Trab2Seg

Davi Mansur Costa

October 2023

1 Introducao

Esse trabalho eh dividido em 2 partes, implementacao do AES e implementacao do modo de operacão CTR. O AES nasceu para servir como uma padronizacão de criptografia, assim, tiveram varios algoritmos concorrentes, e o vencedor por ser o mais adequado ao ver do órgão NIST(National Institute of Standards and Technology) foi o Rijndael que é o AES amplamente utilizado hoje, ele consiste em nao utilizar apenas um modo de criptografia como substituicao, mas varios, tendo assim varia etapas e repeticoes dessas etapas

2 Implementacao AES

2.1 Implementacao das funções

2.1.1 keyexpansion

Essa função consiste em expandir a chave de 16 bytes(128 bits) para 175 bytes, atraves de 4 outras funções: rotword, subword, rcon e ek.// Segue a explicacao de cada uma: //

- rotword: Consiste em rotacionar os 4 bytes da word fornecida para a esquerda.
- subword: Consiste em substituir cada um dos 4 bytes da word fornecida pelo byte correspondente na sbox.
- rcon: Consiste em fornecer uma sequência de bytes de acordo com o round e a tabela abaixo:

```
Rcon(0)     = 01000000
Rcon(1)     = 02000000
Rcon(2)     = 04000000
Rcon(3)     = 08000000
Rcon(4)     = 10000000
Rcon(5)     = 20000000
Rcon(6)     = 40000000
Rcon(7)     = 80000000
Rcon(8)     = 1B000000
Rcon(9)     = 36000000
Rcon(10)    = 6C000000
Rcon(11)    = D8000000
Rcon(12)    = AB000000
Rcon(13)    = 4D000000
Rcon(14)    = 9A000000
```

Figure 1: Tabela do Rcon.

- ek: Consiste em pegar os 4 bytes de um round

The input will be 16 byte Key: **0f1571c947d9e8590cb7add6af7f6798**

The output will be **keywords** (w0 to w43) as shown in the table below.

Key Words	Auxiliary Function
w0 = 0f 15 71 c9 w1 = 47 d9 e8 59 w2 = 0c b7 ad d6 w3 = af 7f 67 98	RotWord(w3)= 7f 67 98 af = x1 SubWord(x1)= d2 85 46 79 = y1 Rcon(1)= 01 00 00 00 y1 ⊕ Rcon(1)= d3 85 46 79 = z1
w4 = w0 ⊕ z1 = dc 90 37 b0 w5 = w4 ⊕ w1 = 9b 49 df e9 w6 = w5 ⊕ w2 = 97 fe 72 3f w7 = w6 ⊕ w3 = 38 81 15 a7	RotWord(w7)= 81 15 a7 38 = x2 SubWord(x4)= 0c 59 5c 07 = y2 Rcon(2)= 02 00 00 00 y2 ⊕ Rcon(2)= 0e 59 5c 07 = z2
w8 = w4 ⊕ z2 = d2 c9 6b b7 w9 = w8 ⊕ w5 = 49 80 b4 5e w10 = w9 ⊕ w6 = de 7e c6 61 w11 = w10 ⊕ w7 = e6 ff d3 c6	RotWord(w11)= ff d3 c6 e6 = x3 SubWord(x2)= 16 66 b4 8e = y3 Rcon(3)= 04 00 00 00 y3 ⊕ Rcon(3)= 12 66 b4 8e = z3
w12 = w8 ⊕ z3 = c0 af df 39 w13 = w12 ⊕ w9 = 89 2f 6b 67 w14 = w13 ⊕ w10 = 57 51 ad 06 w15 = w14 ⊕ w11 = b1 ae 7e c0	RotWord(w15)= ae 7e c0 b1 = x4 SubWord(x3)= e4 f3 ba c8 = y4 Rcon(4)= 08 00 00 00 y4 ⊕ Rcon(4)= ec f3 ba c8 = 4
w16 = w12 ⊕ z4 = 2c 5c 65 f1 w17 = w16 ⊕ w13 = a5 73 0e 96 w18 = w17 ⊕ w14 = f2 22 a3 90 w19 = w18 ⊕ w15 = 43 8c dd 50	RotWord(w19)= 8c dd 50 43 = x5 SubWord(x4)= 64 c1 53 1a = y5 Rcon(5)= 10 00 00 00 y5 ⊕ Rcon(5)= 74 c1 53 1a = z5
w20 = w16 ⊕ z5 = 58 9d 36 eb w21 = w20 ⊕ w17 = fd ee 38 7d w22 = w21 ⊕ w18 = 0f cc 9b ed w23 = w22 ⊕ w19 = 4c 40 46 bd	RotWord(w23)= 40 46 bd 4c = x6 SubWord(x5)= 09 5a 7a 29 = y6 Rcon(6)= 20 00 00 00 y6 ⊕ Rcon(6)= 29 5a 7a 29 = z6
w24 = w20 ⊕ z6 = 71 c7 4c c2 w25 = w24 ⊕ w21 = 8c 29 74 bf w26 = w25 ⊕ w22 = 83 e5 ef 52 w27 = w26 ⊕ w23 = cf a5 a9 ef	RotWord(w27)= a5 a9 ef cf = x7 SubWord(x6)= 06 d3 df 8a = y7 Rcon(7)= 40 00 00 00 y7 ⊕ Rcon(7)= 46 d3 df 8a = z7
w28 = w24 ⊕ z7 = 37 14 93 48 w29 = w28 ⊕ w25 = bb 3d e7 f7 w30 = w29 ⊕ w26 = 38 d8 08 a5 w31 = w30 ⊕ w27 = f7 7d a1 4a	RotWord(w31)= 7d a1 4a f7 = x8 SubWord(x7)= ff 32 d6 68 = y8 Rcon(8)= 80 00 00 00 y8 ⊕ Rcon(8)= 7f 32 d6 68 = z8
w32 = w28 ⊕ z8 = 48 26 45 20 w33 = w32 ⊕ w29 = f3 1b a2 d7 w34 = w33 ⊕ w30 = cb c3 aa 72 w35 = w34 ⊕ w32 = 3c be 0b 38	RotWord(w35)= be 0b 38 3c = x9 SubWord(x8)= ae 2b 07 eb = y9 Rcon(9)= 1B 00 00 00 y9 ⊕ Rcon(9)= b5 2b 07 eb = z9
w36 = w32 ⊕ z9 = fd 0d 42 cb w37 = w36 ⊕ w33 = 0e 16 e0 1c w38 = w37 ⊕ w34 = c5 d5 4a 6e w39 = w38 ⊕ w35 = f9 6b 41 56	RotWord(w39)= 6b 41 56 f9 = x10 SubWord(x9)= 7f 83 b1 99 = y10 Rcon(10)= 36 00 00 00 y10 ⊕ Rcon(10)= 49 83 b1 99 = z10
w40 = w36 ⊕ z10 = b4 8e f3 52 w41 = w40 ⊕ w37 = ba 98 13 4e w42 = w41 ⊕ w38 = 7f 4d 59 20 w43 = w42 ⊕ w39 = 86 26 18 76	

