

# Trabalho Individual INE5429

## Segurança em Computação

### AES e S-AES

Bruno Marques do Nascimento\*

21 de Abril de 2018

## 1 S-AES

Tabela 1 – Dados de entrada

-	Decimal	Hex
<b>Texto Claro</b>	10022	0x2726
<b>Chave secreta</b>	8022	0x1F56

Tabela 2 – Representação de bits - Texto claro

0010	0010
0111	0110

Tabela 3 – Representação de nibbles - Texto claro

2	2
7	6

Tabela 4 – Representação de bits - Chave secreta

$w_0$	$w_1$
0001 1111	0101 0110

---

\*brunomn95@gmail.com - Universidade Federal de Santa Catarina - Matrícula: 15104098

## 1.1 Expansão da chave

$$\begin{aligned}
\mathbf{w}_2 &= w_0 && \oplus g(w_1) \\
&= w_0 && \oplus Rcon(1) && \oplus SubNib(RotNib(w_1)) \\
&= w_0 && \oplus Rcon(1) && \oplus SubNib(RotNib(0101\ 0110)) \\
&= w_0 && \oplus Rcon(1) && \oplus SubNib(0110\ 0101) \\
&= w_0 && \oplus Rcon(1) && \oplus 1000\ 0001 \\
&= w_0 && \oplus 1000\ 0000 && \oplus 1000\ 0001 \\
&= w_0 && \oplus 0000\ 0001 \\
&= 0001\ 1111 && \oplus 0000\ 0001 \\
&= \mathbf{0001\ 1110}
\end{aligned}$$

$$\begin{aligned}
\mathbf{w}_3 &= w_2 \oplus w_1 \\
&= 0001\ 1110 \oplus 0101\ 0110 \\
&= \mathbf{0100\ 1000}
\end{aligned}$$

$$\begin{aligned}
\mathbf{w}_4 &= w_2 && \oplus g(w_3) \\
&= w_2 && \oplus Rcon(2) && \oplus SubNib(RotNib(w_3)) \\
&= w_2 && \oplus Rcon(2) && \oplus SubNib(RotNib(0100\ 1000)) \\
&= w_2 && \oplus Rcon(2) && \oplus SubNib(1000\ 0100) \\
&= w_2 && \oplus Rcon(2) && \oplus 0110\ 1101 \\
&= w_2 && \oplus (10000 \bmod 10011)|0000 && \oplus 0110\ 1101 \\
&= w_2 && \oplus 0011\ 0000 && \oplus 0110\ 1101 \\
&= w_2 && \oplus 0101\ 1101 \\
&= 0001\ 1110 && \oplus 0101\ 1101 \\
&= \mathbf{0100\ 0011}
\end{aligned}$$

$$\begin{aligned}
\mathbf{w}_5 &= w_4 && \oplus w_3 \\
&= 0100\ 0011 && \oplus 0100\ 1000 \\
&= \mathbf{0000\ 1011}
\end{aligned}$$

Tabela 5 – Expansão - Chave secreta

$w_0$	$w_1$	$w_2$	$w_3$	$w_4$	$w_5$
0001 1111	0101 0110	0001 1110	0100 1000	0100 0011	0000 1011
1 F	5 6	1 E	4 8	4 3	0 B

## 1.2 Encriptação

### 1.2.1 Rodada 0

#### 1.2.1.1 Incluir chave da rodada

Tabela 6 – Inclusão da chave

0010 (0x2)	0010 (0x2)	$\oplus$	0001 (0x1)	0101 (0x5)	$=$	0011 (0x3)	0111 (0x7)
0111 (0x7)	0110 (0x6)		1111 (0xF)	0110 (0x6)		1000 (0x8)	0000 (0x0)

Bits (Hexadecimal)

