Stream Cipher

Encrypts a digital data stream one bit or one byte at a time

Examples:

- Autokeyed Vigenère cipher
- Vernam cipher

In the ideal case a one-time pad version of the Vernam cipher would be used, in which the keystream is as long as the plaintext bit stream

If the cryptographic keystream is random, then this cipher is unbreakable by any means other than acquiring the keystream

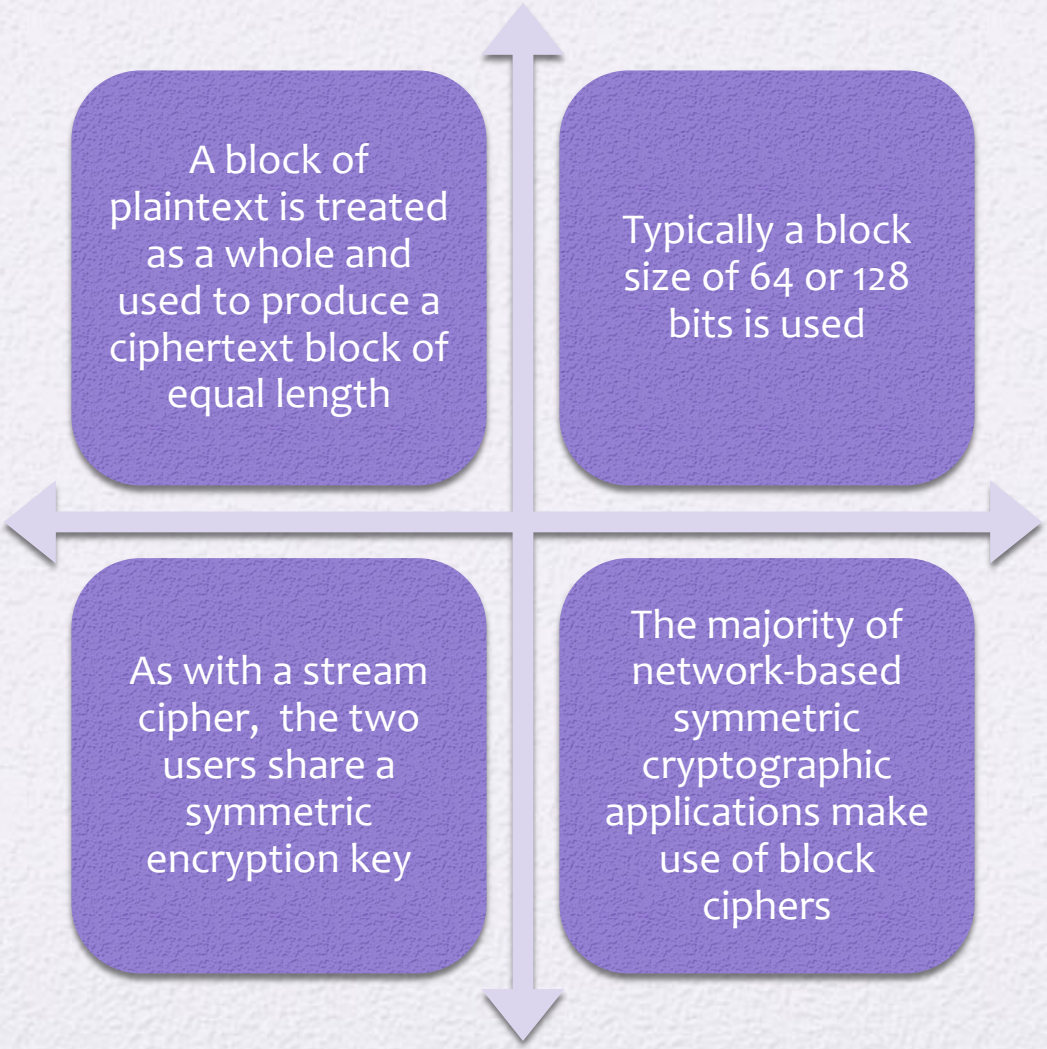
- Keystream must be provided to both users in advance via some independent and secure channel
- This introduces insurmountable logistical problems if the intended data traffic is very large

For practical reasons the bit-stream generator must be implemented as an algorithmic procedure so that the cryptographic bit stream can be produced by both users

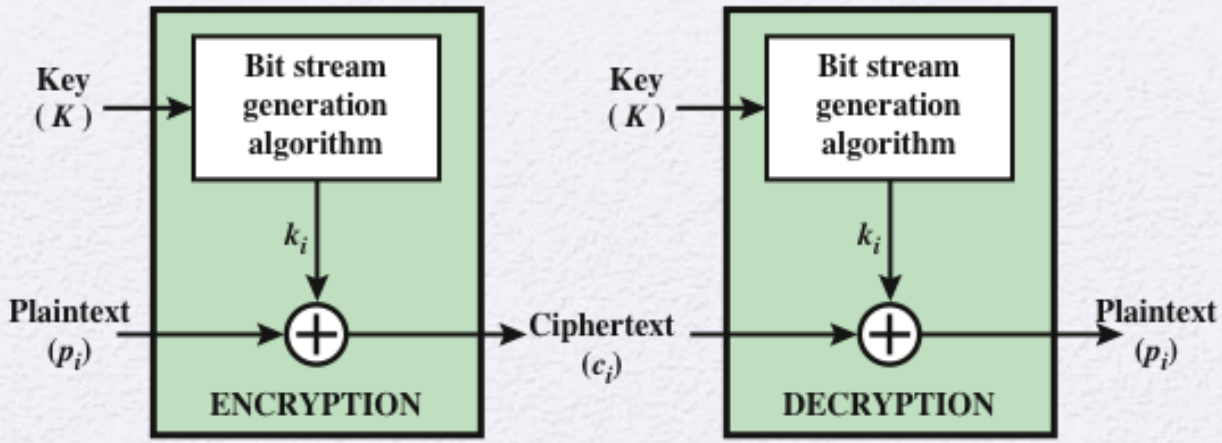
It must be computationally impractical to predict future portions of the bit stream based on previous portions of the bit stream

The two users need only share the generating key and each can produce the keystream

