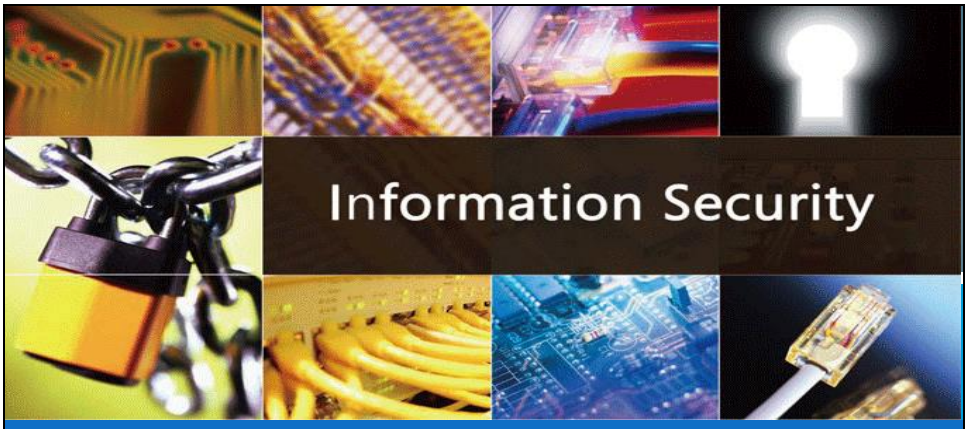


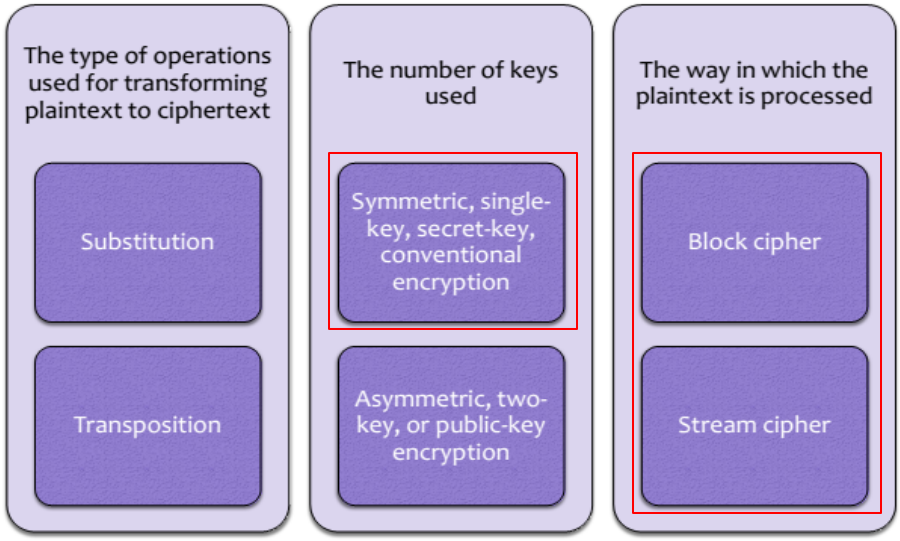
Symmetric encryption

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Objective

- Introduction
- Block Cipher Scheme
- Data Encryption Standard
- Mangler Function
- S-Box
- Security of DES
- Triple DES
- AES

Taxonomy of Cryptography



Symmetric encryption

- **Introduction**
- **Model**
- **Block Cipher vs. Stream Cipher**
- **The Data Encryption Standard**
  - DES Encryption
  - DES Decryption
  - AES

Introduction: components

- There are two requirements for secure use of conventional encryption:

  - A strong encryption algorithm.
  - A secret key

- Symmetric encryption:
  - transforms plaintext into ciphertext using a secret key and an encryption algorithm.
  - recoveres from the ciphertext to the plaintext using the same key and a decryption algorithm

Introduction: advantage and limit

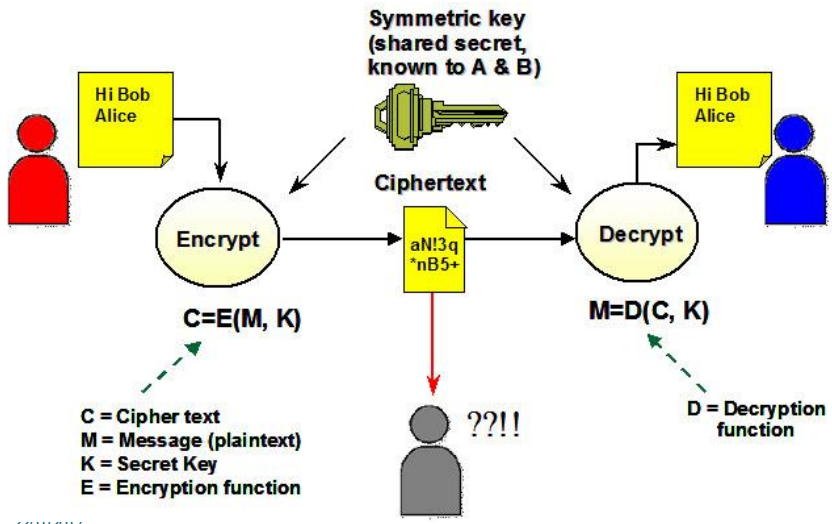
- Modern symmetric algorithms are great at all of the following:
  Preserving (protective, maintaining) confidentiality
  Increasing speed
  Ensuring simplicity (relatively speaking, of course)
  Providing authenticity (legitimacy)