### 1.2.2 Rodada 1

#### 1.2.2.1 Substituição de nibble

Tabela 7 – Substituição de nibble

$s_{0,0}$ 0011 (0x3)	$\rightarrow$	S	$\rightarrow$	$s_{0,0}$ 1011 (0xB)
$s_{1,0}$ 1000 (0x8)	$\rightarrow$	S	$\rightarrow$	$s_{1,0}$ 0110 (0x6)
$s_{0,1}$ 0111 (0x7)	$\rightarrow$	S	$\rightarrow$	$s_{0,1}$ 0101 (0x5)
$s_{1,1}$ 0000 (0x0)	$\rightarrow$	S	$\rightarrow$	$s_{1,1}$ 1001 (0x9)

Bits (Hexadecimal)

#### 1.2.2.2 Deslocar linhas

Tabela 8 – Deslocamento de linha

1011 (0xB)	0101 (0x5)	$\rightarrow$	1011 (0xB)	0101 (0x5)
0110 (0x6)	1001 (0x9)		1001 (0x9)	0110 (0x6)

Bits (Hexadecimal)

### 1.2.2.3 Misturar colunas

$$\begin{aligned}
\mathbf{S}'_{0,0} &= S_{0,0} \oplus (4 \cdot S_{1,0}) \\
&= 1011 \oplus ((x^2 \cdot (x^3 + 1)) \bmod (x^4 + x + 1)) \\
&= 1011 \oplus ((x^5 + x^2) \bmod (x^4 + x + 1)) \\
&= 1011 \oplus (-x) \\
&= 1011 \oplus (x) \\
&= 1011 \oplus 0010 \\
&= \mathbf{1001}
\end{aligned}$$

$$\begin{aligned}
\mathbf{S}'_{1,0} &= (4 \cdot S_{0,0}) \oplus S_{1,0} \\
&= ((x^2 \cdot (x^3 + x + 1)) \bmod (x^4 + x + 1)) \oplus 1001 \\
&= ((x^5 + x^3 + x^2) \bmod (x^4 + x + 1)) \oplus 1001 \\
&= (x^3 - x) \oplus 1001 \\
&= (x^3 + x) \oplus 1001 \\
&= 1010 \oplus 1001 \\
&= \mathbf{0011}
\end{aligned}$$

$$\begin{aligned}
\mathbf{S}'_{0,1} &= S_{0,1} \oplus (4 \cdot S_{1,1}) \\
&= 0101 \oplus (x^2 \cdot (x^2 + x)) \bmod (x^4 + x + 1) \\
&= 0101 \oplus (x^4 + x^3) \bmod (x^4 + x + 1) \\
&= 0101 \oplus (x^3 - x - 1) \\
&= 0101 \oplus 1011 \\
&= \mathbf{1110}
\end{aligned}$$

$$\begin{aligned}
\mathbf{S}'_{1,1} &= (4 \cdot S_{0,1}) \oplus S_{1,1} \\
&= (x^2 \cdot (x^2 + 1) \bmod (x^4 + x + 1)) \oplus 0110 \\
&= (x^4 + x^2) \bmod (x^4 + x + 1) \oplus 0110 \\
&= (x^2 - x - 1) \oplus 0110 \\
&= 0111 \oplus 0110 \\
&= \mathbf{0001}
\end{aligned}$$

Tabela 9 – Saída: Mistura de colunas

1001 (0x9)	1110 (0xE)
0011 (0x3)	0001 (0x1)

Bits (Hexadecimal)

### 1.2.2.4 Incluir chave da rodada

Tabela 10 – Inclusão da chave

1001 (0x9)	1110 (0xE)	$\oplus$	0001 (0x1)	0100 (0x4)	$=$	1000 (0x8)	1010 (0xA)
0011 (0x3)	0001 (0x1)		1110 (0xE)	1000 (0x8)		1101 (0xD)	1001 (0x9)

Bits (Hexadecimal)

