Segurança Computacional - Relatório Trabalho 2

Felipe Fontenele dos Santos - 190027622

Novembro 2023

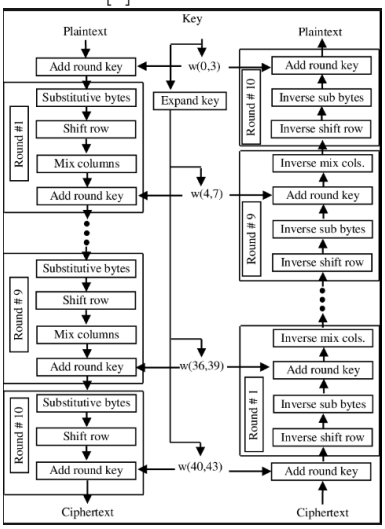
1 Introdução

Este relatório descreve a implementação bem-sucedida da cifra AES (Advanced Encryption Standard) com blocos de 128 bits e chaves de 128 bits utilizando a linguagem de programação python, juntamente com o modo de operação CTR (Counter Mode) em conformidade com o que foi exigido na especificação do trabalho em questão. O objetivo principal foi criar uma implementação funcional do AES e do CTR, permitindo a cifração e decifração de arquivos. O relatório também detalha as partes que foram concluídas, aquelas que não foram implementadas e quais partes do trabalho precisam ser aprimoradas.

2 Desenvolvimento

2.1 AES

A implementação da cifração e decifração do AES foi feita seguindo o algorítimo já existente [1].



1. Valida state: é feito uma validação nos valores e no tamanho da matriz state para garantir que ela é 4x4 e todos seus valores estão dentro dos 255 valores permitidos.

2. Realiza geração da chave da rodada: é feita uma conversão da chave de entrada em uma matriz de 128 bits, verifica-se se o tamanho da matriz é igual a 128 e inicia um loop que faz a substituição, rotação e combinação dos bytes nas colunas da matriz da chave da rodada anterior gerando novas colunas.

3. Adiciona a chave da rodada: antes de começar a realizar os rounds, é realizada a geração da chave e a passada 0 na chave da rodada fazendo o xor entre os dois elementos de cada um dos valores da matriz 4 por 4 com 128 bits no total.

4. Inicia o loop no intervalo dos rounds informados: inicia realizando a subtração dos bytes, realiza o deslocamento das linhas, embaralha as colunas (utilizando a multiplicação de galois) e, ao final, atualiza a chave da rodada.

5. Fim: ao final, realiza a subtração, o deslocamento e a última atualização da chave da rodada para retornar a matriz 4x4 com o resultado.

2.2 CTR

O programa principal tem acesso ao método AES apenas através dos métodos ctr_cipher e ctr_decipher.

- ctr_cipher (**Cifragem no Modo Counter - CTR**): Este método é responsável por cifrar dados usando o modo de operação CTR em conjunto com um algoritmo de criptografia AES. Ele recebe como parâmetro o texto a ser cifrado e a chave utilizada na cifra. De inicío, o texto simples é convertido em bytes no formato UTF-8 e armazenado. Os bytes são divididos em blocos de 16 bytes (128 bits), e quaisquer bytes extras que não preencham um bloco completo são armazenados separadamente na variável pt_end. Para cada bloco de texto simples ele gera um "bloco contador" com base na chave. O bloco de texto de entrada é cifrado realizando um XOR com a saída da cifra AES e o mesmo é adicionado à uma lista. Todos os blocos cifrados são unidos em um único objeto de bytes e retornados como resultado da cifragem.

- ctr_decipher (**Decifragem no Modo Counter - CTR**): Método responsável por realizar a decifragem. Recebe uma chave, o texto cifrado e a quantidade de rounds a ser interado. Os passos inciais são bem semelhantes ao de realizar a cifra em si. Ao realizar a iteração ele faz um XOR com o bloco contador e a saída de decifragem AES. No final, ele faz um XOR também entre os bytes extras e uma parte truncadad a saída da cifra AES e retorna o texto simples decifrado como como uma string unicode.

3 Executando o código

Para executar o código, basta utilizar o compilador do python chamando o arquivo *main.py* na pasta raiz da seguinte maneira:

```
python3 main.py
```

4 Conclusão

A implementação atende satisfatoriamente aos requisitos da parte I do trabalho, permitindo a cifragem e decifragem de arquivos. No entanto, é importante observar que os testes de corretudo utilizando o openssl não foi realizado e não foi realizada também o desafio da imagem. Além disso, o modo de cifração autenticada GCM ainda não foi implementado.

Portanto, embora haja desafios não totalmente superados, a implementação pode ser considerada bem-sucedida. Podemos afirmar que o processo foi relativamente simples e, em certa medida, até mesmo divertido.

References

[1] Daniel Vecchiato. *Criptografia e Segurança de Dados - AES (Advanced Encryption Standard)*. 2020. URL: https://www.youtube.com/watch?v=-lybDqNi-bM.