- Symmetric algorithms have their drawbacks:
  Key management issues
  Lack of nonrepudiation features

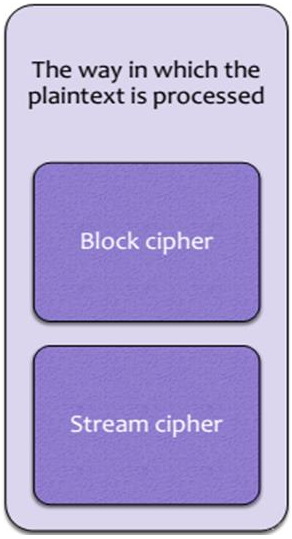
Introduction: common algorithms

- **Data Encryption Standard (DES)** Originally adopted by the U.S. government in 1977. DES is a 56-bit key algorithm => too short to be used today for any serious security applications.
- **Triple DES (3DES):** an extension of the DES algorithm, which is three times more powerful than the DES algorithm. Used a 168-bit key.
- **Blowfish (by** B.Schneier.)**:** strong, fast, and simple in its design. The algorithm uses a 448-bit key and is optimized for use in today's 32- and 64-bit processors.
- **International Data Encryption Algorithm (IDEA)** (1990, Switzerland). It used to protect the privacy of e-mail, data.. This algorithm is seen in applications such as the Pretty Good Privacy (PGP) system
- **MARS** This AES finalist was developed by IBM and supports key lengths of 128–256 bits.
- **Advanced Encryption Standard (AES)** The successor to DES and chosen to be the new U.S. encryption standard by NIST. The algorithm is very compact and fast and can use keys that are 128, 192, or 256 bits long.
- RC2,4,5,6

Symmetric encryption model



Block Cipher & Stream Cipher



Block Cipher & Stream Cipher

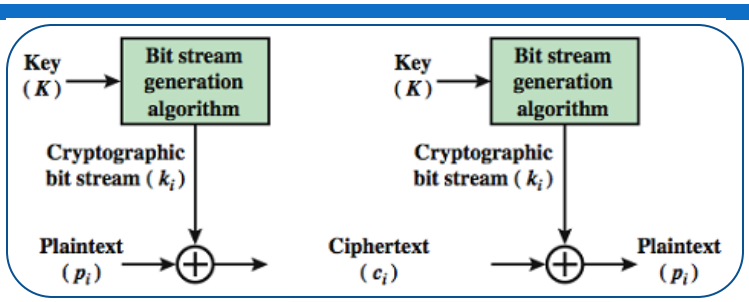
- **Block Cipher vs. Stream Cipher**
- **Block Cipher Principles**
  - Stream Ciphers and Block Ciphers
  - Motivation for the Feistel Cipher Structure
  - The Feistel Cipher
- **The Data Encryption Standard**
  - DES Encryption
  - DES Decryption

Block Cipher vs. Stream Cipher

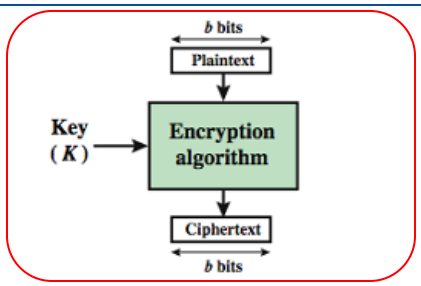
- A block cipher is one in which ***a block*** **of plaintext is treated as *a whole* and used to produce a ciphertext block of *equal length***
  - **Typically, a block size of 64 or 128 bits is used**
- **A stream cipher is one that encrypts a digital data stream *one bit* or *one byte* at a time**

Block Cipher vs. Stream Cipher

Stream Cipher



Block Cipher



Stream Cipher

- Encryption:
  - plaintext one byte at a time, although a stream cipher may be designed to operate on one bit at a time or on units larger than a byte at a time
- Key:
  - is input to a bit fake generator - produce a random 8-bit line => generate an output key stream,
  - It combines one byte at a time with the plaintext using exclusive-OR operation (XOR) operation

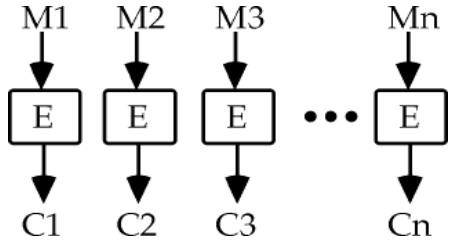
```
  11001100  plaintext
⊕ 01101100  key stream
  10100000  ciphertext

  10100000  ciphertext
⊕ 01101100  key stream
  11001100  plaintext
```