## 1.2.3 Rodada 2

### 1.2.3.1 Substituição de nibble

Tabela 11 – Substituição de nibble

$s_{0,0}$ 1000 (0x8)	$\rightarrow$	S	$\rightarrow$	$s_{0,0}$ 0110 (0x6)
$s_{1,0}$ 1101 (0xD)	$\rightarrow$	S	$\rightarrow$	$s_{1,0}$ 1110 (0xE)
$s_{0,1}$ 1010 (0xA)	$\rightarrow$	S	$\rightarrow$	$s_{0,1}$ 0000 (0x0)
$s_{1,1}$ 1001 (0x9)	$\rightarrow$	S	$\rightarrow$	$s_{1,1}$ 0010 (0x2)

Bits (Hexadecimal)

### 1.2.3.2 Deslocar linhas

Tabela 12 – Deslocamento de linha

0110 (0x6)	0000 (0x0)	$\rightarrow$	0110 (0x6)	0000 (0x0)
1110 (0xE)	0010 (0x2)		0010 (0x2)	1110 (0xE)

Bits (Hexadecimal)

### 1.2.3.3 Incluir chave da rodada

Tabela 13 – Inclusão da chave

0110 (0x6)	0000 (0x0)	$\oplus$	0100 (0x4)	0000 (0x0)	$=$	0010 (0x2)	0000 (0x0)
0010 (0x2)	1110 (0xE)		0011 (0x3)	1011 (0xB)		0001 (0x1)	0101 (0x5)

Bits (Hexadecimal)

#### 1.2.3.4 Saída: Texto Cifrado

**Binário:** 0010 0001 0000 0101

**Hexadecimal:** 0x2105

### 1.3 Deciptação

#### 1.3.1 Rodada 0

##### 1.3.1.1 Incluir chave da rodada

Tabela 14 – Inclusão da chave

0010 (0x2)	0000 (0x0)	$\oplus$	0100 (0x4)	0000 (0x0)	$=$	0110 (0x6)	0000 (0x0)
0001 (0x1)	0101 (0x5)		0011 (0x3)	1011 (0xB)		0010 (0x2)	1110 (0xE)

Bits (Hexadecimal)

#### 1.3.2 Rodada 1

##### 1.3.2.1 Deslocar linhas invertidas

Tabela 15 – Deslocamento de linha invetida

0110 (0x6)	0000 (0x0)	$\longrightarrow$	0110 (0x6)	0000 (0x0)
0010 (0x2)	1110 (0xE)		1110 (0xE)	0010 (0x2)

Bits (Hexadecimal)

##### 1.3.2.2 Substituição de nibble invertido

Tabela 16 – Substituição de nibble invertido

$s_{0,0}$ 0110 (0x6)	$\longrightarrow$	S	$\longrightarrow$	$s_{0,0}$ 1000 (0x8)
$s_{1,0}$ 1110 (0xE)	$\longrightarrow$	S	$\longrightarrow$	$s_{1,0}$ 1101 (0xD)
$s_{0,1}$ 0000 (0x0)	$\longrightarrow$	S	$\longrightarrow$	$s_{0,1}$ 1010 (0xA)
$s_{1,1}$ 0010 (0x2)	$\longrightarrow$	S	$\longrightarrow$	$s_{1,1}$ 1001 (0x9)

Bits (Hexadecimal)

### 1.3.2.3 Incluir chave da rodada

Tabela 17 – Inclusão da chave

1000 (0x8)	1010 (0xA)	$\oplus$	0001 (0x1)	0100 (0x4)	$=$	1001 (0x9)	1110 (0xE)
1101 (0xD)	1001 (0x9)		1110 (0xE)	1000 (0x8)		0011 (0x3)	0001 (0x1)

Bits (Hexadecimal)