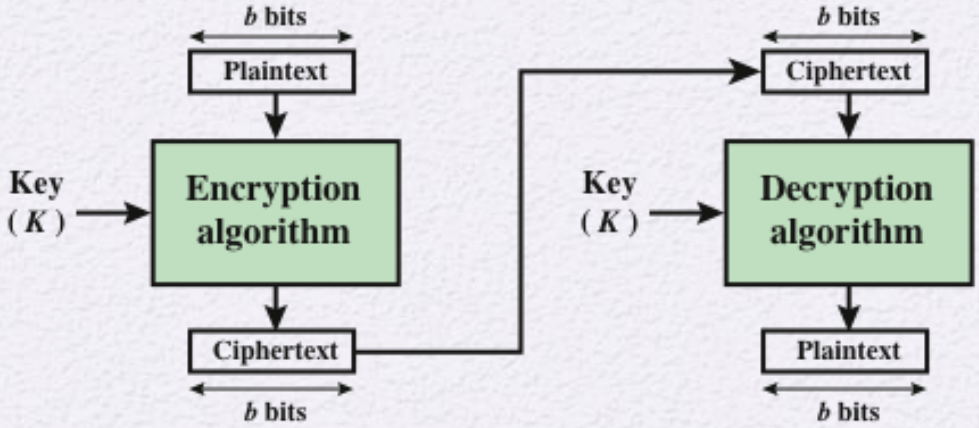
Block Cipher



Stream Cipher and Block Cipher



(a) Stream Cipher Using Algorithmic Bit Stream Generator



(b) Block Cipher

Figure 3.1 Stream Cipher and Block Cipher

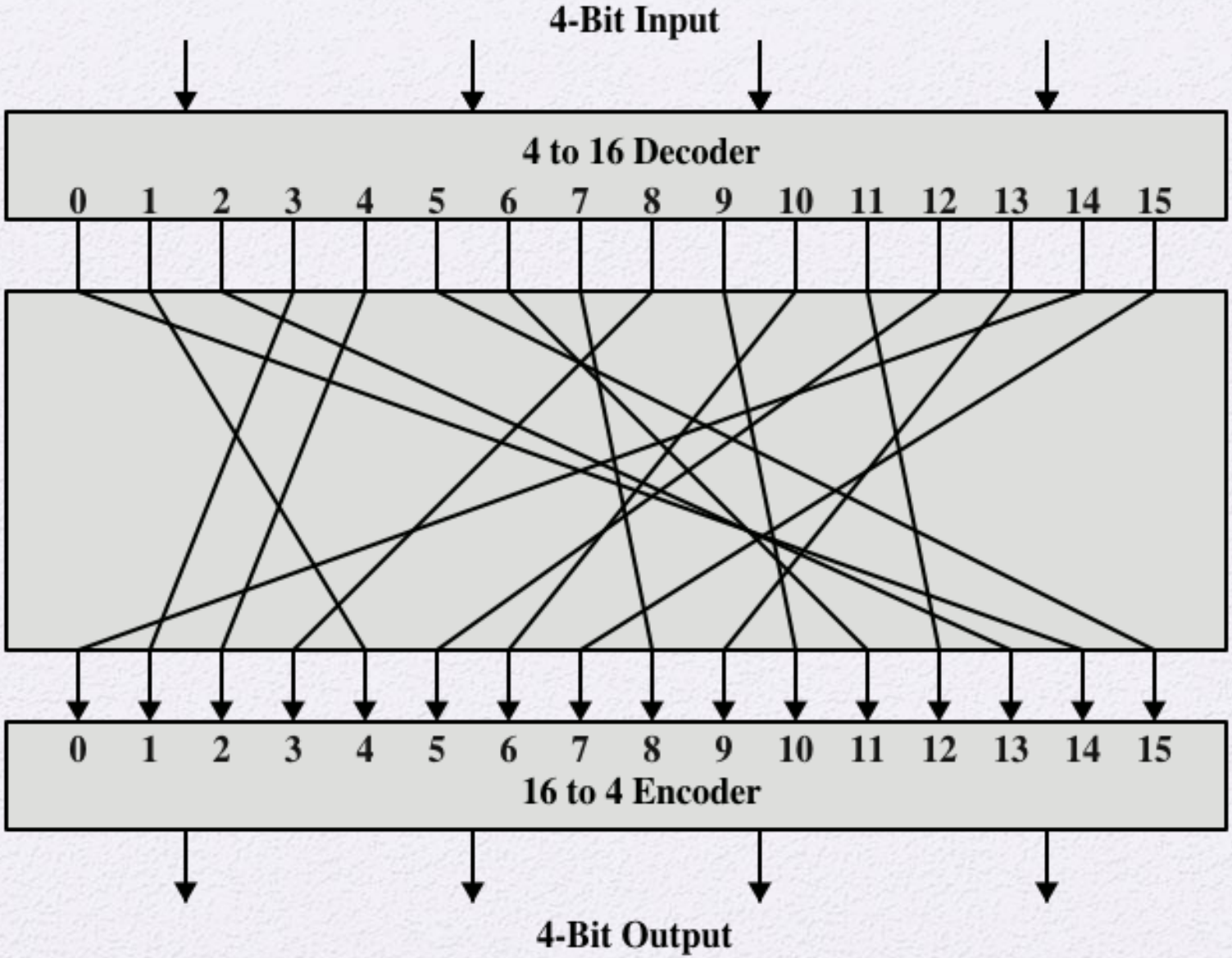


Figure 3.2 General *n*-bit-*n*-bit Block Substitution (shown with $n = 4$)

Mapping

Reversible Mapping	
Plaintext	**Ciphertext**
00	11
01	10
10	00
11	01

Irreversible Mapping	
Plaintext	**Ciphertext**
00	11
01	10
10	01
11	01

Contd…

- Transformations are: $2^n!$.
- Key here is (4 bits) * 16 rows = 64 bits.
- For 64bit: (64 bits) * 2^64 = 2^70 = 10^21 bits.

Table 3.1

Encryption and Decryption Tables for Substitution Cipher of Figure 3.2

Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Ciphertext	Plaintext
0000	1110
0001	0011
0010	0100
0011	1000
0100	0001
0101	1100
0110	1010
0111	1111
1000	0111
1001	1101
1010	1001
1011	0110
1100	1011
1101	0010
1110	0000
1111	0101

Next approach

$$
\begin{aligned}
y_1 &= k_{11}x_1 + k_{12}x_2 + k_{13}x_3 + k_{14}x_4 \\
y_2 &= k_{21}x_1 + k_{22}x_2 + k_{23}x_3 + k_{24}x_4 \\
y_3 &= k_{31}x_1 + k_{32}x_2 + k_{33}x_3 + k_{34}x_4 \\
y_4 &= k_{41}x_1 + k_{42}x_2 + k_{43}x_3 + k_{44}x_4
\end{aligned}
$$

- Here the key sixe is n^2. similar to Hill Cipher.

Feistel Cipher

- Proposed the use of a cipher that alternates substitutions and permutations

Substitutions

- Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements

Permutation

- No elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed

- Is a practical application of a proposal by Claude Shannon to develop a product cipher that alternates confusion and diffusion functions
- Is the structure used by many significant symmetric block ciphers currently in use

Diffusion and Confusion

- Terms introduced by Claude Shannon to capture the two basic building blocks for any cryptographic system
  - Shannon's concern was to thwart cryptanalysis based on statistical analysis

Diffusion

- The statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext
- This is achieved by having each plaintext digit affect the value of many ciphertext digits

Confusion

- Seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible
- Even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex as to make it difficult to deduce the key

