Capítulo 4

Criptografia Convencional

Algoritmo Blowfish

Blowfish

Desenvolvido por: Bruce Schneier, 1993

Características:
- **Rápido**: (cpu 32 bits) 18 ciclos de relógio por byte
- **Compacto**: < 5K bytes de memória
- **Simples**
- **Segurança variável**: 32 ≤ Chave ≤ 448
- **Tamanho do bloco**: 64 bits

Subchaves e Caixas S

- Inicializar **P** e as caixas **S** com parte fracionária de π
  - P1 = 243F6A88
  - P2 = 85A308D3
  - ...
  - S4,254 = 578FDFE3
  - S4,255 = 3AC372E6

$P_1, P_2, \ldots, P_{18}$

$S_{1,0}, S_{1,1}, \ldots, S_{1,255}$
$S_{2,0}, S_{2,1}, \ldots, S_{2,255}$
$S_{3,0}, S_{3,1}, \ldots, S_{3,255}$
$S_{4,0}, S_{4,1}, \ldots, S_{4,255}$

- $P \oplus K$
  - $P_1 = P_1 \oplus K_1, P_2 = P_2 \oplus K_2, \ldots, P_{14} = P_{14} \oplus K_{14}, P_{15} = P_{15} \oplus K_1, \ldots, P_{18} = P_{18} \oplus K_4$

$K_1, K_2, \ldots, K_j \quad 1 \leq j \leq 14$

Subchaves e Caixas S

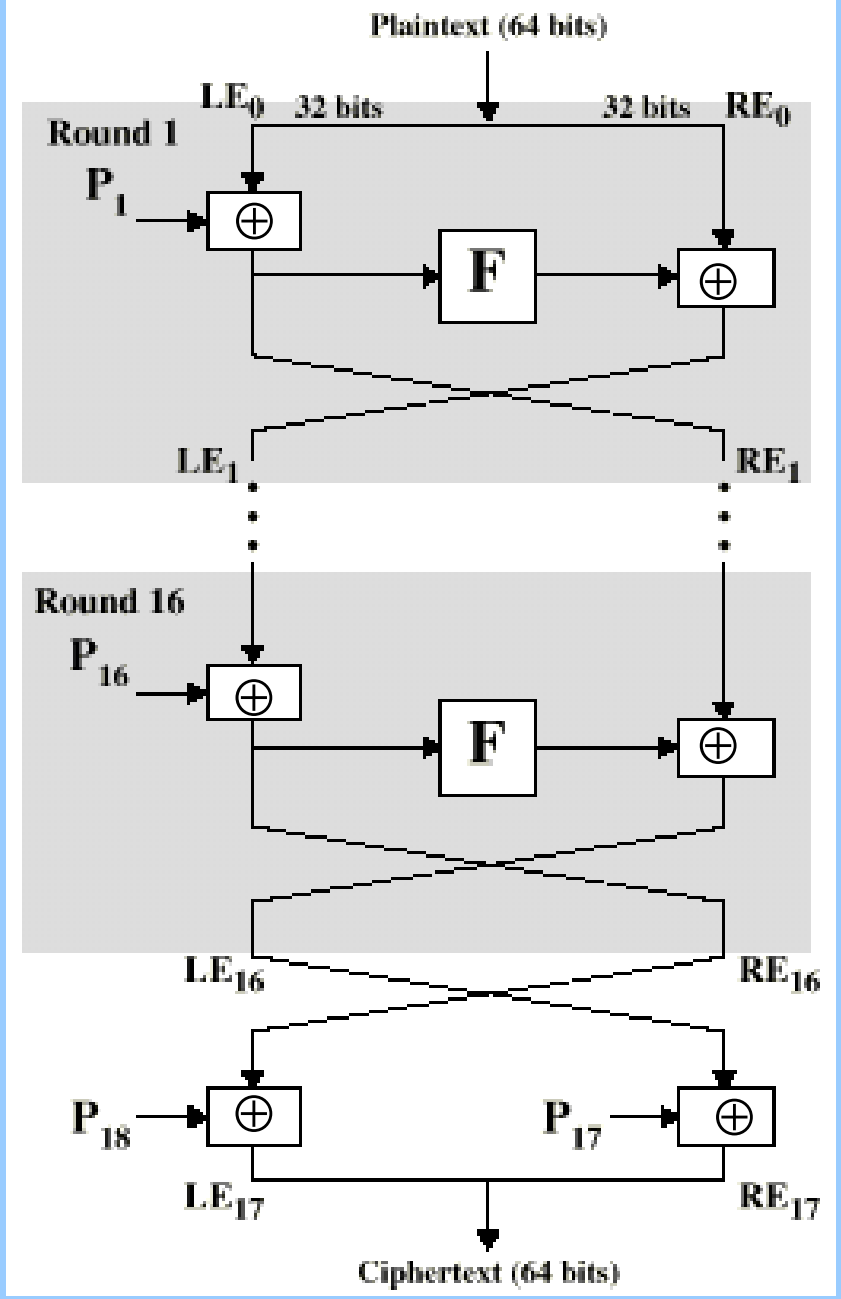
- 521 execuções de E
- > 4 Kbytes de Memória