### 1.3.2.4 Misturar colunas invertidas

$$\begin{aligned}
\mathbf{S}'_{0,0} &= (9 \cdot S_{0,0}) \oplus (2 \cdot S_{1,0}) \\
&= ((x^3 + 1) \cdot (x^3 + 1)) \mod (x^4 + x + 1) \oplus (x \cdot (x + 1)) \\
&= ((x^6 + 2x^3 + 1) \mod (x^4 + x + 1)) \oplus (x^2 + x) \\
&= (x^3 - x^2 + 1) \oplus (x^2 + x) \\
&= 1101 \oplus 0110 \\
&= 1011
\end{aligned}$$

$$\begin{aligned}
\mathbf{S}'_{1,0} &= (2 \cdot S_{0,0}) \oplus (9 \cdot S_{1,0}) \\
&= (x \cdot (x^3 + 1)) \oplus ((x^3 + 1) \cdot (x + 1)) \\
&= (x^4 + x) \mod (x^4 + x + 1) \oplus (x^4 + x^3 + x + 1) \mod (x^4 + x + 1) \\
&= -1 \oplus x^3 \\
&= 0001 \oplus 1000 \\
&= 1001
\end{aligned}$$

$$\begin{aligned}
\mathbf{S}'_{0,1} &= (9 \cdot S_{0,1}) \oplus (2 \cdot S_{1,1}) \\
&= ((x^3 + 1) \cdot (x^3 + x^2 + x) \mod (x^4 + x + 1)) \oplus x \cdot 1 \\
&= (x^6 + x^5 + x^4 + x^3 + x^2 + x) \mod (x^4 + x + 1) \oplus x \\
&= -x^2 - x - 1 \oplus x \\
&= 0111 \oplus 0010 \\
&= 0101
\end{aligned}$$

$$\begin{aligned}
\mathbf{S}'_{1,1} &= (2 \cdot S_{0,1}) \oplus (9 \cdot S_{1,1}) \\
&= (x \cdot (x^3 + x^2 + x)) \mod (x^4 + x + 1) \oplus (x^3 + 1) \cdot 1 \\
&= (x^4 + x^3 + x^2) \mod (x^4 + x + 1) \oplus (x^3 + 1) \\
&= (x^3 + x^2 + x + 1) \oplus (x^3 + 1) \\
&= 1111 \oplus 1001 \\
&= 0110
\end{aligned}$$

Tabela 18 – Saída: Mistura de colunas invertidas

1011 (0xB)	0101 (0x5)
1001 (0x9)	0110 (0x6)

Bits (Hexadecimal)

### 1.3.3 Rodada 2

#### 1.3.3.1 Deslocar linhas invertidas

Tabela 19 – Deslocamento de linha invertida

1011 (0xB)	0101 (0x5)	→	1011 (0xB)	0101 (0x5)
1001 (0x9)	0110 (0x6)		0110 (0x6)	1001 (0x9)

Bits (Hexadecimal)

#### 1.3.3.2 Substituição de nibble invertido

Tabela 20 – Substituição de nibble invertido

$s_{0,0}$ 1011 (0xB)	→	S	→	$s_{0,0}$ 0011 (0x3)
$s_{1,0}$ 0110 (0x6)	→	S	→	$s_{1,0}$ 1000 (0x8)
$s_{0,1}$ 0101 (0x5)	→	S	→	$s_{0,1}$ 0111 (0x7)
$s_{1,1}$ 1001 (0x9)	→	S	→	$s_{1,1}$ 0000 (0x0)

Bits (Hexadecimal)

#### 1.3.3.3 Incluir chave da rodada

Tabela 21 – Inclusão da chave

0011 (0x3)	0111 (0x7)	⊕	0001 (0x1)	0101 (0x5)	=	0010 (0x2)	0010 (0x2)
1000 (0x8)	0000 (0x0)		1111 (0xF)	0110 (0x6)		0111 (0x7)	0110 (0x6)

Bits (Hexadecimal)



#### 1.3.3.4 Saída: Texto Decifrado

**Binário:** 0010 0111 0010 0110

**Hexadecimal:** 0x2726

Decimal: 10022

## 2 AES

Para a simulação do AES 128bits foi utilizada como base a planilha disponibilizada por (NAYUKI, 2016).

