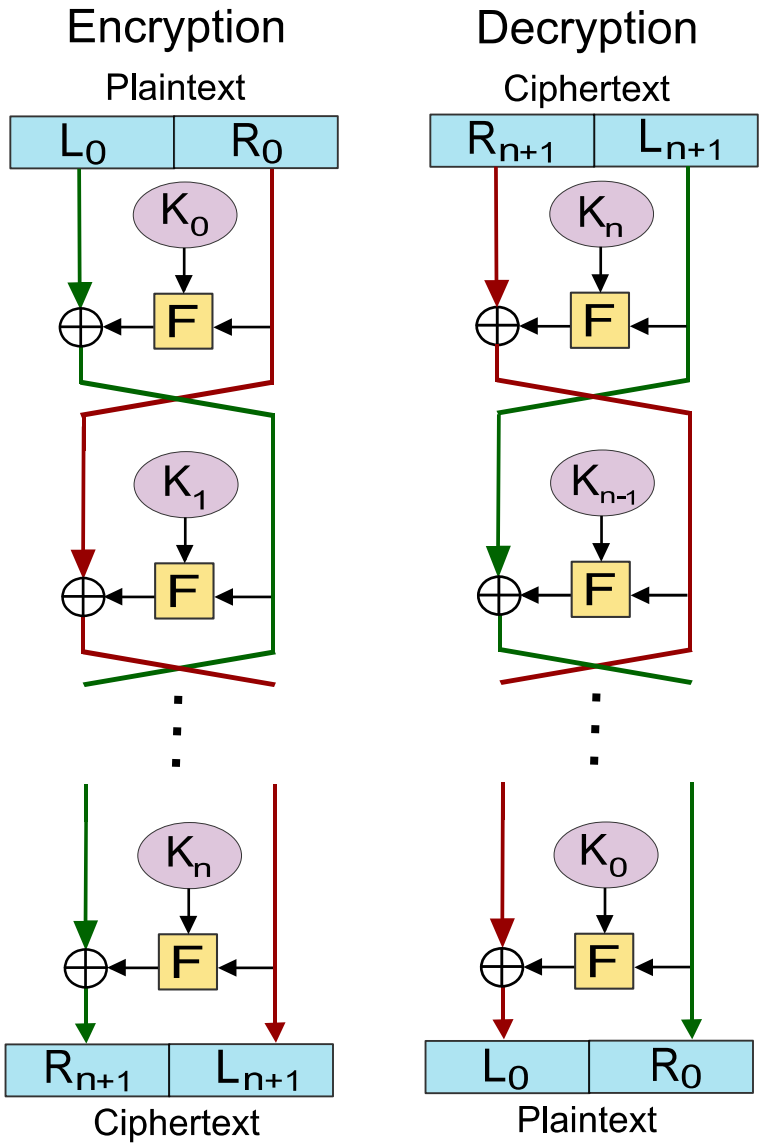
Cifradores Simétricos

- Mesma chave para cifrar e decifrar
- 2 categorias:
  - Bloco
    - Considera um bloco como um todo
    - Cifradores de bloco ideais são impraticáveis
    - Feistel propôs componentes implementáveis
  - Stream
    - Bit a bit / Byte a byte
    - Minoria

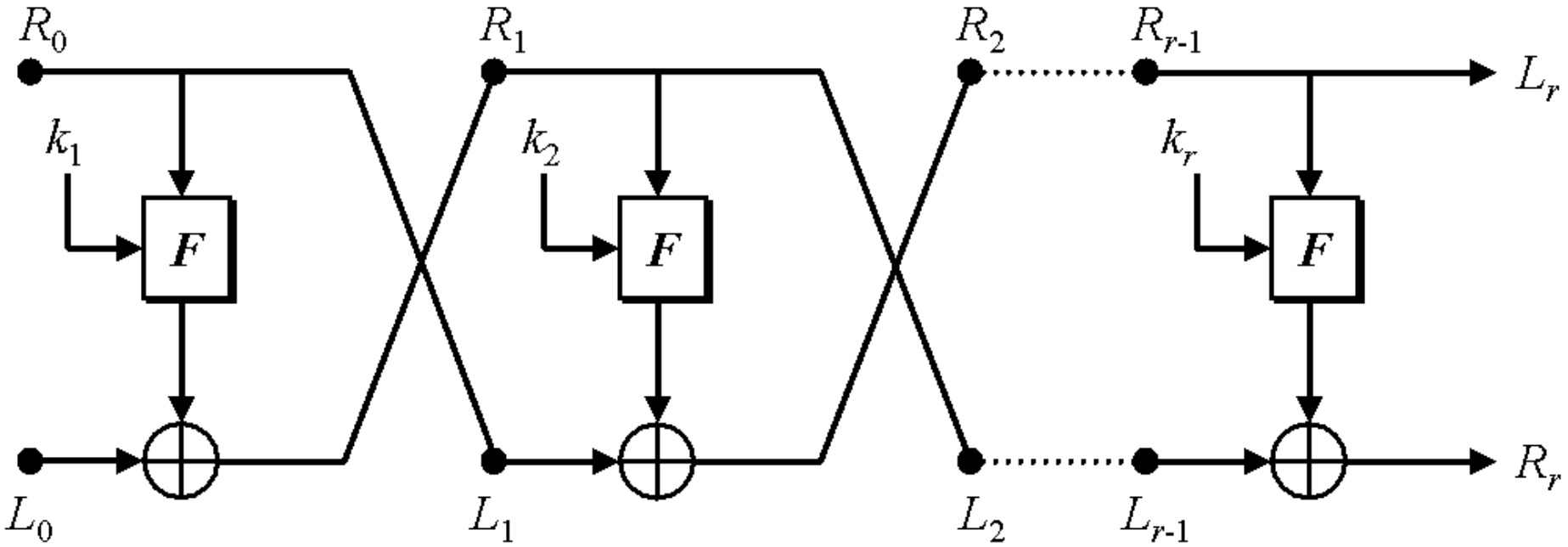
Confusão x Difusão

- Proposto por Claude Shannon (1945)
- Confusão:
  - Complexidade da relação texto cifrado x chave
  - Protege a chave
  - Substituição deve ser complexa
- Difusão:
  - Dissipação da estrutura estatística
  - 1 dígito de entrada afeta n dígitos de saída
  - Dissimula freqüência do texto claro

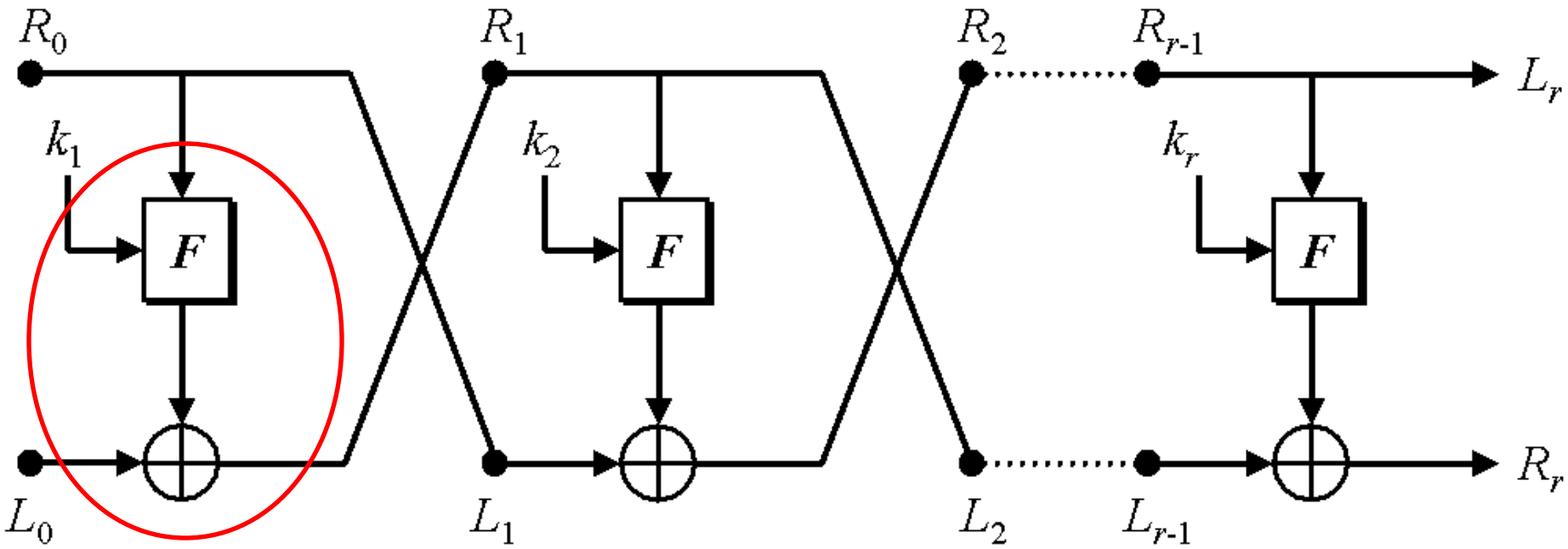
Redes de Feistel



Redes de Feistel

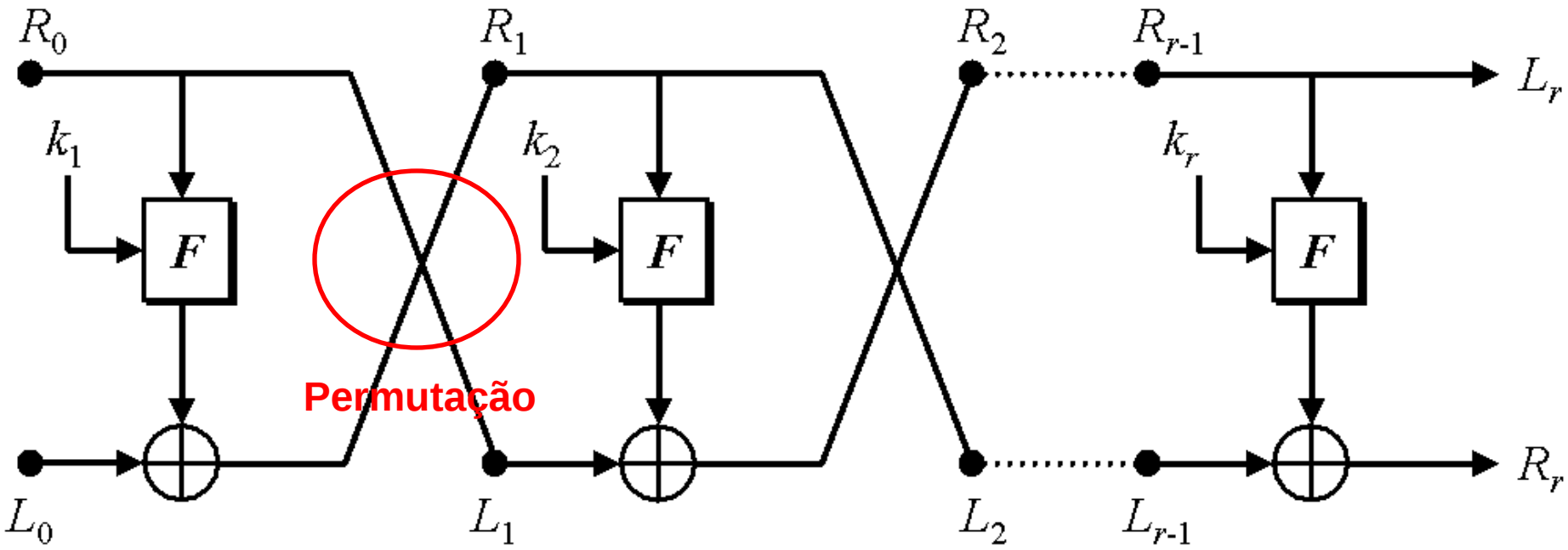


Redes de Feistel



Substituição

Redes de Feistel



Design de Redes de Feistel

- Tamanho de Bloco
  - ⇑ Tamanho ⇑Segurança
  - ⇑ Tamanho ⇓Velocidade
  - Relacionado com a difusão
  - 64 bits em média
- Tamanho de Chave
  - Mesmas características do bloco
  - Relacionado com a confusão
  - 128 bits pelo menos

