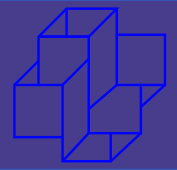


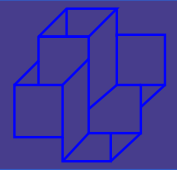
O algoritmo AES: Apresentação e Descrição da Estrutura

Raquel de Araújo

Fábio Borges

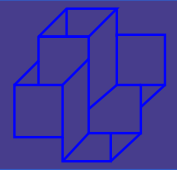
Gerson Nunes

História do Algoritmo



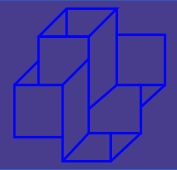
- Em 1997, o NIST *(National Institute of Standards and Technology)*, órgão dos EUA, lançou um concurso para adotar um novo algoritmo de criptografia simétrica para proteger informações confidenciais.
- O novo algoritmo, que passaria a se chamar AES *(Advanced Encryption Standard)*, substituiria o DES *(Data Encryption Standard)*.

História do Algoritmo



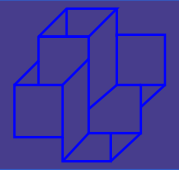
- O novo algoritmo deveria ter pré-requisitos como:
  - Não possuir patentes;
  - Cifrar em blocos de 128 bits com chaves de 128, 192 ou 256 bits;
  - Possibilidade de implementação tanto em software quanto em hardware;
  - Ser mais rápido do que o 3DES.

História do Algoritmo



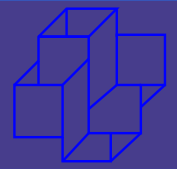
- Em 1998, apresentaram-se 15 candidatos e, um ano depois, 5 destes foram escolhidos como finalistas: MARS, RC6, Rijndael, Serpent e Twofish.
- Em 2000, após análises da comunidade criptográfica mundial, é escolhido como padrão o algoritmo Rijndael, criado pelos belgas Vincent Rijmen e Joan Daemen.

Conceitos Básicos



- $Nb \longrightarrow$ número de bits do bloco dividido por 32.
- $Nk \longrightarrow$ número de bits da chave dividido por 32.
- $Nr \longrightarrow$ número de rodadas, que é igual a 10, 12 e 14 para Nk igual a 4, 6 ou 8, respectivamente.

Conceitos Básicos



- *Estado* é o bloco de dados, ou seja, a matriz que contém inicialmente a mensagem e possui 4 linhas e *Nb* colunas.

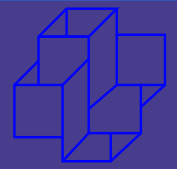
Exemplo de estado

P	A	L	E
S	T	R	A
∅	N	O	∅
L	N	C	C

$\xrightarrow{ASCII}$

50	41	4c	45
53	54	52	41
20	4e	4f	20
4c	4e	43	43

Conceitos Básicos



- A chave principal é alocada em uma matriz de 4 linhas e *Nk* colunas.

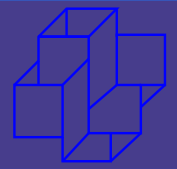
Exemplo de chave principal

B	O	L	S
I	S	T	A
∅	D	O	∅
C	N	P	q

$\xrightarrow{ASCII}$

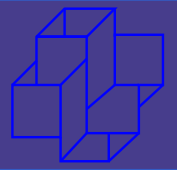
42	4f	4c	53
49	53	54	41
20	44	4f	20
43	4e	50	71

Etapas do Algoritmo



- **SubBytes** - Substitui cada byte individualmente por outro em uma caixa de substituição.
- **ShiftRows** - Rotaciona ciclicamente os bytes de cada linha, trocando sua posição.
- **MixColumns** - Multiplicação, sobre $GF(2^8)$, de uma matriz fixa pelo estado.
- **AddRoundKey** - É um XOR byte a byte entre o estado e a chave da rodada.