$$P_1, P_2 = E_{P,S}[0]$$
$$P_3, P_4 = E_{P,S}[P_1 \| P_2]$$
$$\ldots$$
$$P_{17}, P_{18} = E_{P,S}[P_{15} \| P_{16}]$$
$$S_{1,0}, S_{1,1} = E_{P,S}[P_{17} \| P_{18}]$$
$$\ldots$$
$$S_{4,254}, S_{4,255} = E_{P,S}[S_{4,252} \| S_{4,253}]$$

Cifrar

Operações Primitivas:
Adição: + (mod 2^{32})
XOR: $\oplus$

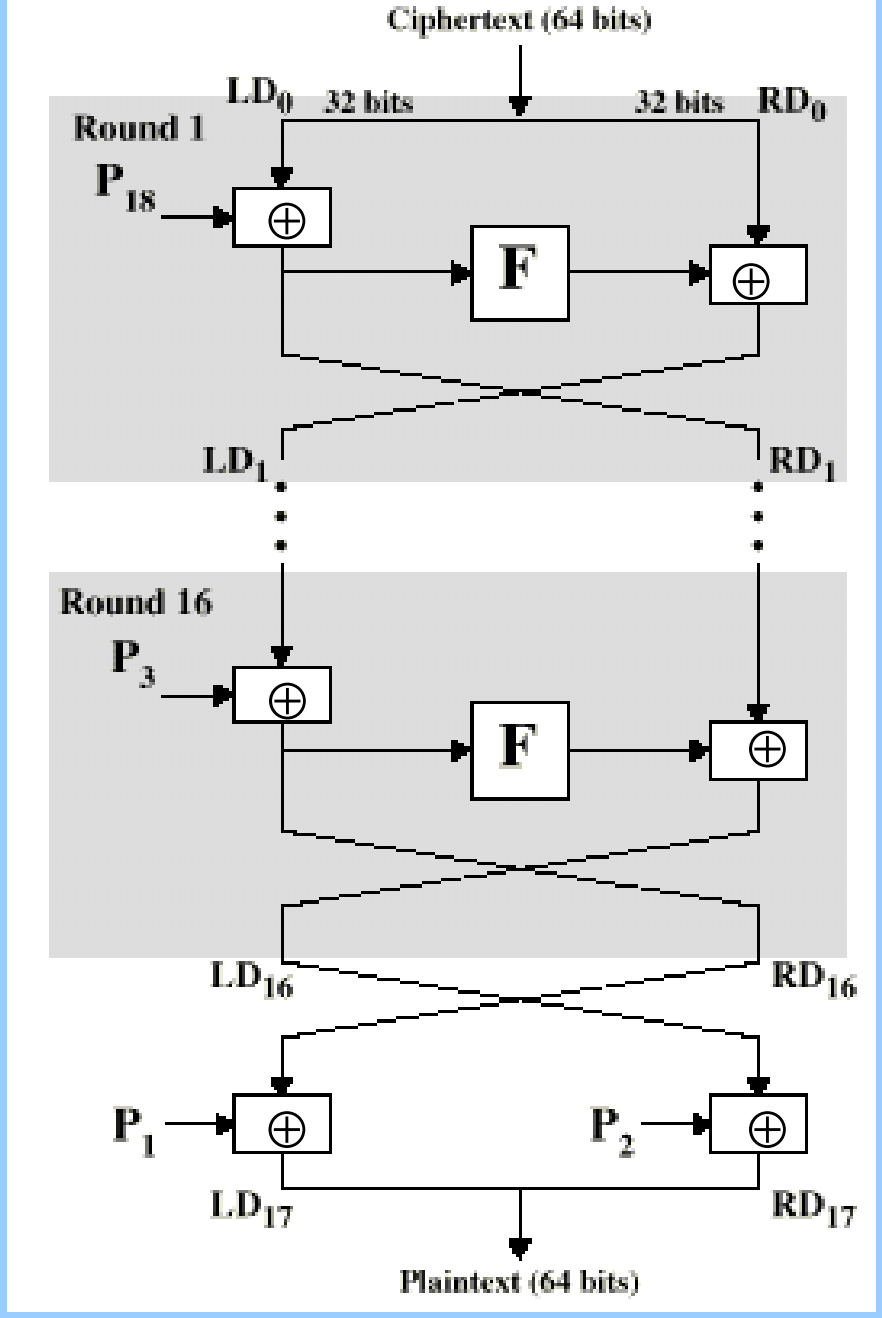
Pseudocódigo:
Para i=1 até 16 Faça
$RE_i = LE_{i-1} \oplus P_i$
$LE_i = F[RE_i] \oplus RE_{i-1}$
Fim Para
$LE_{17} = RE_{16} \oplus P_{18}$
$RE_{17} = LE_{16} \oplus P_{17}$



