Criptografia - AES

Larissa Fiorini Martins

Escola Politécnica – Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
Porto Alegre – RS – Brasil

larissa.martins@edu.pucrs.br

Abstract. *This article describes an implementation of a program that does encryption and decryption of a text using AES (Advanced Encryption Standard) with operation modes CBC and CTR, with a known key. The program behavior will be detailed, with a description of the operation modes and the results obtained.*

Resumo. *Este artigo descreve uma implementação de um programa que cifra e decifra um texto usando a cifra de blocos AES (Advanced Encryption Standard) com os modos de operação CBC e CTR, sendo a chave utilizada conhecida. Será detalhado o funcionamento do programa, com uma descrição dos modos de operação e, por fim, serão mostrados os resultados obtidos.*

1. Introdução

O *AES* (*Advanced Encryption Standard*) é uma cifra de blocos simétrica bastante utilizada atualmente que surgiu em 1997 como sucessor do *DES (Data Encryption Standard)*, que estava começando a ser vulnerável à ataques de força bruta por possuir uma chave de tamanho muito pequeno *(NIST, 2019)*. O *AES* é uma criptografia confiável que possui um tamanho de bloco fixo em 128 *bits*, e uma chave com tamanho de 128, 192 ou 256 *bits*.

Neste artigo será apresentada uma implementação em *Java* para cifrar e decifrar um texto com *AES* e uma chave conhecida. Será mostrada uma descrição do funcionamento do código e dos modos de operação utilizados. As tarefas propostas foram inseridas no programa através de testes unitários que podem ser executados para a realização da cifragem e decifragem com os diferentes modos de operação.

2. Modos de operação

As criptografias simétricas de blocos, como o *AES*, contam com diversos modos de operação para melhorar ou obter diferentes resultados. Neste trabalho a implementação foi realizada utilizando os modos de operação *CBC* e *CTR*. O modo de operação *CBC* (*Cypher Block Chaining)* se caracteriza por em cada bloco de texto claro ser realizado a operação *XOR* junto com o bloco cifrado anterior antes de ele ser criptografado, assim os blocos futuros são dependentes dos blocos anteriores. Dessa forma, utilizando um *IV* aleatório, é possível manter a aleatoriedade do texto cifrado. No modo de operação CTR (*Counter)* ocorre a transformação da cifra de bloco em cifra de fluxo, utilizando um contador para gerar aleatoriedade. Para cifrar e decifrar o texto é também necessário escolher um *padding*. Para essa implementação, no *CTR* não foi utilizado *padding* e no *CBC* utilizou-se o "*PKCS5",* conforme parâmetros abaixo, que correspondem à *"algorithm/mode/padding"*:

"AES/CTR/NoPadding"

"AES/CBC/PKCS5Padding"

Figura 1. Modos de operação

3. Cifragem do texto

Para a cifragem do texto claro em hexadecimal é necessário a utilização da senha e da geração de um *IV* (vetor de inicialização) de 16 *bytes,* que consiste em um bloco escolhido de maneira aleatória e anexado na frente do texto cifrado, com o objetivo de gerar aleatoriedade no sistema (Oracle, 2019). Para a execução da cifragem no sistema implementado é necessário fornecer o texto claro, a chave e o modo de operação que se deseja utilizar.

4. Decifragem do texto

Para a decifragem do texto em hexadecimal, primeiramente, é extraído do texto cifrado o *IV* de 16 *bytes* em hexadecimal que foi anexado na frente do texto durante a cifragem. Após, será realizada a decifragem do texto cifrado utilizando esse *IV* e a chave. Para a execução da decifragem no sistema implementado é necessário fornecer o texto cifrado, a chave e o modo de operação.

5. Resultados obtidos

5.1 Tarefa 1 - Decifrar com modo de operação CBC

CBC key: *140b41b22a29beb4061bda66b6747e14*
CBC Ciphertext:
4ca00ff4c898d61e1edbf1800618fb2828a226d160dad07883d04e008a7897ee
2e4b7465d5290d0c0e6c6822236e1daafb94ffe0c5da05d9476be028ad7c1d81
Resultado: “Basic CBC mode encryption needs padding.”