Feistel Cipher Structure

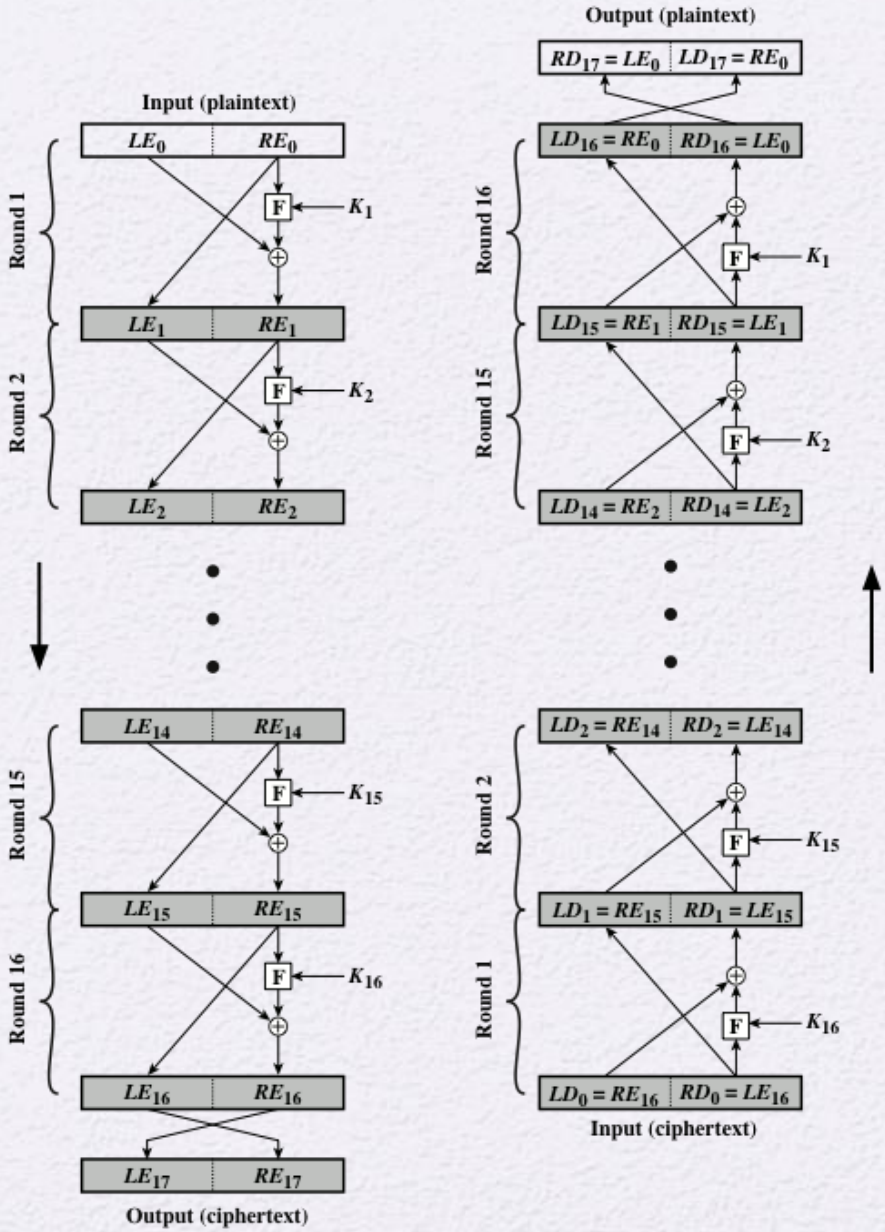


Figure 3.3 Feistel Encryption and Decryption (16 rounds)

Feistel Cipher Design Features

- Block size
  - Larger block sizes mean greater security but reduced encryption/decryption speed for a given algorithm
- Key size
  - Larger key size means greater security but may decrease encryption/decryption speeds
- Number of rounds
  - The essence of the Feistel cipher is that a single round offers inadequate security but that multiple rounds offer increasing security
- Subkey generation algorithm
  - Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis
- Round function F
  - Greater complexity generally means greater resistance to cryptanalysis
- Fast software encryption/decryption
  - In many cases, encrypting is embedded in applications or utility functions in such a way as to preclude a hardware implementation; accordingly, the speed of execution of the algorithm becomes a concern
- Ease of analysis
  - If the algorithm can be concisely and clearly explained, it is easier to analyze that algorithm for cryptanalytic vulnerabilities and therefore develop a higher level of assurance as to its strength

Feistel Example

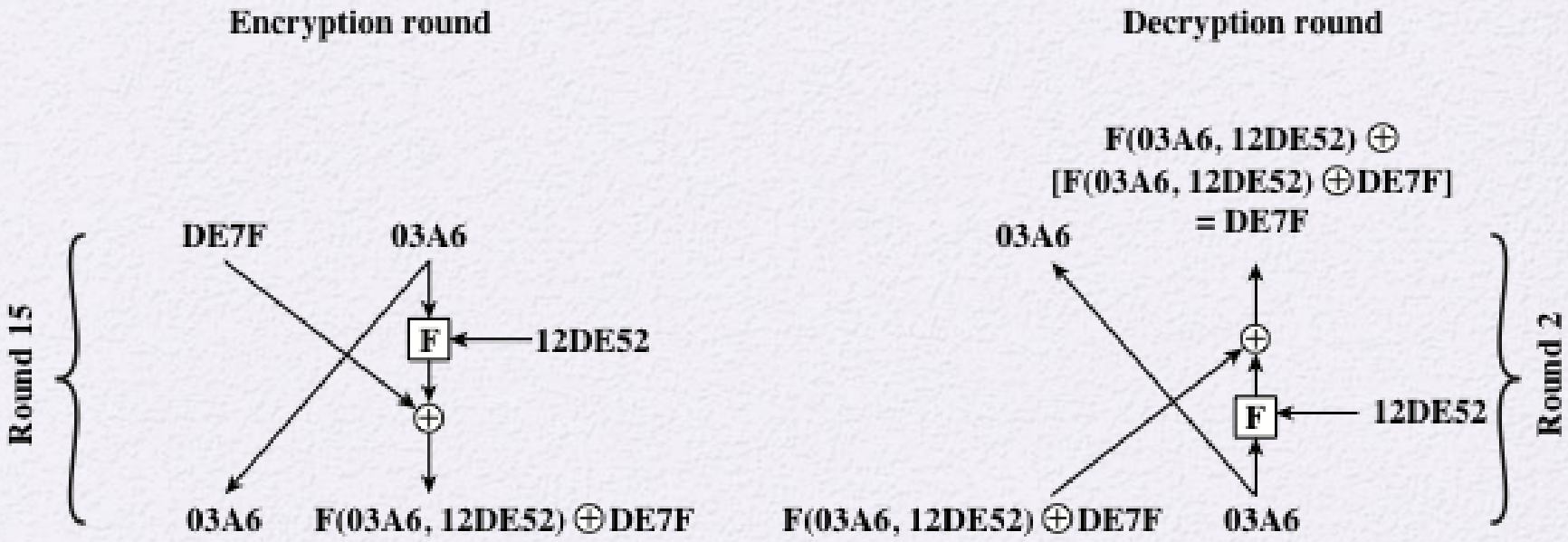


Figure 3.4 Feistel Example

Data Encryption Standard (DES)

- Issued in 1977 by the National Bureau of Standards (now NIST) as Federal Information Processing Standard 46
- Was the most widely used encryption scheme until the introduction of the Advanced Encryption Standard (AES) in 2001
- Algorithm itself is referred to as the Data Encryption Algorithm (DEA)
  - Data are encrypted in 64-bit blocks using a 56-bit key
  - The algorithm 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

