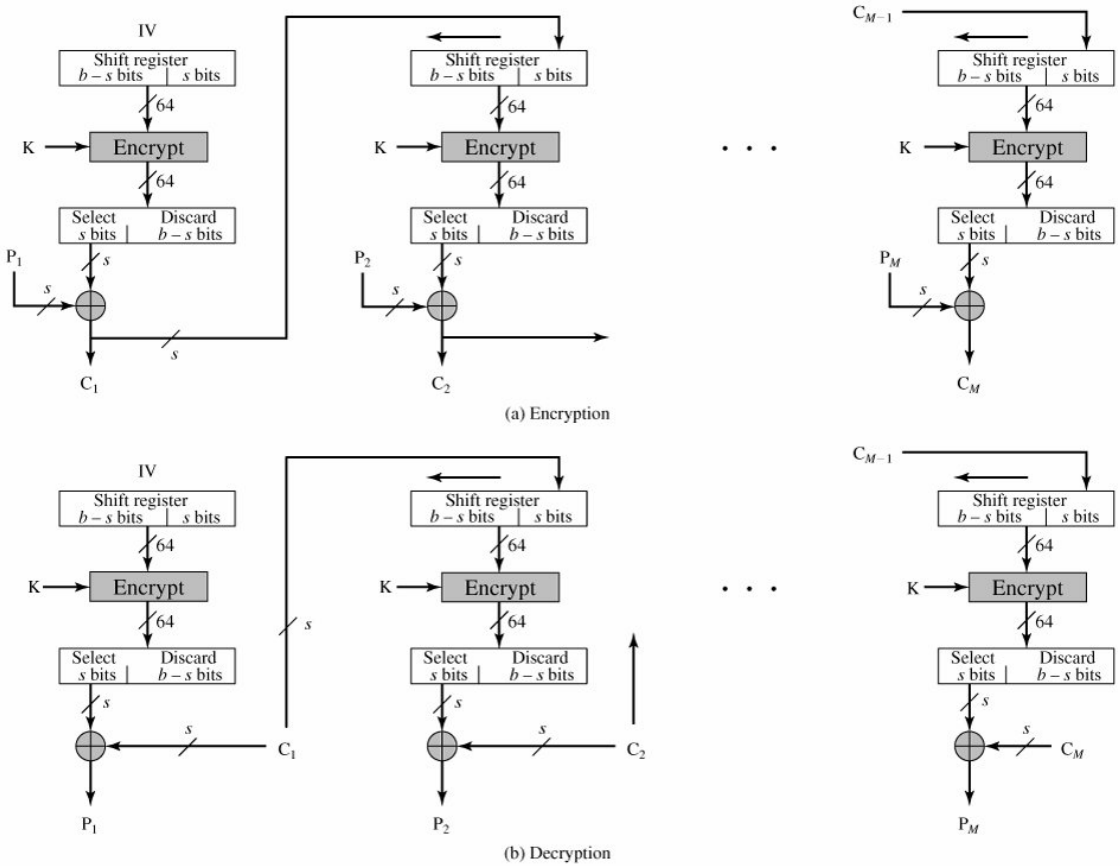


CBC (Cipher Block Chaining Mode)



