Algoritmos simétricos

Palavras chave

- Fluxo;
- Bloco;
- Hexadecimal;
- Binário.

Caracter	Binário
Espaço	0010 0000
!	0010 0001
"	0010 0010
#	0010 0011
$	0010 0100
%	0010 0101
&	0010 0110
'	0010 0111
(	0010 1000
)	0010 1001
*	0010 1010
+	0010 1011
,	0010 1100
-	0010 1101
.	0010 1110
/	0010 FFFF
0	0011 0000
1	0011 0001
2	0011 0010
3	0011 0011
4	0011 0100
5	0011 0101
6	0011 0110
7	0011 0111

Caracter	Binário
8	0011 1000
9	0011 1001
:	0011 1010
;	0011 1011
<	0011 1100
=	0011 1101
>	0011 1110
?	0011 1111
@	0100 0000
A	0100 0001
B	0100 0010
C	0100 0011
D	0100 0100
E	0100 0101
F	0100 0110
G	0100 0111
H	0100 1000
I	0100 1001
J	0100 1010
K	0100 1011
L	0100 1100
M	0100 1101
N	0100 1110
O	0100 1111

Caracter	Binário
P	0101 0000
Q	0101 0001
R	0101 0010
S	0101 0011
T	0101 0100
U	0101 0101
V	0101 0110
W	0101 0111
X	0101 1000
Y	0101 1001
Z	0101 1010
[	0101 1011
\	0101 1100
]	0101 1101
^	0101 1110
_	0101 1111
`	0110 0000
a	0110 0001
b	0110 0010
c	0110 0011
d	0110 0100
e	0110 0101
f	0110 0110
g	0110 0111

Caracter	Binário
h	0110 1000
i	0110 1001
j	0110 1010
k	0110 1011
l	0110 1100
m	0110 1101
n	0110 1110
o	0110 1111
p	0111 0000
q	0111 0001
r	0111 0010
s	0111 0011
t	0111 0100
u	0111 0101
v	0111 0110
w	0111 0111
x	0111 1000
y	0111 1001
z	0111 1010
{	0111 1011
|	0111 1100
}	0111 1101
~	0111 1110
DELETE	0111 1111

Tabela hexadecimal

Decimal	Hexadecimal	Binário
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Fluxo

- O texto original é transformado num fluxo de valores hexadecimais.
- Por exemplo: Brasil
- B: 0100 0010 : 42
- r: 0111 0010: 72
- a: 0110 0001: 61
- s: 0111 0011: 73
- i: 0110 1001: 69
- l: 0110 1100: 6E
- Fluxo binário: 0100 0010 0111 0010 0110 0001 0111 0011 0110 1001 0110 1100
- Fluxo hexadecimal: 42 72 61 73 69 6E

Cifra de blocos

- O texto é separado em blocos de tamanho único;
- 0100 0010 0111 0010 0110 0001 0111 0011 0110 1001 0110 1100
- 48 bits
- Mas se eu quiser blocos de 7 bits?
- E se quiser blocos de 47 bits?

Segredo

- Segredos geralmente possuem um tamanho fixo;
- Uma quebra por tentativa e erro envolve 2^n possibilidades;
- Uma chave de 56 bits exigiria 2^{56} tentativas.

Uso do operador XOR

A	B	Y
0	0	0
0	1	1
1	0	1
1	1	0

One time pad

Texto plano: Brasil

Segredo: ABA

0100 0010 0111 0010 0110 0001 0111 0011 0110 1001 0110 1100

0100 0001 0100 0010 0100 0001 0100 0001 0100 0010 0100 0001

0000 0011 0011 0000 0010 0000 0011 0000 0010 1011 0010 1101

Operações lógicas

- Expressões:
  - (A and B) or not (C xor D)
  - A=1. B=0, C=1, D=0
  - (1 and 0) or not (1 xor 0)
  - 0 or not(1)
  - 0 or 0 = 0

Operações lógicas

- Deslocamento: 1100 com shift esquerda : 1001
- Somas;
- Subtrações;
- XOR;

