Aluno: José Luis Bressan Ruas
Matricula: 10202969

1 - AES Simplificado

Aniversário = 09
P = 10009 = 0x2719
K = 8009 = 0x1F49

Expansão da Chave:
w0 = **0x1F**
w1 = 0x49

w2 = 0x1F xor 0x80 xor SubNib(RotNib(0x49)) =
0x1F xor 0x80 xor SubNib(0x94) =
0x1F xor 0x80 xor 0x2D = **0xB2**

w3 = 0xB2 xor 0x49 = **0xFB**

w4 = 0xB2 xor 0x30 xor SubNib(RotNib(0xFB)) =
0xB2 xor 0x30 xor SubNib(0xBF) =
0xB2 xor 0x30 xor 0x37 = **0xB5**

w5 = 0xFB xor 0xB5 = **0x4E**

K0 = **0x1F49**
K1 = **0xB2FB**
K2 = **0xB54E**

Cifra (AK2 - SR - NS - AK1 - MC - SR - NS - AK0):

Sbox:

		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

Incluir chave da rodada (AK0):

P’ = P xor K0 = 0x3850

Substituição de nibble (NS): Rodada 1

P’ = Sbox(0x3850) = 0xB619

Deslocamento de linha (SR): Rodada 1

Antes deslocamento:

0xB	0x1
0x6	0x9

Depois deslocamento:

0xB	0x1
0x9	0x6

P’ = 0xB916

Embaralhando colunas (MC): Rodada 1

Antes de embaralhar:

0xB	0x1
0x9	0x6

$S'_{0,0}$ = 0xB xor (0x4 * 0x9) = 0xB xor ($x^2(x^3 + 1)$ = 0xB xor 0x2 = **0x9**
$x^5 + x^2$ mod $x^4 + x + 1 = x$ = 0x2

$S'_{0,1}$ = 0x1 xor (0x4 * 0x6) = 0x1 xor ($x^2(x^2 + x)$ = 0x1 xor 0xB = **0xA**
$x^4 + x^3$ mod $x^4 + x + 1 = x^3 + x + 1$ = 0xB

--
$S'_{1,0}$ = (0x4 * 0xB) xor 0x9 = ($x^2(x^3 + x + 1)$) xor 0x9 = 0xA xor 0x9 = **0x3**
$x^5 + x^3 + x^2$ mod $x^4 + x + 1 = x^3 + x$ = 0xA

$S'_{1,1}$ = 0x4 xor 0x6 = **0x2**

Depois de embaralhar:

0x9	0xA

0x3	0x2

P’ = 0x93A2

Incluindo chave da rodada (AK1): Rodada 1

P’ = 0x93A2 xor 0xB2FB = 0x2159

Substituição de nibble (NS): Rodada 2

P’ = Sbox(0x2159) = 0xA412

Deslocamento de linha: Rodada 2

Antes deslocamento:

0xA	0x1
0x4	0x2

Depois deslocamento:

0xA	0x1
0x2	0x4

P’ = 0xA214

Incluindo chave da rodada (AK2): Rodada 2

P’ = 0xA214 xor 0xB54E = 0x175A = **Palavra cifrada**

Decifra (AK0 - INS - ISR - IMC - AK1 - INS - ISR - AK2):

Sbox Inversa:

		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

Seja V o futuro texto decifrado.

Incluindo chave da rodada (AK2):

V = 0x175A xor 0xB54E = 0xA214

Deslocar linhas invertidas (ISR): Rodada 1

Antes deslocamento:

0xA	0x1
0x2	0x4

Depois deslocamento:

0xA	0x1
0x4	0x2

V = 0xA412

Substituir nibble invertido (INS):

V = Sbox(0xA412) = 0x2159

Incluindo chave da rodada (AK1): Rodada 1

V = 0x2159 xor 0xB2FB = 0x93A2

Embaralhar colunas invertidas (MC): Rodada 1

Antes embaralhamento invertido:

0x9	0xA
0x3	0x2

$S'_{0,0}$ = (0x9 * 0x9) xor (0x2 * 0x3) = $x^6 + 1$ xor 0x6 = 0xD xor 0x6 = **0xB**
$x^6 + 1$ mod $x^4 + x + 1 = x^3 + x^2 + 1$ = 0xD

$S'_{0,1}$ = (0x9 * 0xA) xor (0x2 * 0x2) = $x^6 + x^4 + x^3 + x$ xor 0x4 = 0x5 xor 0x4 = **0x1**
$x^6 + x^4 + x^3 + x$ mod $x^4 + x + 1 = x^2 + 1$ = 0x5

