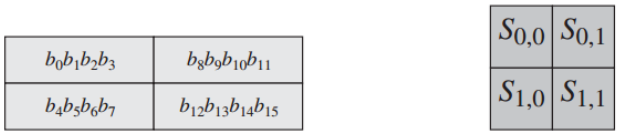
Atividade 1 – Cifrar com o AES Simplificado

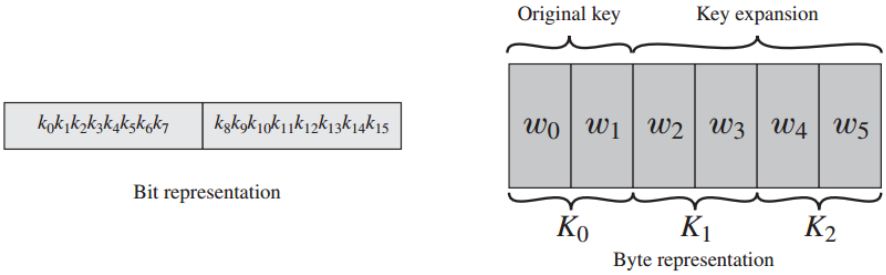
Modo	Chave	Entrada	Saída
Cifração	00101101 01010101	10100111 01001001	?

Estrutura geral dos dados

State – matriz que recebe o entrada do algoritmo
Key – seqüência de chave e sub-chaves geradas
Nibble – seqüência de 4 bits
W – word – seqüência de 8 bits



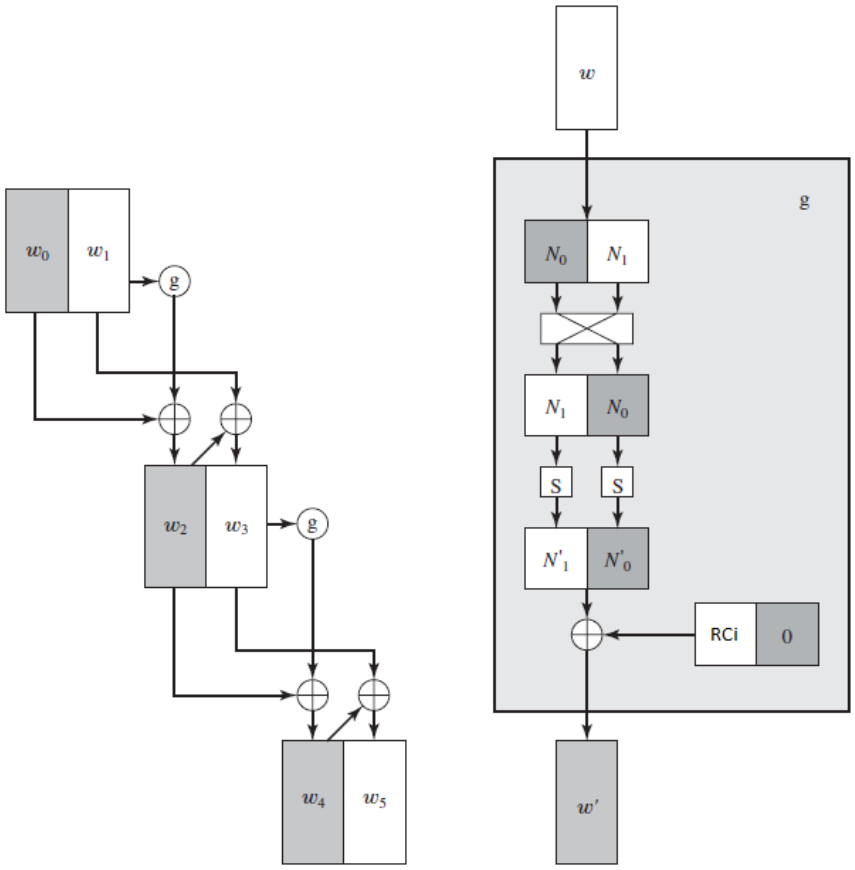
(a) State matrix



(b) Key

Geração de sub-chaves

i = número da rodada
RC1 = 1000
RC2 = 0011



(a) Overall algorithm (b) Function g

Substituição nas caixas S feita da seguinte forma:

- 2 primeiros bits = linha
- 2 últimos bits = coluna

Valores da caixa estão definidos em hexa-decimal.

