

Capítulo 3

Criptografia Convencional

Técnicas Modernas

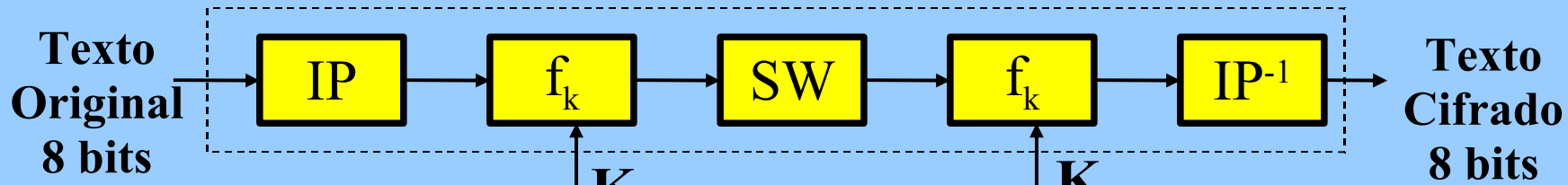
Plano de Curso

- DES Simplificado (Prof. Edward Schaefer)
- Princípios dos Cifradores de Bloco
- DES
- Criptanálise Diferencial e Linear
- Projeto dos Cifradores de Bloco
- Modos de Operação
- Funções Bent

DES Simplificado

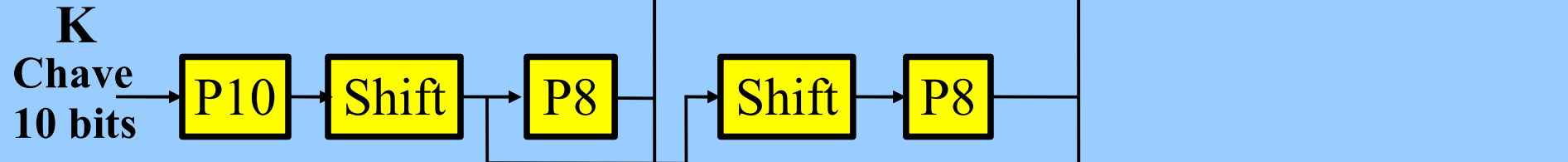
IP - Permutação Inicial
 f_k - função complexa
SW - permutação simples

Cifrar



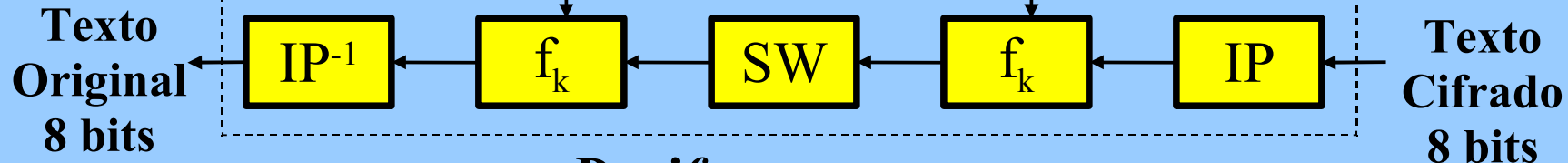
K_1

K_2



K_1

K_2



Decifrar

Geração das subchaves

Chave = $b_1b_2b_3b_4b_5b_6b_7b_8b_9b_{10}$
 $P10(Chave) = b_3b_5b_2b_7b_4b_{10}b_1b_9b_8b_6$