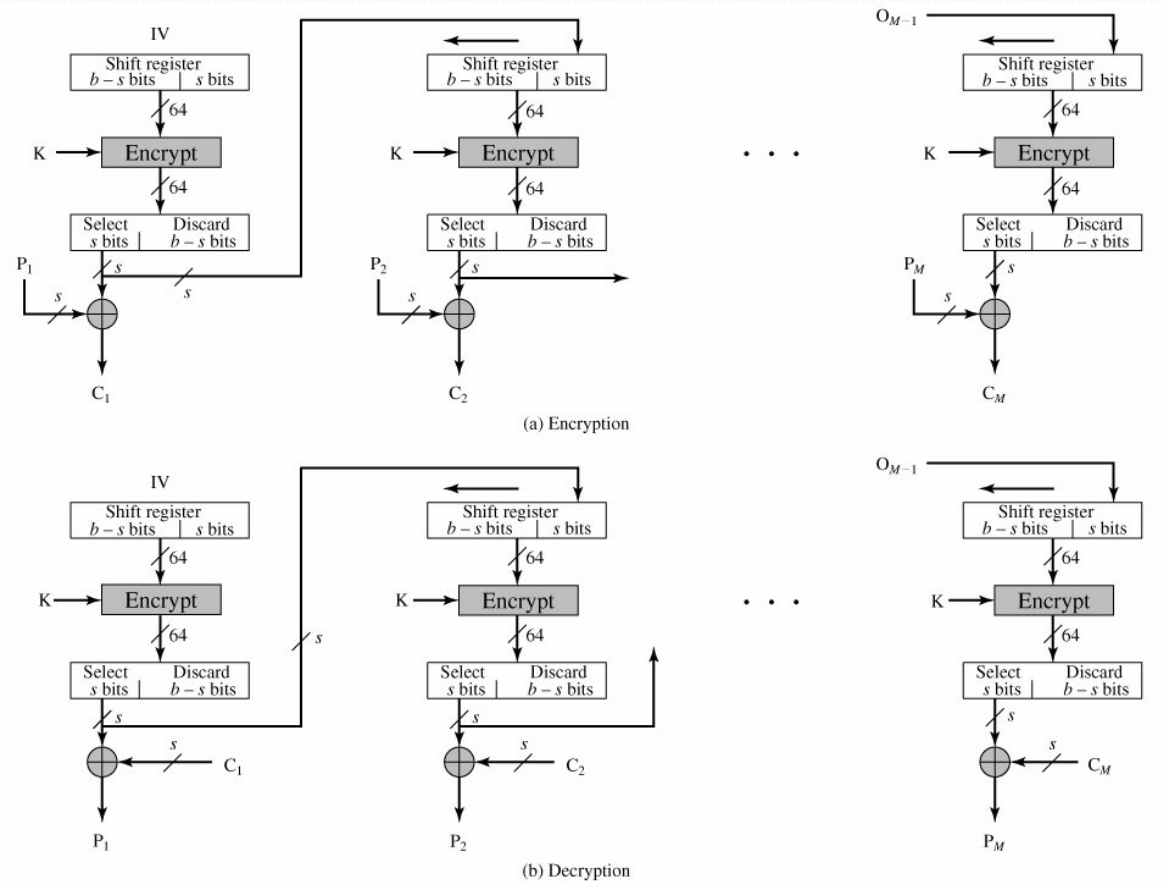
CFB (Cipher Feedback Mode)