Tabela 22 – Dados de entrada

[illegible]

## 2.1 Encriptação

Tabela 23 – Execução AES(18bits) - Encriptação

Rodadas	Início da Rodada				Após SubBytes				Após ShiftRows				Após MixColumns				Chave de Rodada							
Rodada 0	00	00	00	00													00	00	00	00				
	00	00	00	00													00	00	00	00				
	00	00	00	27																	00	00	00	1F
	00	00	00	26																	00	00	00	56
Rodada 1	00	00	00	00	63	63	63	63	63	63	63	63	51	07	63	63	62	62	62	62				
	00	00	00	00	63	63	63	63	63	63	63	63	51	CF	63	63	C0	C0	C0	C0				
	00	00	00	38	63	63	63	07	63	07	63	63	35	AB	63	63	B1	B1	B1	AE				
	00	00	00	70	63	63	63	51	51	63	63	63	07	07	63	63	63	63	63	35				
Rodada 2	33	65	01	01	C3	4D	7C	7C	C3	4D	7C	7C	03	7A	FA	A1	DA	B8	DA	B8				
	91	0F	A3	AD	81	76	0A	0A	76	0A	0A	81	5A	C6	CA	FB	24	E4	24	E4				
	84	1A	D2	C3	5F	A2	B5	BD	B5	BD	5F	A2	0C	E3	0D	07	27	96	27	89				
	64	64	00	56	43	43	63	B1	B1	43	43	63	E4	E6	57	61	C9	AA	C9	FC				
Rodada 3	D9	C2	20	19	35	25	B7	D4	35	25	B7	D4	7F	F3	F6	2B	B7	0F	D5	6D				
	7E	22	EE	1F	F3	93	28	C0	93	28	C0	F3	62	86	0D	9E	83	67	43	A7				
	2B	75	2A	8E	F1	9D	E5	19	E5	19	F1	9D	95	4C	F5	1B	97	01	26	AF				
	2D	4C	9E	9D	D8	29	0B	5E	5E	D8	29	0B	95	F5	A1	1F	A5	0F	C6	3A				
Rodada 4	C8	FC	23	46	E8	B0	26	5A	E8	B0	26	5A	81	83	20	C1	E3	EC	39	54				
	E1	E1	4E	39	F8	F8	2F	12	F8	2F	12	F8	96	66	B6	0A	FA	9D	DE	79				
	02	4D	D3	B4	77	E3	66	8D	66	8D	77	E3	9D	92	AD	EB	17	16	30	9F				
	30	FA	67	25	04	2D	85	3F	3F	04	2D	85	C3	61	55	E4	99	96	50	6A				
Rodada 5	62	6F	19	95	AA	A8	D4	2A	AA	A8	D4	2A	19	A8	2F	90	45	A9	90	C4				
	6C	FB	68	73	50	0F	45	8F	0F	45	8F	50	4F	31	3B	00	21	BC	62	1B				
	8A	84	9D	74	7E	5F	5E	92	5E	92	7E	5F	32	0B	1F	79	15	03	33	AC				
	5A	F7	05	8E	BE	68	6B	19	19	BE	68	6B	86	53	46	A7	B9	2F	7F	15				
Rodada 6	5C	01	BF	54	4A	7C	08	20	4A	7C	08	20	35	C8	26	D8	CA	63	F3	37				
	6E	8D	59	1B	9F	5D	CB	AF	5D	CB	AF	9F	54	81	12	47	B0	0C	6E	75				
	27	08	2C	D5	CC	30	71	03	71	03	CC	30	AC	2E	14	E9	4C	4F	7C	D0				
	3F	7C	39	B2	75	10	12	37	37	75	10	12	9C	A6	5B	EB	A5	8A	F5	E0				
Rodada 7	FF	AB	D5	EF	16	62	03	DF	16	62	03	DF	A5	F4	F3	15	17	74	87	B0				
	E4	8D	7C	32	69	5D	10	23	5D	10	23	69	48	66	0C	C3	C0	CC	A2	D7				
	E0	61	68	39	E1	EF	45	12	45	12	E1	EF	BC	60	6A	44	AD	E2	9E	4E				
	B9	2C	AE	0B	12	71	E4	2B	2B	12	71	E4	74	80	25	2F	3F	B5	40	A0				
Rodada 8	B2	80	74	A5	37	CD	92	06	37	CD	92	06	4D	62	3E	05	9F	ED	6A	DA				
	88	AA	AE	14	C4	AC	E4	FA	AC	E4	FA	C4	DD	04	76	ED	EF	23	81	56				
	11	82	F4	0A	82	13	BF	67	BF	67	82	13	6B	29	D6	33	4D	AF	31	7F				
	4B	35	65	8F	B3	96	4D	73	73	B3	96	4D	AC	B2	E2	47	D8	6D	2D	8D				
Rodada 9	D4	8F	54	DF	48	73	20	9E	48	73	20	9E	3F	E5	0C	8C	33	DE	B4	6E				
	32	27	F7	BB	23	CC	68	EA	CC	68	EA	23	18	4A	73	9E	3D	1E	9F	C9				
	26	86	E7	4C	F7	44	94	29	94	29	F7	44	2B	E4	8E	B0	10	1B	8E	F1				
	74	DF	CF	CA	92	9E	8A	74	74	92	9E	8A	68	EB	5A	D1	8F	E2	CF	42				
Rodada 10	0C	3B	B8	E2	FE	E2	6C	98	FE	E2	6C	98					D8	06	B2	DC				
	25	54	EC	57	3F	20	CE	5B	20	CE	5B	3F					9C	82	1D	D4				
	3B	5B	08	41	E2	39	30	83	30	83	E2	39					3C	83	0D	FC				
	E7	09	95	93	94	01	2A	DC	DC	94	01	2A					10	F2	3D	7F				
Saída	26	E4	DE	44																				
	BC	4C	46	EB																				
	0C	00	EF	C5																				
	CC	66	3C	55																				