Design de Redes de Feistel

- Numero de rodadas
  - ↑Rodadas ↑Segurança
  - Normalmente 16
- Geração de sub-chaves
  - ↑Complexidade ↑Dificuldade na criptoanalise
- Função de rodada
  - Mesma característica da geração de chaves

Velocidade X Segurança

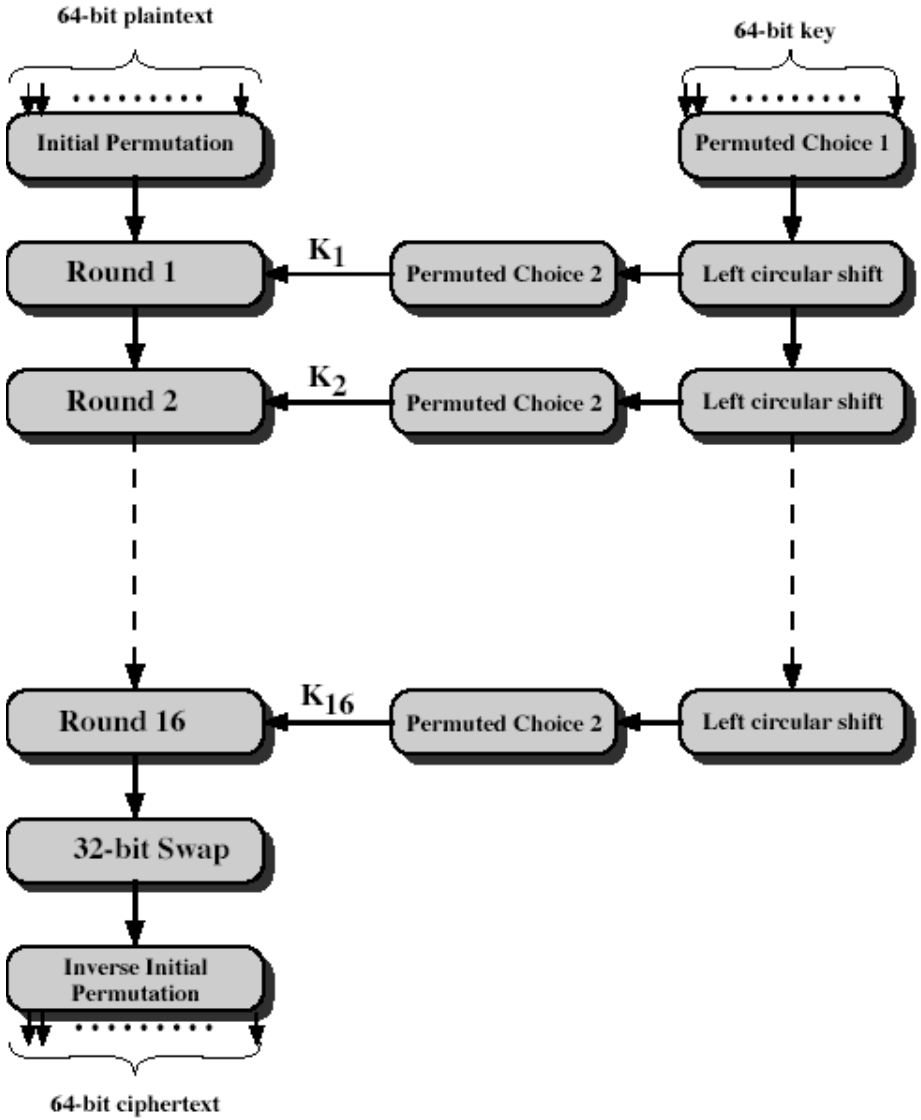
Redes de Feistel

- $Re_i = Le_{i-1}$ xor $F(Re_{i-1}, K_i)$
- $Le_i = Re_{i-1}$
- Cifragem e Decifragem com o mesmo algoritimo (chaves em ordem inversa)
- Pelo menos 3 rodadas para começar a ter difusão e confusão

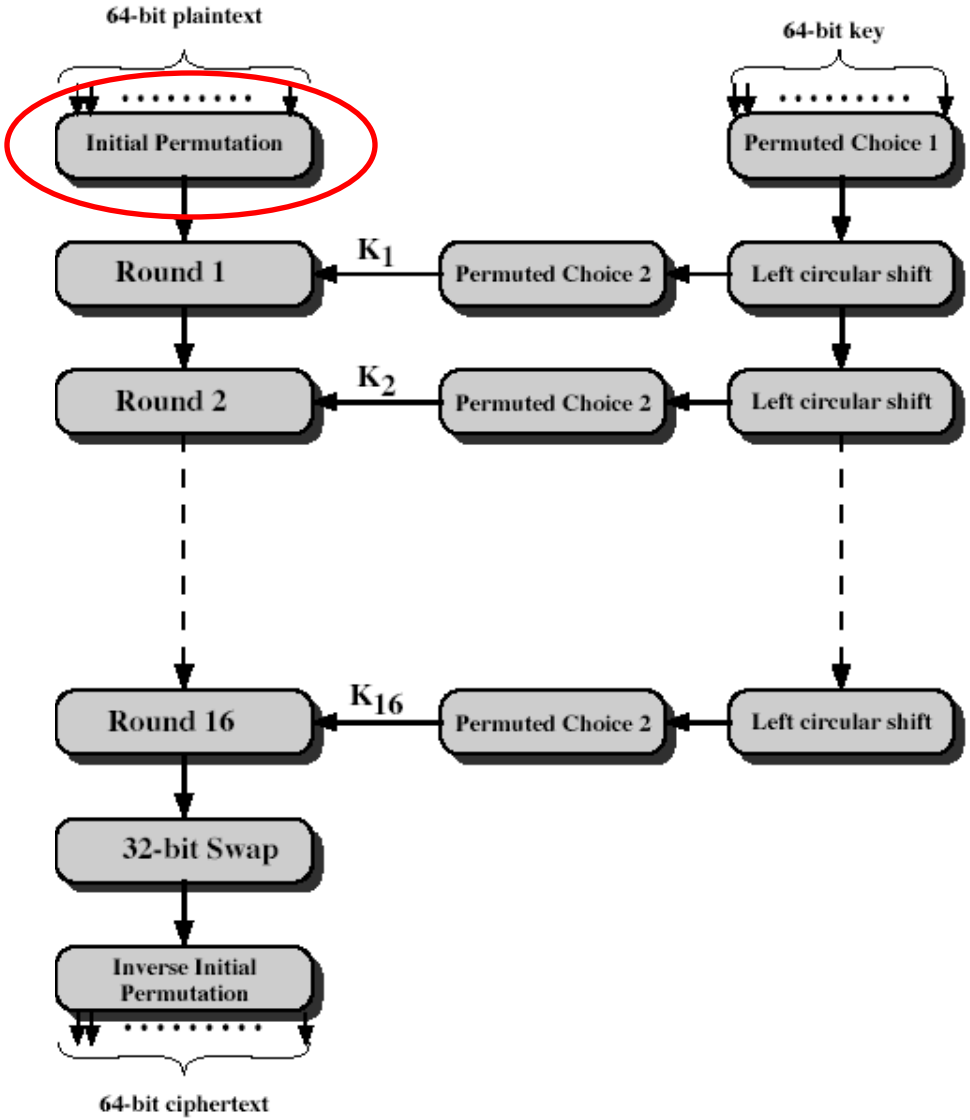
DES – Data Encryption Standard

- Federal Information Processing Standard 46 (FIPS PUB 46) [1977]
- IBM Lucifer [1971]
- Baseado em rede de Feistel
- Chave de 56 bits (para caber em um chip)
- Blocos de 64 bits
- Ótima implementação em Hardware

DES Ilustrado



DES Ilustrado



DES – Permutação inicial

(a) Initial Permutation (IP)

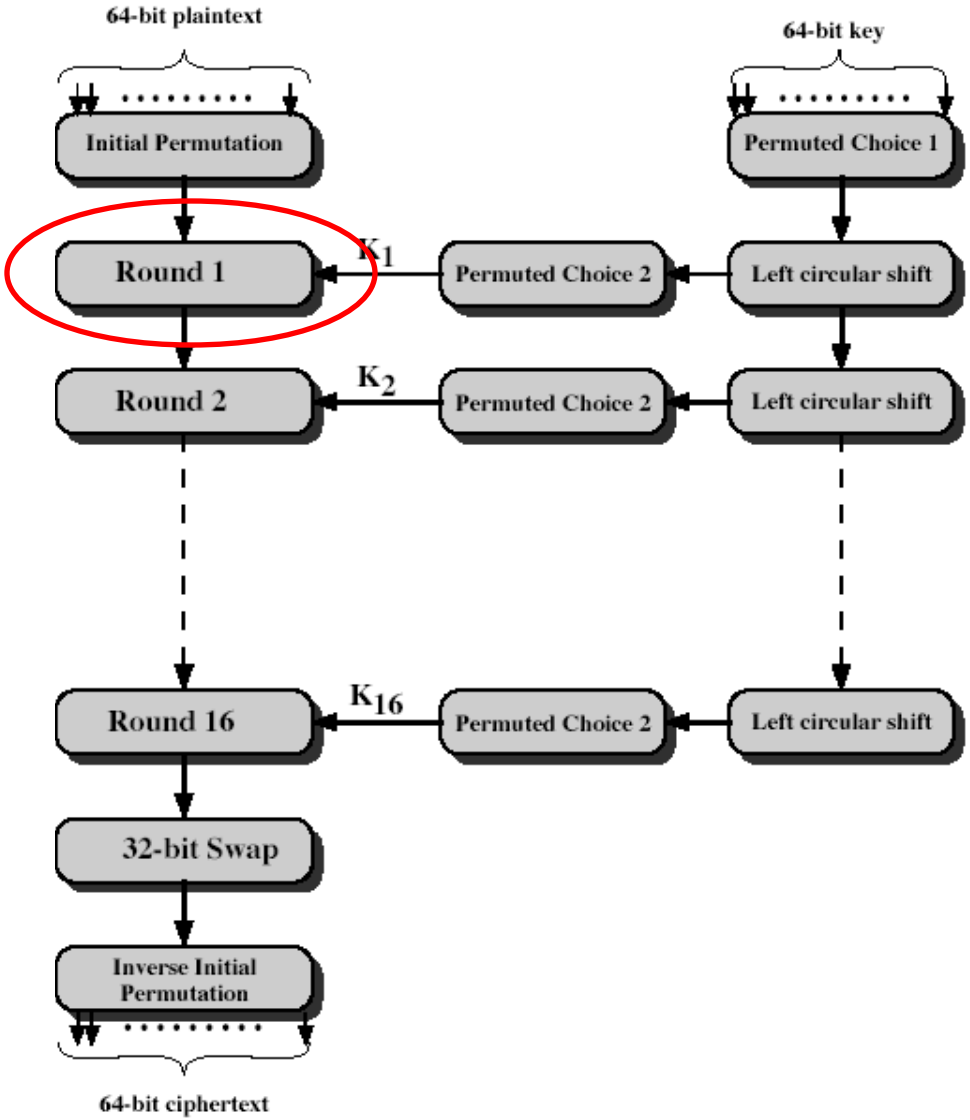
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(b) Inverse Initial Permutation (IP^{-1})