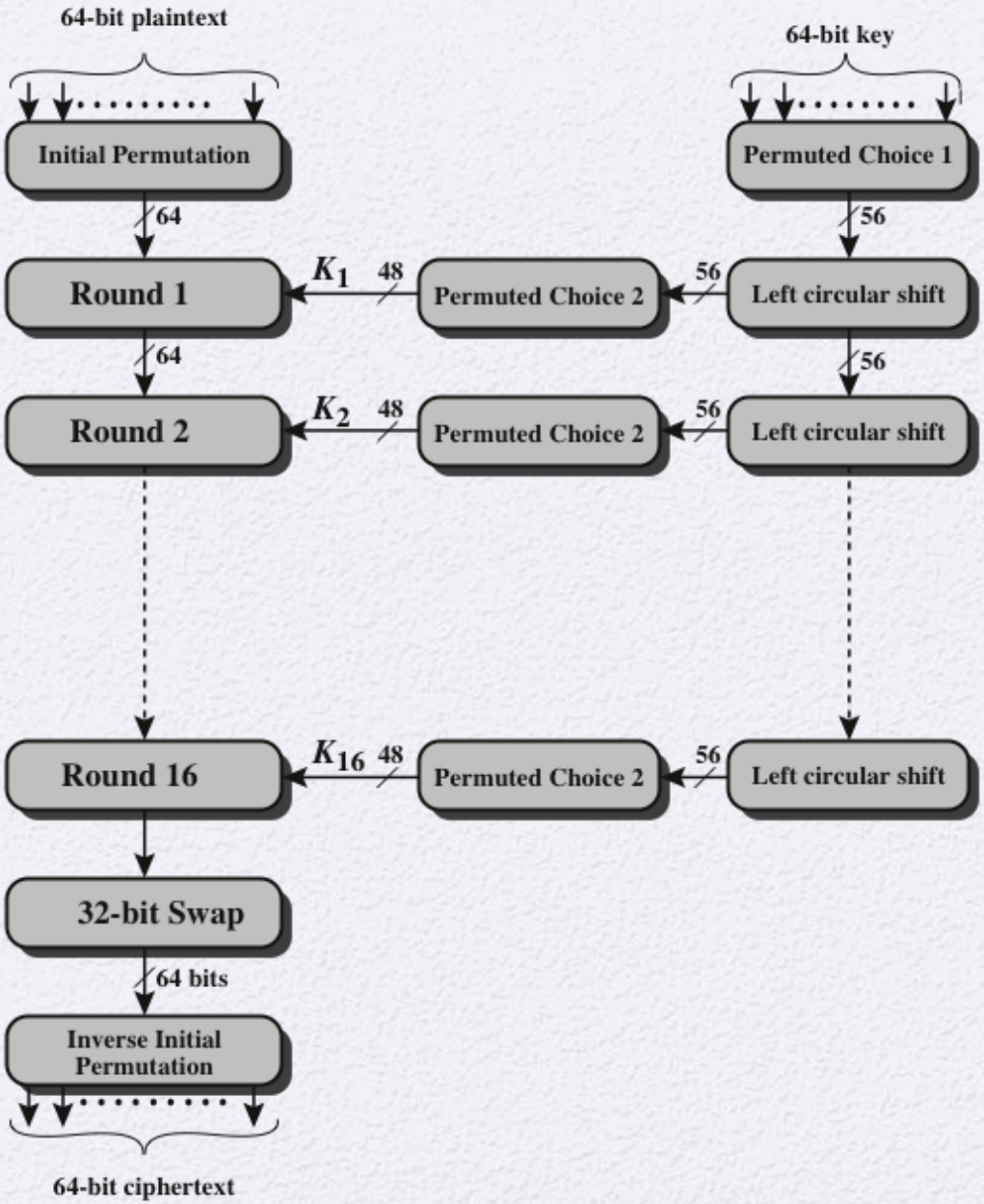


Figure 3.5 General Depiction of DES Encryption Algorithm

DES Encryption Algorithm

Table 3.2

DES Example

(Table can be found on page 75 in textbook)

Round	*Ki*	*Li*	*Ri*
IP		5a005a00	3cf03c0f
1	1e030f03080d2930	3cf03c0f	bad22845
2	0a31293432242318	bad22845	99e9b723
3	23072318201d0c1d	99e9b723	0bae3b9e
4	05261d3824311a20	0bae3b9e	42415649
5	3325340136002c25	42415649	18b3fa41
6	123a2d0d04262a1c	18b3fa41	9616fe23
7	021f120b1c130611	9616fe23	67117cf2
8	1c10372a2832002b	67117cf2	c11bfc09
9	04292a380c341f03	c11bfc09	887fbc6c
10	2703212607280403	887fbc6c	600f7e8b
11	2826390c31261504	600f7e8b	f596506e
12	12071c241a0a0f08	f596506e	738538b8
13	300935393c0d100b	738538b8	c6a62c4e
14	311e09231321182a	c6a62c4e	56b0bd75
15	283d3e0227072528	56b0bd75	75e8fd8f
16	2921080b13143025	75e8fd8f	25896490
IP–1		da02ce3a	89ecac3b

Note: DES subkeys are shown as eight 6-bit values in hex format

Round		δ
	02468aceeca86420 12468aceeca86420	1
1	3cf03c0fbad22845 3cf03c0fbad32845	1
2	bad2284599e9b723 bad3284539a9b7a3	5
3	99e9b7230bae3b9e 39a9b7a3171cb8b3	18
4	0bae3b9e42415649 171cb8b3ccaca55e	34
5	4241564918b3fa41 ccaca55ed16c3653	37
6	18b3fa419616fe23 d16c3653cf402c68	33
7	9616fe2367117cf2 cf402c682b2cefbc	32
8	67117cf2c11bfc09 2b2cefbc99f91153	33

Round		δ
9	c11bfc09887fbc6c 99f911532eed7d94	32
10	887fbc6c600f7e8b 2eed7d94d0f23094	34
11	600f7e8bf596506e d0f23094455da9c4	37
12	f596506e738538b8 455da9c47f6e3cf3	31
13	738538b8c6a62c4e 7f6e3cf34bc1a8d9	29
14	c6a62c4e56b0bd75 4bc1a8d91e07d409	33
15	56b0bd7575e8fd8f 1e07d4091ce2e6dc	31
16	75e8fd8f25896490 1ce2e6dc365e5f59	32
IP–1	da02ce3a89ecac3b 057cde97d7683f2a	32

Table 3.3 Avalanche Effect in DES: Change in Plaintext

Round		δ
	02468aceeca86420 02468aceeca86420	0
1	3cf03c0fbad22845 3cf03c0f9ad628c5	3
2	bad2284599e9b723 9ad628c59939136b	11
3	99e9b7230bae3b9e 9939136b768067b7	25
4	0bae3b9e42415649 768067b75a8807c5	29
5	4241564918b3fa41 5a8807c5488dbe94	26
6	18b3fa419616fe23 488dbe94aba7fe53	26
7	9616fe2367117cf2 aba7fe53177d21e4	27
8	67117cf2c11bfc09 177d21e4548f1de4	32

Round		δ
9	c11bfc09887fbc6c 548f1de471f64dfd	34
10	887fbc6c600f7e8b 71f64dfd4279876c	36
11	600f7e8bf596506e 4279876c399fdc0d	32
12	f596506e738538b8 399fdc0d6d208dbb	28
13	738538b8c6a62c4e 6d208dbbb9bdeeaa	33
14	c6a62c4e56b0bd75 b9bdeeaad2c3a56f	30
15	56b0bd7575e8fd8f d2c3a56f2765c1fb	33
16	75e8fd8f25896490 2765c1fb01263dc4	30
IP–1	da02ce3a89ecac3b ee92b50606b62b0b	30

Table 3.4 Avalanche Effect in DES: Change in Key

Table 3.5

Average Time Required for Exhaustive Key Search

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.8×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 9.8×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 1.8×10^{60} years	1.8×10^{56} years
26 characters (permutation)	Monoalphabetic	$26! = 4 \times 10^{26}$	2×10^{26} ns = 6.3×10^{9} years	6.3×10^{6} years