Block Cipher Principles

- Most symmetric block ciphers are *based on a Feistel Cipher Structure*
- Needed since must be able to decrypt ciphertext to recover messages efficiently
- Block ciphers look like an extremely large substitution
- Would need table of 264 entries for a 64-bit block
- Instead create from smaller building blocks
- Using idea of a product cipher

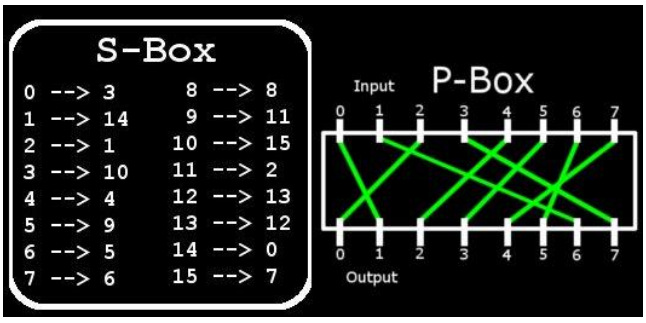
Block Cipher

- Plaintext M = M1,M2…, encrypted with the same key.
- Feistel cipher is a **block cipher** operates on a plaintext block of ***n bits*** **to produce a ciphertext block of *n bits*.**
  - *Ex:* for DES a big letter is a 64-bit block and number of different letters is 2^{64}



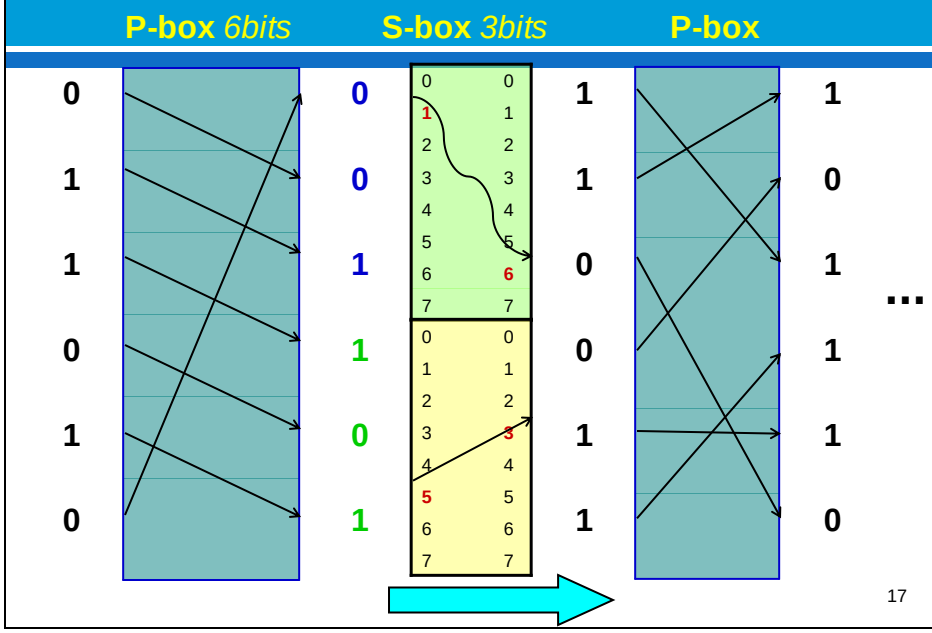
Substitution – Permutation Network

- S-P Network (proposed by Claude Shannon) formed the basic of block cryptography
- S-P Network based on 2 transformations:
  - *Substitution & Permutation*



16

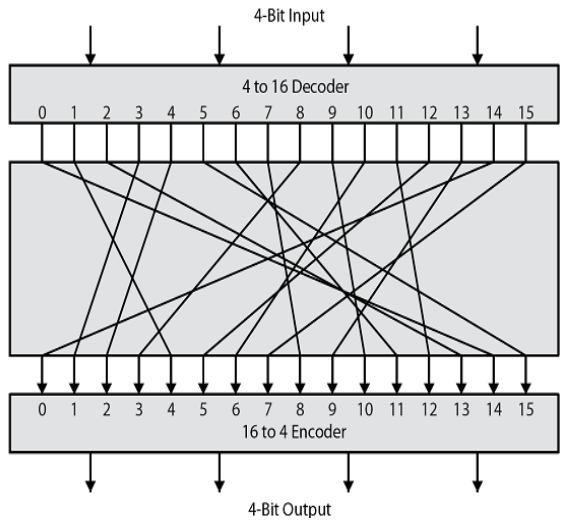
Combine P-box and S-box



Ideal Block Cipher

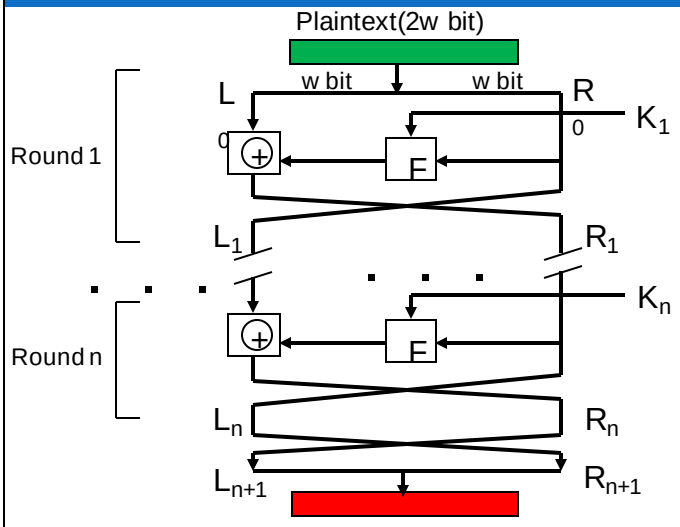
Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111

