UNIVERSIDADE DE BRASÍLIA
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO

CIC0201 - Segurança Computacional - 2023.2 - Turma 01

Trabalho de Implementação 2

Cifra de bloco e modo de operação

CTR

Rafael Rodrigues Gama D. de Aragão - 190134780

1. Introdução

Este trabalho explora a cifra de bloco AES (Advanced Encryption Standard) de 128 bits e o modo de operação CTR (contador), tendo três partes: implementação da cifra, do modo de operação e teste. A cifra de bloco AES é um algoritmo de criptografia simétrica que utiliza uma série de transformações matemáticas, como substituições não-lineares, permutações e operações de mistura, para garantir a confidencialidade dos dados. A cifra opera em blocos de 128 bits de dados e pode utilizar chaves de 128, 192 ou 256 bits para realizar a criptografia e a descriptografia. Neste trabalho, é implementada a versão de chave de 128 bits.

2. Fundamentação teórica

O Advanced Encryption Standard (AES) especifica um algoritmo criptográfico aprovado pelo FIPS que pode ser usado para proteger dados eletrônicos. O algoritmo AES é uma cifra de bloco simétrico que pode criptografar (codificar) e descriptografar (decifrar) informações. O algoritmo AES é capaz de usar chaves criptográficas de 128, 192 e 256 bits para criptografar e descriptografar dados em blocos de 128 bits.

O AES utiliza blocos de 128 bits para cifração, isso significa que se a mensagem a ser cifrada não tiver um número de bits múltiplo desse valor, é necessário que haja um preenchimento (*padding)*. Para isso, é utilizado o *PKCS padding method* que adiciona bytes a mensagem antes dela ser criptografada. Após isso, a mensagem é dividida em blocos de 16 bytes (128 bits) que é chamado de estado. Cada estado passa pelo processo de cifração. No modo de operação de bloco ECB (*Electronic Codebook)*, os estados, após serem criptografados, são concatenados e resultam na mensagem cifrada.

Durante o processo de cifração do AES o estado passa por várias rodadas de manipulações, cada rodada recebe o estado atual e retorna ao estado após certa manipulação. Por padrão, para chaves de 128 bits, são realizadas 11 rodadas de cifração, sendo que a primeira e a última rodada possuem um comportamento específico. Cada rodada necessita de uma chave de 128 bits diferente. Desse modo, são derivadas 11 chaves a partir da chave inicial, utilizando o algoritmo *Rijndael's key schedule*.

Cada rodada utiliza uma ou mais das operações abaixo.

AddRoundKey

Consiste na operação de XOR bit a bit do estado com a chave.

SubBytes

Consiste na substituição de cada byte por outro de acordo com uma caixa de substituição (S-Box).

ShiftRows

Consiste em organizar o estado em uma matriz 4x4 coluna por coluna e depois realizar um deslocamento de cada linha para a esquerda. Cada linha i é deslocada i vezes para a esquerda, com i variando de 0 a 3.

MixColumns

Consiste na multiplicação entre matrizes no espaço de Galois do estado pela matriz mostrada abaixo. Essa multiplicação é feita utilizando a multiplicação no campo de Galois, que consiste no XOR entre 2 bytes.

2 3 1 1
1 2 3 1
1 1 2 3
3 1 1 2

Etapas

Para uma encriptação de 128 bits o algoritmo AES realiza as seguintes etapas:

Primeira rodada:
- AddRoundKey

Rodadas 2 à 9:
- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

Rodada final (totalizando 11 rodadas):
- SubBytes
- ShiftRows
- AddRoundKey

Decifração

Para decifração, o algoritmo segue as mesmas etapas na ordem inversa, além de inverter a lógica de algumas etapas. A decifração utiliza as chaves de trás para frente. AddRoundKey não é modificada pois a operação XOR é investível. ShiftRows é substituída por InvShiftRows em que as linhas do estado são deslocadas de volta para a posição original. SubBytes é substituída por InvSubBytes que utiliza a tabela de substituição invertida. MixColumns é substituída por InvMixColumns que utiliza a matriz abaixo.

0E 0B 0D 09
09 0E 0B 0D
0D 09 0E 0B
0B 0D 09 0E

Modo CTR

Diferente do modo ECB em que cada estado é cifrado utilizando a mesma chave, permitindo que um mesmo texto seja cifrado da mesma forma, no modo CTR cada estado utiliza uma chave diferente. A chave é formada por um vetor de inicialização somado a um contador. A soma é então cifrada utilizando o algoritmo de cifração do AES e o resultado é utilizado para cifrar o texto fazendo a operação XOR entre o estado e a chave cifrada. A cada bloco cifrado o contador é incrementado em um, fazendo com que cada bloco seja cifrado com uma chave diferente.

3. Metodologia

Para implementação da cifra foi utilizada a linguagem de programação Python. O código está disponível em https://github.com/rafael2903/AES-128-cipher. O arquivo AES.py contém a implementação das funções de encriptação e desencriptação. O arquivo tests.py contém alguns testes unitários que testam essas funções. Para executar os testes é necessário rodar o comando `python -m unittest -v tests.py`.Também foi adicionado ao programa uma interface de linha de comando, sendo possível executar todas as funções pelo terminal passando um arquivo de entrada. A seguir são mostrados alguns exemplos de utilização dessa interface.

Encriptação

```
python AES.py -e -in text.txt -out text.enc -k
2b7e151628aed2a6abf7158809cf4f3c -m CTR -iv
00112233445566778899aabbccddeeff -v
```

Desencriptação

```
python AES.py -d -in text.enc -out text.txt -k
2b7e151628aed2a6abf7158809cf4f3c -m CTR -iv
00112233445566778899aabbccddeeff -v
```

Mais informações sobre o uso estão disponíveis no GitHub citado.

4. Conclusão

Este trabalho possibilitou o aprofundamento e a prática dos conhecimentos em criptografia avançada por meio da implementação da cifra AES-128 no modo de operação CTR. Além disso, fortaleceu nossas habilidades de programação e resolução de problemas, enriquecendo nosso conhecimento em segurança da informação e contribuindo significativamente para nossa formação acadêmica nessa área.

5. Referências

- Advanced Encryption Standard. Disponível em: <https://pt.wikipedia.org/wiki/Advanced_Encryption_Standard>.
- Rijndael S-box. Disponível em: <https://en.wikipedia.org/wiki/Rijndael_S-box>.
- AES - Padrão de criptografia avançado: o que é e como funciona. Disponível em: <https://cryptoid.com.br/criptografia/aes-padrao-de-criptografia-avancado-o-que-e-e-como-funciona/>.
- Rijndael's key schedule. Disponível em: <https://www.samiam.org/key-schedule.html>.
- AES' Galois field. Disponível em: <https://www.samiam.org/galois.html>. Acesso em: 29 out. 2023.
- Written By: Adam Berent AES (Advanced Encryption Standard) Simplified. [s.l: s.n.]. Disponível em: <https://www.ime.usp.br/~rt/cranalysis/AESSimplified>. Acesso em: 29 out. 2023.
- PKCS padding method. Disponível em: <https://www.ibm.com/docs/en/zos/2.4.0?topic=rules-pkcs-padding-method>.
- WIKIPEDIA CONTRIBUTORS. Block cipher mode of operation. Disponível em: <https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation>.