- Block cipher → stream cipher

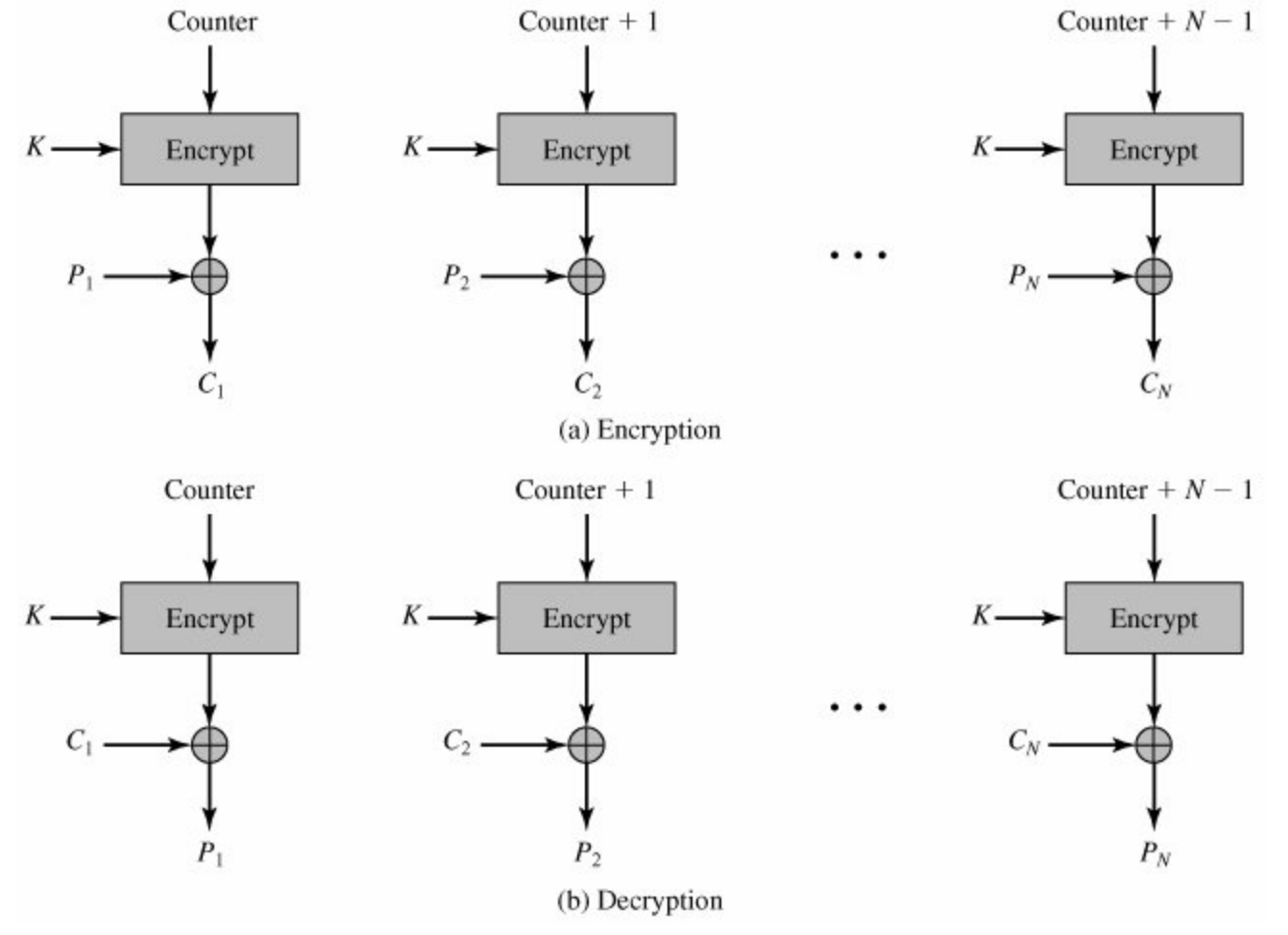


OFB (Output Feedback Mode)