P10

3 5 2 7 4 10 1 9 8 6

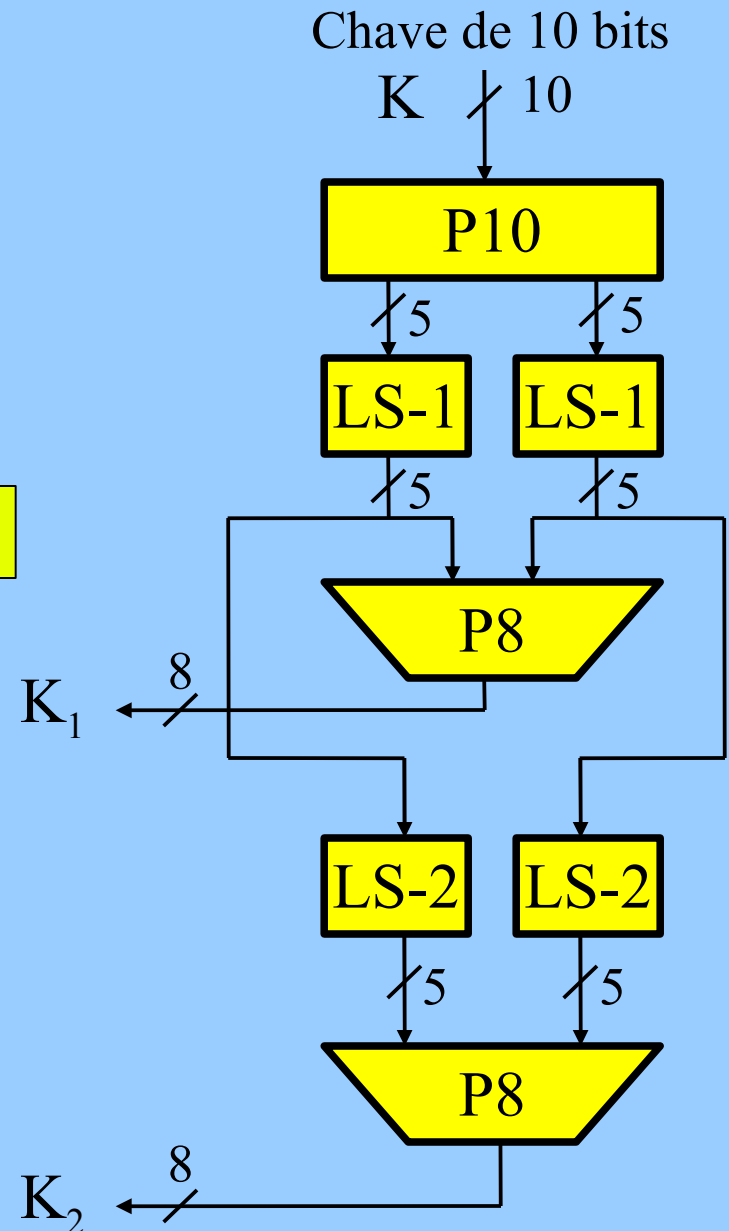
P8

6 3 7 4 8 5 10 9

LS-1

2 3 4 5 1

Exemplo:
 chave: 1010000010
 K_1 : 10100100
 K_2 : 01000011



IP

2 6 3 1 4 8 5 7

E/P

4 1 2 3 2 3 4 1

IP⁻¹

4 1 3 5 7 2 8 6

P4

2 4 3 1

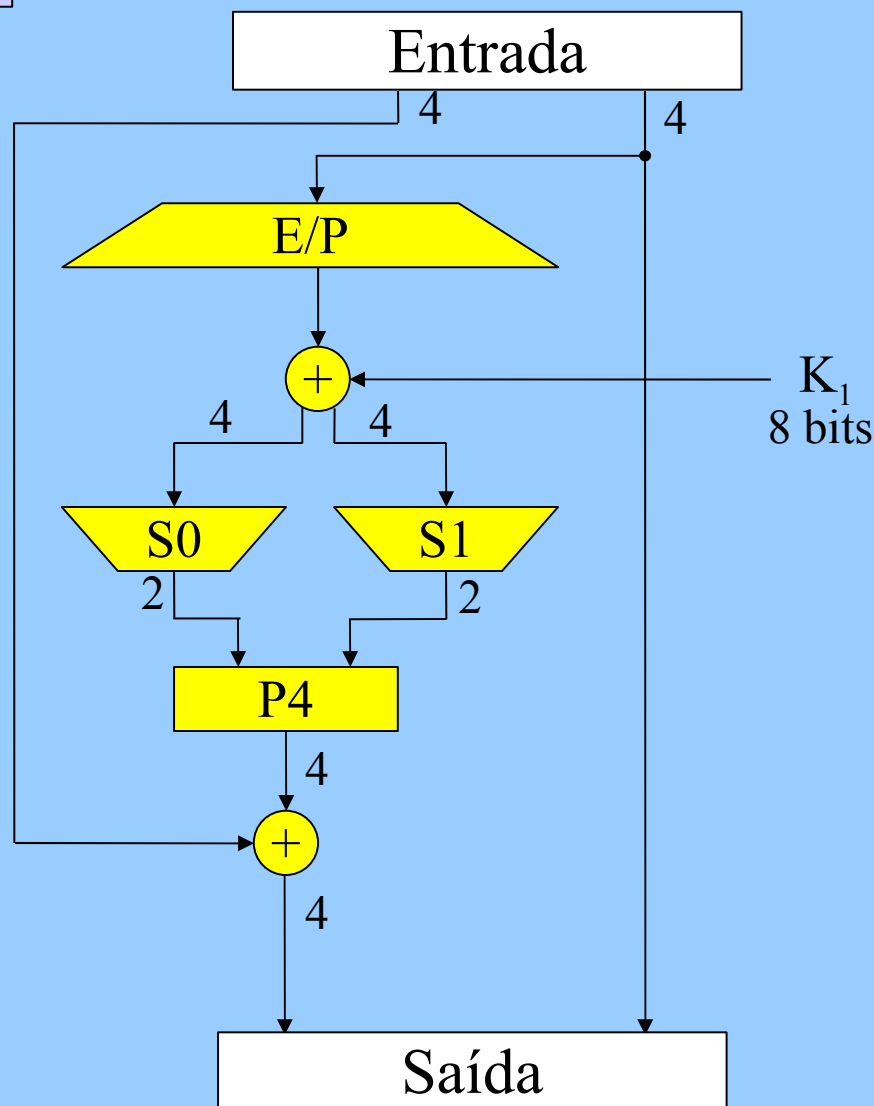
S0 =

01	00	11	10
11	10	01	00
00	10	01	11
11	01	11	10

S1 =

01	01	10	11
10	00	01	11
11	00	01	00
10	01	00	11

Função f_k



Análise do S-DES

$2^{10}=1024$ possibilidades
Equações não lineares -> Caixas S

4 bits de Entrada

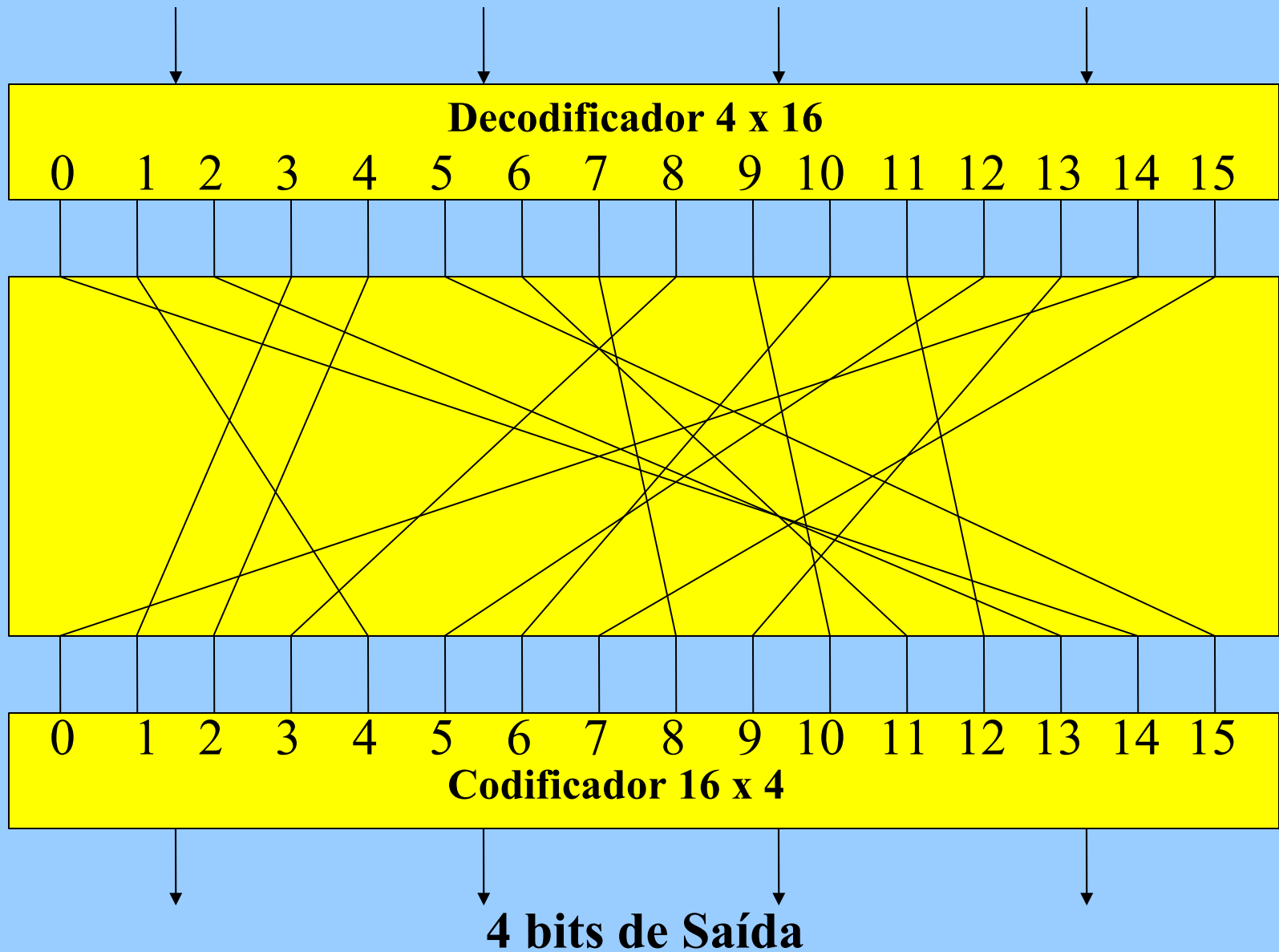


Tabela de Substituição n=4

Texto Original	Texto Cifrado	Texto Cifrado	Texto Plano
0000 - 1110	0000 - 1110	0000 - 1110	
0001 - 0100	0001 - 0011	0001 - 0011	
0010 - 1101	0010 - 0100	0010 - 0100	
0011 - 0001	0011 - 1000	0011 - 1000	
0100 - 0010	0100 - 0001	0100 - 0001	
0101 - 1111	0101 - 1100	0101 - 1100	
0110 - 1011	0110 - 1010	0110 - 1010	
0111 - 1000	0111 - 1111	0111 - 1111	
1000 - 0011	1000 - 0111	1000 - 0111	
1001 - 1010	1001 - 1101	1001 - 1101	
1010 - 0110	1010 - 1001	1010 - 1001	
1011 - 1100	1011 - 0110	1011 - 0110	
1100 - 0101	1100 - 1011	1100 - 1011	
1101 - 1001	1101 - 0010	1101 - 0010	
1110 - 0000	1110 - 0000	1110 - 0000	
1111 - 0111	1111 - 0101	1111 - 0101	