Strength of DES

- Timing attacks
  - One in which information about the key or the plaintext is obtained by observing how long it takes a given implementation to perform decryptions on various ciphertexts
  - Exploits the fact that an encryption or decryption algorithm often takes slightly different amounts of time on different inputs
  - So far it appears unlikely that this technique will ever be successful against DES or more powerful symmetric ciphers such as triple DES and AES

Block Cipher Design Principles: Number of Rounds

The greater the number of rounds, the more difficult it is to perform cryptanalysis

In general, the criterion should be that the number of rounds is chosen so that known cryptanalytic efforts require greater effort than a simple brute-force key search attack

If DES had 15 or fewer rounds, differential cryptanalysis would require less effort than a brute-force key search

Block Cipher Design Principles: Design of Function F

- The heart of a Feistel block cipher is the function F
- The more nonlinear F, the more difficult any type of cryptanalysis will be
- The SAC and BIC criteria appear to strengthen the effectiveness of the confusion function

The algorithm should have good avalanche properties

Strict avalanche criterion (SAC)

States that any output bit j of an S-box should change with probability 1/2 when any single input bit i is inverted for all i , j

Bit independence criterion (BIC)

States that output bits j and k should change independently when any single input bit i is inverted for all i , j , and k

Block Cipher Design Principles: Key Schedule Algorithm

- With any Feistel block cipher, the key is used to generate one subkey for each round
- In general, we would like to select subkeys to maximize the difficulty of deducing individual subkeys and the difficulty of working back to the main key
- It is suggested that, at a minimum, the key schedule should guarantee key/ciphertext Strict Avalanche Criterion and Bit Independence Criterion

Summary

- Traditional Block Cipher Structure
  - Stream ciphers
  - Block ciphers
  - Feistel cipher
- The Data Encryption Standard (DES)
  - Encryption
  - Decryption
  - Avalanche effect

- The strength of DES
  - Use of 56-bit keys
  - Nature of the DES algorithm
  - Timing attacks
- Block cipher design principles
  - DES design criteria
  - Number of rounds
  - Design of function F
  - Key schedule algorithm

- DES exhibits the classic _____ block cipher structure, which consists of a number of identical rounds of processing.
- A) Feistel
- B) SAC
- C) Shannon
- D) Rendell

- A sequence of plaintext elements is replaced by a _____ of that sequence which means that no elements are added, deleted or replaced in the sequence, but rather the order in which the elements appear in the sequence is changed.

- A) permutation
- B) diffusion
- C) stream
- D) substitution

- A _____ cipher is one that encrypts a digital data stream one bit or one byte at a time.
- A) product B) block
- C) key D) stream

- The vast majority of network-based symmetric cryptographic applications make use of _____ ciphers.

- A) linear
- B) block
- C) permutation
- D) stream

- A _____ cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.
- A) bit B) product
- C) stream D) block

- _____ is when each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements.

- A) Substitution
- B) Diffusion
- C) Streaming
- D) Permutation

- Key sizes of _____ or less are now considered to be inadequate.

- A) 128 bits
- B) 32 bits
- C) 16 bits
- D) 64 bits

- Feistel proposed that we can approximate the ideal block cipher by utilizing the concept of a _____ cipher, which is the execution of two or more simple ciphers in sequence in such a way that the final result or product is cryptographically stronger than any of the component ciphers.

- A) linear
- B) permutation
- C) differential
- D) product

- The criteria used in the design of the _____ focused on the design of the S-boxes and on the P function that takes the output of the S-boxes.
- A) Avalanche Attack B) Data Encryption Standard
- C) Product Cipher D) Substitution Key
-

- The greater the number of rounds, the _____ it is to perform cryptanalysis.
- A) easier
- B) less difficult
- C) equally difficult
- D) harder

- The function F provides the element of _____ in a Feistel cipher.
- A) clarification B) alignment
- C) confusion D) stability

- One of the most intense areas of research in the field of symmetric block ciphers is _____ design.

- A) S-box
- B) F-box
- C) E-box
- D) D-box

- Mister and Adams proposed that all linear combinations of S-box columns should be _____ which are a special class of Boolean functions that are highly nonlinear according to certain mathematical criteria.

- A) horizontal functions B) angular functions

- C) bent functions D) vertical functions

- Allowing for the maximum number of possible encryption mappings from the plaintext block is referred to by Feistel as the _____ .
- A) ideal substitution cipher B) round function
- C) ideal block cipher D) diffusion cipher
-

- _____ seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible so that even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex it is difficult to deduce the key.
-

- Many block ciphers have a _____ structure which consists of a number of identical rounds of processing and in each round a substitution is performed on one half of the data being processed, followed by a permutation that interchanges the two halves.

- Feistel's is a practical application of a proposal by Claude Shannon to develop a product cipher that alternates confusion and _____ functions.
- The _____ criterion is defined as: "An S-box satisfies GA of order y if, for a 1-bit input change, at least y output bits change."

- In _____ the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits.
- A change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. This is referred to as the _____ effect.

- Two areas of concern regarding the level of security provided by DES are the nature of the algorithm and the _____ .
- A _____ attack exploits the fact that an encryption or decryption algorithm often takes slightly different amounts of time on different inputs.
- Two alternatives to DES are AES and _____ DES

- The cryptographic strength of a Feistel cipher derives from three aspects of the design: the function F, the key schedule algorithm, and _____ .

- **Example:** Let **M** be the plain text message **M** = 0123456789ABCDEF, where **M** is in hexadecimal (base 16) format. Rewriting **M** in binary format, we get the 64-bit block of text:

- **M** = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111
  L = 0000 0001 0010 0011 0100 0101 0110 0111
  R = 1000 1001 1010 1011 1100 1101 1110 1111

- Let **K** be the hexadecimal key **K** = 133457799BBCDFF1. This gives us as the binary key (setting 1 = 0001, 3 = 0011, etc., and grouping together every eight bits, of which the last one in each group will be unused):
- **K** = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001

PC-1

57 49 41 33 25 17 9

- 1 58 50 42 34 26 18
- 10 2 59 51 43 35 27
- 19 11 3 60 52 44 36
- 63 55 47 39 31 23 15
- 7 62 54 46 38 30 22
- 14 6 61 53 45 37 29
- 21 13 5 28 20 12 4

- **K+** = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111
- C_o = 1111000 0110011 0010101 0101111
  D_o = 0101010 1011001 1001111 0001111

Iteration Number	Number of Left Shifts
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2

Round & Left shift

- 1 1
- 2 1
- 3 2
- 4 2
- 5 2
- 6 2
- 7 2
- 8 2
- 9 1

. 10 2

- 11 2
- 12 2
- 13 2
- 14 2
- 15 2
- 16 1

- C_0 = 1111000011001100101010101111
  D_0 = 0101010101100110011110001111
- C_1 = 1110000110011001010101011111
  D_1 = 1010101011001100111100011110
- C_2 = 1100001100110010101010111111
  D_2 = 0101010110011001111000111101
- C_3 = 0000110011001010101011111111
  D_3 = 0101011001100111100011110101

PC 2 56 bit to 48 bit

- 14 17 11 24 1 5
- 3 28 15 6 21 10
- 23 19 12 4 26 8
- 16 7 27 20 13 2
- 41 52 31 37 47 55
- 30 40 51 45 33 48
- 44 49 39 56 34 53
- 46 42 50 36 29 32