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

- IP-1(IP(M))=M
- Adicionam Difusão

DES Ilustrado



DES – Estrutura de 1 Rodada

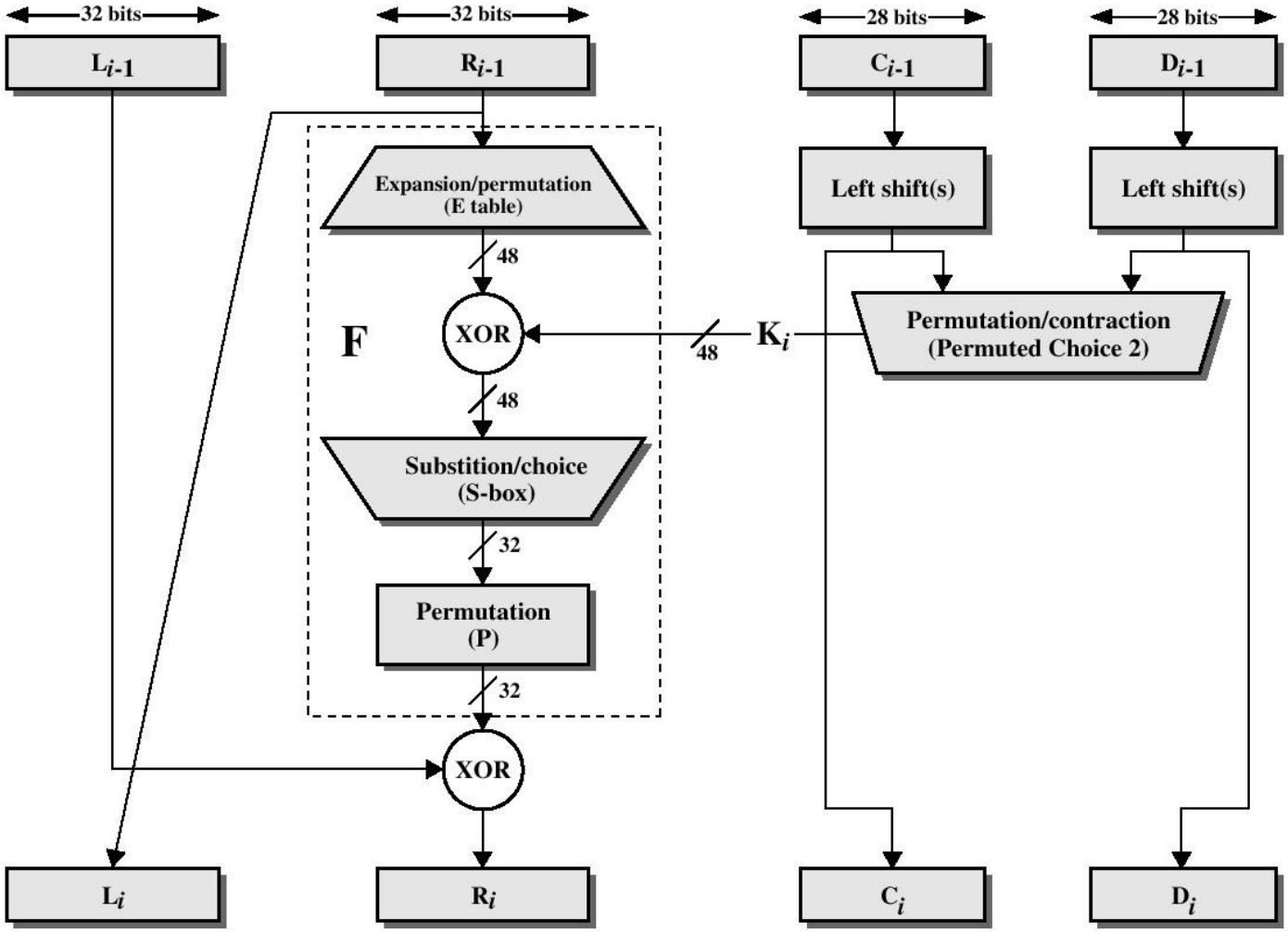


Figure 2.4 Single Round of DES Algorithm

DES – Estrutura de 1 Rodada

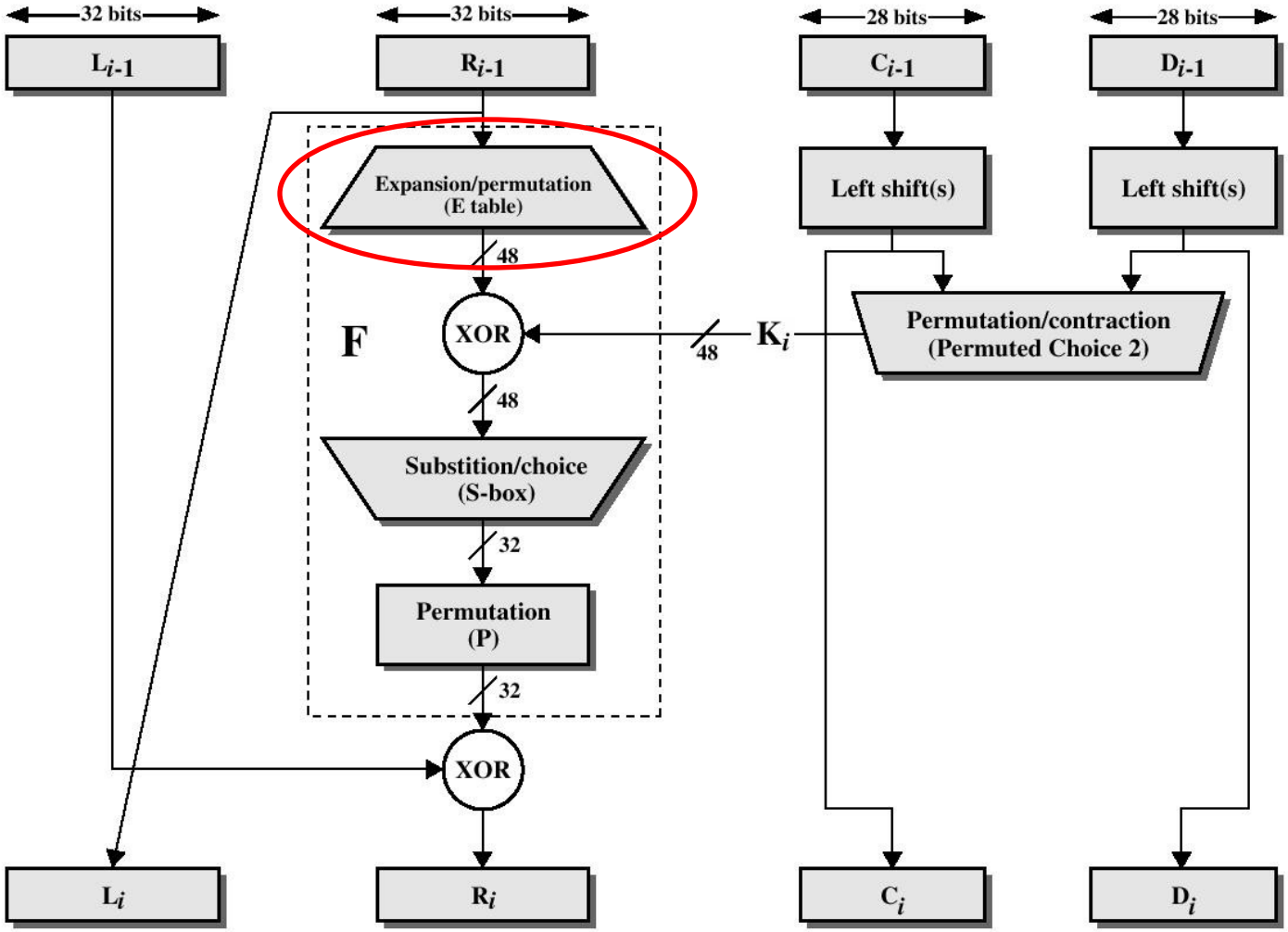


Figure 2.4 Single Round of DES Algorithm

DES - Permutação de Expansão

(c) Expansion Permutation (E)