Chave = 64 bits

$$\text{Chave} = n * 2^n \text{ bits}$$

Exemplo: $n = 64$ bits

$$\text{Chave} = n 2^n = 64 * 2^{64} = 2^{70} = 10^{21} \text{ bits}$$

Mapeamentos Reversíveis

$$n - 2^n!$$

$$2 - 2^2! = 24$$

$$3 - 2^3! = 40320$$

$$4 - 2^4! = 2,1 \times 10^{13}$$

$$8 - 2^8! =$$

$$64 - 2^{64}! = 10^{34380000000000000000} > 10^{10^{20}}$$

Mapeamento Linear

$$n = 4$$

Nº. Chaves
 $n^2 = 16$ bits

$$y_1 = k_{11}x_1 + k_{12}x_2 + k_{13}x_3 + k_{14}x_4$$

$$y_2 = k_{21}x_1 + k_{22}x_2 + k_{23}x_3 + k_{24}x_4$$

$$y_3 = k_{31}x_1 + k_{32}x_2 + k_{33}x_3 + k_{34}x_4$$

$$y_4 = k_{41}x_1 + k_{42}x_2 + k_{43}x_3 + k_{44}x_4$$

Cifrador de Feistel

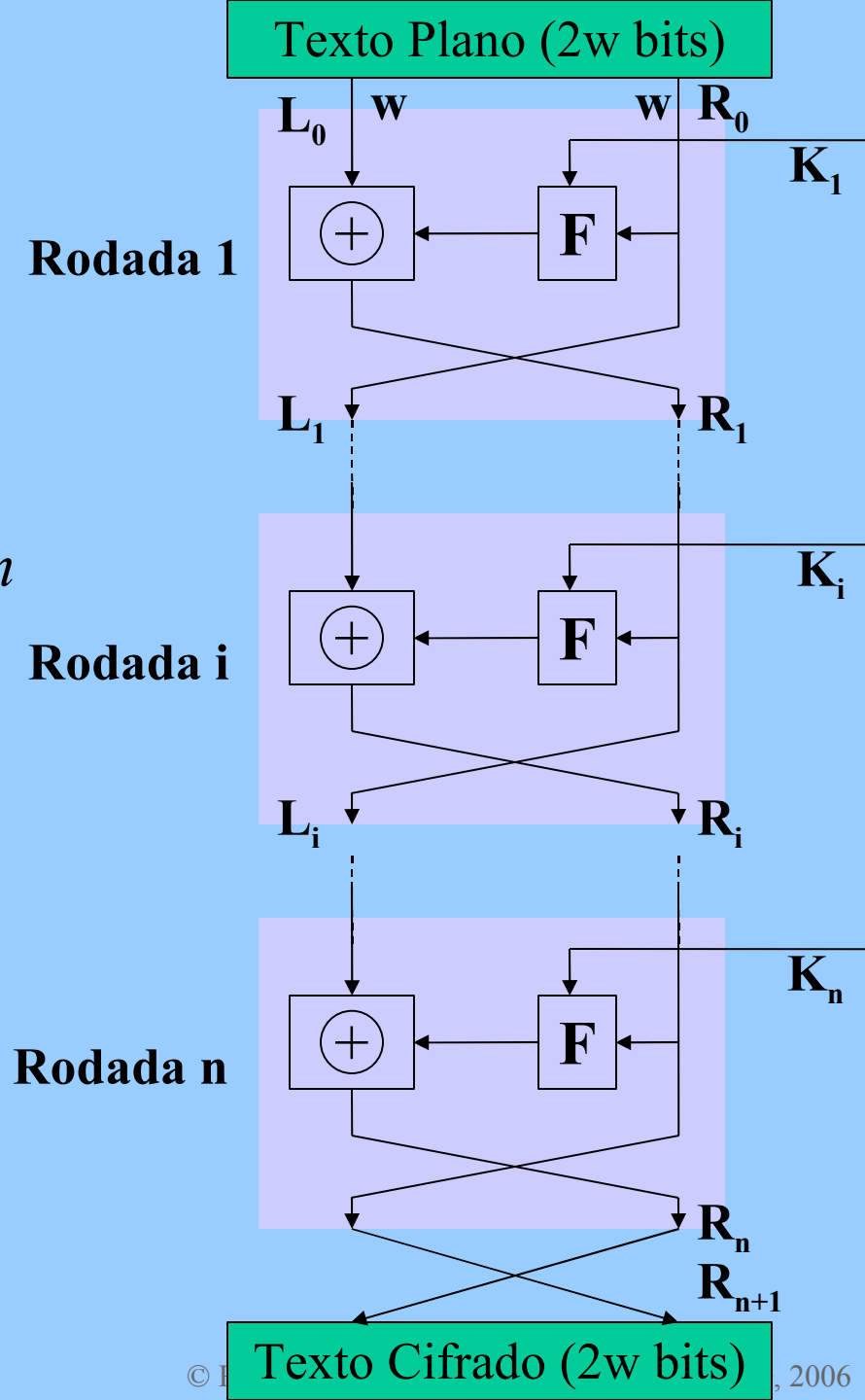
- Aproximação por cifradores produto
- Uso de substituições e Permutações
- Claude Shannon
 - *Confusão*
 - *Difusão*

Estrutura do Cifrador de Feistel

Caso particular da Rede de Substituição-Permutação de Shannon

Parâmetros e Características de Projeto

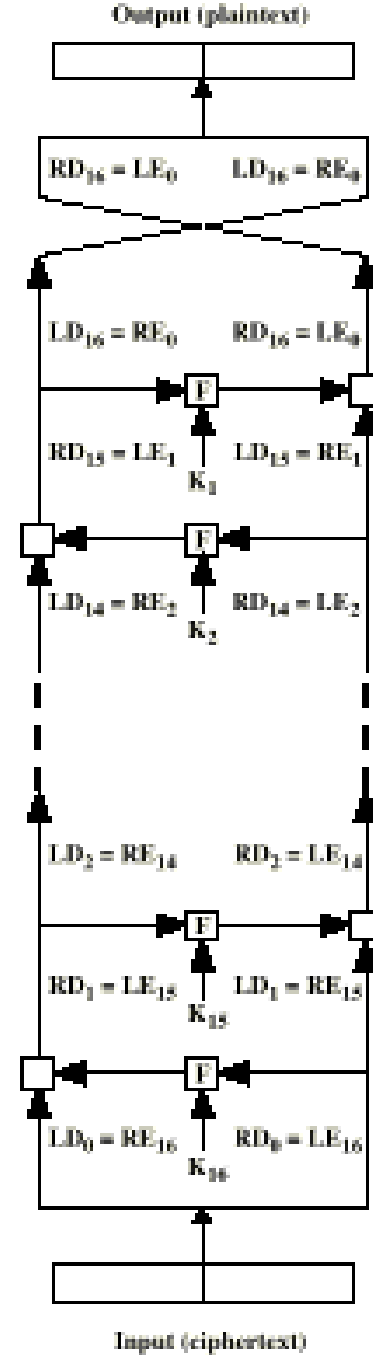
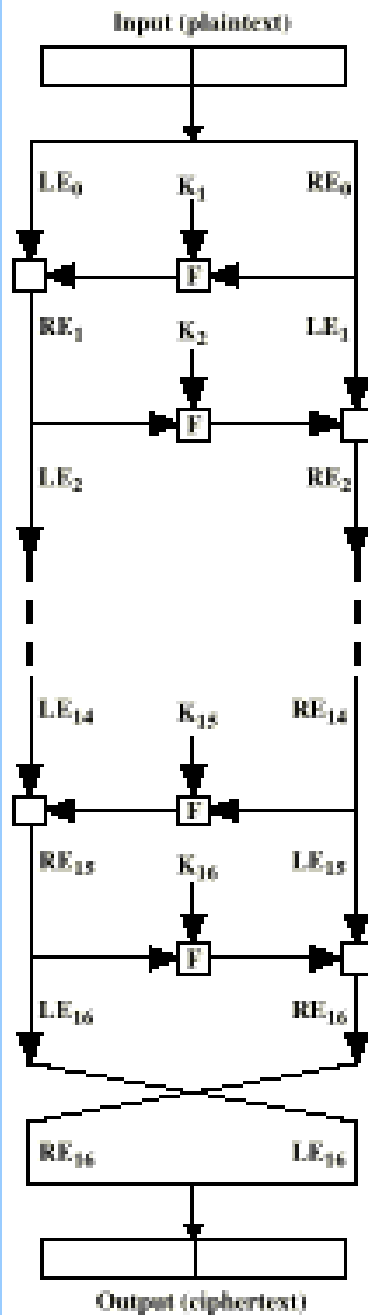
- Tamanho do Bloco
- Tamanho da Chave
- Número de Rodadas
- Algoritmo de Geração das Subchaves
- Função Ciclo (F)
- Software Rápido (E e D)
- Fácil Análise