SubBytes



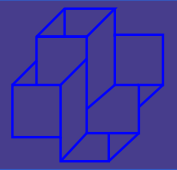
Exemplo da transformação SubBytes

a6	72	c1	f7
45	00	35	d4
82	fc	e6	50
be	15	09	99

$\xrightarrow{SubBytes}$

24	40	78	68
6e	63	96	48
13	b0	8e	53
ae	59	01	ee

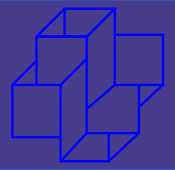
SubBytes



S-box usada no AES

		x														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
y	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

InvSubBytes



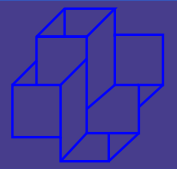
Exemplo da transformação InvSubBytes

24	40	78	68
6e	63	96	48
13	b0	8e	53
ae	59	01	ee

$$\xrightarrow{InvSubBytes}$$

a6	72	c1	f7
45	00	35	d4
82	fc	e6	50
be	15	09	99

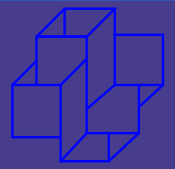
InvSubBytes



S-box inversa usada no AES

		x														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
y	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

ShiftRows



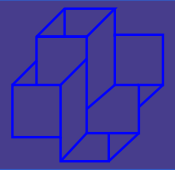
Exemplo da transformação ShiftRows

24	40	78	68
6e	63	96	48
13	b0	8e	53
ae	59	01	ee

$\xrightarrow{ShiftRows}$

24	40	78	68
63	96	48	6e
8e	53	13	b0
ee	ae	59	01

InvShiftRows



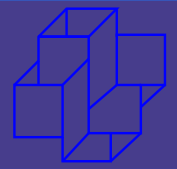
Exemplo da transformação InvShiftRows

24	40	78	68
63	96	48	6e
8e	53	13	b0
ee	ae	59	01

$$\xrightarrow{InvShiftRows}$$

24	40	78	68
6e	63	96	48
13	b0	8e	53
ae	59	01	ee

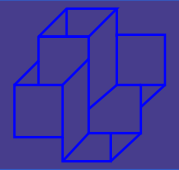
MixColumns



$$\begin{bmatrix} S'_{1,1} & S'_{1,2} & S'_{1,3} & S'_{1,4} \\ S'_{2,1} & S'_{2,2} & S'_{2,3} & S'_{2,4} \\ S'_{3,1} & S'_{3,2} & S'_{3,3} & S'_{3,4} \\ S'_{4,1} & S'_{4,2} & S'_{4,3} & S'_{4,4} \end{bmatrix} =$$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \odot \begin{bmatrix} S_{1,1} & S_{1,2} & S_{1,3} & S_{1,4} \\ S_{2,1} & S_{2,2} & S_{2,3} & S_{2,4} \\ S_{3,1} & S_{3,2} & S_{3,3} & S_{3,4} \\ S_{4,1} & S_{4,2} & S_{4,3} & S_{4,4} \end{bmatrix}$$

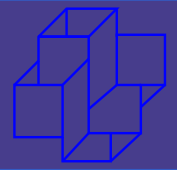
InvMixColumns



$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \odot \begin{bmatrix} S'_{1,1} & S'_{1,2} & S'_{1,3} & S'_{1,4} \\ S'_{2,1} & S'_{2,2} & S'_{2,3} & S'_{2,4} \\ S'_{3,1} & S'_{3,2} & S'_{3,3} & S'_{3,4} \\ S'_{4,1} & S'_{4,2} & S'_{4,3} & S'_{4,4} \end{bmatrix} =$$

$$\begin{bmatrix} S_{1,1} & S_{1,2} & S_{1,3} & S_{1,4} \\ S_{2,1} & S_{2,2} & S_{2,3} & S_{2,4} \\ S_{3,1} & S_{3,2} & S_{3,3} & S_{3,4} \\ S_{4,1} & S_{4,2} & S_{4,3} & S_{4,4} \end{bmatrix}$$

AddRoundKey

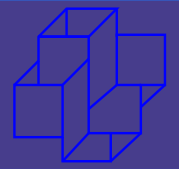


Transformação AddRoundKey

$$
\begin{array}{|c|c|c|c|}
\hline
s_{1,1} & s_{1,2} & s_{1,3} & s_{1,4} \\
\hline
s_{2,1} & s_{2,2} & s_{2,3} & s_{2,4} \\
\hline
s_{3,1} & s_{3,2} & s_{3,3} & s_{3,4} \\
\hline
s_{4,1} & s_{4,2} & s_{4,3} & s_{4,4} \\
\hline
\end{array}
\oplus
\begin{array}{|c|c|c|c|}
\hline
k_{1,1} & k_{2,1} & k_{3,1} & k_{4,1} \\
\hline
k_{1,2} & k_{2,2} & k_{3,2} & k_{4,2} \\
\hline
k_{1,3} & k_{2,3} & k_{3,3} & k_{4,3} \\
\hline
k_{1,4} & k_{2,4} & k_{3,4} & k_{4,4} \\
\hline
\end{array}
=
$$

$$
\begin{array}{|c|c|c|c|}
\hline
s'_{1,1} & s'_{1,2} & s'_{1,3} & s'_{1,4} \\
\hline
s'_{2,1} & s'_{2,2} & s'_{2,3} & s'_{2,4} \\
\hline
s'_{3,1} & s'_{3,2} & s'_{3,3} & s'_{3,4} \\
\hline
s'_{4,1} & s'_{4,2} & s'_{4,3} & s'_{4,4} \\
\hline
\end{array}
$$

