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 funcoes

2.1.1 keyexpansion

2.1.2 addroundkey

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.

```
def round(dado,last):
    dado = subbytes(dado)
    dado = bytes_to_block(dado)
    dado = shift_rows(dado)
    if last == True:
        pass
    else:
        dado = mixcolumns(dado)
    addroundkey()
    return dado
def encryption(number,dado):
n=0
while n < number:
    if n == 0:
        dado = round(dado,True)
    elif n == number:
        dado = block_to_bytes(dado)
        dado = round(dado,True)
    else:
        dado = block_to_bytes(dado)
        dado = round(dado,False)
    n+=1
```

```
return dado
```

2.3 Decifracao

3 Implementacao CTR

4 Conclusao