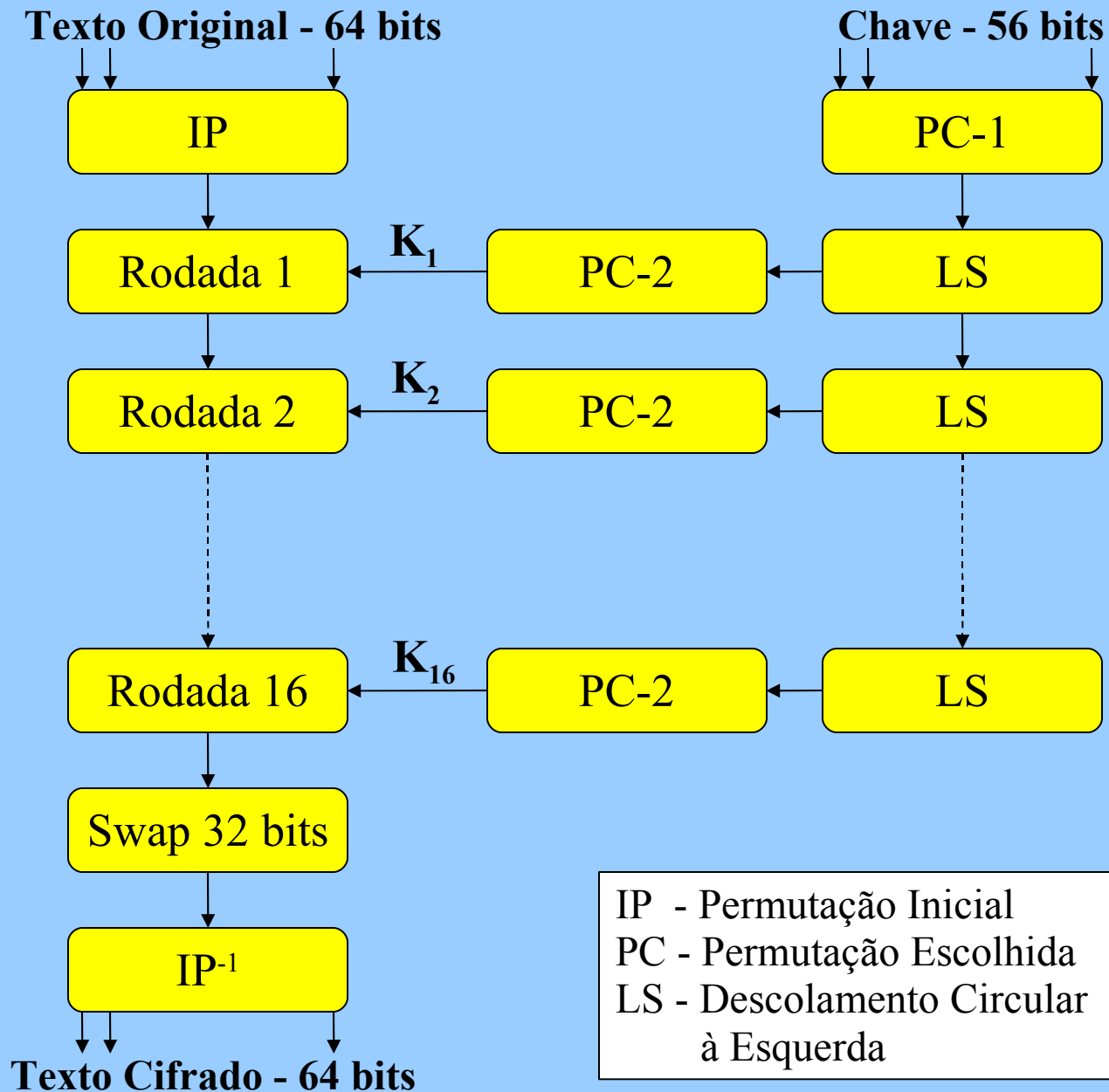
Redes de Feistel

- É um método geral para transformar qualquer função em uma permutação
- Inventada por Horst Feistel para o Lucifer
- Usada por muitos criptadores
 - DES, FEAL, GOST, Khufu e Khafre
 - Loki, Cast, Blowfish, RC5, Mars ...

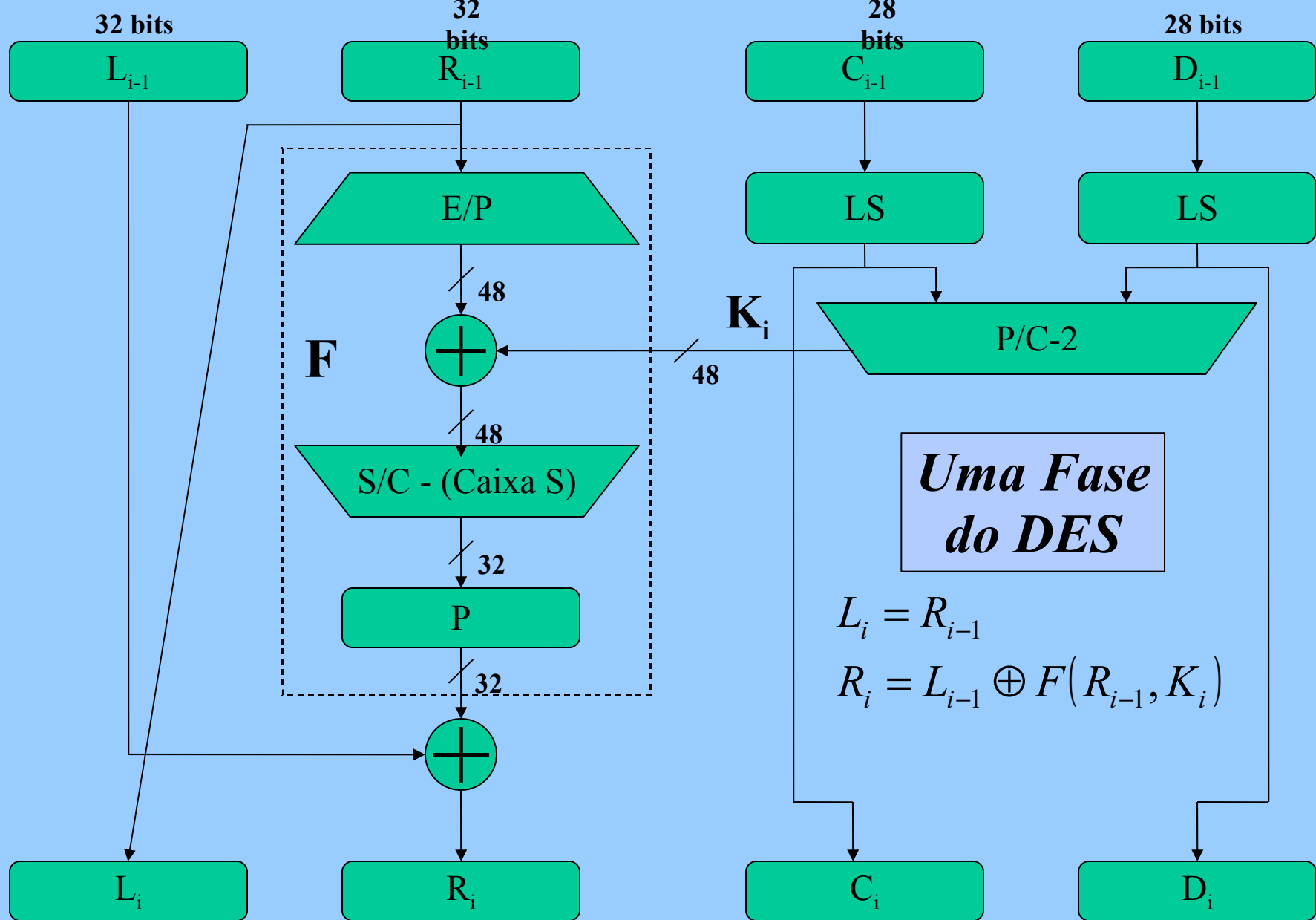
Encriptação/Decriptação



Texto Original - 64 bits



IP - Permutação Inicial
PC - Permutação Escolhida
LS - Descolamento Circular
à Esquerda



Tabelas de Permutação

IP
Permutação Inicial

58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

IP⁻¹ - Inversa da
Permutação Inicial

40	08	48	16	56	24	64	32
39	07	47	15	55	23	63	31
38	06	46	14	54	22	62	30
37	05	45	13	53	21	61	29
36	04	44	12	52	20	60	28
35	03	43	11	51	19	59	27
34	02	42	10	50	18	58	26
33	01	41	09	49	17	57	25