- K_1 = 000110 110000 001011 101111 111111 000111 000001 110010

- For the other keys we have

- K_2 = 011110 011010 111011 011001 110110 111100 100111 100101
  K_3 = 010101 011111 110010 001010 010000 101100 111110 011001
  K_4 = 011100 101010 110111 010110 110110 110011 010100 011101
  K_5 = 011111 001110 110000 000111 111010 110101 001110 101000
  K_6 = 011000 111010 010100 111110 010100 000111 101100 101111
  K_7 = 111011 001000 010010 110111 111101 100001 100010 111100
  K_8 = 111101 111000 101000 111010 110000 010011 101111 111011
  K_9 = 111000 001101 101111 101011 111011 011110 011110 000001
  K_{10} = 101100 011111 001101 000111 101110 100100 011001 001111
  K_{11} = 001000 010101 111111 010011 110111 101101 001110 000110
  K_{12} = 011101 010111 000111 110101 100101 000110 011111 101001
  K_{13} = 100101 111100 010111 010001 111110 101011 101001 000001
  K_{14} = 010111 110100 001110 110111 111100 101110 011100 111010
  K_{15} = 101111 111001 000110 001101 001111 010011 111100 001010
  K_{16} = 110010 110011 110110 001011 000011 100001 011111 110101

Encode Data - IP

- 58 50 42 34 26 18 10 2
- 60 52 44 36 28 20 12 4
- 62 54 46 38 30 22 14 6
- 64 56 48 40 32 24 16 8
- 57 49 41 33 25 17 9 1
- 59 51 43 35 27 19 11 3
- 61 53 45 37 29 21 13 5
- 63 55 47 39 31 23 15 7

- L_o = 1100 1100 0000 0000 1100 1100 1111 1111
  R_o = 1111 0000 1010 1010 1111 0000 1010 1010

- $L_n = R_{n-1}$
  $R_n = L_{n-1} + f(R_{n-1}, K_n)$

- when n=1

- K_1 = 000110 110000 001011 101111 111111 000111 000001 110010
  $L_1 = R_o$ = 1111 0000 1010 1010 1111 0000 1010 1010
  $R_1 = L_o + f(R_o, K_1)$

Expansion

- ***f***, we first expand each block R_{n-1} from 32 bits to 48 bits
- 32 1 2 3 4 5
- 4 5 6 7 8 9
- 8 9 10 11 12 13
- 12 13 14 15 16 17
- 16 17 18 19 20 21
- 20 21 22 23 24 25
- 24 25 26 27 28 29
- 28 29 30 31 32 1

- XOR the output $\mathbf{E}(\boldsymbol{R}_{n-1})$ with the key $\boldsymbol{K}_n$
- Kn + E(Rn-1) =B1B2B3B4B5B6B7B8,
- where each Bi is a group of six bits. We now calculate
- S1(B1)S2(B2)S3(B3)S4(B4)S5(B5)S6(B6)S7(B7)S8(B8)
- where Si(Bi) referres to the output of the i-th S box.

- Row
- No. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
- 0 14 4 13 1 2 15 11 8 3 10 6 12 5 9 0 7
- 1 0 15 7 4 14 2 13 1 10 6 12 11 9 5 3 8
- 2 4 1 14 8 13 6 2 11 15 12 9 7 3 10 5 0
- 3 15 12 8 2 4 9 1 7 5 11 3 14 10 0 6 13

Permutation of 32 bits

- 16 7 20 21
- 29 12 28 17
- 1 15 23 26
- 5 18 31 10
- 2 8 24 14
- 32 27 3 9
- 19 13 30 6
- 22 11 4 25

Inverse permutation(after 16 rounds)

- 40 8 48 16 56 24 64 32
- 39 7 47 15 55 23 63 31
- 38 6 46 14 54 22 62 30
- 37 5 45 13 53 21 61 29
- 36 4 44 12 52 20 60 28
- 35 3 43 11 51 19 59 27
- 34 2 42 10 50 18 58 26
- 33 1 41 9 49 17 57 25

DES Modes

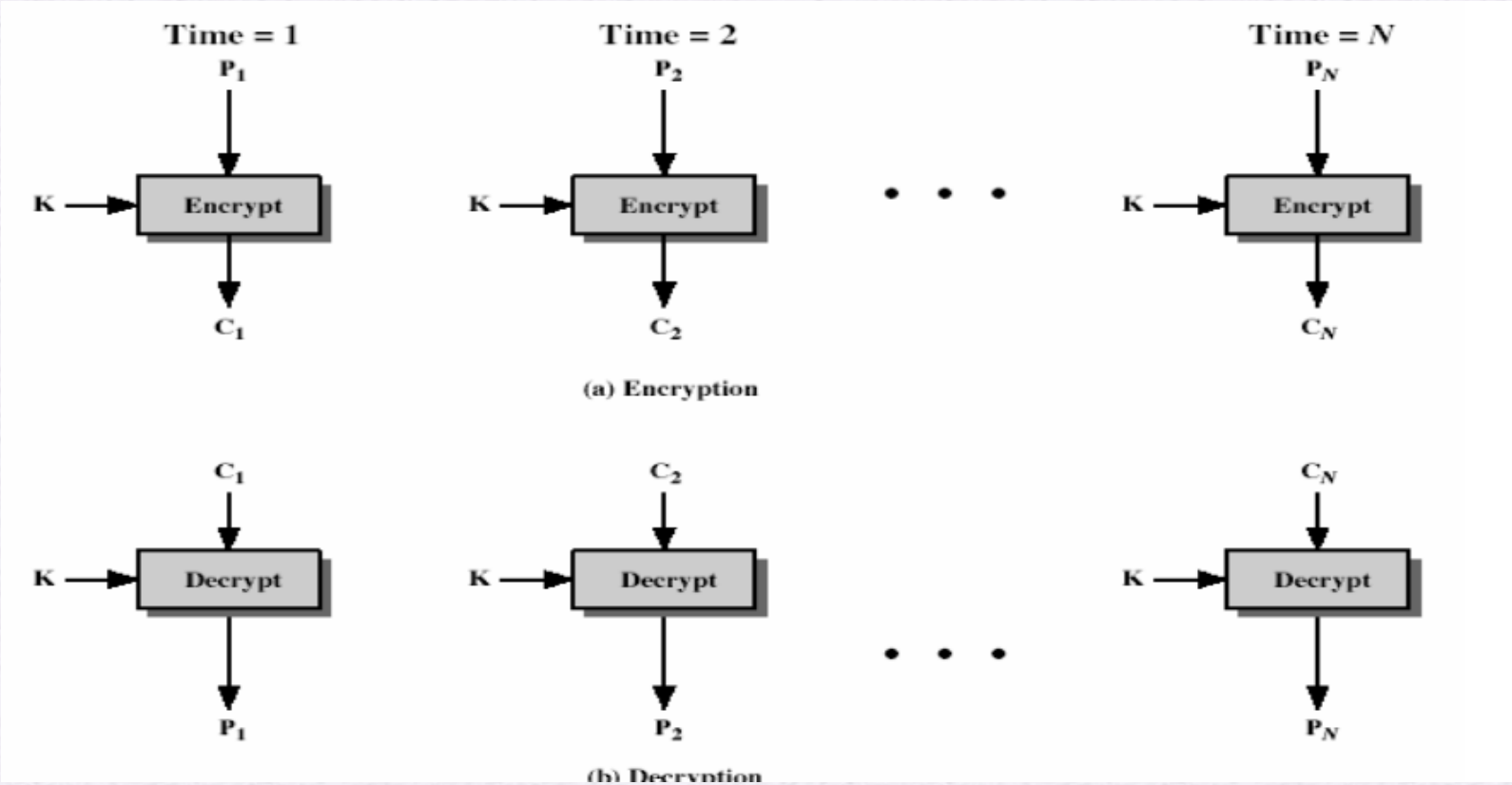
- The DES algorithm turns a 64-bit message block **M** into a 64-bit cipher block **C**. If each 64-bit block is encrypted individually, then the mode of encryption is called ***Electronic Code Book***(ECB) mode.