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

DES – Estrutura de 1 Rodada

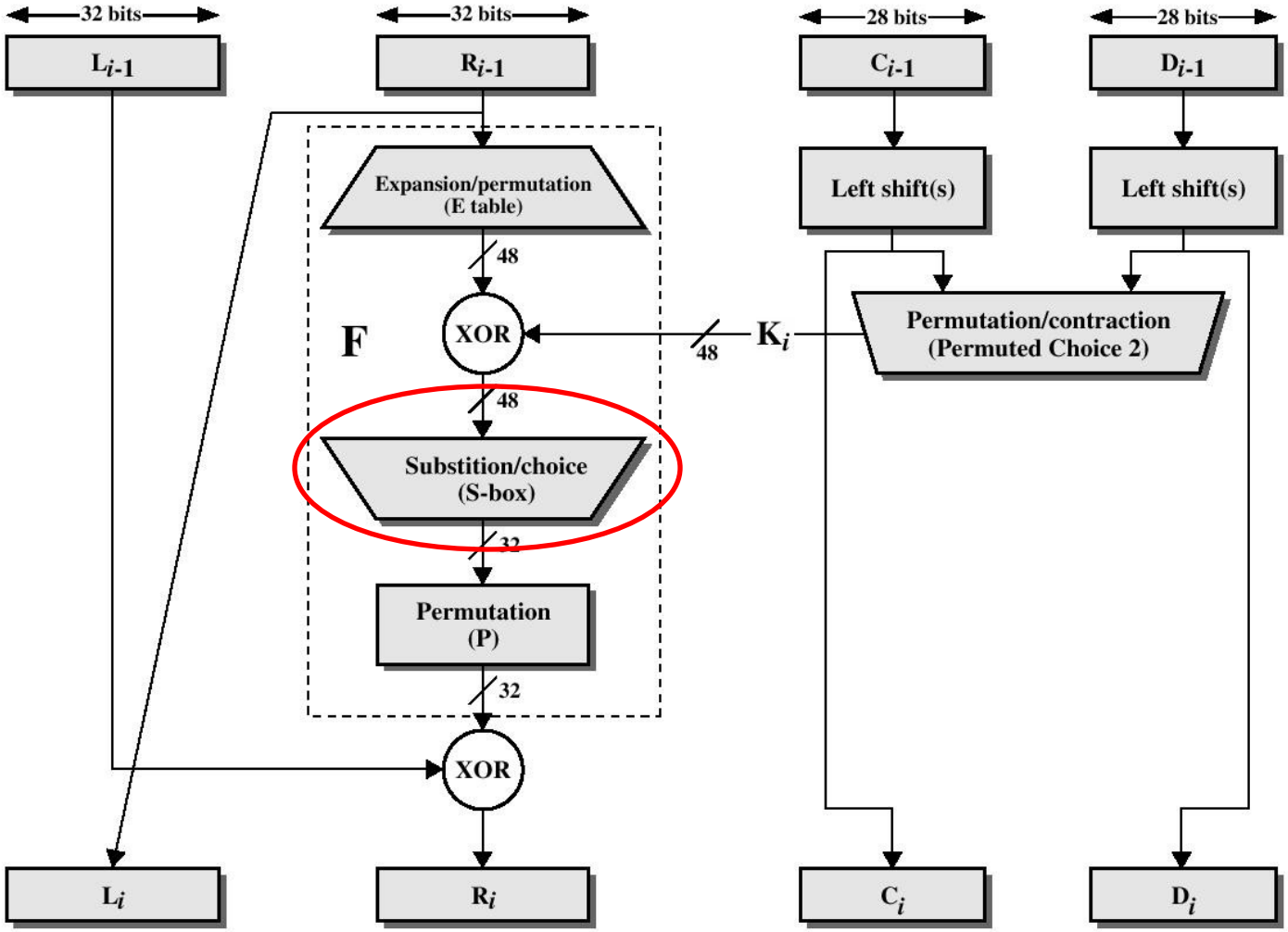


Figure 2.4 Single Round of DES Algorithm

DES – Caixas S

Table 3.3 Definition of DES S-Boxes

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

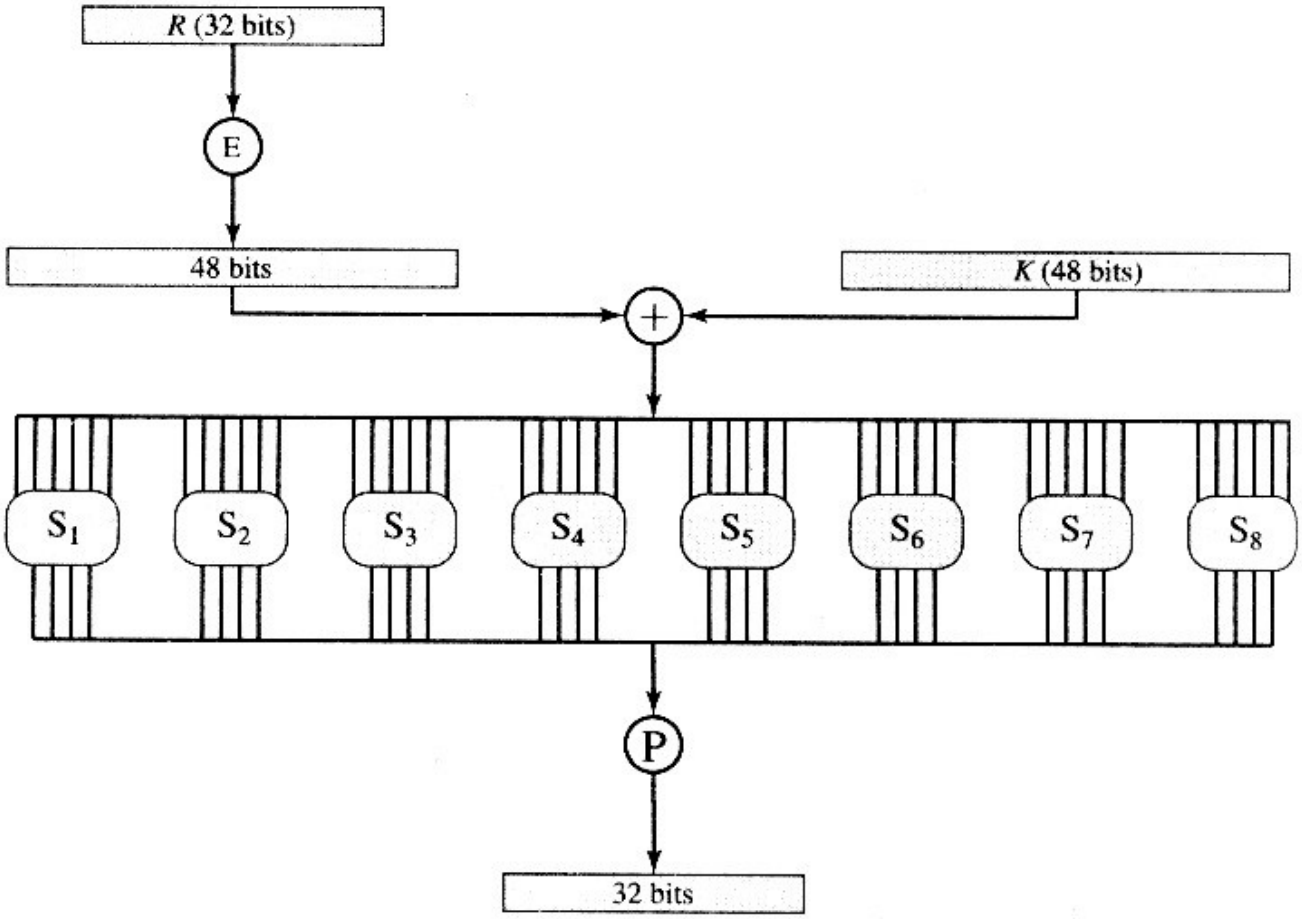
S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

DES – Função (R,K)



DES – Estrutura de 1 Rodada

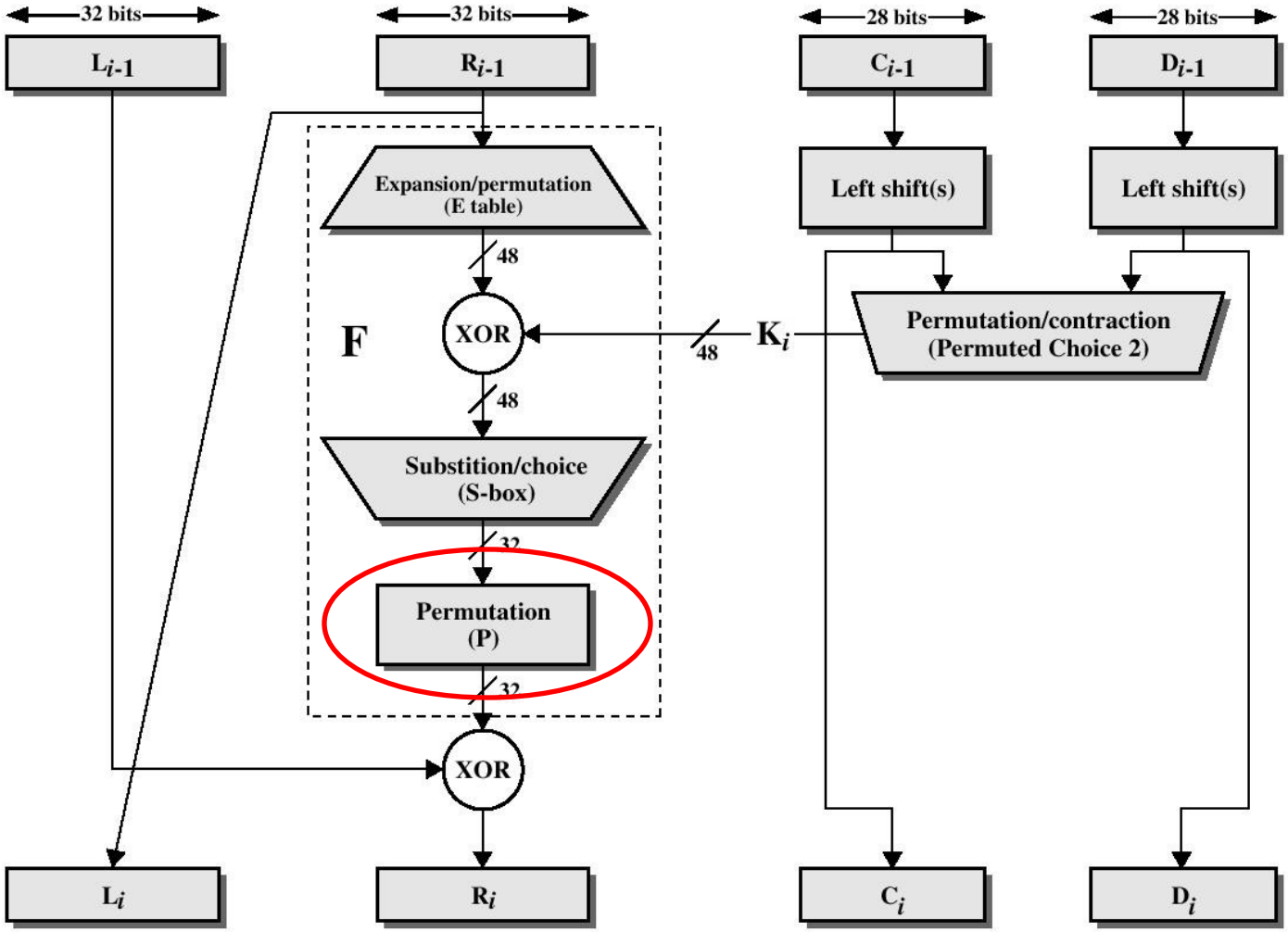


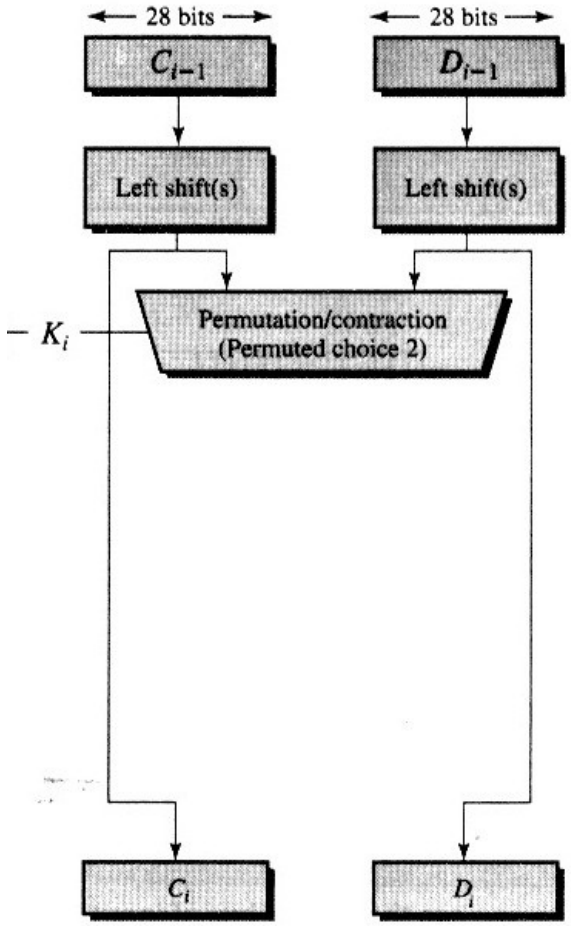
Figure 2.4 Single Round of DES Algorithm