DES

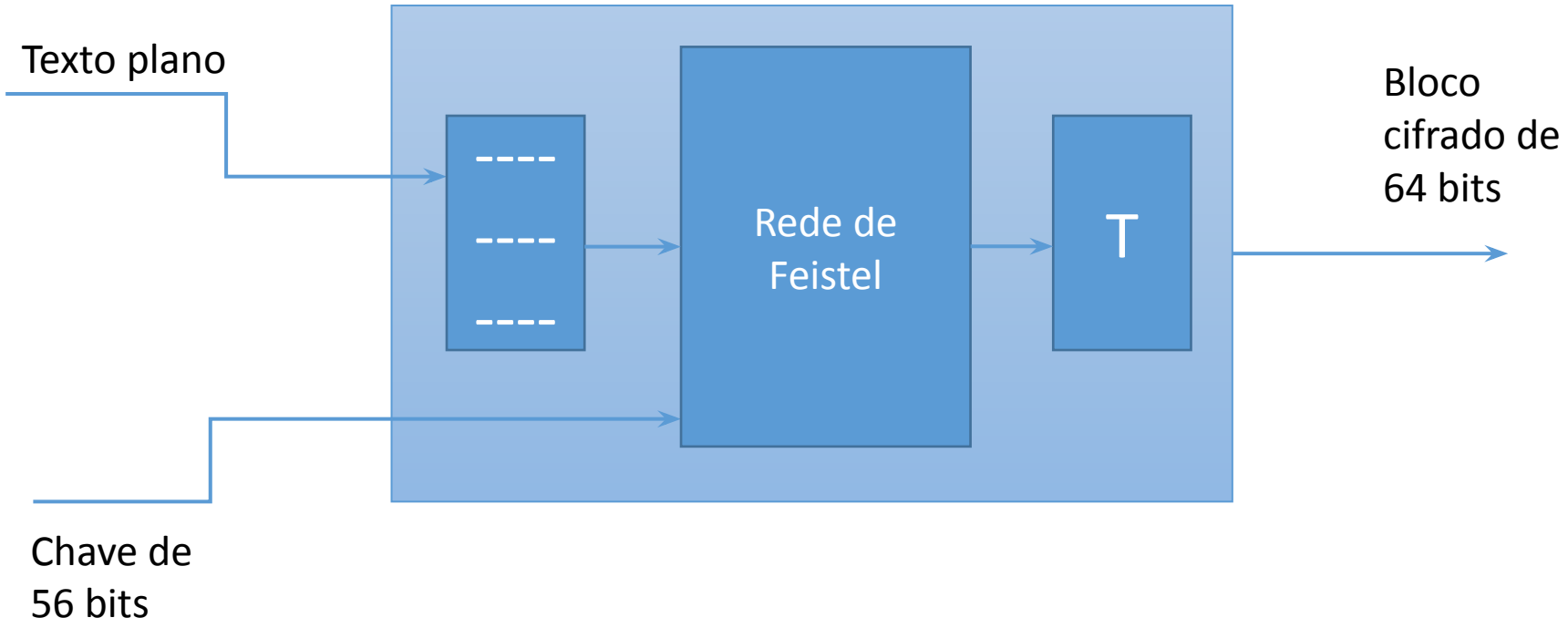
Histórico

- Princípios de Difusão e confusão (Shannon)
- Algoritmo Lucifer, de Horst Feistel, nos anos 70 usava chave de 128 bits e blocos de 128 bits.
- Data Encryption Standard surge em 1975;
- IBM e NSA tornam o DES como padrão em 1976. Bloco de 64 bits e chave de 56 bits.