5.2 Tarefa 2 - Decifrar com modo de operação CBC

CBC key: *140b41b22a29beb4061bda66b6747e14*
CBC Ciphertext:
5b68629feb8606f9a6667670b75b38a5b4832d0f26e1ab7da33249de7d4afc48
e713ac646ace36e872ad5fb8a512428a6e21364b0c374df45503473c5242a253
Resultado: “Our implementation uses rand. IV”

5.3 Tarefa 3 - Decifrar com modo de operação CTR

CTR key: *36f18357be4dbd77f050515c73fcf9f2*
CTR Ciphertext:
69dda8455c7dd4254bf353b773304eec0ec7702330098ce7f7520d1cbbb20fc3
88d1b0adb5054dbd7370849dbf0b88d393f252e764f1f5f7ad97ef79d59ce29f5f
51eeca32eabedd9afa9329
Resultado: “CTR mode lets you build a stream cipher from a block cipher.”

5.4 Tarefa 4 - Decifrar com modo de operação CTR

CTR key: *36f18357be4dbd77f050515c73fcf9f2*
CTR Ciphertext:
770b80259ec33beb2561358a9f2dc617e46218c0a53cbeca695ae45faa8952aa
0e311bde9d4e01726d3184c34451
Resultado: “Always avoid the two time pad!”

5.5 Tarefa 5 - Cifrar com modo de operação CTR

CTR key: *36f18357be4dbd77f050515c73fcf9f2*
CTR Plaintext:
5468697320697320612073656e74656e636520746f20626520656e6372797074656420757369 6e67204145532061 6e6420435452206d6f64652e
Resultado:
37333EEE7D0B5093D298EBEE6A621A964B504FD1CC6FE158BA8D5B2203A207D71F29 7C3E97DD1268628E9DF33BC18C05D5E434D8F3FD7D74CD9F6D8437387EB9119F48C C15B8A64640DD824C844B718DE631065B496600E3FA15D9CCDC330EB900FEE7A...

5.6 Tarefa 6 - Cifrar com modo de operação CBC

CTR key: *140b41b22a29beb4061bda66b6747e14*
CTR Plaintext:
4e6578742054687572736461792 06f6e65206f662074686520626573742074656 16d7320696e 2074686520776f726c642077696c6c20666163652061206269672063686 16c6c656e67652069 6e20746865204c6962657274616 46f72657320646120416d6572696361204368616d70696f6e 736869702e
Resultado:
37333EEE7D0B5093D298EBEE6A621A964B504FD1CC6FE158BA8D5B2203A207D71F29 7C3E97DD1268628E9DF33BC18C05D5E434D8F3FD7D74CD9F6D8437387EB9119F48C C15B8A64640DD824C844B718DE631065B496600E3FA15D9C...

6. Conclusão

O desenvolvimento deste trabalho permitiu um melhor entendimento do funcionamento do *AES* bem como seu desenvolvimento na linguagem *Java,* que possui bibliotecas que possibilitam facilitar a implementação e também configurar os detalhes da cifragem e decifragem com os modos de operação desejados. Conclui-se que a implementação atingiu seu objetivo pois conseguiu com sucesso cifrar e decifrar os textos propostos.

Referências

NIST - National Institute of Standards and Technology(2019) “Advanced Encryption Standard”, https://www.nist.gov/publications/advanced-encryption-standard-aes.

Tutorials Point (2019) “Advanced Encryption Standard”, https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm.

Oracle (2019) “Cipher”,

http://docs.oracle.com/javase/7/docs/api/javax/crypto/Cipher.html

Oracle (2019) “Secure Random”,

https://docs.oracle.com/javase/8/docs/api/java/security/SecureRandom.html