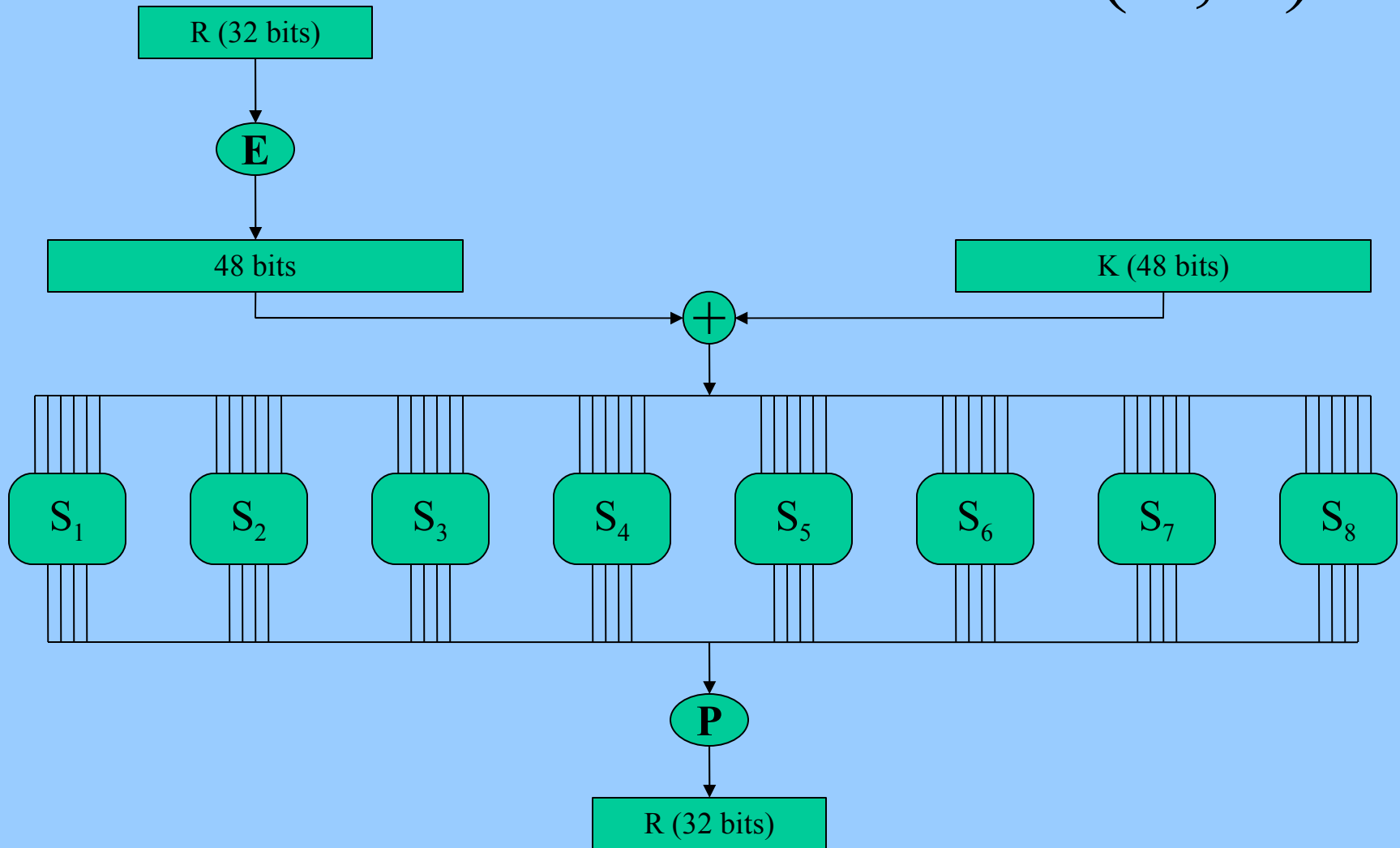
EP
Expansão Permutação

32	01	02	03	04	05
04	05	06	07	08	09
08	09	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	01

P
Função Permutação

16	07	20	21	29	12	28	17	01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09	19	13	30	06	22	11	04	25

Cálculo de $F(R,K)$



Definição das Caixas S do DES

S_1

14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

S_5

02	12	04	01	07	10	11	06	08	05	03	15	13	00	14	09
14	11	02	12	04	07	13	01	05	00	15	10	03	09	08	06
04	02	01	11	10	13	07	08	15	09	12	05	06	03	00	14
11	08	12	07	01	14	02	13	06	15	00	09	10	04	05	03

S_2

15	01	08	14	06	11	03	04	09	07	02	13	12	00	05	10
03	13	04	07	15	02	08	14	12	00	01	10	06	09	11	05
00	14	07	11	10	04	13	01	05	08	12	06	09	03	02	15
13	08	10	01	03	15	04	02	11	06	07	12	00	05	14	09

S_6

12	01	10	15	09	02	06	08	00	13	03	04	14	07	05	11
10	15	04	02	07	12	09	05	06	01	13	14	00	11	03	08
09	14	15	05	02	08	12	03	07	00	04	10	01	13	11	06
04	03	02	12	09	05	15	10	11	14	01	07	06	00	08	13

S_3

10	00	09	14	06	03	15	05	01	13	12	07	11	04	02	08
13	07	00	09	03	04	06	10	02	08	05	14	12	11	15	01
13	06	04	09	08	15	03	00	11	01	02	12	05	10	14	07
01	10	13	00	06	09	08	07	04	15	14	03	11	05	02	12

S_7

04	11	02	14	15	00	08	13	03	12	09	07	05	10	06	01
13	00	11	07	04	09	01	10	14	03	05	12	02	15	08	06
01	04	11	13	12	03	07	14	10	15	06	08	00	05	09	02
06	11	13	08	01	04	10	07	09	05	00	15	14	02	03	12

S_4

07	13	14	03	00	06	09	10	01	02	08	05	11	12	04	15
13	08	11	05	06	15	00	03	04	07	02	12	01	10	14	09
10	06	09	00	12	11	07	13	15	01	03	14	05	02	08	04
03	15	00	06	10	01	13	08	09	04	05	11	12	07	02	14

S_8

13	02	08	04	06	15	11	01	10	09	03	14	05	00	12	07
01	15	13	08	10	03	07	04	12	05	06	11	00	14	09	02
07	11	04	01	09	12	14	02	00	06	10	13	15	03	05	08
02	01	14	07	04	10	08	13	15	12	09	00	03	05	06	11

Tabelas Usadas para o Cálculo da Chave

PC-1

57	49	41	33	25	17	09	01	58	50	42	34	26	18
10	02	59	51	43	35	27	19	11	03	60	52	44	36
63	55	47	39	31	23	15	07	62	54	46	38	30	22
14	06	61	53	45	37	29	21	13	05	28	20	12	04

PC-2

14	17	11	24	01	05	03	28	15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02	41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56	34	53	46	42	50	36	29	32

Deslocamentos Circulares à Esquerda por rodada

Rodada	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotacionados	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Efeito Avalanche

Mudança no Texto Plano

Rodada	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Número de Bits que Diferem	1	6	21	35	39	34	32	31	29	42	44	32	30	30	26	29	34

Mudança na Chave

Rodada	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Número de Bits que Diferem	1	2	14	28	32	30	32	35	34	40	38	31	33	28	26	34	35

A Força do DES

Custo da Máquina

\$100.000

\$1.000.000

\$10.000.000

Tempo de Busca

6 horas

35 Minutos

210 Segundos

Estimado em 1997

CI's comerciais

Fab.	Chip	Ano	Clock [MHz]	Taxa [Mbyte/s]
AMD	AmZ8068	1982	4	1,7
CE-infosys	CE99C003A	1994	30	20
Newbridge	CA95C68	1993	33	14,67
VLSI Tech	VM007	1993	32	200

Velocidade DES em Software

Processador	Velocidade [MHz]	Taxa [Kbyte/s]
8088	4,7	2,9
68040	40	180
80486	66	336
Pentium III	500	6.700
Sun ELS		203
HP 9000/887		1.530

Boas Caixas S

- Nenhum bit de saída deve ser uma função linear dos bits da entrada
- Toda linha deve incluir todas as 16 possíveis saídas
- Se duas entradas diferem em 1 bit, a saída deve diferir em pelo menos 2 bits
- Se duas entradas diferem nos 2 bits do meio, a saída deve diferir em pelo menos 2 bits
- Se duas entradas diferem nos 2 primeiros bits e são iguais nos 2 últimos, as 2 saídas devem ser diferentes
- Para qualquer diferença em 6 bits na entrada, não mais que 8 dos 32 pares de entradas exibindo essa diferença podem resultar na mesma diferença na saída
- Idem para 3 caixas S

Projeto de P

- 4 bits na fase (i) são distribuídos tal que:
 - 2 afetam bits do meio na fase (i+1)
 - 2 afetam bits terminais
- 4 bits de cada caixa S afetam 6 diferentes caixas S da próxima fase e não 2 afetam a mesma caixa S
- Se 1 bit de saída da caixa S_j afeta 1 bit do meio da caixa S_k na próxima fase, então 1 bit da saída de S_k não pode afetar 1 bit do meio da caixa S_j

Número de Rodadas

- Esforço através da Criptoanálise seja maior que o ataque pela força bruta

Schneier em 1996 →

Criptoanálise Diferencial de
16 Fases do DES = $2^{55,1}$
Força Bruta = 2^{55}

Projeto da Função F

- Não Linear
- Critério da Avalanche Estrita (**SAC**)
 - qq bit de saída j deveria trocar com probabilidade $1/2$
- Critério da Independência dos bits (**BIC**)
- Tamanho das Caixas S
- Função Bent
- Critério da Avalanche Garantida (**GA**)

Projeto das Caixas S


- Randômica
 - Caixas Randômicas dependentes da Chave (Blowfish)
- Randômica com Teste
- Manual
- Princípios Matemáticos (CAST)

Projeto do Algoritmo de Geração das Sub-Chaves

- Ainda não foram definidos princípios gerais

Garantir, no mínimo:

- o critério da Avalanche Estrita entre a Chave e o Texto Cifrado
- o critério da independência de bits



Adams, C. Simple and Effective Key Scheduling for Symmetric Ciphers. Proceedings, Workshop in Selected Areas of Cryptography, SAC'94. 1994.