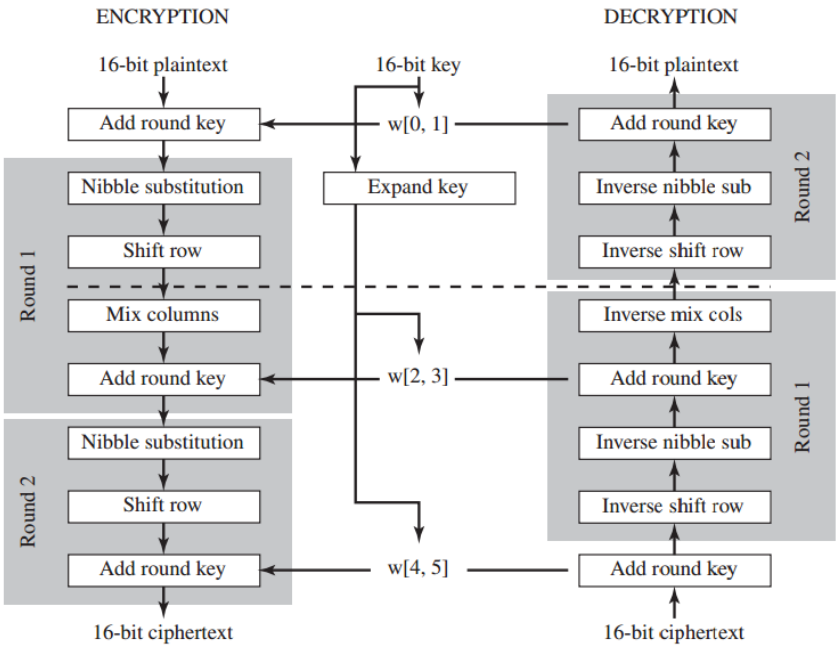
		j			
		00	**01**	**10**	**11**
i	**00**	9	4	A	B
	01	D	1	8	5
	10	6	2	0	3
	11	C	E	F	7

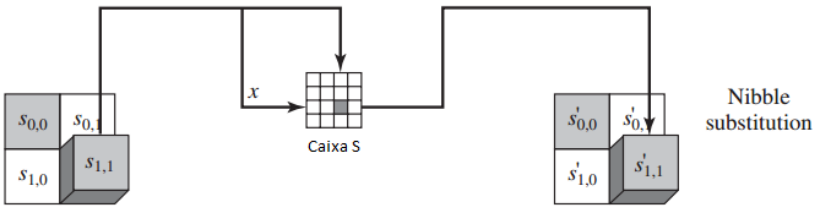
(a) S-Box

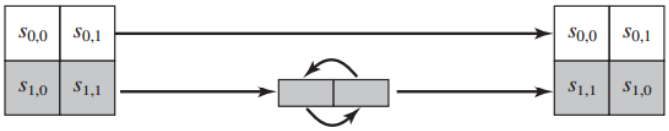
		j			
		00	**01**	**10**	**11**
i	**00**	A	5	9	B
	01	1	7	8	F
	10	6	0	2	3
	11	C	4	D	E

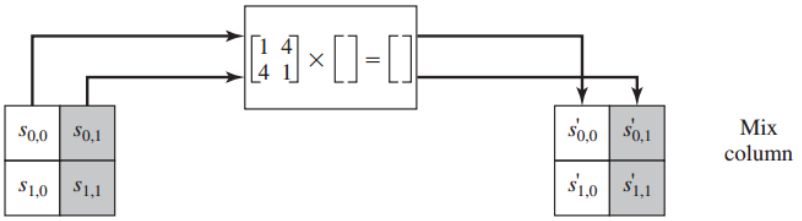
(b) Inverse S-Box

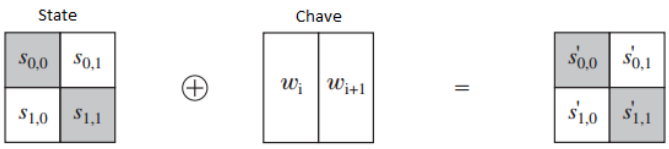
Cifrador


ENCRYPTION
DECRYPTION
16-bit plaintext
16-bit key
16-bit plaintext
Add round key
w[0, 1]
Add round key
Nibble substitution
Expand key
Inverse nibble sub
Round 2
Shift row
Inverse shift row
Round 1
Mix columns
Inverse mix cols
Add round key
w[2, 3]
Add round key
Nibble substitution
Inverse nibble sub
Round 1
Round 2
Shift row
Inverse shift row
Add round key
w[4, 5]
Add round key
16-bit ciphertext
16-bit ciphertext


x
Caixa S
Nibble substitution


Shift row


Mix column


State
Chave
Add key

Nibble Substitution

Substituição nas caixas S feita da seguinte forma:

- 2 primeiros bits = linha
- 2 últimos bits = coluna

Valores da caixa estão definidos em hexa-decimal.

		j			
		00	**01**	**10**	**11**
i	**00**	9	4	A	B
	01	D	1	8	5
	10	6	2	0	3
	11	C	E	F	7

(a) S-Box

		j			
		00	**01**	**10**	**11**
i	**00**	A	5	9	B
	01	1	7	8	F
	10	6	0	2	3
	11	C	4	D	E

(b) Inverse S-Box

Mix Column

Operações de multiplicação de polinômio operadas sob o corpo finito GP(2^4), com polinômio irredutível $x^4 + x + 1$.

$$\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} \\ s_{1,0} & s_{1,1} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} \\ s'_{1,0} & s'_{1,1} \end{bmatrix}$$

$$S'_{0,0} = S_{0,0} \oplus (4 \bullet S_{1,0})$$
$$S'_{1,0} = (4 \bullet S_{0,0}) \oplus S_{1,0}$$
$$S'_{0,1} = S_{0,1} \oplus (4 \bullet S_{1,1})$$
$$S'_{1,1} = (4 \bullet S_{0,1}) \oplus S_{1,1}$$