DES – Função de Permutação

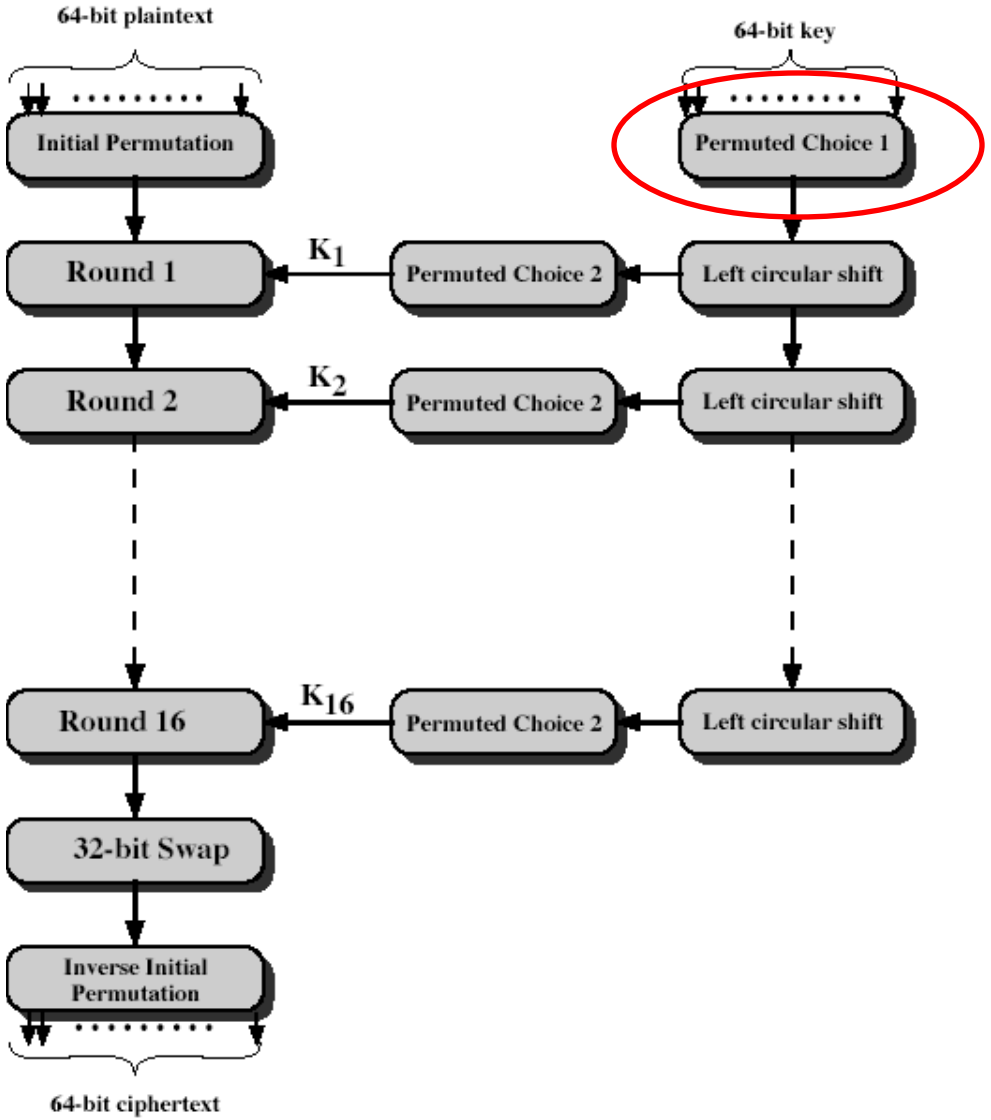
(d) Permutation Function (P)