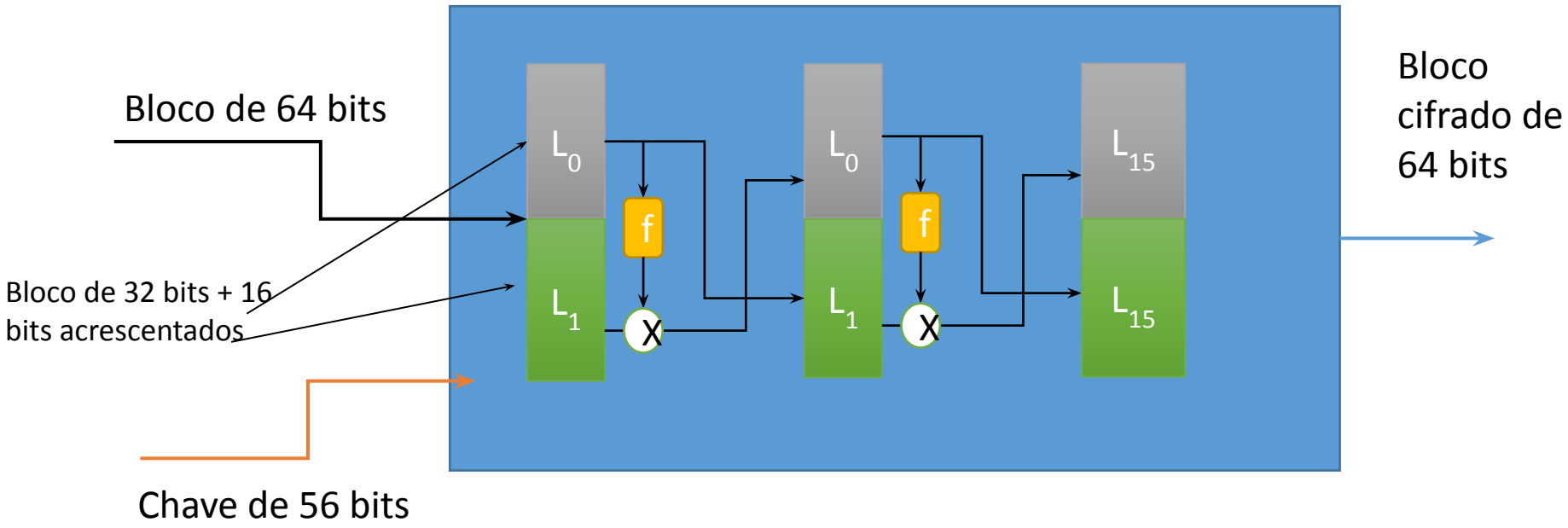
Descrição básica

- Uma substituição fixa, chamada de permutação inicial, de 64 bits em 64 bits;
- Uma transformação, que depende de uma chave de 48 bits, e que preserva a metade direita;
- Uma troca das duas metades de 32 bits cada uma;
- Repetem-se os passos 2 e 3 durante 16 vezes;
- Inversão da permutação inicial.