Ciphertext	Plaintext
0000	1110
0001	0011
0010	0100
0011	1000
0100	0001
0101	1100



This is the most general form of block cipher

Feistel Cipher Structure



64 bit input

Input permutation

L and R words

Apply round function

Outputs are inputs to next round

Swap left and right words

Apply inverse of IP

64 bit output

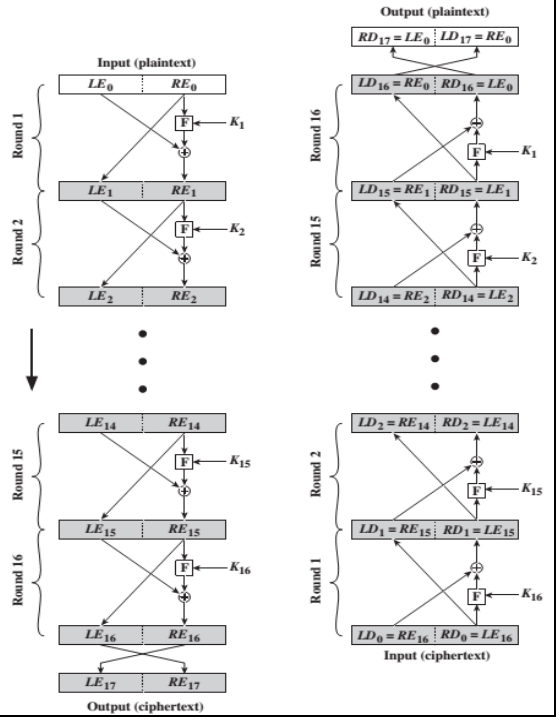
Feistel Encryption and Decryption

- Encryption:

$L_i = R_{i-1}$; $R_i = L_{i-1}$ XOR $F(R_{i-1}, K_i)$;

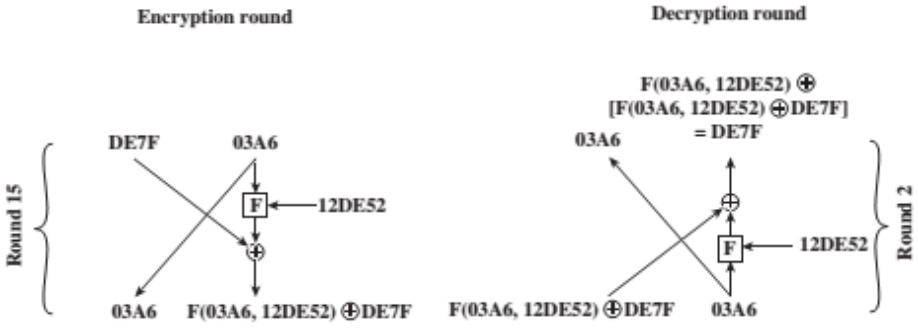
- Dencryption:

$R_{i-1} = L_i$; $L_{i-1} = R_i$ XOR $F(L_i, K_i)$



Feistel ex

- 1 round



Feistel Cipher Design Elements

- Some elements:
  - block size: larger – more secure
  - key size: longer - more secure
  - number of rounds: more - more secure
  - subkey generation algorithm: more complex – difficult to break
  - round function: more complex – difficult to break
  - fast software en/decryption
  - ease of analysis

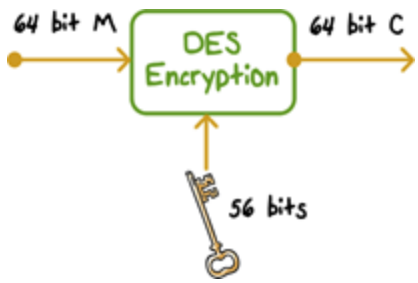
Modern block ciphers

- Modern block ciphers include:
  - **DES -** Data Encryption Standard
  - **AES,**
  - Blowfish,
  - IDEA,
  - LOKi,
  - RC5,
  - etc.