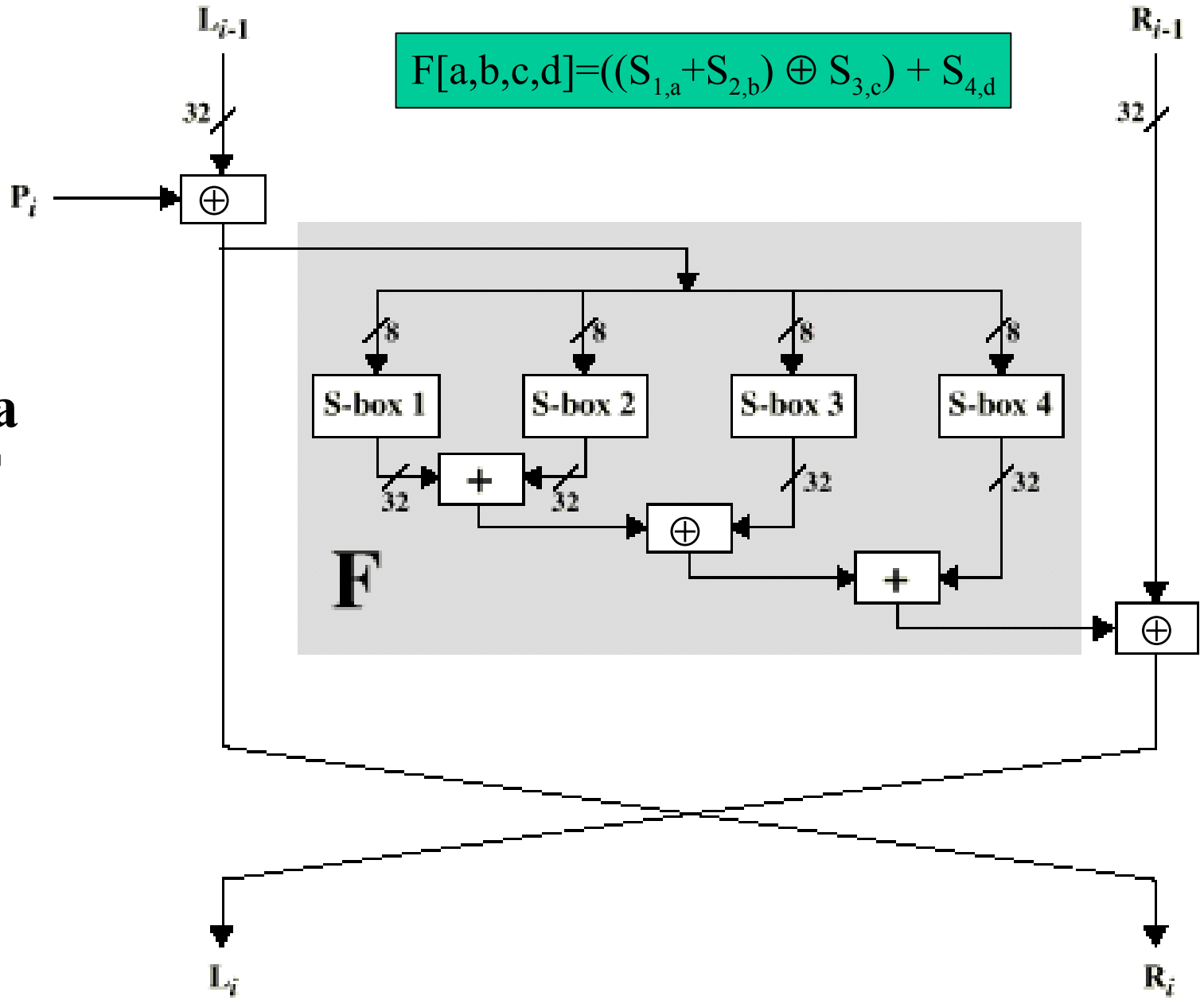
Decifrar

Operações Primitivas:
Adição: + (mod 2^{32})
XOR: $\oplus$

Pseudocódigo:
Para i=1 até 16 Faça
$RD_i = LD_{i-1} \oplus P_{19-i}$
$LD_i = F[RD_i] \oplus RD_{i-1}$
Fim Para
$LD_{17} = RD_{16} \oplus P_1$
$RD_{17} = LD_{16} \oplus P_2$



Detalhe da Função F



Comparação de Velocidade

Algoritmo	Ciclos de Clock por Rodada	# de Rodadas	# de ciclos de clock por byte encriptado
Blowfish	9	16	18
RC5	12	16	23
DES	18	16	45
IDEA	50	8	50
3DES	18	48	108

Aula Prática

- Usar o OpenSSL para mostrar o Blowfish