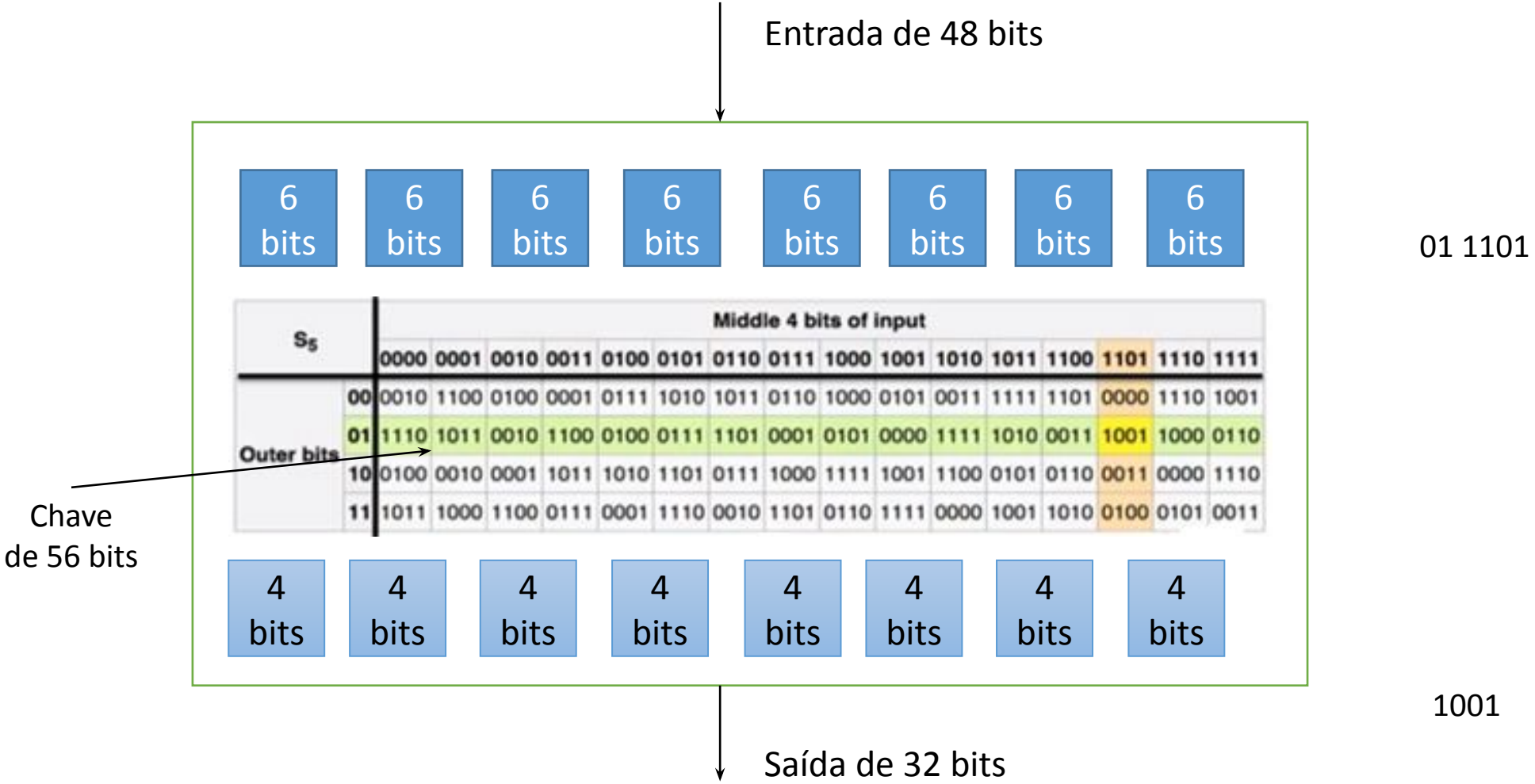
Modelo


Texto plano
Rede de Feistel
T
Bloco cifrado de 64 bits
Chave de 56 bits

Rede de Feistel



Transformação (Sand Box)



S_5	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
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

Caraterísticas

- Nunca foi quebrado;
- Obtém-se resultado somente por tentativa e erro;
- Chave de 56 bits é quebrada em tempo aceitável quando se usa uma Render Farm;
- 3DES repete o DES três vezes;