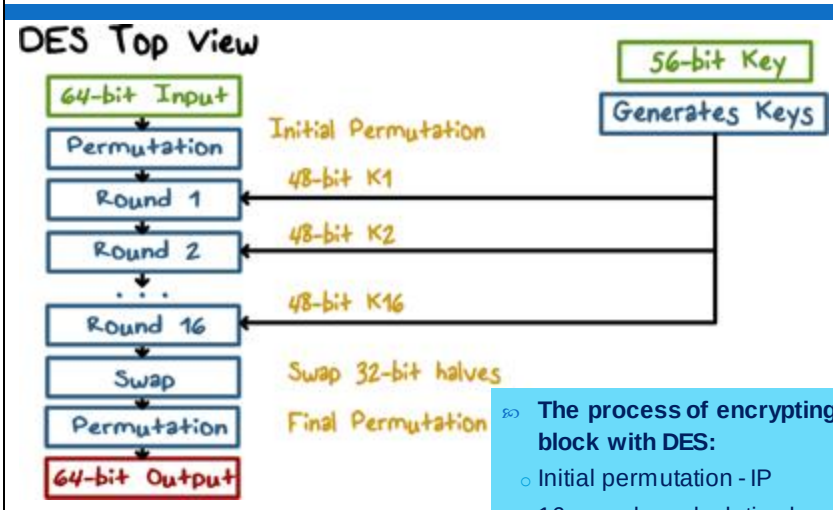
- **DEA:** Data Encryption Algorithm
  - has the exact structure of Feistel Cipher but without Initial Permutation (IP) and Inverse Initial Permutation
  - transforms 64-bit input in a series of steps into a 64-bit output.
  - The same steps, with the same key, are used to reverse the encryption

Data Encryption Standard

- **DES:** Data Encryption Standard
  - published in 1977 by the National Bureau of Standards
  - is referred to as the Data Encryption Algorithm (DEA).
  - data are encrypted in ***64-bit blocks* using a *56-bit key*.**
  - **Key:** 64 bit quantity=8-bit parity+56-bit key
    - Every 8th bit is a parity bit



Data Encryption Standard



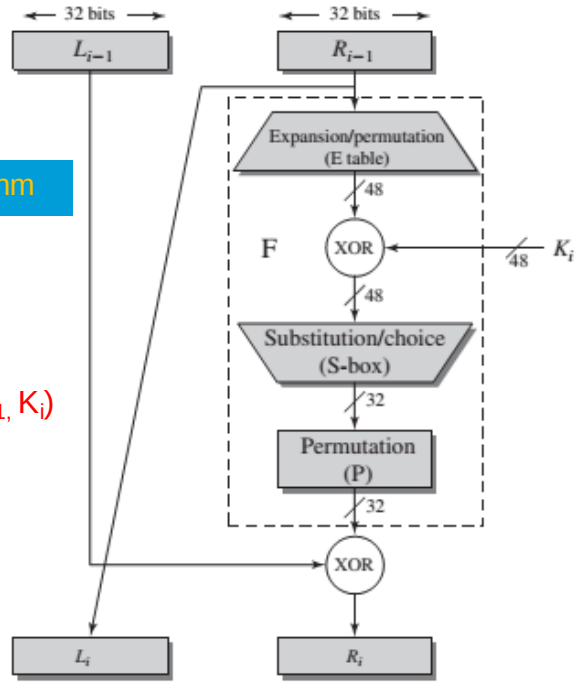
- **The process of encrypting a 64-bit block with DES:**
  - Initial permutation - IP
  - 16 complexcalculation loops using key
  - Permutation end (be the inverse of IP)

DES E/D

Single Round of DES Algorithm

- full
- 1 Round:

$L_i=R_{i-1}$; $R_i=L_{i-1}$ XOR $F(R_{i-1}, K_i)$



XOR Quiz

Use the XOR function and the given key to encrypt the word “Hi”.