Figure 2: Exemplo mostrando o funcionamento passo a passo da extensão.

2.1.2 addroundkey

Essa etapa eh feita dando xor em cada um dos bytes do estado com os bytes da chave extendida correspondente a parte mais perto da chave que ainda nao foi utilizada, entao a primeira vez vai comparar o estado aos primeiros 16 bytes da chave, a segunda do byte 16 ao 32, a terceira do 32 ao 48 e assim em diante, ate completar os 9 rounds da criptografia e os 175 bytes da chave.

2.1.3 subbytes

Para essa etapa é só substituir cada elemento pelo correspondente na tabela de consulta forward S Box, a qual foi implementada por um dicionário com as chaves sendo uma dupla de digitos hexadecimais(1 byte) e o valor seu byte equivalente em base 16 também.

2.1.4 resubbytes

Para essa etapa é só substituir cada elemento pelo correspondente na tabela de consulta reverse S Box, a qual foi implementada por um dicionário com as chaves

sendo uma dupla de digitos hexadecimais(1 byte) e o valor seu byte equivalente em base 16 também.

2.1.5 shiftrows

Para essa etapa foi feito um deslocamento para esquerda de cada elemento da tabela um número X de vezes, sendo X o número da linha da tabela, fazendo o X número da linha ser o primeiro.

2.1.6 deshiftrows

Essa etapa foi feito o mesmo de shiftrows, porem, com deslocamento para a direita .

2.1.7 mixcolumns

Essa etapa consiste em uma multiplicar por uma matriz especifica no corpo de Galois, ou seja, essa parte funciona da seguinte forma: Para descobrir cada novo elemento na matriz, deve ser pega cada coluna e multiplicada por cada linha de uma tabela fixa mas diferente de uma multiplicação padrão de matrizes, ela deve usar a operacão xor de cada multiplicação individual no corpo de Galois para formar o valor total da multiplicação da coluna.

2.1.8 mixcolumnsinverse

Essa etapa foi feito o mesmo de mixcolumns, porem, com uma tabela diferente.

2.2 Cifracao

Para cifrar foi implementada uma funcao round que aplica 5 etapas:subbytes,bytes to block,shift rows,mixcolumns e addroundkey.E uma funcao encryption que define quantas rodadas vai ter a cifra, chamando a funcao round esse numero de vezes.

2.3 Decifracao

3 Implementacao CTR

4 Conclusao