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

DES – Geração de Subchaves



DES Ilustrado



DES – Escolha Permutada 1

(b) Permuted Choice One (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

DES – Geração de Subchaves

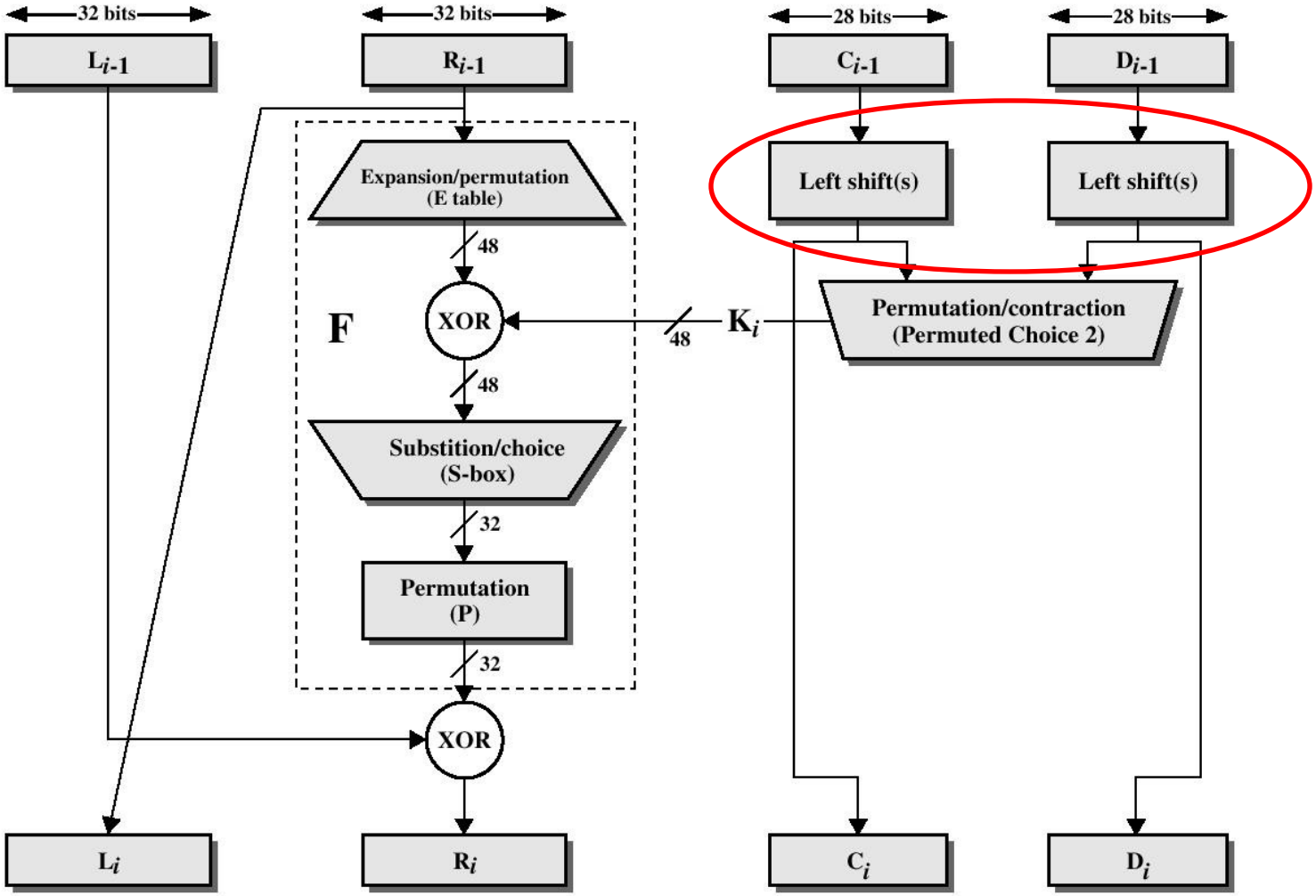


Figure 2.4 Single Round of DES Algorithm

DES – Tabela de Rotação a Esquerda

(d) Schedule of Left Shifts

Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

DES – Geração de Subchaves

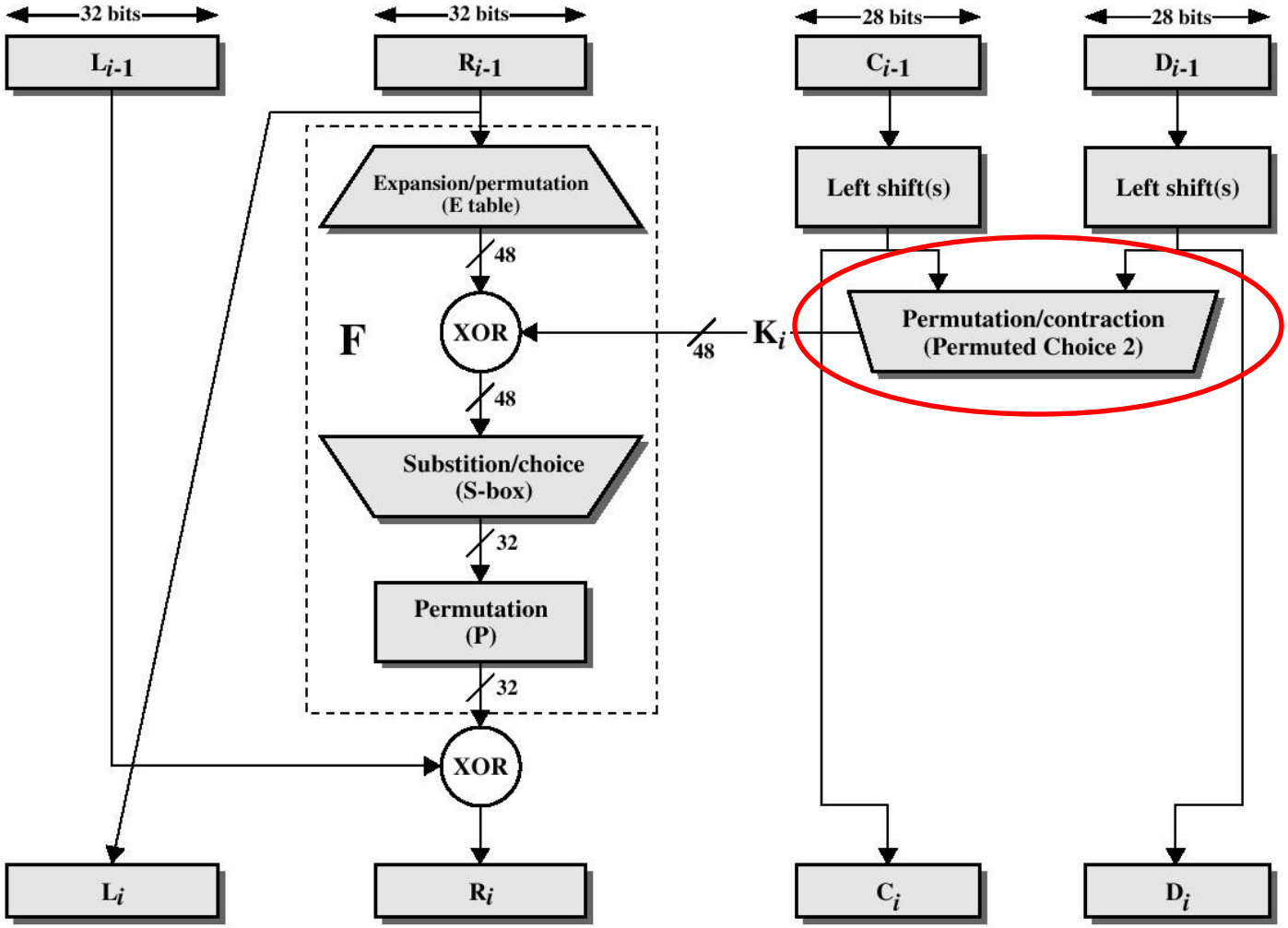


Figure 2.4 Single Round of DES Algorithm

DES – Escolha Permutada 2

(c) Permuted Choice Two (PC-2)

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

Efeito Avalanche no DES

Table 3.5 Avalanche Effect in DES

(a) Change in Plaintext		(b) Change in Key	
Round	**Number of bits that differ**	**Round**	**Number of bits that differ**
0	1	0	0
1	6	1	2
2	21	2	14
3	35	3	28
4	39	4	32
5	34	5	30
6	32	6	32
7	31	7	35
8	29	8	34
9	42	9	40
10	44	10	38
11	32	11	31
12	30	12	33
13	30	13	28
14	26	14	26
15	29	15	34
16	34	16	35

DES - Força Criptográfica

- $2^{56} = 7.2 \times 10^{16}$
- 1977 → US$ 20 Milhões = 10 horas
- 1998 → US$ 250mil = 70 horas
- Hoje → US$ 10mil = minutos
- Importante lembrar que é necessário conhecer a natureza do texto claro
- Não foram descobertas ate hoje falhas nas caixas S

Criptoanálise Diferencial

- Não foi discutido na literatura até 1990
- Ataque no DES por Biham e Shamir (1993)
  - Redução do espaço de busca para 2^{47}
- Factível em versões com menos rodadas
- Conhecida pela equipe do LUCIFER em 1974
- Baseado na diferença XOR de dois textos claros
- Probabilidade de bits em caixas S

Criptoanálise Linear

- Ataque baseado em aproximações lineares
  - Redução do espaço de busca para 2^{43}
- Ataque de texto claro escolhido
- Pode ser usado uma rodada de cada vez por ser linear
- Combina os resultados achados em várias rodadas

AES – Advance Encryption Standard

- Cifrador de bloco para substituir o DES
- Competição em 2001, Chamada em 1997
  - 21 algoritmos, 15 candidatos, 5 finalistas, Rijndael vencedor
- Suporte a 128, 192 e 256 bits
- Não usa Feistel, processa o bloco inteiro
- Rounds:
  - Substituição de bytes, permutação, operação sobre corpo finito, e XOR com a chave

AES – Critérios de Avaliação Inicial

- Segurança:
  - Esforço comprovado para ataque de criptoanálise
- Custo Computacional:
  - Eficiente em software e hardware. Links de alta velocidade
- Características do Algoritmo:
  - Flexibilidade, compatibilidade e simplicidade

AES – Critérios Intermediários

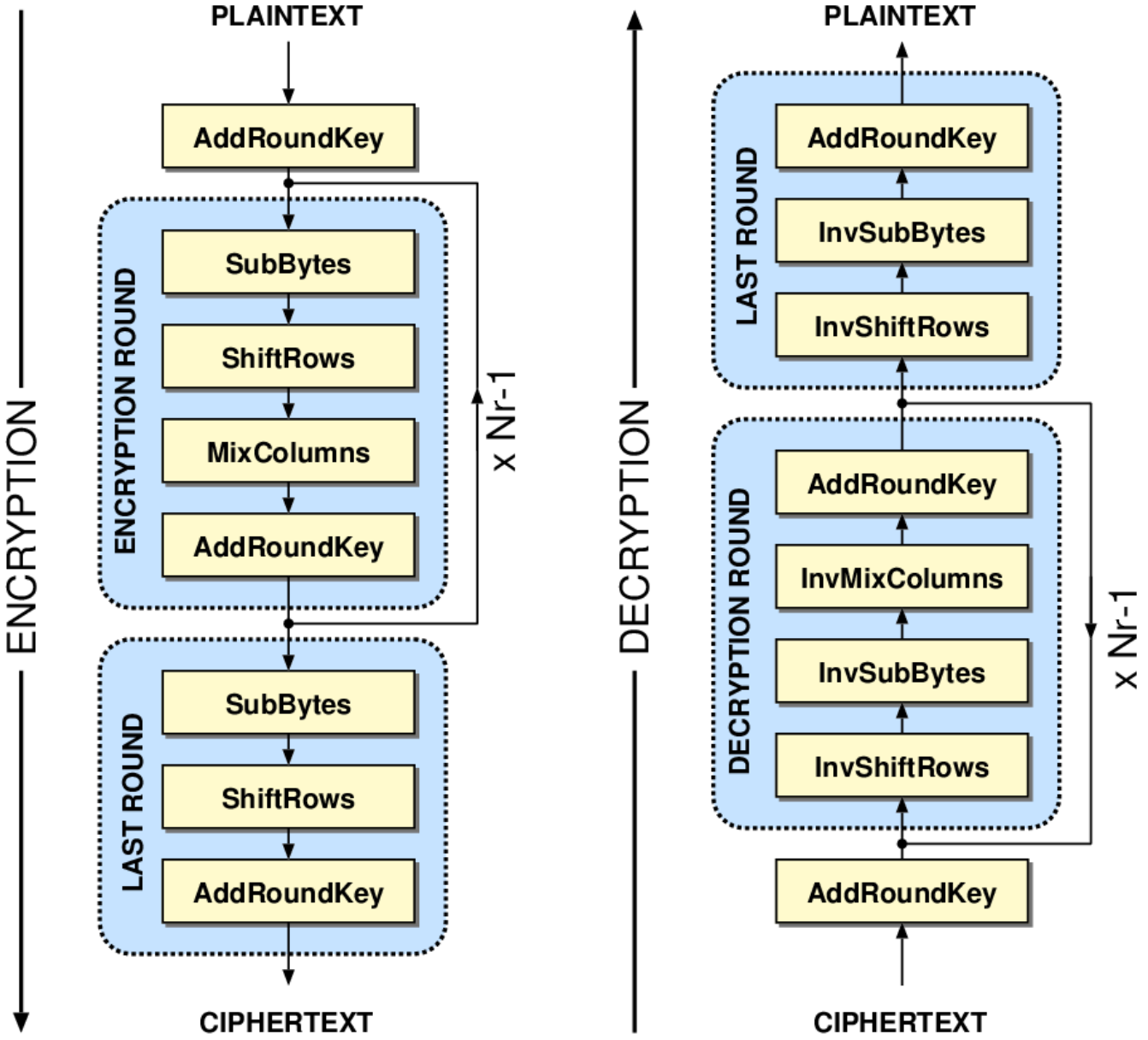
- Segurança verificada pela comunidade
- Implementação em Software
- Restrições de espaço e implementação em hardware
- Ataques nas implementações
- Cifragem x Decifragem
- Agilidade de chaves
- Paralelismo em nível de instrução

AES - Cifrador

- Tamanho de bloco sempre 128 bits
- Tamanho de Chave Variável (128,192,256)
- Rijndael
  - Resistência a ataques conhecidos
  - Velocidade e tamanho em variadas plataformas
  - Simplicidade

Key size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext block size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of rounds	10	12	14
Round key size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded key size (words/bytes)	44/176	52/208	60/240

AES – Cifragem e Decifragem

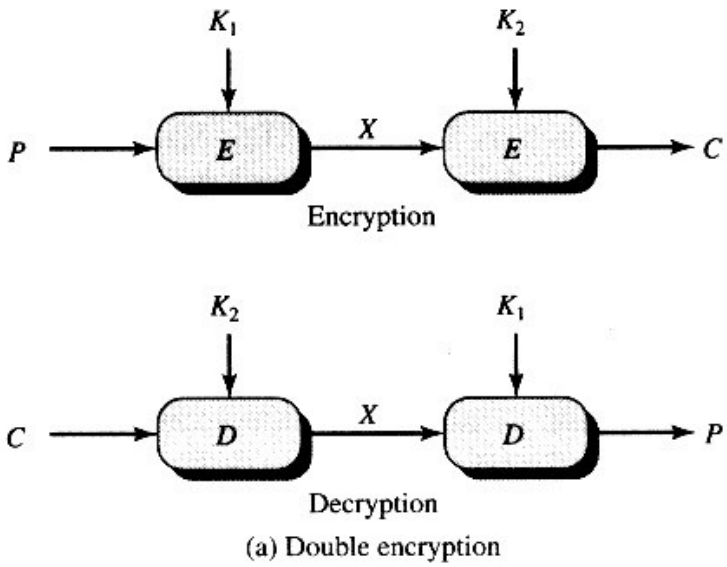


Cifragem Múltipla

- Aplicação do mesmo algoritmos múltiplas vezes com diferentes chaves
  - Objetivo: Aumentar o espaço de busca da chave
- Meet-in-the-Middle [DIFF77]
  - Ataque de texto claro conhecido
  - Quebra qualquer cifrador com dois pares de blocos

Double DES

- Aumento da chave para 112 bits
- Produz mapeamentos que não são diretamente deriváveis por 1 aplicação
- Meet-in-the-middle com esforço de 2^{56} , não muito maior do que 2^{55} requerido pelo DES