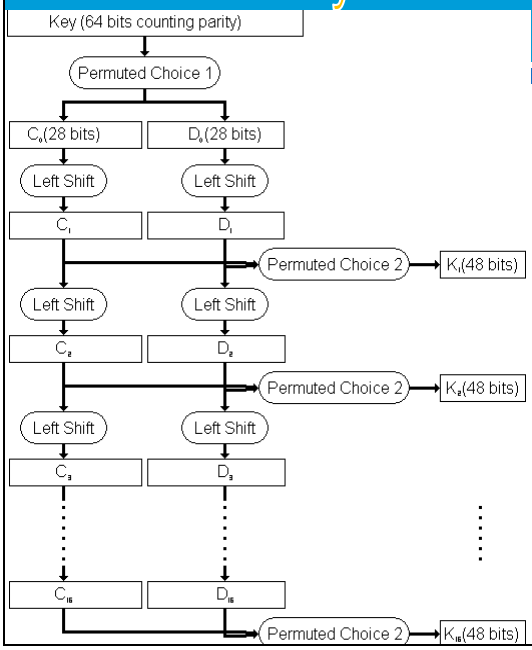
key = FA F2

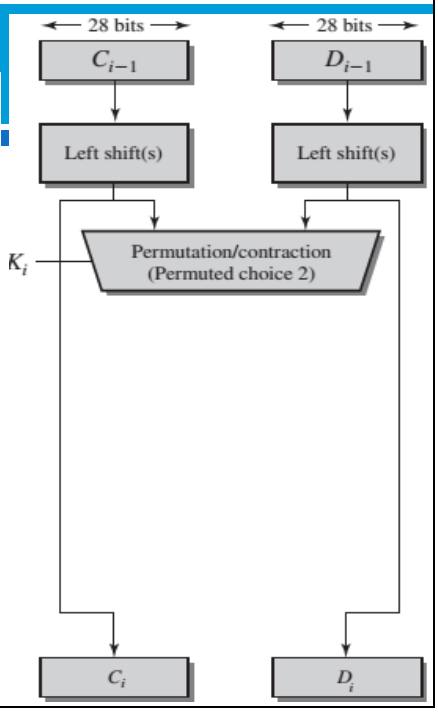
Hi =

FA F2 =

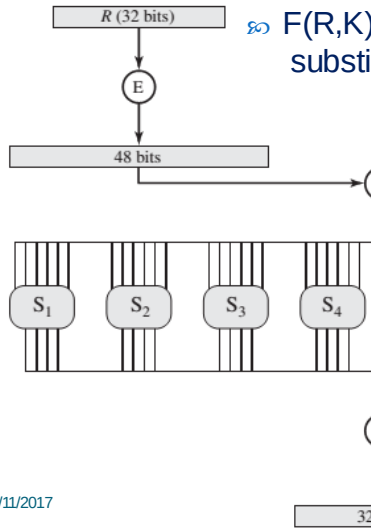
Hi encrypted =

Generate key





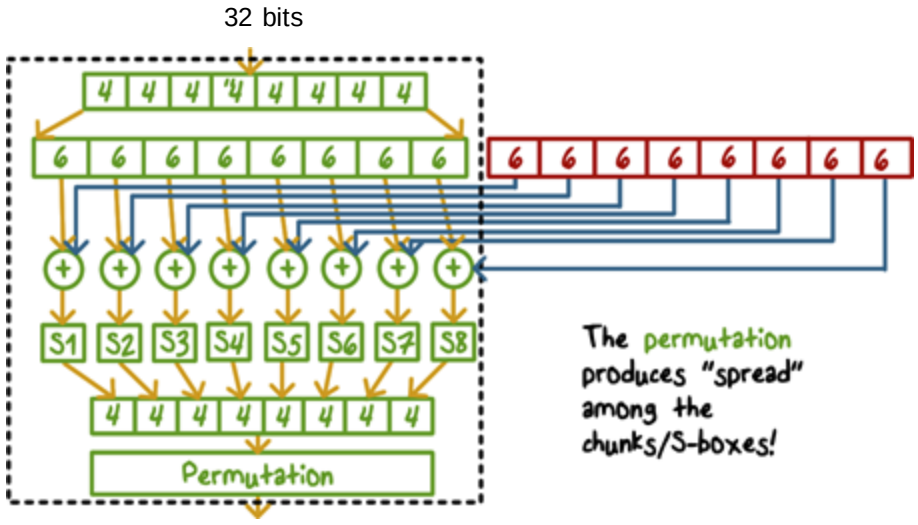
The role of the S-boxes in F(R, K)



- F(R,K): 48-bit input passes through a substitution function that produces a 32-bit output

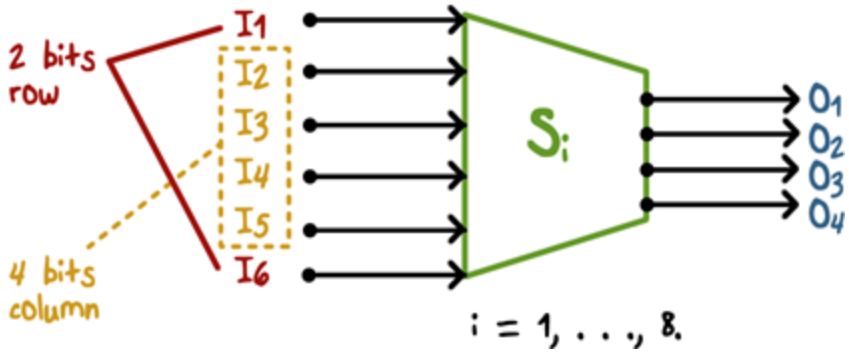
S-boxes, each of which accepts 6 bits as input and produces 4 bits as output

Function F(R, K)



S-Box (Substitute and Shrink)

- 48 bits => 32 bits. (8*6 => 8*4)
- 2 bits used to select amongst 4 substitutions for the rest of the 4-bit quantity



S-Box Quiz

For the given input, determine the output.

S_5		Middle 4 bits of input															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Input: 011011 **Output:**

Security of DES

- **Key space is too small**
  - With a key length of 56 bits, there are 2^{56} possible keys, which is approximately $7.2 * 10^{16}$ keys. Thus, on the face of it, a brute-force attack appears impractical.
- **S-box design criteria have been kept secret**
- **Highly resistant** to cryptanalysis techniques published years after DES
- **The Nature of the DES Algorithm**
- **Timing Attacks**
  - an encryption or decryption algorithm often takes slightly different amounts of time on different input