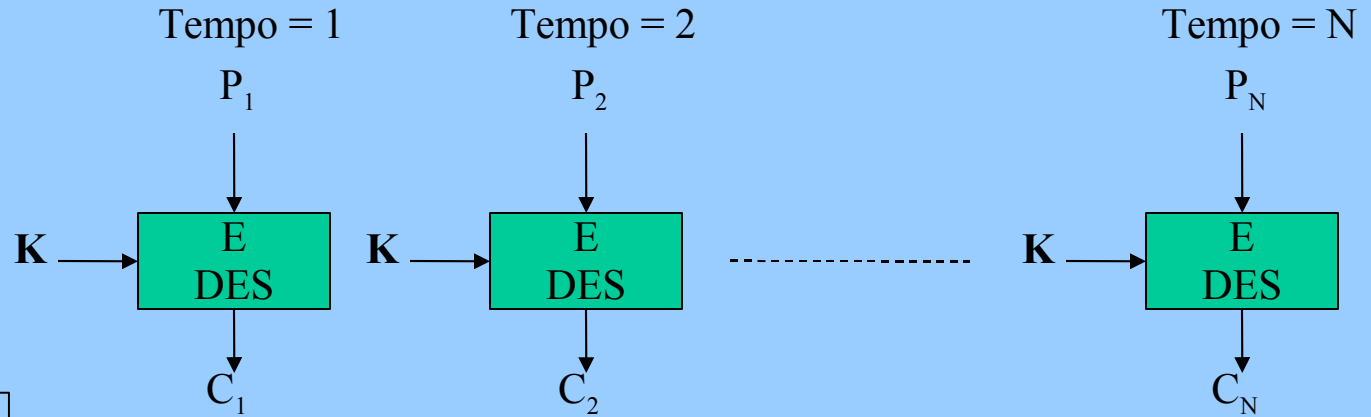
Modos de Operação dos Cifradores de Bloco

(FIPS PUB 74, 81)

- ECB - Codebook Eletrônico
- CBC - Encadeamento de Blocos Cifrados
- CFB - Cifrador Retroalimentado
- OFB - Saída Retroalimentada
- CTR - Contador

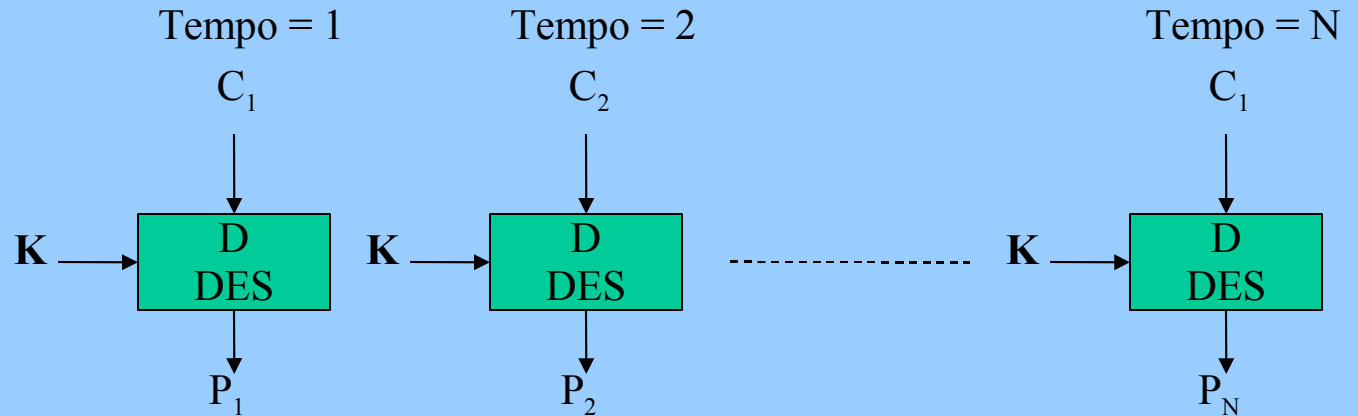
Codebook Eletrônico (ECB)

Cifrar



Transmissão Segura de
Pequenas Informações

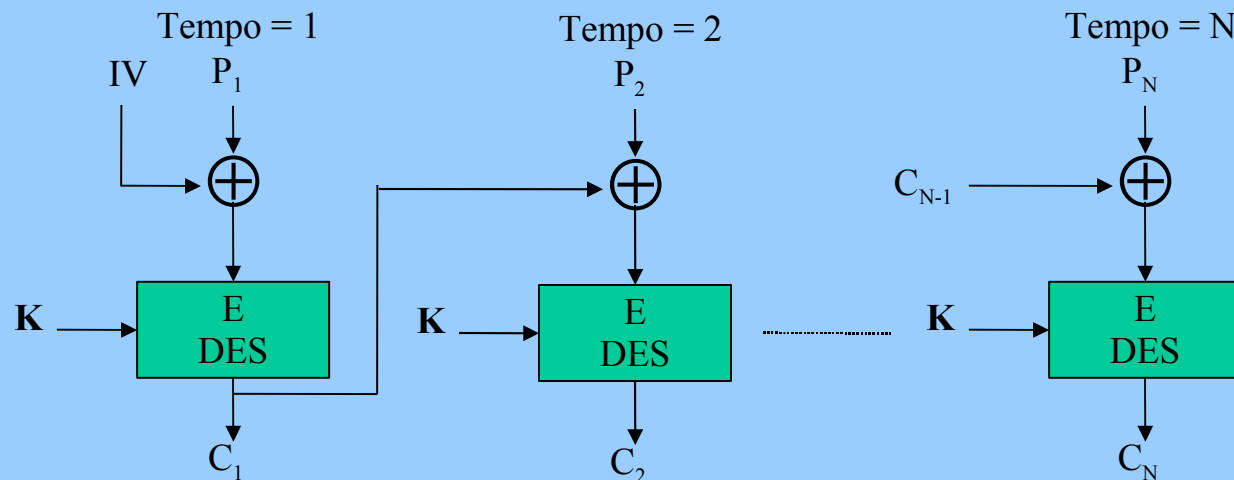
Decifrar



Encadeamento de Blocos Cifrados (CBC)

