AES: Advanced Encryption Standard

INE5429 - Segurança em Computação

Caique Rodrigues Marques
c.r.marques@grad.ufsc.br

Nota: As tabelas da *S-box* e da *S-box* inversa foram retiradas do livro-texto[2].

1 AES Simplificado

1.1 Cifração

A entrada t para o AES corresponde ao número do dia do aniversário acrescido de 10000, portanto, $10000+25 = 10025$. A chave k é o número do aniversário somado a 8000, portanto, $8000 + 25 = 8025$. Em hexadecimal, temos que $t =$ `2729` e $k =$ `1F59`.

1. **Incluir chave de rodada**: Esta função apenas consiste na operação de ou-exclusivo (XOR) de 16 bits entre a entrada t com a chave k. Abaixo está representada em tabelas a operação realizada:

$$\begin{array}{|c|c|} \hline 2 & 2 \\ \hline 7 & 9 \\ \hline \end{array} \oplus \begin{array}{|c|c|} \hline 1 & 5 \\ \hline F & 9 \\ \hline \end{array} = \begin{array}{|c|c|} \hline 3 & 7 \\ \hline 8 & 0 \\ \hline \end{array}$$

$$\begin{aligned} 2 \oplus 1 &= 0010 \oplus 0001 = 3 \\ 7 \oplus F &= 0111 \oplus 1111 = 8 \\ 2 \oplus 5 &= 0010 \oplus 0101 = 7 \\ 9 \oplus 9 &= 1001 \oplus 1001 = 0 \end{aligned}$$

2. **Substituir *nibble***: A função de substituição do *nibble* é apenas uma pesquisa em uma tabela. O AES define uma matriz 4x4 dos valores de *nibbles*, chamada de *S-box*, que consiste em uma permutação de todos os possíveis valores de 4 bits. Cada *nibble* da entrada é mapeada para o novo *nibble* definido na *S-box* da seguinte maneira: os dois bits mais à esquerda correspondem à linha da *S-box*, enquanto os dois bits mais à direita correspondem à coluna da *S-box*. Por exemplo, o valor hexadecimal `8`, em binário é 1000, é mapeado para a linha 2 e coluna 0 da S-box, que resulta no valor `6`. A seguir, à esquerda está a *S-box*, enquanto à direita está a substituição dos *nibbles* da saída do passo anterior.

		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

$$\begin{array}{|c|c|} \hline 3 & 7 \\ \hline 8 & 0 \\ \hline \end{array} \rightarrow \begin{array}{|c|c|} \hline B & 5 \\ \hline 6 & 9 \\ \hline \end{array}$$

3. **Deslocar linhas**: A função de deslocar linhas realiza uma rotação circular de um *nibble* da segunda linha, enquanto a primeira linha permanece inalterada, assim:

$$\begin{array}{|c|c|} \hline B & 5 \\ \hline 6 & 9 \\ \hline \end{array} \rightarrow \begin{array}{|c|c|} \hline B & 5 \\ \hline 9 & 6 \\ \hline \end{array}$$

4. **Embaralhar colunas**: A transformação pode ser definida pelas seguintes operações, onde o operador $\cdot$ corresponde à multiplicação em $GF(2^4)$.

$$S'_{0,0} = (B \cdot 1) \oplus (4 \cdot 9) = B \oplus 2 = 9$$
$$S'_{1,0} = (B \cdot 4) \oplus (1 \cdot 9) = A \oplus 9 = 3$$
$$S'_{0,1} = (5 \cdot 1) \oplus (4 \cdot 6) = 5 \oplus B = E$$
$$S'_{1,1} = (5 \cdot 4) \oplus (1 \cdot 6) = 7 \oplus 6 = 1$$

5. **Expansão da chave**: O algoritmo de expansão é definido a seguir, onde, da chave k, temos $w_0 =$ `1F` e $w_1 = 59$; `RotNib` corresponde à rotação circular à esquerda de um *nibble*; `SubNib` refere-se aos *nibbles* correspondentes na *S-box*. A partir da chave k de 16 bits, ela é expandida para seis palavras de 8 bits cada uma.