Render farm

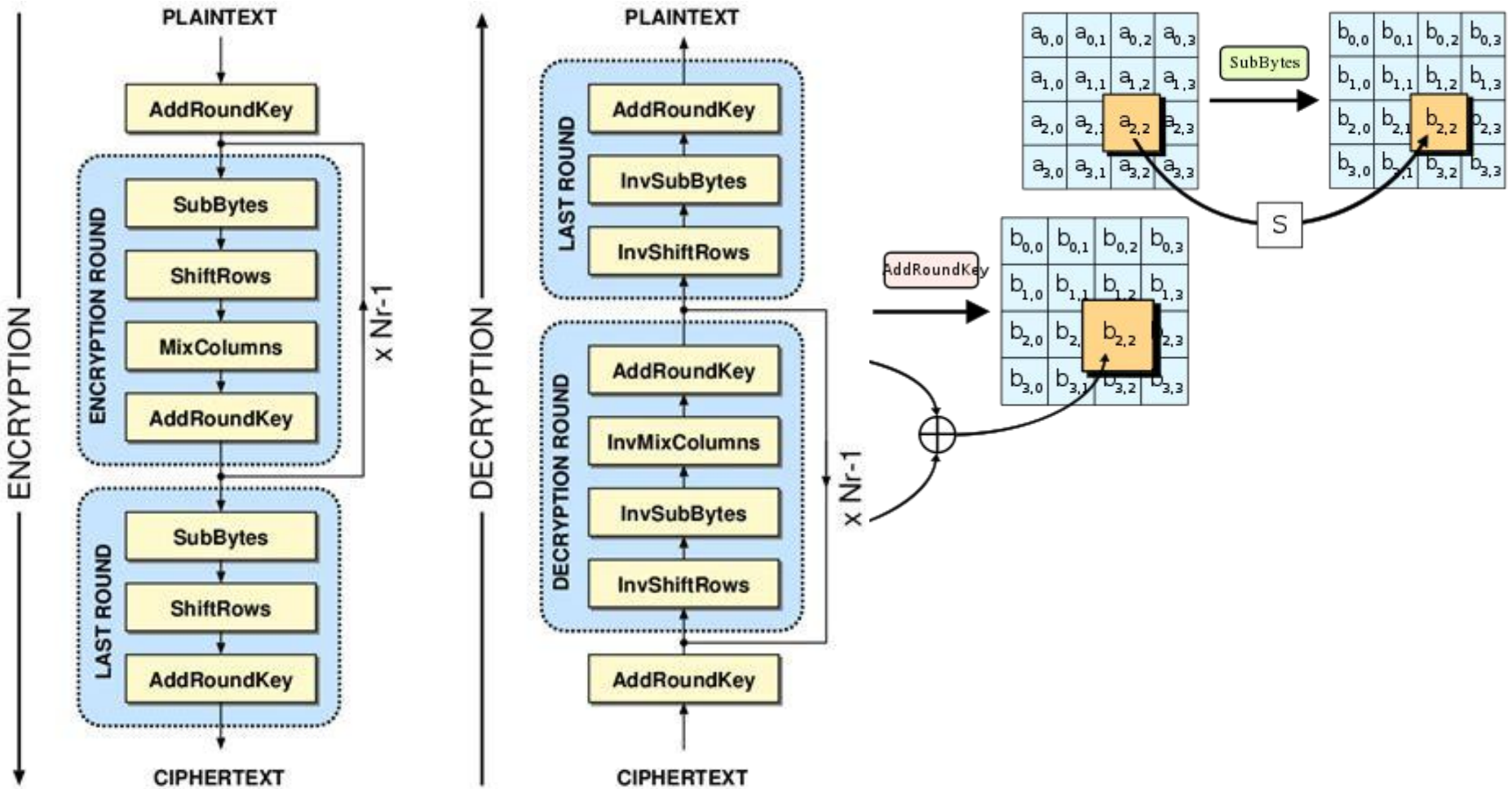
AES

Advanced Encryption Standard

Características

- Surgiu da necessidade de substituir o DES;
- Foi feito concurso pelo NIST em 2001;
- Permite trabalhar com vários cenários:
  - Processamento, memória, comunicação, armazenamento;
- Utiliza matrizes para embaralhamento;

Algoritmo


ENCRYPTION
PLAINTEXT
AddRoundKey
ENCRYPTION ROUND
SubBytes
ShiftRows
MixColumns
AddRoundKey
x Nr-1
LAST ROUND
SubBytes
ShiftRows
AddRoundKey
CIPHERTEXT
DECRYPTION
PLAINTEXT
LAST ROUND
AddRoundKey
InvSubBytes
InvShiftRows
DECRYPTION ROUND
AddRoundKey
InvMixColumns
InvSubBytes
InvShiftRows
x Nr-1
AddRoundKey
CIPHERTEXT
SubBytes
S
AddRoundKey

Modos de cifragem

- ECB: dividida em blocos
- CBC: utiliza XOR no bloco posterior
- CFB: se parece com cifra de fluxo. Usada em stream;