Geração de Chaves

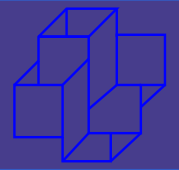


$w_i \longrightarrow$ seqüência de 4 bytes

Chaves de rodada

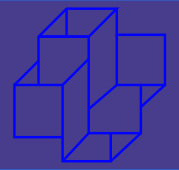
w_0	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}	$\ldots$
chave da rodada 0				chave da rodada 1				$\ldots$			

Geração de Chaves



- RotWord - Rotaciona a palavra uma posição (correspondente a um byte) à esquerda;
- SubWord - Aplica a S-box do AES em cada byte da palavra;
- Rcon(j) - É uma constante diferente a cada rodada (j). Essa constante é dada por Rcon(j)=(RC[j],00,00,00), onde RC[1]=1 e RC[j]=2 · RC[j-1], com a multiplicação sobre $GF(2^8)$.

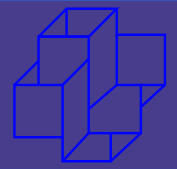
Geração de Chaves



Em pseudocódigo, para $Nk \leqslant 6$:

```
KeyExpansion (byte key [4*Nk],word w[Nb*(Nr+1)],Nk)
  word temp
  for i from 0 to Nk-1
    w[i]=word(key[4*i],key[4*i+1],key[4*i+2],key[4*i+3])
  for i from Nk to Nb*(Nr + 1)-1
    temp=w[i - 1]
    if (i mod Nk=0)
      temp=SubWord(RotWord(temp)) xor Rcon[i/Nk]
    w[i]=w[i - Nk] xor temp
```