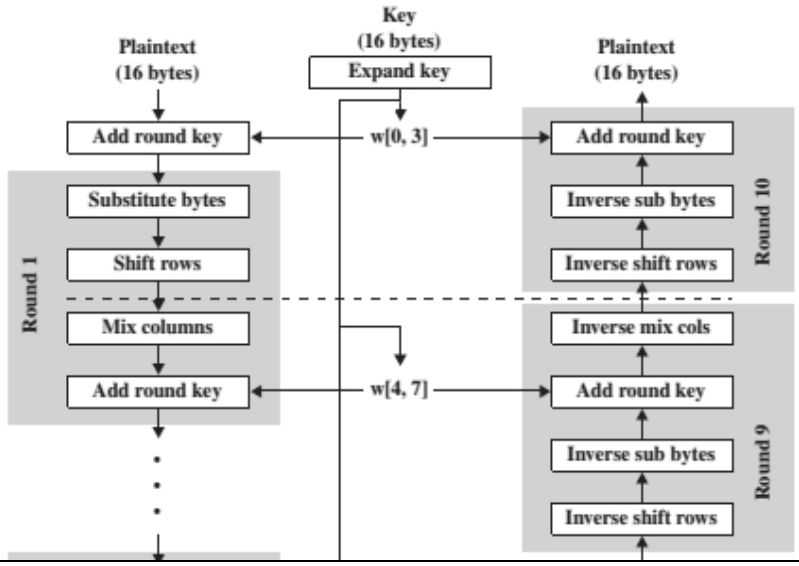
DES Cryptanalysis

- Use 56-bit key, DES has fast calculation speed.
- **DES was cryptanalyzed:**
  - 1997 by large computer networks in a few months
  - 1998 by special key finding machine in 56 hours
  - 1999 by a combination of computers in 22 hours 15'
- In theory, DES can be cryptanalyzed by using differential (vp) or linear cryptanalysis

AES - Advanced Encryption Standard

- AES:
  - intended to replace DES for commercial applications.
  - It uses a 128-bit block size and a key size of 128, 192, or 256 bits.
  - does not use a Feistel structure (take ½ block data >< entire data).
- Operation: each full round consists of four separate functions:
  - **Substitute bytes:** Uses an S-box to perform a byte-by-byte substitution of the block
  - **ShiftRows:** A simple permutation
  - **MixColumns:** A substitution that makes use of arithmetic over GF(28)
  - **AddRoundKey:** A simple bitwise XOR of the current block with a portion of the expanded key

AES – Encryption/ Decryption

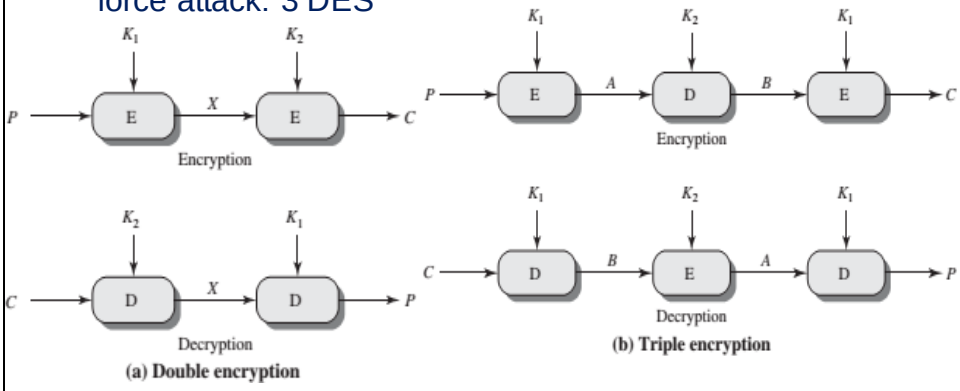


AES Requirements

- Requirements:
  - Block cryptography, using private key
  - 128-bit data block,128/192/256-bit key
  - Stronger and faster than Triple-DES
  - Available time: 20-30 years
  - Full decryption of the technical details and design

Multiple-encryption scheme: 3DES

- To resist the potential vulnerability of DES to a brute-force attack: 3 DES



$C = E(K_2, E(K_1, P))$
$P = D(K_1, D(K_2, C))$

Man in the Middle attack
$X = E(K_1, P) = D(K_2, C)$

$C = E(K_1, D(K_2, E(K_1, P)))$
$P = D(K_1, E(K_2, D(K_1, C)))$

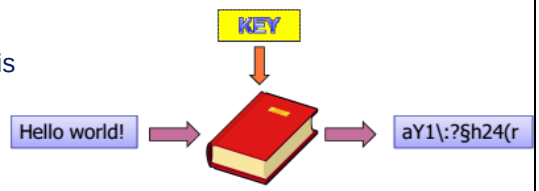
38

Block Cipher Operation

- 5 Operations have been standardized by NIST for use with symmetric block ciphers such as DES and AES:
  - electronic codebook mode - ECB
  - cipher block chaining mode - CBC
  - cipher feedback mode - CFB
  - output feedback mode – OFB
  - counter mode - CRT

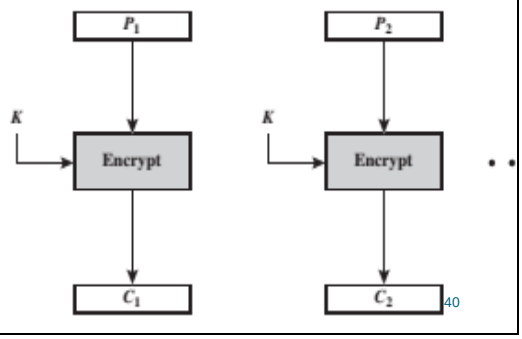
Electronic Codebook - ECB

- Each block of 64 plaintext bits is encoded independently using the same key.