$S'_{1,0}$ = (0x2 * 0x9) xor (0x9 * 0x3) = $x^4 + x$ xor $x^4 + x^3 + x + 1$ = 0x1 xor 0x8 = **0x9**
$x^4 + x$ mod $x^4 + x + 1 = 1$ = 0x1
$x^4 + x^3 + x + 1$ mod $x^4 + x + 1 = x^3$ = 0x8

$S'_{1,1}$ = (0x2 * 0xA) xor (0x2 * 0x9) = $x^4 + x^2$ xor 0x1= 0x7 xor 0x1 = **0x6**
$x^4 + x^2$ mod $x^4 + x + 1 = x^2 + x + 1$ = 0x7

Depois embaralhamento invertido:

0xB	0x1
0x9	0x6

V = 0xB916

Deslocar linhas invertidas (ISR): Rodada 2

Antes deslocamento:

0xB	0x1
0x9	0x6

Depois deslocamento:

0xB	0x1
0x6	0x9

V = 0xB619

Substituir nibble invertido (INS): Rodada 2

V = SboxInversa(0xB619) = 0x3850

Incluir chave da rodada (AK0): Rodada 2

V = 0x3850 xor 0x1F49 = **0x2719**

P = V.

2 - AES-128

Cifra:
Resultado:

Plaintext (input)				Key (input)				Ciphertext (output)			
00	00	00	00	00	00	00	00	27	71	4B	03
00	00	00	00	00	00	00	00	30	4C	1F	50
00	00	00	27	00	00	00	1F	A2	42	2F	2B
00	00	00	19	00	00	00	49	BE	AB	8D	8B

String Representations	
Plaintext:	00000000000000000000000000002719
Key:	0000000000000000000000000000001F49
Ciphertext:	2730A2BE714C42AB4B1F2F8D03502B8B

Rodadas com suas respectivas chaves:

	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	50	00	00	00	49	
Round 1	63	63	63	63	63	63	63	63	53	07	63	63	31	65	01	01	62	62	62	62	01
	63	63	63	63	63	63	63	63	53	CF	63	63	93	0F	A3	A3	C0	C0	C0	C0	
	63	63	63	07	63	07	63	63	33	AB	63	63	08	90	58	47	3B	3B	3B	24	
	63	63	63	53	53	63	63	63	03	07	63	63	60	64	00	49	63	63	63	2A	
Round 2	C7	4D	7C	7C	C7	4D	7C	7C	5E	F4	95	84	84	4C	4F	3C	DA	B8	DA	B8	02
	DC	76	0A	0A	76	0A	0A	DC	AE	72	7B	1C	58	44	8D	2A	F6	36	F6	36	
	30	60	6A	A0	6A	A0	30	60	28	77	D3	C5	F6	92	0D	3F	DE	E5	DE	FA	
	D0	43	63	3B	3B	D0	43	63	38	C6	38	FE	F1	6C	F1	1D	C9	AA	C9	E3	
Round 3	5F	29	84	EB	5F	29	84	EB	E0	61	35	9D	3B	02	8C	9C	DB	63	B9	01	04
	6A	1B	5D	E5	1B	5D	E5	6A	AF	AD	C3	4F	74	40	D8	62	DB	ED	1B	2D	
	42	4F	D7	75	D7	75	42	4F	06	66	15	E7	C9	4C	E1	E9	CF	2A	F4	0E	
	A1	50	A1	A4	A4	A1	50	A1	7E	0A	90	5A	DB	05	56	7F	A5	0F	C6	25	
Round 4	E2	77	64	DE	E2	77	64	DE	EE	EA	9B	92	E5	82	4A	42	0B	68	D1	D0	08
	92	09	61	AA	09	61	AA	92	31	2E	3C	2B	41	B3	BA	80	70	9D	86	AB	
	DD	29	F8	1E	F8	1E	DD	29	6D	FA	D2	D6	9D	20	FC	F6	F0	DA	2E	20	
	B9	6B	B1	D2	D2	B9	6B	B1	73	8F	0D	BB	AA	59	1D	8E	D9	D6	10	35	
Round 5	D9	13	D6	2C	D9	13	D6	2C	B7	CF	6E	D5	CE	DE	AE	C5	79	11	C0	10	10
	83	6D	F4	CD	6D	F4	CD	83	D1	8A	7E	57	16	D0	A2	20	C7	5A	DC	77	
	5E	B7	B0	42	B0	42	5E	B7	E4	8C	E1	2D	82	30	73	9F	66	BC	92	B2	
	AC	CB	A4	19	19	AC	CB	A4	9F	C0	7F	13	36	BF	10	49	A9	7F	6F	5A	