Cifrar

$$C_n = D_k[C_{n-1} \oplus P_n]$$



**Propósito Geral
Autenticação**

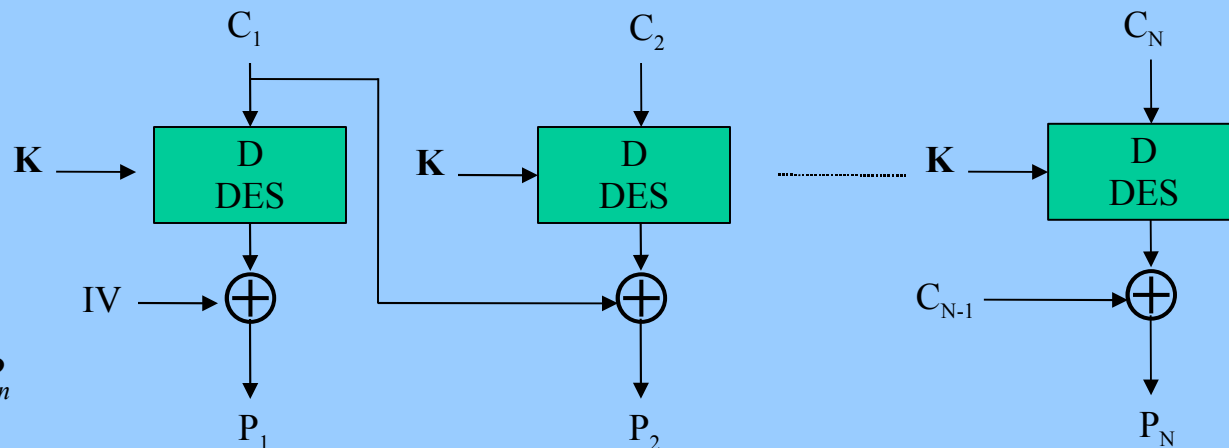
Decifrar

$$D_k[C_n] = D_k[E_k(C_{n-1} \oplus P_n)]$$

$$D_k[C_n] = (C_{n-1} \oplus P_n)$$

$$C_{n-1} \oplus D_k[C_n] = C_{n-1} \oplus C_{n-1} \oplus P_n$$

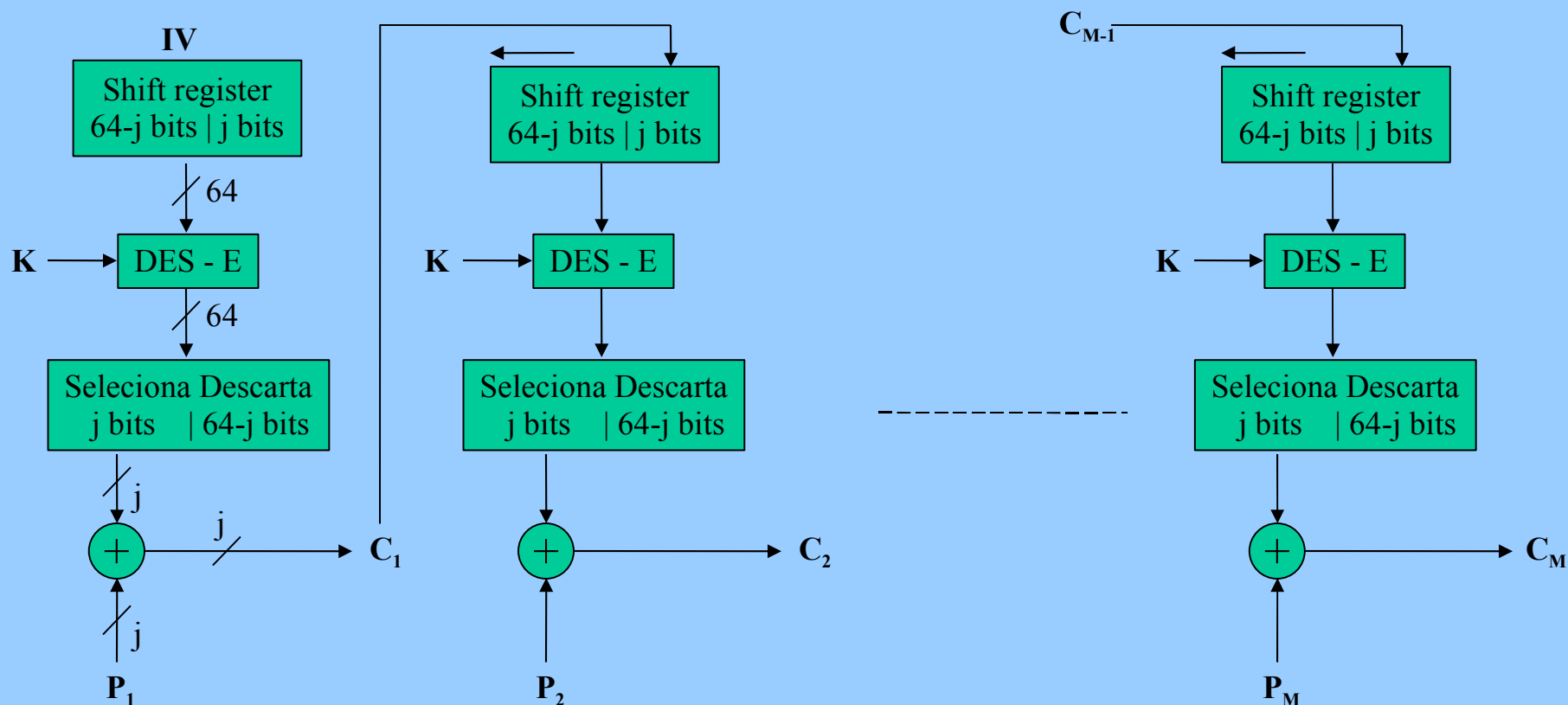
$$C_{n-1} \oplus D_k[C_n] = P_n$$



Modo Retroalimentado de j bits - CFB

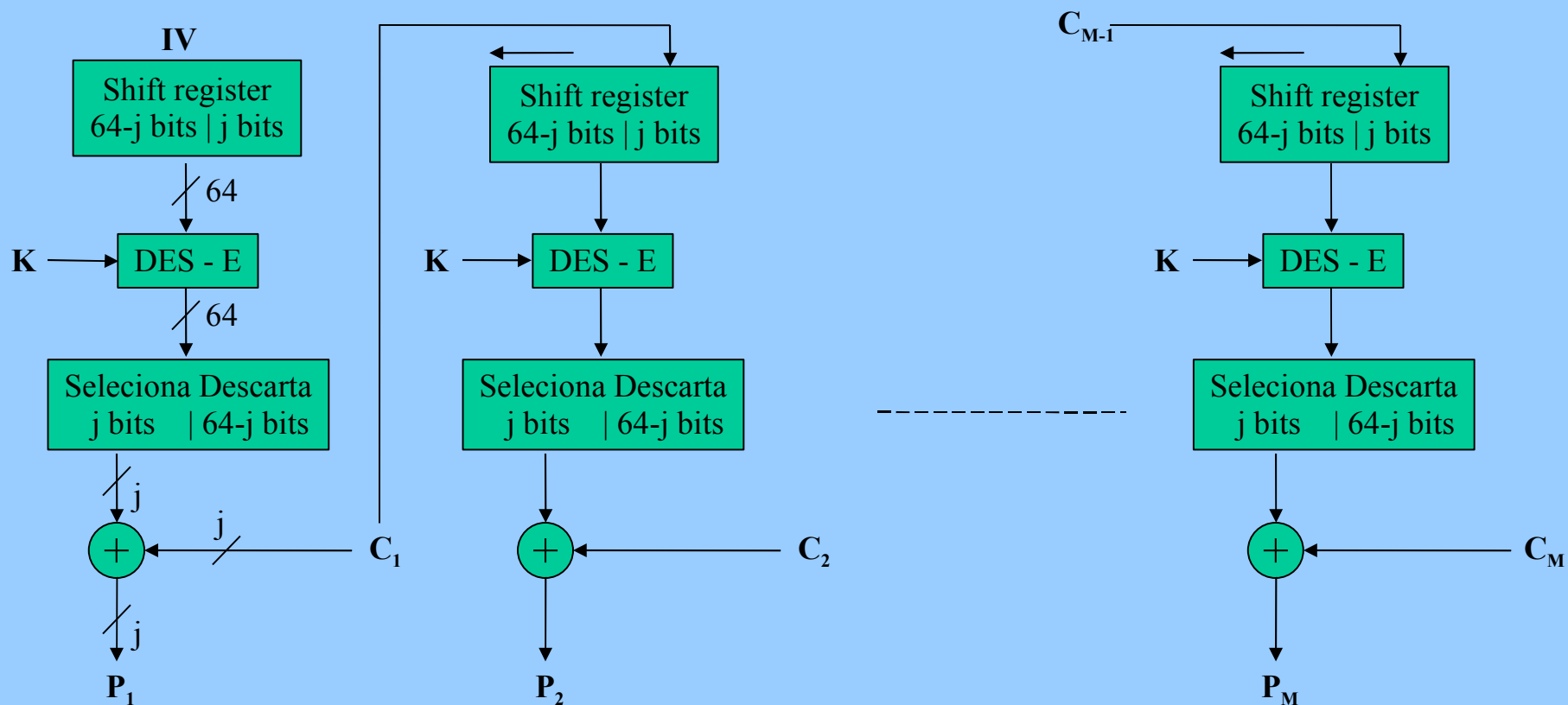
Cifrar

Transmissão em Cadeia de Propósito Geral
Autenticação



Modo Retroalimentado de j bits - CFB

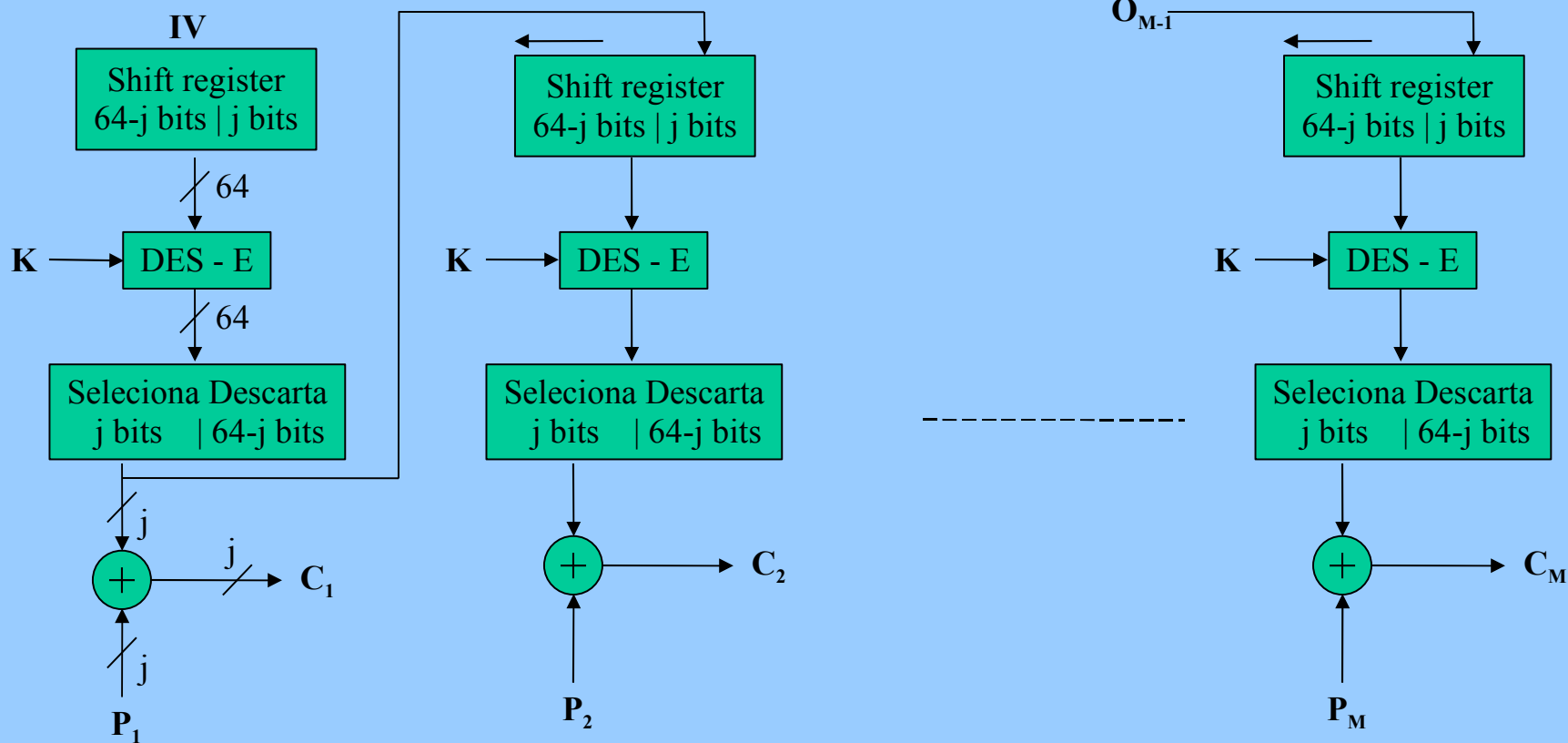
Decifrar



Modo de Saída Retroalimentada com j bits - OFB

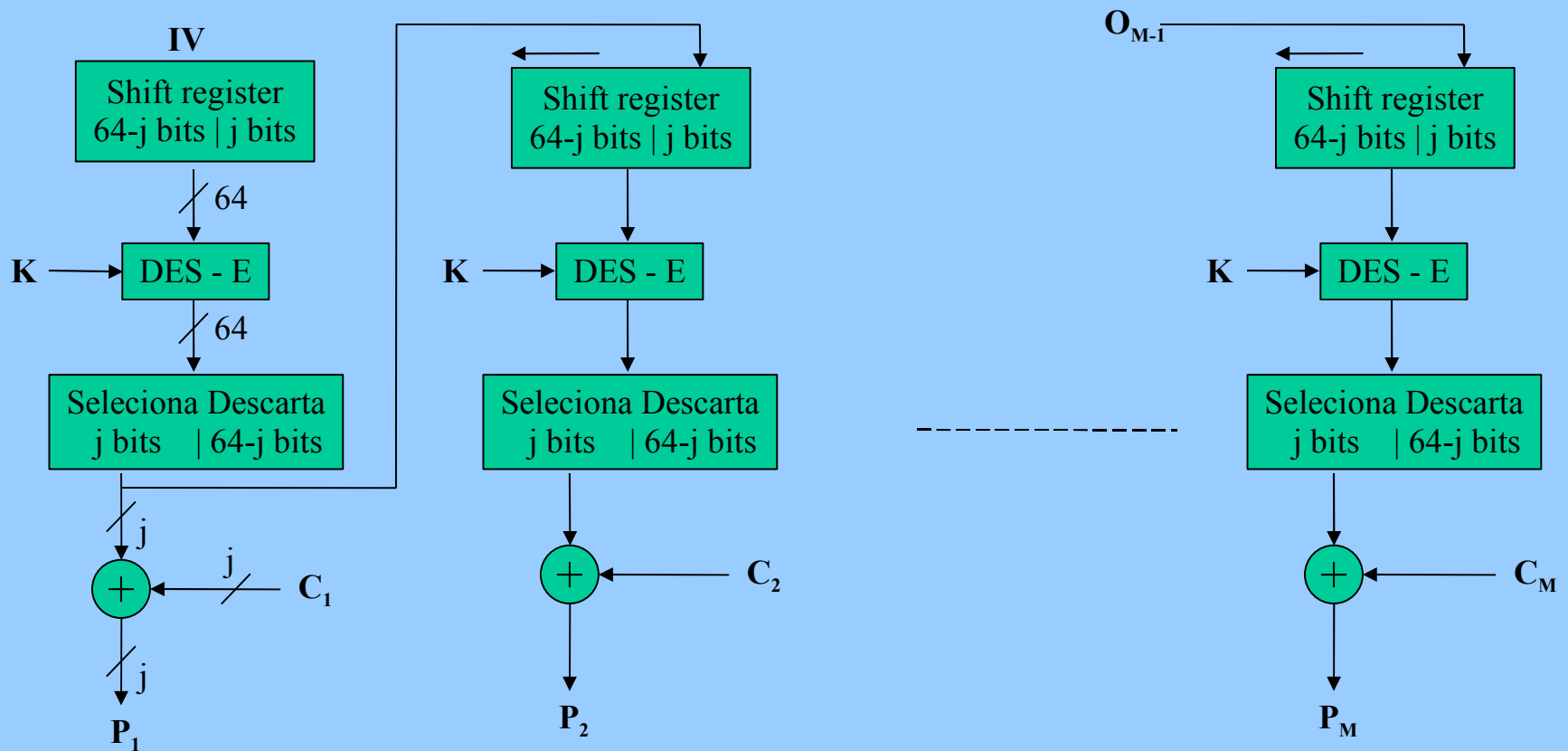
Cifrar

Transmissão em Cadeia sobre Canais Ruidosos



Modo de Saída Retroalimentada com j bits - OFB

Decifrar



Funções Bent

$$f : \{0,1\}^n \rightarrow \{0,1\}$$

Transformada Walsh

$$W_f(w) = \sum_{x=0}^{2^n-1} (-1)^{f(x)+w \bullet x}$$

$$w \bullet x = w_{n-1}x_{n-1} \oplus \dots \oplus w_0x_0$$

$$-2^n \leq W_f(w) \leq 2^n$$

Conjunto de Funções Bent
n par

$$W_f(w) = \pm 2^{\frac{n}{2}}$$

$$\forall w \in \{0,1\}^n$$

Transformada Walsh Inversa

$$f(x) = \frac{1}{2^n} \sum_{w=0}^{2^n-1} W_f(w) (-1)^{w \bullet x}$$

Ref:

ADAMS, C; Tavares, S.
Generating and Counting
Binary Bent Sequences.
IEEE Transactions on
Information Theory, 1990.