- Application:

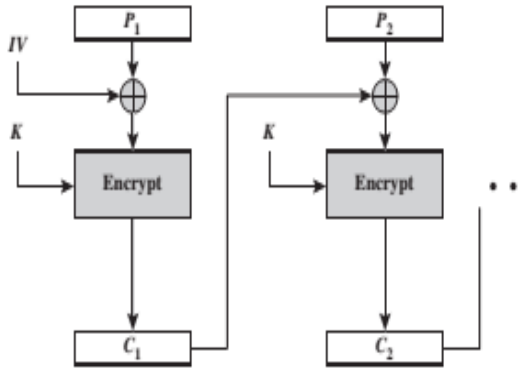
Secure transmission of single values (e.g., an encryption key)



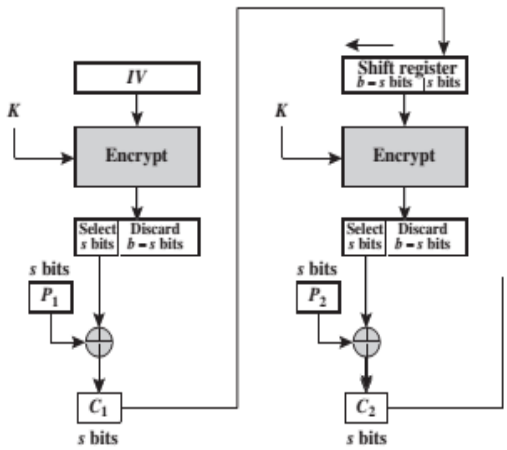
Cipher Block Chaining - CBC

- The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.
- Application:

- General-purpose block oriented transmission
- Authentication



s-bit Cipher Feedback (CFB)



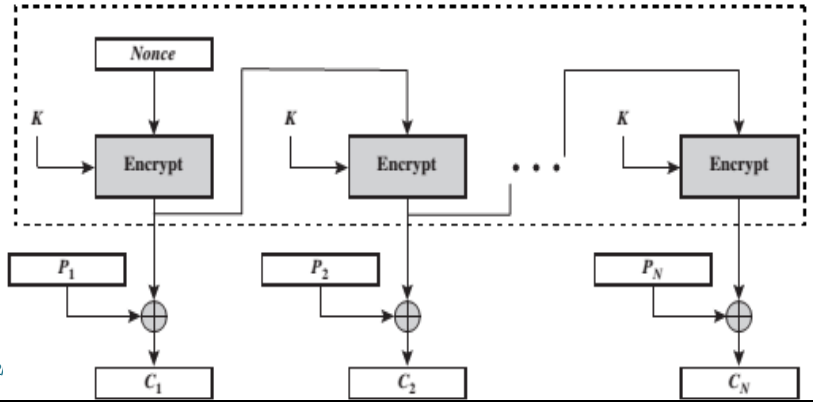
- Input is processed s bits at a time.
- Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.
- Application:

- General-purpose stream oriented transmission
- Authentication

Output Feedback - OFB

- Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.
- Application:

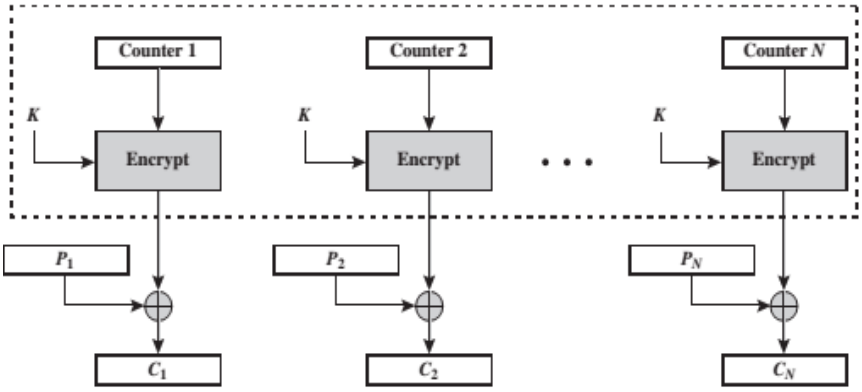
Stream-oriented transmission over noisy channel (satellite communication)



22 43

Counter (CTR)

- Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.
  - General-purpose block oriented transmission
  - Useful for high-speed requirements



Block cipher cryptanalysis

- **Some of block cipher cryptanalysis are**:
  - **Exhaustive Key Search**
  - **Structural Attacks**
    - differential cryptanalysis
    - linear cryptanalysis
    - related key attacks
  - **Implementation Attacks**
    - timing attacks
    - power attacks
    - differential fault analysis
  - **Inventing Attacks**

45

Q & A