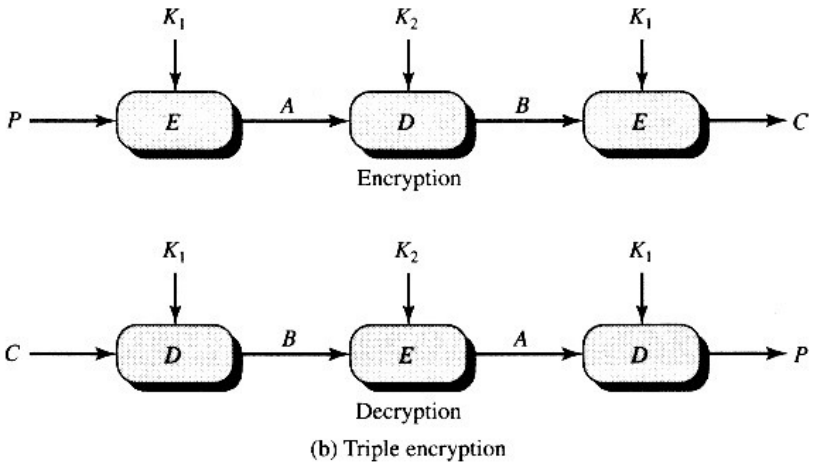
(a) Double encryption

Cifragem Múltipla

- Meet-in-the-Middle [DIFF77]
  - $C = E(K_2, E(K_1,P)) \rightarrow X = E(K_1,P) = D(K_2,C)$
  - Dois pares de P e C são conhecidos
  - Cifrar P com todas as possíveis chaves
  - Decifrar C com todas as possíveis chaves
  - Quando encontrar dois resultados iguais, testar as chaves para o outro par
  - Se os blocos coincidirem, então assume-se a chave como sendo verdadeira

Triple DES

- Chave de 112 ou 168 bits
- Evita Meet-in-the-middle
- Pode ser EDE, ou EEE. A decifragem não muda nada criptograficamente



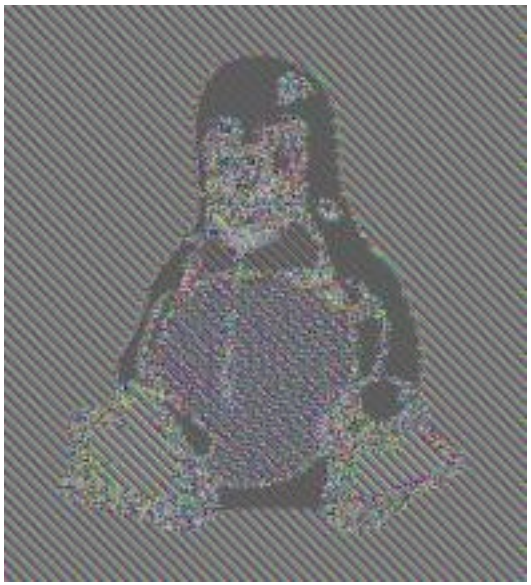
(b) Triple encryption

Modos de Operação

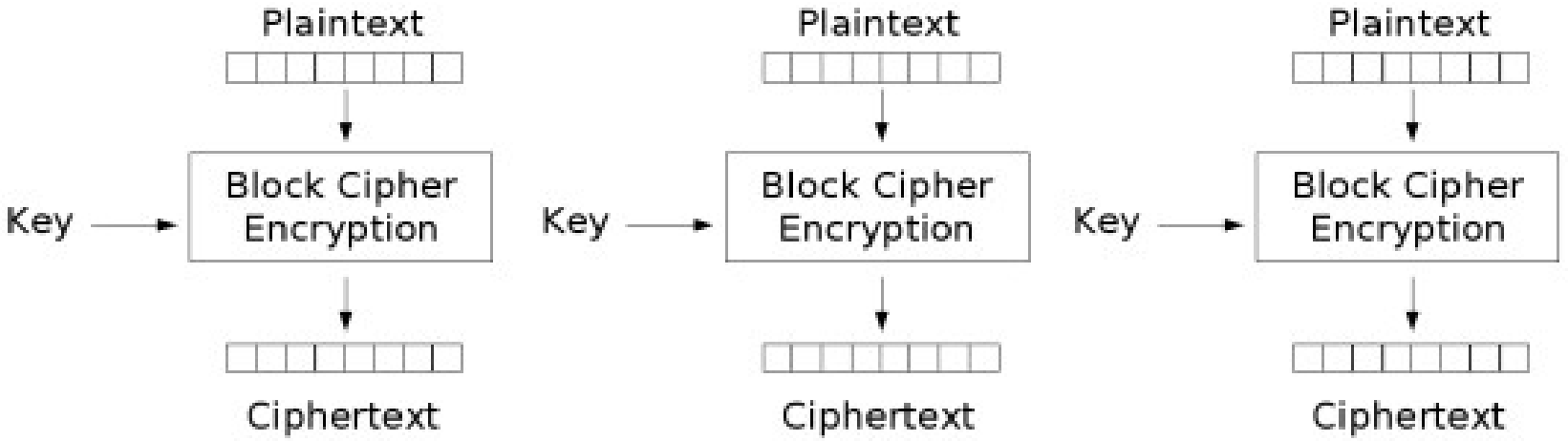
- Electronic Codebook - ECB
- Cipher Block Chaining - CBC
- Cipher Feedback - CFB
- Output Feedback - OFB
- Counter Mode - CTR

Electronic Codebook - ECB

- Cada bloco é codificado de forma independente
- Segurança para transmissão de dados únicos e pequenos
- (senhas)



ECB

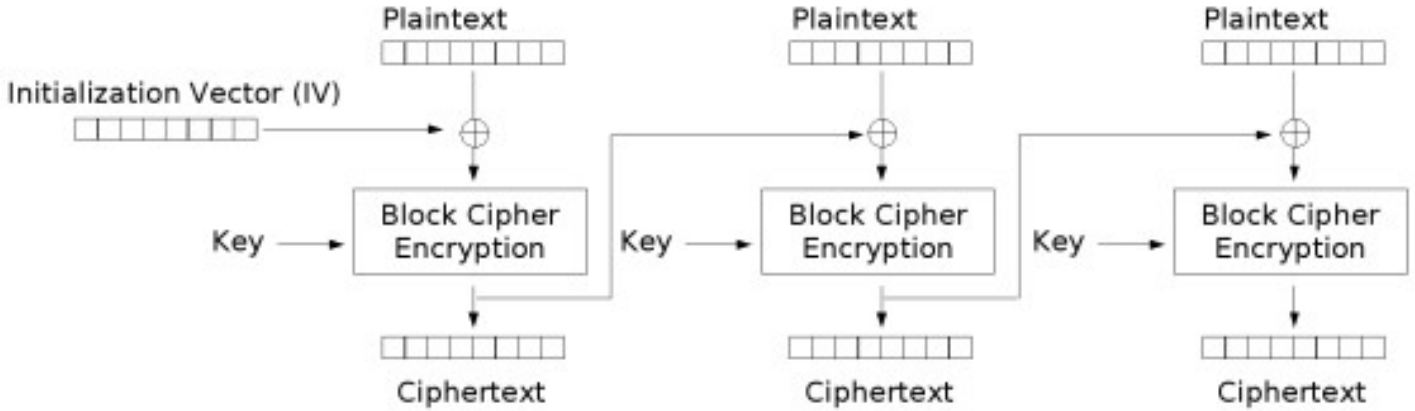


Electronic Codebook (ECB) mode encryption

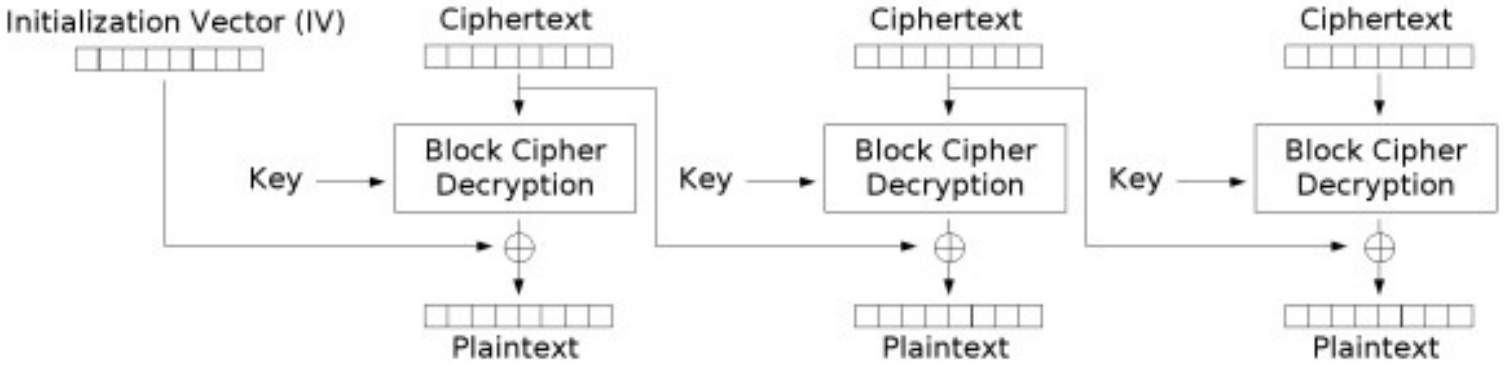
Cipher Block Chaining - CBC

- A entrada é XOR do próximo bloco de texto claro e o bloco anterior cifrado
- Uso pra transmissão de dados gerais e autenticação
- Decifragem paralelizável