   $w_2 = w_0 \oplus g(w_1)$
   $= w_0 \oplus Rcon(1) \oplus SubNib(RotNib(w_1))$
   $= 00011111 \oplus 10000000 \oplus SubNib(10010101)$
   $= 00011111 \oplus 10000000 \oplus 00100001 = 10111110$

   $w_3 = w_2 \oplus w_1 = 10111110 \oplus 01011001 = 11100111$

   $w_4 = w_2 \oplus g(w_3)$
   $= w_2 \oplus Rcon(2) \oplus SubNib(RotNib(w_3))$
   $= 10111110 \oplus 00110000 \oplus SubNib(01111110)$
   $= 10111110 \oplus 00110000 \oplus 01011111 = 11010001$

   $w_5 = w_4 \oplus w_3 = 11010001 \oplus 11100111 = 00110110$

6. **Incluir chave de rodada**: Operação de ou-exclusivo entre o resultado do embaralhamento de colunas (passo 4) e a concatenação de w_2 e w_3, do passo anterior:

9	E
3	1

$\oplus$

B	E
E	7

$=$

2	0
D	6

$$9 \oplus B = 1001 \oplus 1011 = 2$$
$$3 \oplus E = 0011 \oplus 1110 = D$$
$$E \oplus E = 1110 \oplus 1110 = 0$$
$$1 \oplus 7 = 0001 \oplus 0111 = 6$$

7. **Substituir *nibble***:Mesmo procedimento realizado no passo 2, o resultado do passo anterior é associado à *S-box*.

2	0
D	6

$\rightarrow$

A	9
E	8

8. **Deslocar linhas**: Similar ao passo 3.

A	9
E	8

$\rightarrow$

A	9
8	E

9. **Incluir chave de rodada**: Similar ao passo 1. A operação de ou-exclusivo é realizada entre o resultado do passo anterior com a concatenação das palavras w_4 e w_5 do passo 5.

A	9
8	E

$\oplus$

D	3
1	6

$=$

7	A
9	8

Assim, o texto cifrado c resultante é `79A8`.

1.2 Decifração

A entrada para o AES é o resultado da cifragem, realizada anteriormente, que é `727A`.

1. **Incluir chave de rodada**: Esta função apenas consiste na operação de ou-exclusivo (XOR) de 16 bits entre a entrada com a concatenação das palavras w_4 e w_5 (ver passo 5 da subseção de cifragem). Abaixo está representada em tabelas a operação realizada:

$$\begin{array}{|c|c|}\hline 7 & A \\ \hline 9 & 8 \\ \hline \end{array} \oplus \begin{array}{|c|c|}\hline D & 3 \\ \hline 1 & 6 \\ \hline \end{array} = \begin{array}{|c|c|}\hline A & 9 \\ \hline 8 & E \\ \hline \end{array}$$

2. **Deslocar linhas invertidas**: A função de deslocar linhas realiza uma rotação circular de um *nibble* da segunda linha, enquanto a primeira linha permanece inalterada, assim:

$$\begin{array}{|c|c|}\hline A & 9 \\ \hline 8 & E \\ \hline \end{array} \rightarrow \begin{array}{|c|c|}\hline A & 9 \\ \hline E & 8 \\ \hline \end{array}$$

3. **Substituir *nibble* invertido**: A função realiza o inverso da *S-box* (ver tabela na parte 2 da seção de cifragem), resultando na tabela *S-box* invertido. A seguir, à esquerda está a *S-box* invertido, enquanto à direita está a substituição dos *nibbles* da saída do passo anterior.

		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

$$\begin{array}{|c|c|}\hline A & 9 \\ \hline E & 8 \\ \hline \end{array} \rightarrow \begin{array}{|c|c|}\hline 2 & 0 \\ \hline D & 6 \\ \hline \end{array}$$

4. **Incluir chave de rodada**: Esta função apenas consiste na operação de ou-exclusivo (XOR) de 16 bits entre a saída do passo anterior com a concatenação das palavras w_2 e w_3 (ver passo 5 da subseção de cifragem). Abaixo está representada em tabelas a operação realizada:

$$\begin{array}{|c|c|}\hline 2 & 0 \\ \hline D & 6 \\ \hline \end{array} \oplus \begin{array}{|c|c|}\hline B & E \\ \hline E & 7 \\ \hline \end{array} = \begin{array}{|c|c|}\hline 9 & E \\ \hline 3 & 1 \\ \hline \end{array}$$

5. **Embaralhar colunas invertidas**: A transformação pode ser definida pelas seguintes operações, onde o operador $\cdot$ corresponde à multiplicação em $GF(2^4)$.

$$\begin{aligned} S'_{0,0} &= (9 \cdot 9) \oplus (2 \cdot 3) = D \oplus 6 = B \\ S'_{1,0} &= (2 \cdot 9) \oplus (9 \cdot 3) = 1 \oplus 8 = 9 \\ S'_{0,1} &= (9 \cdot E) \oplus (2 \cdot 1) = 7 \oplus 2 = 5 \\ S'_{1,1} &= (2 \cdot E) \oplus (9 \cdot 1) = F \oplus 9 = 6 \end{aligned}$$