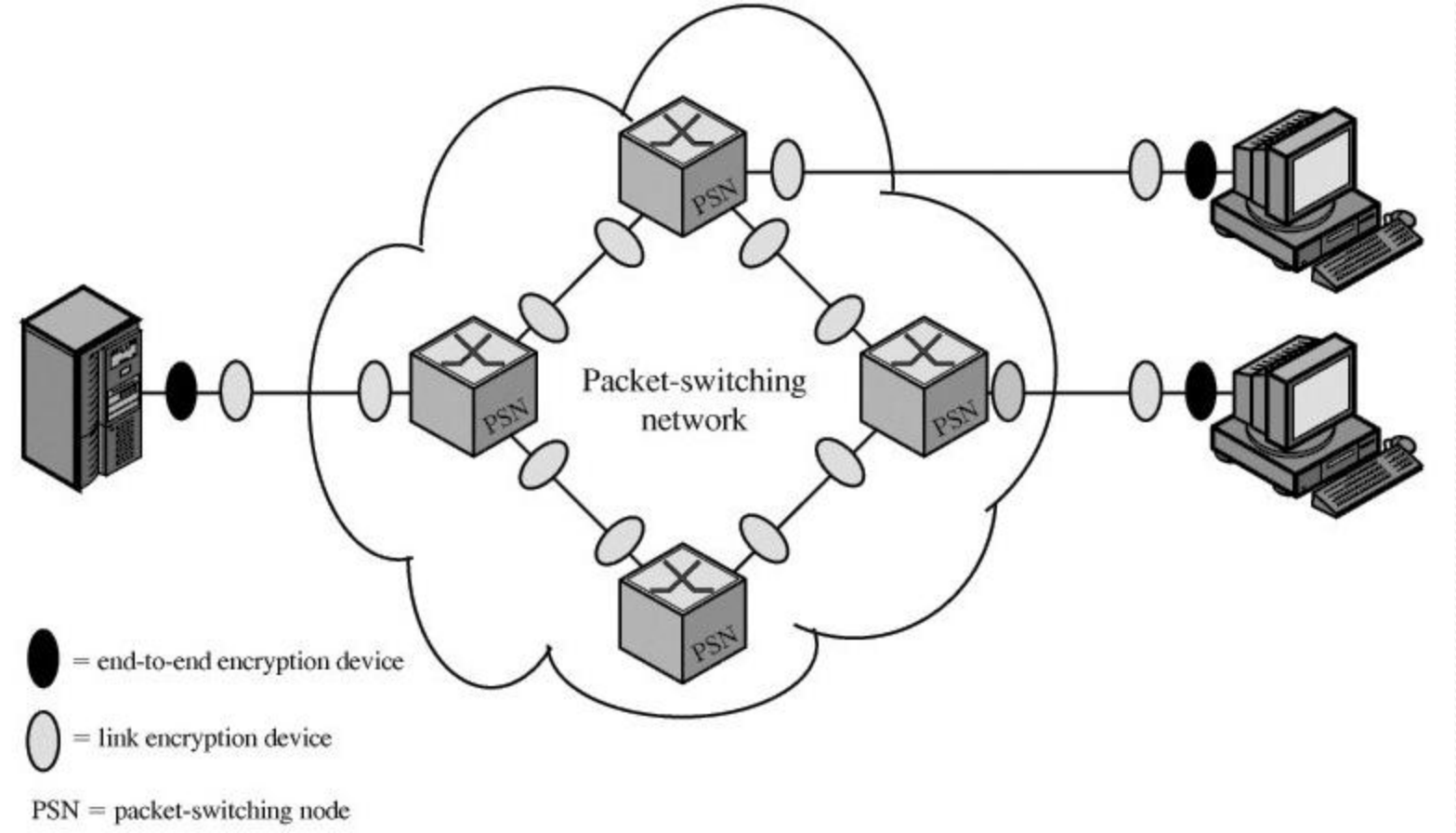
- Block cipher → Stream cipher



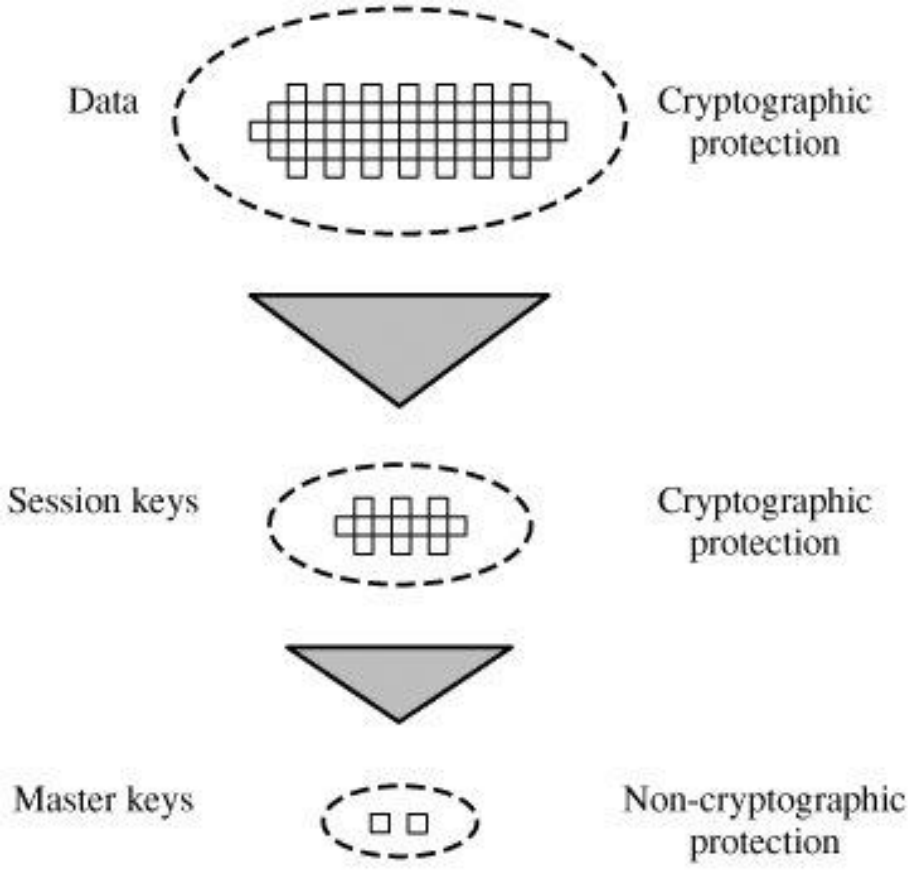
CTR (Counter Mode)



Location of Encryption Function



Key Hierarchy



Key Distribution Center