## 2.2 Decriptação

Tabela 24 – Execução AES(18bits) - Decriptação

Rodadas	Final da rodada	ShiftRows	SubBytes	Key Schedule	MixColumns
Saída	00 00 00 00 00 00 00 00 00 00 00 27 00 00 00 26				
Rodada 10	51 07 63 63 51 CF 63 63 35 AB 63 63 07 07 63 63	63 63 63 63 63 63 63 63 63 63 63 07 63 63 63 51	00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 70	00 00 00 00 00 00 00 00 00 00 00 1F 00 00 00 56	63 63 63 63 63 63 63 63 63 07 63 63 51 63 63 63
Rodada 9	03 7A FA A1 5A C6 CA FB 0C E3 0D 07 E4 E6 57 61	C3 4D 7C 7C 81 76 0A 0A 5F A2 B5 BD 43 43 63 B1	33 65 01 01 91 0F A3 A3 84 1A D2 CD 64 64 00 56	62 62 62 62 C0 C0 C0 C0 B1 B1 B1 AE 63 63 63 35	C3 4D 7C 7C 76 0A 0A 81 B5 BD 5F A2 B1 43 43 63
Rodada 8	7F F3 F6 2B 62 86 0D 9E 95 4C F5 1B 95 F5 A1 1F	35 25 B7 D4 F3 93 28 C0 F1 9D E5 19 D8 29 0B 5E	D9 C2 20 19 7E 22 EE 1F 2B 75 2A 8E 2D 4C 9E 9D	DA B8 DA B8 24 E4 24 E4 27 96 27 89 C9 AA C9 FC	35 25 B7 D4 93 28 C0 F3 E5 19 F1 9D 5E D8 29 0B
Rodada 7	81 83 20 C1 96 66 B6 0A 9D 92 AD EB C3 61 55 E4	E8 B0 26 5A F8 F8 2F 12 77 E3 66 8D 04 2D 85 3F	C8 FC 23 46 E1 E1 4E 39 02 4D D3 B4 30 FA 67 25	B7 0F D5 6D 83 67 43 A7 97 01 26 AF A5 0F C6 3A	E8 B0 26 5A F8 2F 12 F8 66 8D 77 E3 3F 04 2D 85
Rodada 6	19 A8 2F 90 4F 31 3B 00 32 0B 1F 79 86 53 46 A7	AA A8 D4 2A 50 0F 45 8F 7E 5F 5E 92 BE 68 6B 19	62 6F 19 95 6C FB 68 73 8A 84 9D 74 5A F7 05 8E	E3 EC 39 54 FA 9D DE 79 17 16 30 9F 99 96 50 6A	AA A8 D4 2A 0F 45 8F 50 5E 92 7E 5F 19 BE 68 6B
Rodada 5	35 C8 26 D8 54 81 12 47 AC 2E 14 E9 9C A6 5B EB	4A 7C 08 20 9F 5D CB AF CC 30 71 03 75 10 12 37	5C 01 BF 54 6E 8D 59 1B 27 08 2C D5 3F 7C 39 B2	45 A9 90 C4 21 BC 62 1B 15 03 33 AC B9 2F 7F 15	4A 7C 08 20 5D CB AF 9F 71 03 CC 30 37 75 10 12