6. **Deslocar linhas invertidas**: A função de deslocar linhas realiza uma rotação circular de um *nibble* da segunda linha, enquanto a primeira linha permanece inalterada, assim:

$$\begin{array}{|c|c|}\hline B & 5 \\ \hline 9 & 6 \\ \hline \end{array} \rightarrow \begin{array}{|c|c|}\hline B & 5 \\ \hline 6 & 9 \\ \hline \end{array}$$

7. **Substituir *nibble* invertido**: Similar ao passo 3 da decifragem.

$$\begin{array}{|c|c|}\hline B & 5 \\ \hline 6 & 9 \\ \hline \end{array} \rightarrow \begin{array}{|c|c|}\hline 3 & 7 \\ \hline 8 & 0 \\ \hline \end{array}$$

8. **Incluir chave de rodada**: Esta função apenas consiste na operação de ou-exclusivo (XOR) de 16 bits entre a saída do passo anterior com a chave k. Abaixo está representada em tabelas a operação realizada:

$$\begin{array}{|c|c|}\hline 3 & 7 \\ \hline 8 & 0 \\ \hline \end{array} \oplus \begin{array}{|c|c|}\hline 1 & 5 \\ \hline F & 9 \\ \hline \end{array} = \begin{array}{|c|c|}\hline 2 & 2 \\ \hline 7 & 9 \\ \hline \end{array}$$

Assim o texto original t resultante é `2729`.

2 AES Padrão

2.1 Cifração

O AES padrão exige que a chave tenha pelo menos 128 bits, então, para resolver o problema, é realizado um *padding* à esquerda com zeros. Assim os valores passam a ser os indicados na tabela abaixo. Os dez rounds de cifração estão indicados na tabela 1 - o resultado está indicado na última linha, na coluna `AddRoundKey`[1].

Texto original:	`00000000000000000000000000002729`
Chave:	`00000000000000000000000000001F59`
Texto cifrado:	`33A0A57199C5876778EA7B2C56970774`

2.2 Decifração

A saída da cifragem é usada como entrada para o decifrador AES padrão. A chave k possui 16 bits, assim, foi realizado um *padding* à esquerda com zeros, até completar 128 bits. Os valores finais estão indicados na tabela abaixo. Os dez rounds de decifração estão indicados na tabela 2 - a saída está apresentada na primeira linha, na coluna `AddRoundKey`.

Texto cifrado	`33A0A57199C5876778EA7B2C56970774`
Chave	`00000000000000000000000000001F59`
Texto original	`00000000000000000000000000002729`

Referências

[1] Nayuki. Aes cipher internals in excel. https://www.nayuki.io/page/aes-cipher-internals-in-excel, 2016.

[2] Stallings, W. *Cryptography and Network Security: Principles and Practice*, 6th ed. Pearson, 2014.

[1] Tabela de cifração e decifração do AES gerada pelo software "AES ciphers internals"[1].

	SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant
Round 0													00	00	00	00	00	00	00	00	
													00	00	00	00	00	00	00	00	
													00	00	00	38	00	00	00	1F	
													00	00	00	70	00	00	00	59	
Round 1	63	63	63	63	63	63	63	63	51	07	63	63	33	65	01	01	62	62	62	62	01
	63	63	63	63	63	63	63	63	51	CF	63	63	91	0F	A3	A3	C0	C0	C0	C0	
	63	63	63	07	63	07	63	63	35	AB	63	63	FE	60	A8	B7	CB	CB	CB	D4	
	63	63	63	51	51	63	63	63	07	07	63	63	64	64	00	59	63	63	63	3A	
Round 2	C3	4D	7C	7C	C3	4D	7C	7C	0E	6E	1E	D3	D4	D6	C4	6B	DA	B8	DA	B8	02
	81	76	0A	0A	76	0A	0A	81	B9	FA	FD	6D	31	B2	75	25	88	48	88	48	
	BB	D0	C2	A9	C2	A9	BB	D0	6C	CB	DE	E3	27	4B	95	7C	4B	80	4B	9F	
	43	43	63	CB	CB	43	43	63	67	F2	B3	13	AE	58	7A	E0	C9	AA	C9	F3	
Round 3	48	F6	1C	7F	48	F6	1C	7F	02	BF	DF	C5	8E	8B	31	93	8C	34	EE	56	04
	C7	37	9D	3F	37	9D	3F	C7	B9	03	47	FE	EA	18	D4	25	53	1B	93	DB	
	CC	B3	2A	10	2A	10	CC	B3	13	7C	1E	B0	55	BA	93	A2	46	C6	8D	12	
	E4	6A	DA	E1	E1	E4	6A	DA	1C	5F	03	5A	B9	50	C5	6F	A5	0F	C6	35	
Round 4	19	3D	C7	DC	19	3D	C7	DC	AA	CE	7B	63	97	C7	9C	D2	3D	09	E7	B1	08
	87	AD	48	3F	AD	48	3F	87	8F	B5	F5	68	15	34	E7	A1	9A	81	12	C9	
	FC	F4	DC	3A	DC	3A	FC	F4	F4	FB	EE	59	24	ED	75	D0	D0	16	9B	89	
	56	53	A6	A8	A8	56	53	A6	11	99	37	5B	05	82	EA	B3	14	1B	DD	E8	
Round 5	88	C6	DE	B5	88	C6	DE	B5	D3	2B	D4	48	23	D2	CA	E7	F0	F9	1E	AF	10
	59	18	94	32	18	94	32	59	69	0E	F3	7F	54	B2	5D	18	3D	BC	AE	67	
	36	55	9D	70	9D	70	36	55	06	0F	B5	D4	4D	52	73	9B	4B	5D	C6	4F	
	6B	13	87	6D	6D	6B	13	87	DC	63	5B	DD	00	A4	41	2F	DC	C7	1A	F2	
Round 6	26	B5	74	94	26	B5	74	94	8F	D2	AE	D0	DA	7E	1C	CD	55	AC	B2	1D	20
	20	37	4C	AD	37	4C	AD	20	D7	72	42	57	6E	77	E9	9B	B9	05	AB	CC	
	E3	00	8F	14	8F	14	E3	00	2B	74	DF	2A	E9	EB	86	3C	C2	9F	59	16	
	63	49	83	15	15	63	49	83	F8	5A	40	9A	5D	38	38	10	A5	62	78	8A	
Round 7	57	F3	9C	BD	57	F3	9C	BD	24	78	06	35	7A	8A	46	68	5E	F2	40	5D	40
	9F	F5	1E	14	F5	1E	14	9F	A0	A5	91	BF	5E	5E	C1	23	FE	FB	50	9C	
	1E	E9	44	EB	44	EB	1E	E9	6F	F4	BD	E2	D3	D7	C7	8E	BC	23	7A	6C	
	4C	07	07	CA	CA	4C	07	07	C7	63	BB	A4	C6	00	A0	35	01	63	1B	91	
Round 8	DA	7E	5A	45	DA	7E	5A	45	17	D9	DB	8C	17	2B	69	63	00	F2	B2	EF	80
	58	58	78	26	58	78	26	58	AD	11	DF	07	03	44	DA	9E	AE	55	05	99	
	66	0E	C6	19	C6	19	66	0E	B4	F3	15	3A	89	ED	71	32	3D	1E	64	08	
	B4	63	E0	96	96	B4	63	E0	DC	90	68	42	91	BE	5D	E6	4D	2E	35	A4	
Round 9	F0	F1	F9	FB	F0	F1	F9	FB	FB	A2	FD	79	0E	A5	48	23	F5	07	B5	5A	1B
	7B	1B	57	0B	1B	57	0B	7B	B6	BB	B3	BE	28	70	7D	E9	9E	CB	CE	57	
	A7	55	A3	23	A3	23	A7	55	3F	78	4E	FE	4B	12	40	F8	74	6A	0E	06	
	81	AE	4C	8E	8E	81	AE	4C	B4	65	FB	A0	26	D9	72	8D	92	BC	89	2D	
Round 10	AB	06	52	26	AB	06	52	26					33	99	78	56	98	9F	2A	70	36
	34	51	FF	1E	51	FF	1E	34					A0	C5	EA	97	F1	3A	F4	A3	
	B3	C9	09	41	09	41	B3	C9					A5	87	7B	07	AC	C6	C8	CE	
	F7	35	40	5D	5D	F7	35	40					71	67	2C	74	2C	90	19	34	
	SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant

Figura 1: Tabela com 10 rounds de cifração.

	SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant
Round 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	29	00	00	00	59	
Round 1	00	00	00	00	63	63	63	63	63	63	63	63	51	07	63	63	62	62	62	62	01
	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	CB	CB	CB	D4	
	00	00	00	70	63	63	63	51	51	63	63	63	07	07	63	63	63	63	63	3A	
Round 2	33	65	01	01	C3	4D	7C	7C	C3	4D	7C	7C	0E	6E	1E	D3	DA	B8	DA	B8	02
	91	0F	A3	A3	81	76	0A	0A	76	0A	0A	81	B9	FA	FD	6D	88	48	88	48	
	FE	60	A8	B7	BB	D0	C2	A9	C2	A9	BB	D0	6C	CB	DE	E3	4B	80	4B	9F	
	64	64	00	59	43	43	63	CB	CB	43	43	63	67	F2	B3	13	C9	AA	C9	F3	
Round 3	D4	D6	C4	6B	48	F6	1C	7F	48	F6	1C	7F	02	BF	DF	C5	8C	34	EE	56	04
	31	B2	75	25	C7	37	9D	3F	37	9D	3F	C7	B9	03	47	FE	53	1B	93	DB	
	27	4B	95	7C	CC	B3	2A	10	2A	10	CC	B3	13	7C	1E	B0	46	C6	8D	12	
	AE	58	7A	E0	E4	6A	DA	E1	E1	E4	6A	DA	1C	5F	03	5A	A5	0F	C6	35	
Round 4	8E	8B	31	93	19	3D	C7	DC	19	3D	C7	DC	AA	CE	7B	63	3D	09	E7	B1	08
	EA	18	D4	25	87	AD	48	3F	AD	48	3F	87	8F	B5	F5	68	9A	81	12	C9	
	55	BA	93	A2	FC	F4	DC	3A	DC	3A	FC	F4	F4	FB	EE	59	D0	16	9B	89	
	B9	50	C5	6F	56	53	A6	A8	A8	56	53	A6	11	99	37	5B	14	1B	DD	E8	
Round 5	97	C7	9C	D2	88	C6	DE	B5	88	C6	DE	B5	D3	2B	D4	48	F0	F9	1E	AF	10
	15	34	E7	A1	59	18	94	32	18	94	32	59	69	0E	F3	7F	3D	BC	AE	67	
	24	ED	75	D0	36	55	9D	70	9D	70	36	55	06	0F	B5	D4	4B	5D	C6	4F	
	05	82	EA	B3	6B	13	87	6D	6D	6B	13	87	DC	63	5B	DD	DC	C7	1A	F2	
Round 6	23	D2	CA	E7	26	B5	74	94	26	B5	74	94	8F	D2	AE	D0	55	AC	B2	1D	20
	54	B2	5D	18	20	37	4C	AD	37	4C	AD	20	D7	72	42	57	B9	05	AB	CC	
	4D	52	73	9B	E3	00	8F	14	8F	14	E3	00	2B	74	DF	2A	C2	9F	59	16	
	00	A4	41	2F	63	49	83	15	15	63	49	83	F8	5A	40	9A	A5	62	78	8A	
Round 7	DA	7E	1C	CD	57	F3	9C	BD	57	F3	9C	BD	24	78	06	35	5E	F2	40	5D	40
	6E	77	E9	9B	9F	F5	1E	14	F5	1E	14	9F	A0	A5	91	BF	FE	FB	50	9C	
	E9	EB	86	3C	1E	E9	44	EB	44	EB	1E	E9	6F	F4	BD	E2	BC	23	7A	6C	
	5D	38	38	10	4C	07	07	CA	CA	4C	07	07	C7	63	BB	A4	01	63	1B	91	
Round 8	7A	8A	46	68	DA	7E	5A	45	DA	7E	5A	45	17	D9	DB	8C	00	F2	B2	EF	80
	5E	5E	C1	23	58	58	78	26	58	78	26	58	AD	11	DF	07	AE	55	05	99	
	D3	D7	C7	8E	66	0E	C6	19	C6	19	66	0E	B4	F3	15	3A	3D	1E	64	08	
	C6	00	A0	35	B4	63	E0	96	96	B4	63	E0	DC	90	68	42	4D	2E	35	A4	
Round 9	17	2B	69	63	F0	F1	F9	FB	F0	F1	F9	FB	FB	A2	FD	79	F5	07	B5	5A	1B
	03	44	DA	9E	7B	1B	57	0B	1B	57	0B	7B	B6	BB	B3	BE	9E	CB	CE	57	
	89	ED	71	32	A7	55	A3	23	A3	23	A7	55	3F	78	4E	FE	74	6A	0E	06	
	91	BE	5D	E6	81	AE	4C	8E	8E	81	AE	4C	B4	65	FB	A0	92	BC	89	2D	
Round 10	0E	A5	48	23	AB	06	52	26					AB	06	52	26	98	9F	2A	70	36
	28	70	7D	E9	34	51	FF	1E					51	FF	1E	34	F1	3A	F4	A3	
	4B	12	40	F8	B3	C9	09	41					09	41	B3	C9	AC	C6	C8	CE	
	26	D9	72	8D	F7	35	40	5D					5D	F7	35	40	2C	90	19	34	
	SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant

Figura 2: Tabela com 10 rounds de decifração.