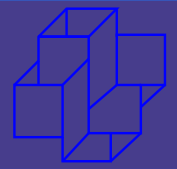
Geração de Chaves

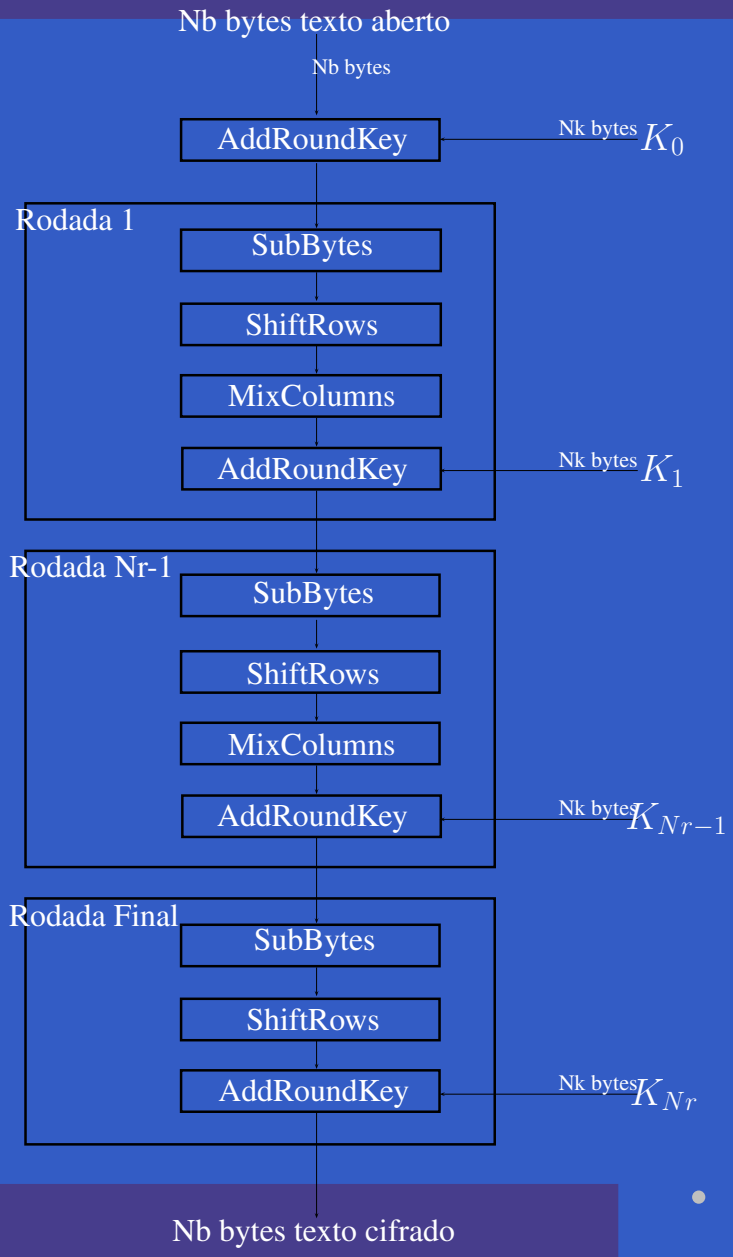


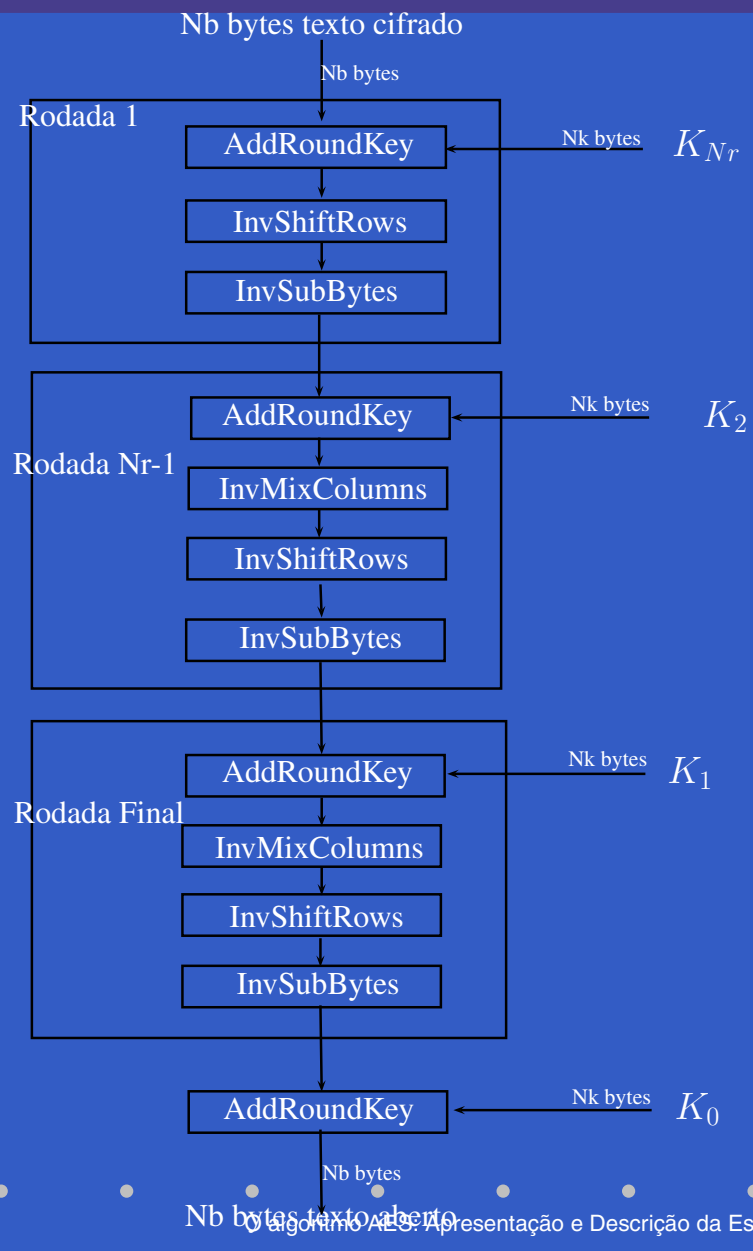
Exemplo Vamos supor que a chave principal tenha 128 bits e a chave de rodada 6 seja: 5c 3a 11 02 14 6f 5b af bc 52 40 dd 50 f4 61 78. Vamos calcular a primeira palavra da chave de rodada 7:

i	28
temp = w[i-1]	50f46178
RotWord	f4617850
SubWord	bfefbc53
Rcon(7)	40000000
temp = SubWord $\oplus$ Rcon(7)	fffebc53
w[i-Nk]	5c3a1102
w[i] = temp $\oplus$ w[i-Nk]	acd5ad51

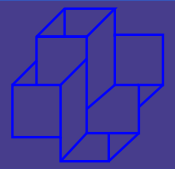
Cifragem e Decifragem







Último Slide



- Obrigado.
- Quaisquer sugestões serão bem-vindas.