ECB

- message is broken into independent blocks which are encrypted
- each block is a value which is substituted, like a codebook
- each block is encoded independently of the other blocks

$$C_i = DES_{K1}(P_i)$$

- uses: secure transmission of single values


Time = 1
Time = 2
Time = N
P1
P2
PN
K
Encrypt
C1
C2
CN
(a) Encryption
C1
C2
CN
Decrypt
P1
P2
PN
(b) Decryption

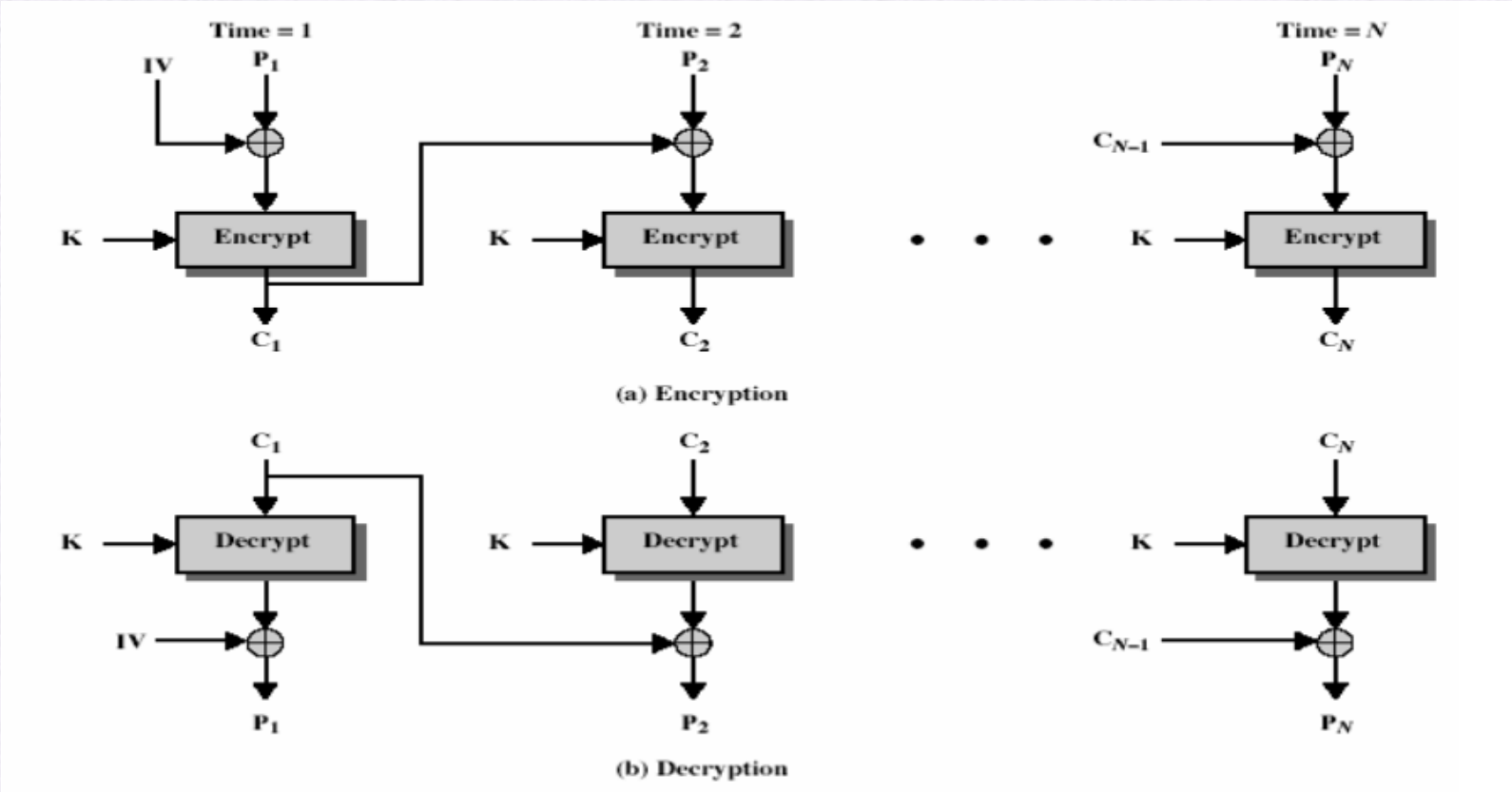
Chain Block Coding

- message is broken into blocks
- but these are linked together in the encryption operation
- each previous cipher blocks is chained with current plaintext block, hence name
- use Initial Vector (IV) to start process