CBC



Cipher Block Chaining (CBC) mode encryption

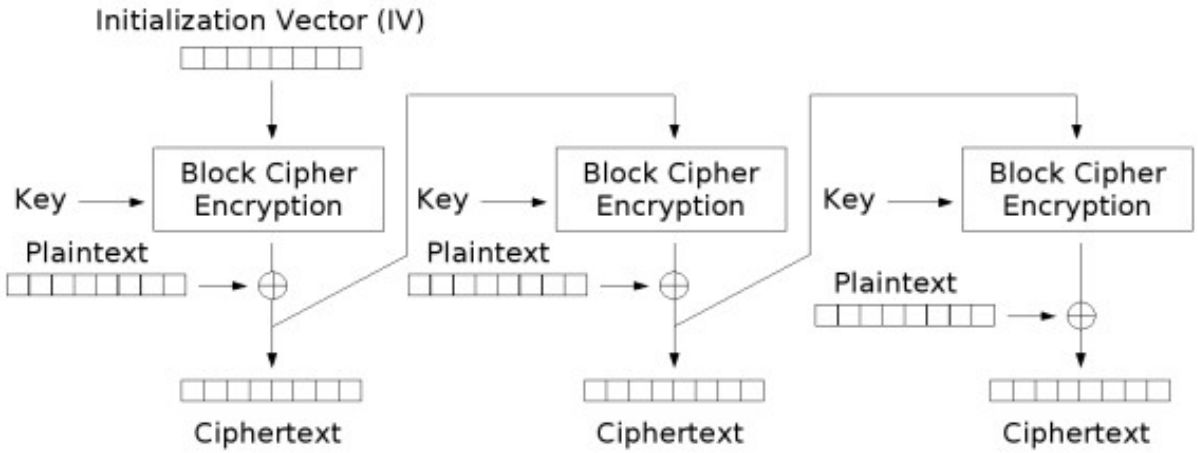


Cipher Block Chaining (CBC) mode decryption

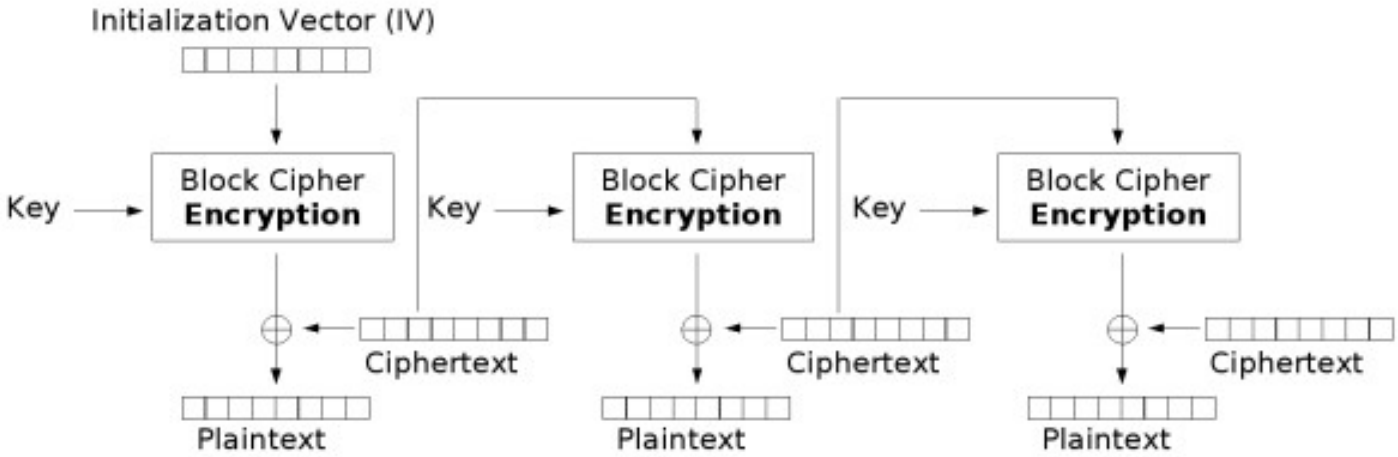
Cipher Feedback - CFB

- O texto cifrado é XOR com o texto claro e retroalimentado no cifrador
- Transforma um cifrador de bloco em uma espécie de cifrador de fluxo
- Uso pra transmissão de dados gerais em **streaming** e autenticação
- Retroalimentação depois do XOR
- Decifragem paralelizável

CFB



Cipher Feedback (CFB) mode encryption

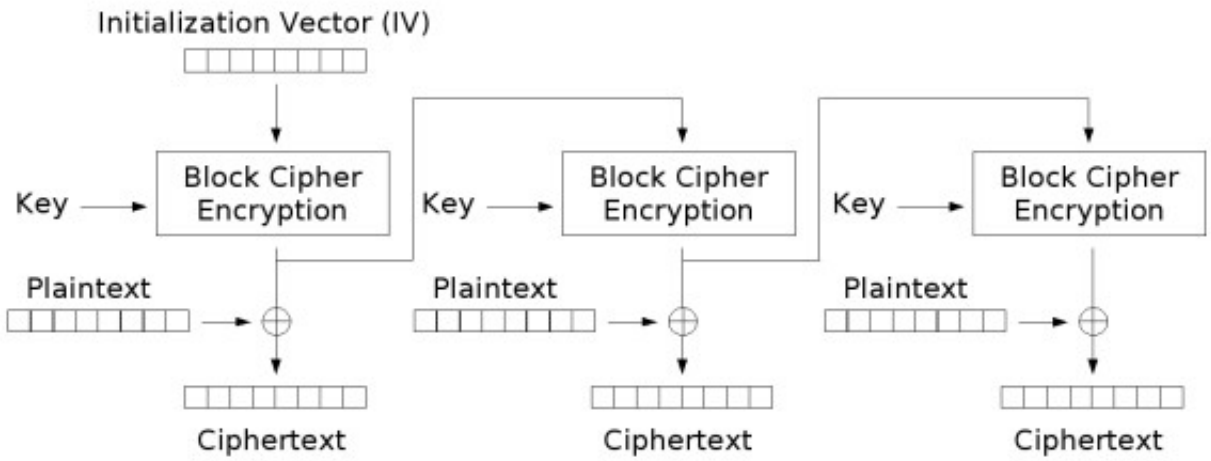


Cipher Feedback (CFB) mode decryption

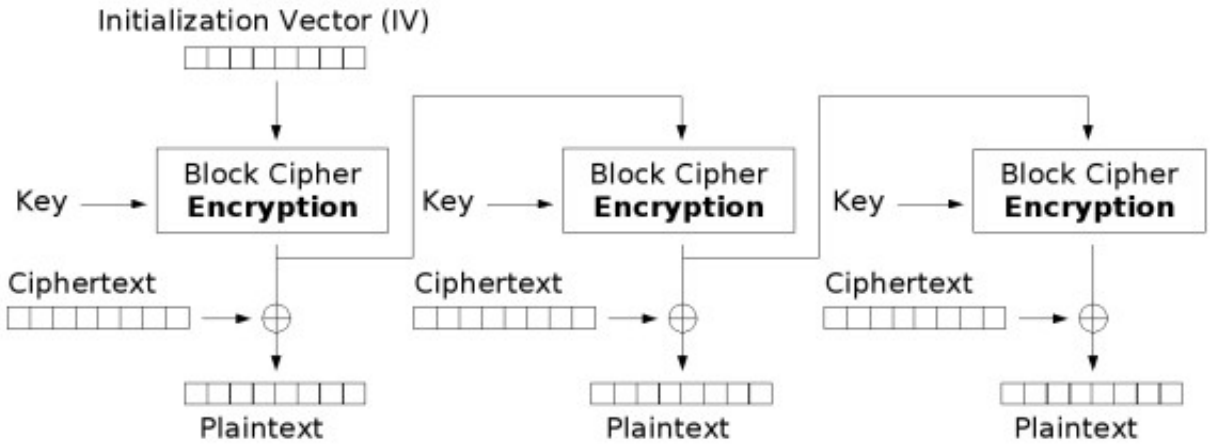
Output Feedback - OFB

- Similar a CFB. A saída do cifrador é retroalimentada para gerar um stream de bits
- Usado em canais ruidosos
- Retroalimentação antes do XOR
- Nem cifragem nem decifragem são paralelizáveis

OFB



Output Feedback (OFB) mode encryption

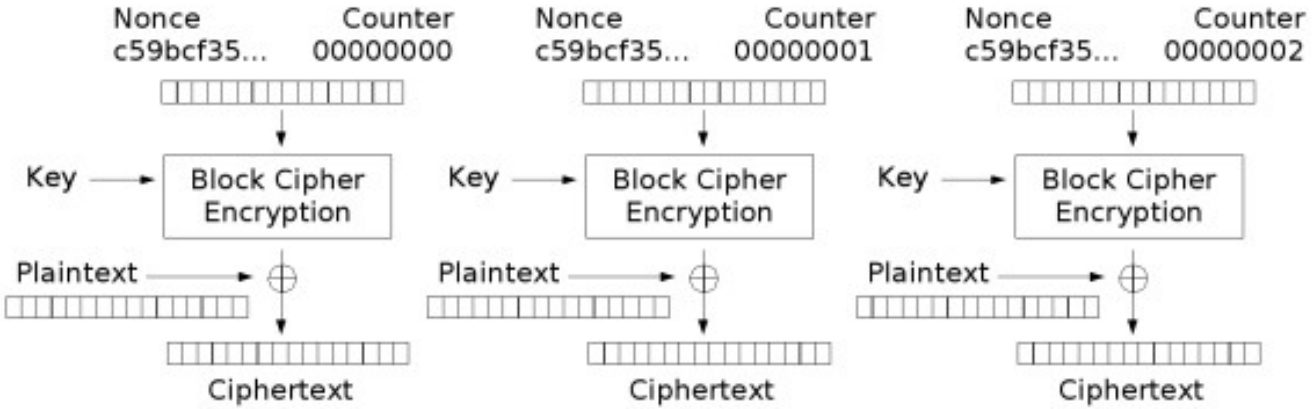


Output Feedback (OFB) mode decryption

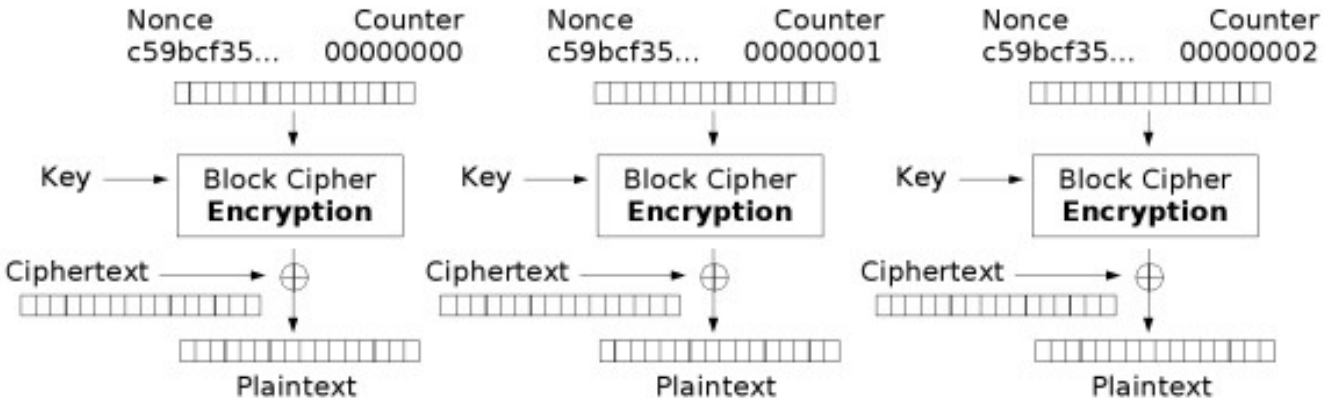
Counter Mode - CTR

- Cada bloco é XORed com um contador cifrado
- Uso geral em transmissão de dados e em links de alta velocidade
- Cifragem e deifragem paralelizáveis

CTR



Counter (CTR) mode encryption



Counter (CTR) mode decryption