Trabalho 2
Cifra de AES

Lucas Resende Silveira Reis, 18/0144421

[1]Dep. Ciência da Computação – Universidade de Brasília (UnB)
CiC 0201 - SEGURANÇA COMPUTACIONAL

toy.lcdv@hotmail.com

Abstract. *This corresponds to project 2, on encryption, decipherment on the AES Cipher.*

Resumo. *Este corresponde ao trabalho 2, sobre cifração, decifração sobre a Cifra de AES.*

1. Introdução

O AES (Advanced Encryption Standard) é uma primitiva criptográfica projetada para ser utilizada na construção de sistemas de criptografia simétrica, onde a mesma chave é usada tanto para cifrar quanto para decifrar dados. Ele é um algoritmo de cifra de bloco, o que significa que ele opera em blocos de tamanho fixo, geralmente 128 bits (ou 16 bytes). Embora seja possível transformá-lo em uma cifra de fluxo para trabalhar com dados de tamanho arbitrário por meio de modos de operação específicos, esse detalhe não é abordado neste contexto. O AES é compatível com diferentes tamanhos de chave, sendo possível utilizá-lo com chaves de 128, 192 ou 256 bits (o algoritmo Rijndael, do qual o AES se originou, permite uma gama maior de tamanhos de chave).

1.1. Parte 1

Aqui foi pedido para implementar cifração e decifração AES de forma que fosse possível escolher o número de rodadas que deseja executar. Para entendermos sobre o AES precisamos de entender um pouco sobre os seguintes temas:

- **Corpos Finitos**: No AES, todas as operações são realizadas em corpos finitos (Galois fields) de 2^8 elementos. Isso envolve operações de adição e multiplicação, onde cada elemento tem um inverso, exceto o zero. A adição é realizada com a operação XOR, e a multiplicação envolve polinômios binários e um ”agente redutor”para manter o resultado dentro do campo.
- **Rijndael S-Box**: A Rijndael S-Box é uma tabela de consulta usada no AES para transformar bytes de entrada em bytes diferentes de forma não linear. Ela opera em cima dos elementos do corpo finito e envolve o cálculo do inverso multiplicativo de um byte, seguido por uma transformação afim. Essa tabela foi projetada para resistir a ataques lineares ou diferenciais.
- **Expansão da Chave**: A expansão da chave no AES envolve a derivação de várias sub-chaves a partir da chave original. Isso é feito usando o algoritmo Rijndael Key Schedule, que produz um conjunto de sub-chaves de 128 bits para cada rodada do algoritmo, dependendo do tamanho da chave (128, 192 ou 256 bits).

- **Rodadas**: O AES opera em múltiplas rodadas, onde cada rodada aplica uma série de operações reversíveis no estado. Isso inclui a adição da chave da rodada, transformações não-lineares dos bytes do estado usando o S-Box, rotações das linhas da matriz do estado e combinações das colunas. As operações são projetadas para garantir que pequenas alterações na chave ou na mensagem resultem em mudanças significativas na cifra, aumentando a segurança do algoritmo.

Essas operaçõessão quebradas nas seguintes funções: ADD ROUND KEY, BYTE SUB, SHIFT ROW , MIX COLUMN.

Aqui podemos ver os resultados da cifração e decifração:

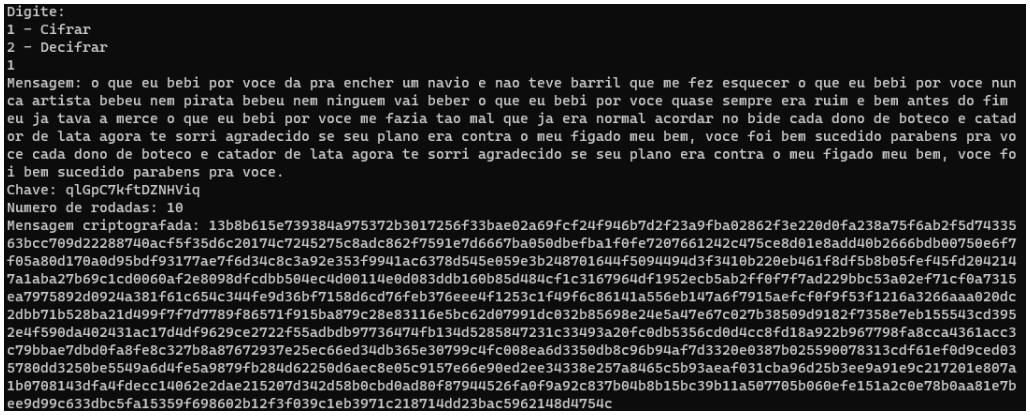

Figura 1. Resultado Cifração

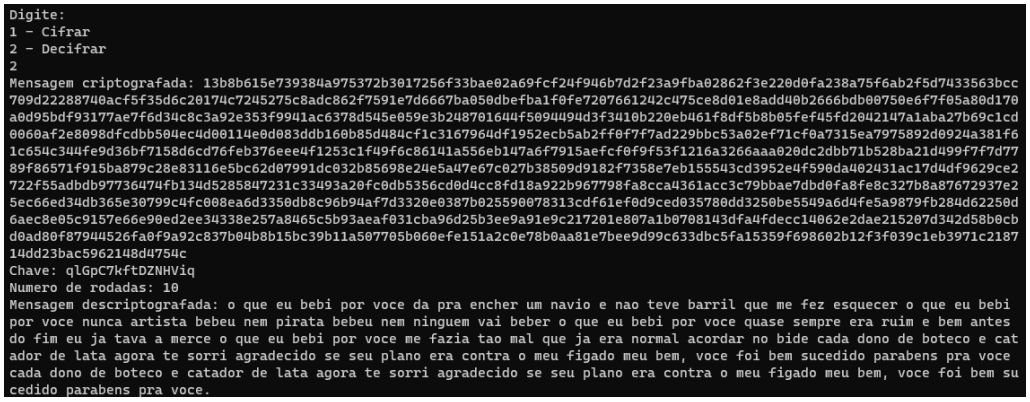

Figura 2. Resultado Decrifração

2. Conclusão

Em resumo, o Advanced Encryption Standard (AES) é um algoritmo de criptografia simétrica altamente confiável e amplamente adotado. Sua base em corpos finitos, a utilização da tabela Rijndael S-Box, a expansão da chave e as múltiplas rodadas de transformações contribuem para sua robustez e resistência a ataques. O AES desempenha um papel fundamental na proteção de dados sensíveis em sistemas de comunicação e armazenamento, oferecendo segurança sólida por meio de sua estrutura matemática e complexidade algorítmica..

Referências

[1] Como funciona o algoritmo de criptografia AES?
https://pt.stackoverflow.com/questions/43492/como-funciona-o-algoritmo-de-criptografia-aes

[2] Rijndael S-box.
https://en.wikipedia.org/wiki/Rijndael_S-box

[3] AES (Advanced Encryption Standard) Simplified
https://www.ime.usp.br/~rt/cranalysis/AESSimplified

[4] Multiple Lookup Table-Based AES Encryption Algorithm Implementation
https://www.sciencedirect.com/science/article/pii/S1875389212005822/pdf?md5=cae0d5bfea1fddc8ab1e89306c2be733&pid=1-s2.0-S1875389212005822-main.pdf

[5] Criptografia e Segurança de Dados - AES (Advanced Encryption Standard)
https://youtu.be/-lybDqNi-bM?si=aNNE16qeMnYcwcqh