$$C_i = DES_{K1}(P_i \text{ XOR } C_{i-1})$$

$$C_{-1} = IV$$

- uses: bulk data encryption, authentication

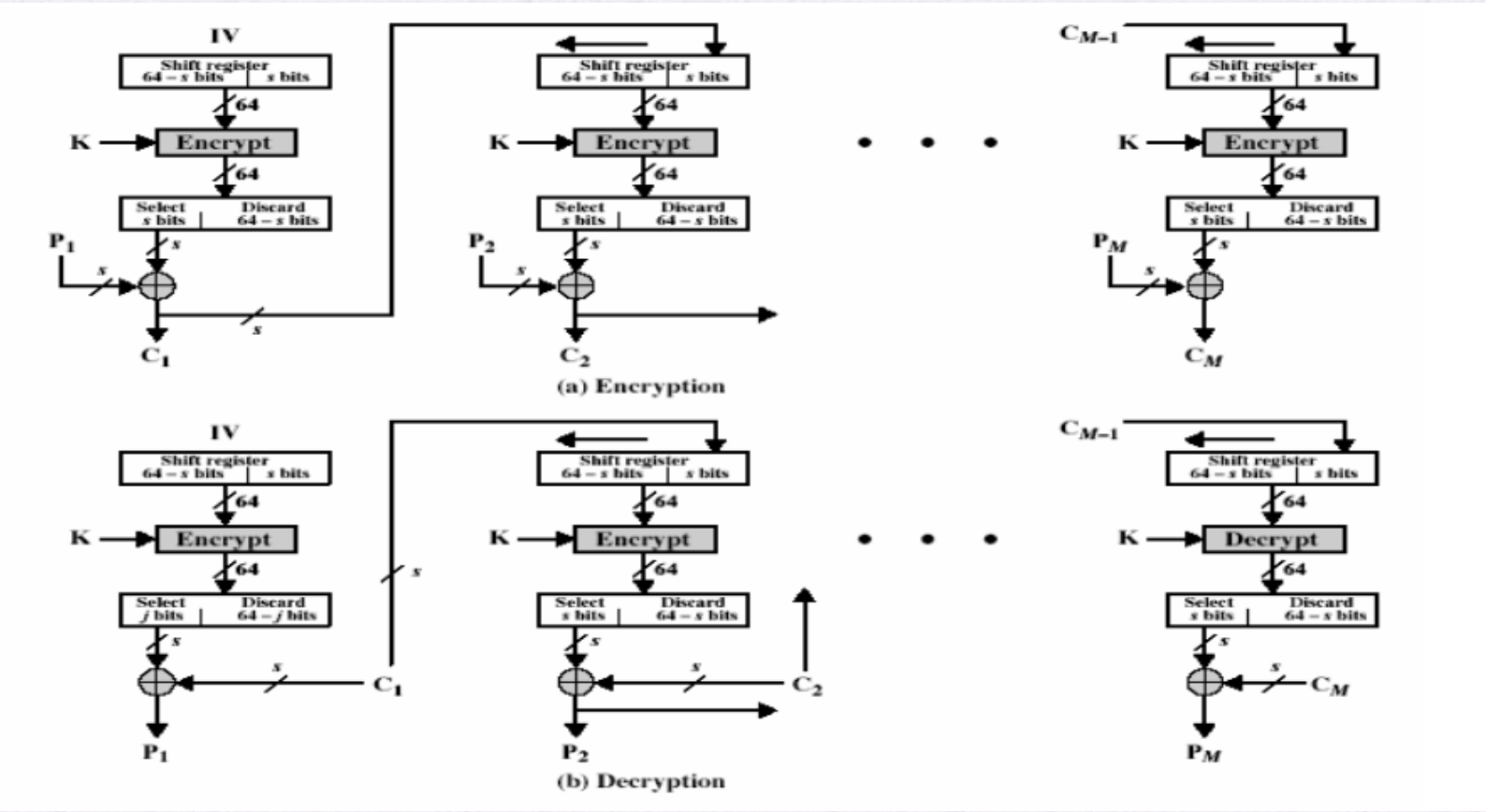

Time = 1
Time = 2
Time = N
IV
P_1
P_2
P_N
C_{N-1}
K
Encrypt
C_1
C_2
C_N
(a) Encryption
Decrypt
(b) Decryption

Cipher Feedback

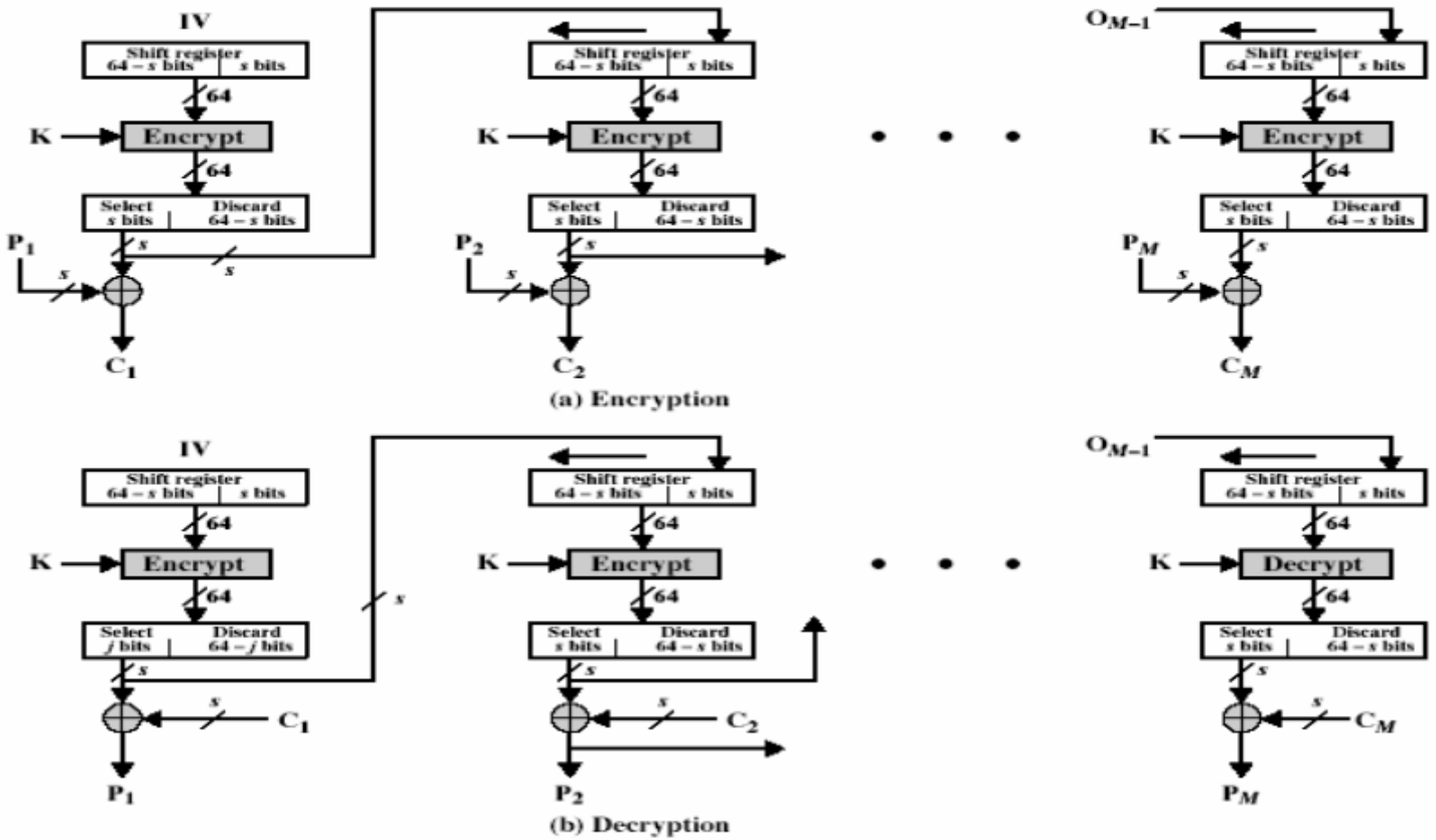
- message is treated as a stream of bits
- added to the output of the block cipher
- result is feed back for next stage (hence name)
- standard allows any number of bit (1,8 or 64 or whatever) to be feed back
  - denoted CFB-1, CFB-8, CFB-64 etc
- is most efficient to use all 64 bits (CFB-64)

$$C_i = P_i \text{ XOR } DES_{K1}(C_{i-1})$$

$$C_{-1} = IV$$


IV
Shift register
64 – s bits
s bits
64
K
Encrypt
Select
s bits
Discard
64 – s bits
P1
P2
PM
C1
C2
CM
CM–1
(a) Encryption
Decrypt
(b) Decryption

Output FeedBack (OFB)



Cracking DES

- "brute force“
- Deep Crack, uses 27 boards each containing 64 chips, 56 hours – 90 billion keys per second

Triple DES

- Triple-DES is just DES with two 56-bit keys applied. Given a plaintext message, the first key is used to DES- encrypt the message. The second key is used to DES-decrypt the encrypted message. (Since the second key is not the right key, this decryption just scrambles the data further.) The twice-scrambled message is then encrypted again with the first key to yield the final ciphertext. This three-step procedure is called triple-DES.

- ciphertext = EK3(DK2(EK1(plaintext)))
- Decryption is the reverse:
- plaintext = DK1(EK2(DK3(ciphertext)))