Rodada 4	A5 F4 F3 15 48 66 0C C3 BC 60 6A 44 74 80 25 2F	16 62 03 DF 69 5D 10 23 E1 EF 45 12 12 71 E4 2B	FF AB D5 EF E4 8D 7C 32 E0 61 68 39 39 2C AE 0B	CA 63 F3 37 B0 0C 6E 75 4C 4F 7C D0 A5 8A F5 E0	16 62 03 DF 5D 10 23 69 45 12 E1 EF 2B 12 71 E4
Rodada 3	4D 62 3E 05 DD 04 76 ED 6B 29 D6 33 AC B2 E2 47	37 CD 92 06 C4 AC E4 FA 82 13 BF 67 B3 96 4D 73	B2 80 74 A5 88 AA AE 14 11 82 F4 0A 4B 35 65 8F	17 74 87 B0 C0 CC A2 D7 AD E2 9E 4E 3F B5 40 A0	37 CD 92 06 AC E4 FA C4 BF 67 82 13 73 B3 96 4D
Rodada 2	3F E5 0C 8C 18 4A 73 9E 2B E4 86 B0 68 EB 5A D1	48 73 20 9E 23 CC 68 EA F7 44 94 29 92 9E 8A 74	D4 8F 54 DF 32 27 F7 BB 26 86 E7 4C 74 DF CF CA	99 ED 6A DA EF 23 81 56 4D AF 31 7F D8 6D 2D 8D	48 73 20 9E CC 68 EA 23 94 29 F7 44 74 92 9E 8A
Rodada 1	FE E2 6C 98 20 CE 5B 3F 30 83 E2 39 DC 94 01 2A	FE E2 6C 98 3F 20 CE 5B E2 39 30 83 94 01 2A DC	0C 3B B8 E2 25 54 EC 57 3B 5B 08 41 E7 09 95 93	33 DE B4 6E 3D 1E 9F C9 10 BF 8E F1 8F E2 CF 42	
Rodada 0	26 E4 DE 44 BC 4C 46 EB 0C 00 EF C5 CC 66 3C 55			D8 06 B2 DC 9C 82 1D D4 3C 83 0D FC 10 F2 3D 7F	

## Referências

NAYUKI. *AES cipher internals in Excel*. [S.l.], 2016. Disponível em: <<https://www.nayuki.io/page/aes-cipher-internals-in-excel>>. Acesso em: 21 Abril 2018. Citado na página 9.

STALLINGS, W. *Cryptography and Network Security (4th Edition)*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 2005. ISBN 0131873164. Nenhuma citação no texto.

STALLINGS, W. *Cryptography and Network Security: Principles and Practice*. 5th. ed. Upper Saddle River, NJ, USA: Prentice Hall Press, 2010. ISBN 0136097049, 9780136097044. Nenhuma citação no texto.