Round 6	8B	1D	E4	A6	8B	1D	E4	A6	29	AA	0A	50	85	17	77	3D	AC	BD	7D	6D	20
	47	70	3A	B7	70	3A	B7	47	DA	1A	AC	EE	2A	B0	DA	EF	F0	AA	76	01	
	13	04	8F	DB	8F	DB	13	04	B3	85	6D	AC	6B	E1	9B	E8	D8	64	F6	44	
	05	08	CA	3B	3B	05	08	CA	0F	CC	83	3D	6C	D0	F0	14	63	1C	73	29	
Round 7	97	F0	F5	27	97	F0	F5	27	E9	C9	84	0E	79	E4	D4	33	90	2D	50	3D	40
	E5	E7	57	DF	E7	57	DF	E5	84	B8	A1	69	6F	F9	96	5F	EB	41	37	36	
	7F	F8	14	9B	14	9B	7F	F8	4D	7A	44	A6	30	63	AB	0D	7D	19	EF	AB	
	50	70	8C	FA	FA	50	70	8C	BE	67	44	77	E1	24	74	6E	5F	43	30	19	
Round 8	B6	69	48	C3	B6	69	48	C3	3A	56	E8	17	2F	6E	80	42	15	38	68	55	80
	A8	99	90	CF	99	90	CF	A8	A6	C8	F7	0C	2F	00	08	C5	89	C8	FF	C9	
	04	FB	62	D7	62	D7	04	FB	51	5F	D5	2B	F8	EF	8A	DF	A9	B0	5F	F4	
	F8	36	92	9F	9F	F8	36	92	1F	17	7F	32	67	2C	74	20	78	3B	0B	12	
Round 9	15	9F	CD	2C	15	9F	CD	2C	46	6E	40	2A	95	85	C3	FC	D3	EB	83	D6	1B
	15	63	30	A6	63	30	A6	15	E6	C3	28	EE	D0	3D	29	26	36	FE	01	C8	
	41	DF	7E	9E	7E	9E	41	DF	48	1C	7A	31	28	CC	F5	4A	60	D0	8F	7B	
	85	71	92	B7	B7	85	71	92	57	05	49	81	D3	BA	FD	27	84	BF	B4	A6	
Round 10	2A	97	2E	B0	2A	97	2E	B0					27	71	4B	03	0D	E6	65	B3	36
	70	27	A5	F7	27	A5	F7	70					30	4C	1F	50	17	E9	E8	20	
	34	4B	E6	D6	E6	D6	34	4B					A2	42	2F	2B	44	94	1B	60	
	66	F4	54	CC	CC	66	F4	54					BE	AB	8D	8B	72	CD	79	DF	
	SubBytes				**ShiftRows**				**MixColumns**				**AddRoundKey**				**Key Schedule**				**Round Constant**

Decifra:

Resultado:

Ciphertext (input)				**Key (input)**				**Plaintext (output)**			
27	71	4B	03	00	00	00	00	00	00	00	00
30	4C	1F	50	00	00	00	00	00	00	00	00
A2	42	2F	2B	00	00	00	1F	00	00	00	27
BE	AB	8D	8B	00	00	00	49	00	00	00	19

String Representations	
Ciphertext:	2730A2BE714C42AB4B1F2F8D03502B8B
Key:	00000000000000000000000000001F49
Plaintext:	00000000000000000000000000002719

Rodadas com suas respectivas chaves:

	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	19	00	00	00	49	
Round 1	00	00	00	00	63	63	63	63	63	63	63	63	53	07	63	63	62	62	62	62	01
	00	00	00	00	63	63	63	63	63	63	63	63	53	CF	63	63	C0	C0	C0	C0	
	00	00	00	38	63	63	63	07	63	07	63	63	33	AB	63	63	3B	3B	3B	24	
	00	00	00	50	63	63	63	53	53	63	63	63	03	07	63	63	63	63	63	2A	
Round 2	31	65	01	01	C7	4D	7C	7C	C7	4D	7C	7C	5E	F4	95	84	DA	B8	DA	B8	02
	93	0F	A3	A3	DC	76	0A	0A	76	0A	0A	DC	AE	72	7B	1C	F6	36	F6	36	
	08	90	58	47	30	60	6A	A0	6A	A0	30	60	28	77	D3	C5	DE	E5	DE	FA	
	60	64	00	49	D0	43	63	3B	3B	D0	43	63	38	C6	38	FE	C9	AA	C9	E3	
Round 3	84	4C	4F	3C	5F	29	84	EB	5F	29	84	EB	E0	61	35	9D	DB	63	B9	01	04
	58	44	8D	2A	6A	1B	5D	E5	1B	5D	E5	6A	AF	AD	C3	4F	DB	ED	1B	2D	
	F6	92	0D	3F	42	4F	D7	75	D7	75	42	4F	06	66	15	E7	CF	2A	F4	0E	
	F1	6C	F1	1D	A1	50	A1	A4	A4	A1	50	A1	7E	0A	90	5A	A5	0F	C6	25	
Round 4	3B	02	8C	9C	E2	77	64	DE	E2	77	64	DE	EE	EA	9B	92	0B	68	D1	D0	08
	74	40	D8	62	92	09	61	AA	09	61	AA	92	31	2E	3C	2B	70	9D	86	AB	
	C9	4C	E1	E9	DD	29	F8	1E	F8	1E	DD	29	6D	FA	D2	D6	F0	DA	2E	20	
	DB	05	56	7F	B9	6B	B1	D2	D2	B9	6B	B1	73	8F	0D	BB	D9	D6	10	35	
Round 5	E5	82	4A	42	D9	13	D6	2C	D9	13	D6	2C	B7	CF	6E	D5	79	11	C0	10	10
	41	B3	BA	80	83	6D	F4	CD	6D	F4	CD	83	D1	8A	7E	57	C7	5A	DC	77	
	9D	20	FC	F6	5E	B7	B0	42	B0	42	5E	B7	E4	8C	E1	2D	66	BC	92	B2	
	AA	59	1D	8E	AC	CB	A4	19	19	AC	CB	A4	9F	C0	7F	13	A9	7F	6F	5A	
Round 6	CE	DE	AE	C5	8B	1D	E4	A6	8B	1D	E4	A6	29	AA	0A	50	AC	BD	7D	6D	20
	16	D0	A2	20	47	70	3A	B7	70	3A	B7	47	DA	1A	AC	EE	F0	AA	76	01	
	82	30	73	9F	13	04	8F	DB	8F	DB	13	04	B3	85	6D	AC	D8	64	F6	44	
	36	BF	10	49	05	08	CA	3B	3B	05	08	CA	0F	CC	83	3D	63	1C	73	29	
Round 7	85	17	77	3D	97	F0	F5	27	97	F0	F5	27	E9	C9	84	0E	90	2D	50	3D	40
	2A	B0	DA	EF	E5	E7	57	DF	E7	57	DF	E5	84	B8	A1	69	EB	41	37	36	
	6B	E1	9B	E8	7F	F8	14	9B	14	9B	7F	F8	4D	7A	44	A6	7D	19	EF	AB	
	6C	D0	F0	14	50	70	8C	FA	FA	50	70	8C	BE	67	44	77	5F	43	30	19	
Round 8	79	E4	D4	33	B6	69	48	C3	B6	69	48	C3	3A	56	E8	17	15	38	68	55	80
	6F	F9	96	5F	A8	99	90	CF	99	90	CF	A8	A6	C8	F7	0C	89	C8	FF	C9	
	30	63	AB	0D	04	FB	62	D7	62	D7	04	FB	51	5F	D5	2B	A9	B0	5F	F4	
	E1	24	74	6E	F8	36	92	9F	9F	F8	36	92	1F	17	7F	32	78	3B	0B	12	
Round 9	2F	6E	80	42	15	9F	CD	2C	15	9F	CD	2C	46	6E	40	2A	D3	EB	83	D6	1B
	2F	00	08	C5	15	63	30	A6	63	30	A6	15	E6	C3	28	EE	36	FE	01	C8	
	F8	EF	8A	DF	41	DF	7E	9E	7E	9E	41	DF	48	1C	7A	31	60	D0	8F	7B	
	67	2C	74	20	85	71	92	B7	B7	85	71	92	57	05	49	81	84	BF	B4	A6	
Round 10	95	85	C3	FC	2A	97	2E	B0					2A	97	2E	B0	0D	E6	65	B3	36
	D0	3D	29	26	70	27	A5	F7					27	A5	F7	70	17	E9	E8	20	
	28	CC	F5	4A	34	4B	E6	D6					E6	D6	34	4B	44	94	1B	60	
	D3	BA	FD	27	66	F4	54	CC					CC	66	F4	54	72	CD	79	DF	
	SubBytes				ShiftRows				MixColumns				AddRoundKey				Key Schedule				Round Constant

Referências

https://www.nayuki.io/page/aes-cipher-internals-in-excel
Livro texto da disciplina