

Trabalho 2

Cifra de AES

Lucas Resende Silveira Reis, 18/0144421

¹Dep. 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 operações são quebradas nas seguintes funções: ADD ROUND KEY, BYTE SUB, SHIFT ROW, MIX COLUMN.

Aqui podemos ver os resultados da cifração e decifração:

```
Digite:
1 - Cifrar
2 - Decifrar
1
Mensagem: o que eu bebi por voce da pra encher um navio e nao teve barril que me fez esquecer o que eu bebi por voce nun
ca artista bebeu nem pirata bebeu nem ninguém vai beber o que eu bebi por voce quase sempre era ruim e bem antes do fim
eu ja tava a merce o que eu bebi por voce me fazia tao mal que ja era normal acordar no bide cada dono de boteco e catad
or de lata agora te sorri agradecido se seu plano era contra o meu figado meu bem, voce foi bem sucedido parabens pra vo
ce cada dono de boteco e catador de lata agora te sorri agradecido se seu plano era contra o meu figado meu bem, voce fo
i bem sucedido parabens pra voce.
Chave: qLpC7kftDZNVHViQ
Numero de rodadas: 10
Mensagem criptografada: 13b8b615e739384a975372b3017256f33bae02a69fcf24f946b7d2f23a9fba02862f3e220d0fa238a75f6ab2f5d74335
63bcc709d2288740acf5f35d6c20174c7245275c8adc862f7591e7d6667ba050dbefbaf0fe7207661242c475ce8d01e8add40b2666bdb00750e6f7
f05a80d170a0d95bdf93177ae7f6d34c8c3a92e353f9941ac6378d545e059e3b248701644f5094494d3f3410b220eb461f8df5b8b05fef45fd204214
7alaba27b69c1cd0060af2e8098dfcddb504ec4d00114e0d083ddb160b85d484cf1c3167964df1952ecb5ab2ff0f7f7ad229bbc53a02ef71cf0a7315
ea7975892d0924a381f61c654c344fe9d36bf7158d6cd76feb376eee4f1253c1f49f6c86141a556eb147a6f7915aefcf0f9f53f1216a3266aaa020dc
2dbb71b528ba21d499f7f7d7789f86571f915ba879c28e83116e5bc62d07991dc032b85698e24e5a47e67c027b38509d9182f7358e7eb155543cd395
2e4f590da402431ac17d4df9629ce2722f55adbdb97736474fb134d5285847231c33493a20fc0db5356cd0d4cc8fd18a922b967798fa8cca4361acc3
c79bbae7dbd0fa8fe8c327b8a87672937e25ec66ed34db365e30799c4fc008ea6d3350db8c96b94af7d3320e0387b025590078313cdf61ef0d9ced03
5780dd3250b5549a6d4fe5a9879fb284d62250d6a8e05c9157e66e90ed2ee34338e257a8465c5b93aea031cba96d25b3ee9a91e9c217201e807a
1b0708143dfa4fdecc14062e2dae215207d342d58b0cb0ad80f87944526fa0f9a92c837b04b8b15bc39b11a507705b060efe151a2c0e78b0aa81e7b
ee9d99c633dbc5fa15359f698602b12f3f039c1eb3971c218714dd23bac5962148d4754c
```

Figura 1. Resultado Cifração

```
Digite:
1 - Cifrar
2 - Decifrar
2
Mensagem criptografada: 13b8b615e739384a975372b3017256f33bae02a69fcf24f946b7d2f23a9fba02862f3e220d0fa238a75f6ab2f5d7433563bcc
709d2288740acf5f35d6c20174c7245275c8adc862f7591e7d6667ba050dbefbaf0fe7207661242c475ce8d01e8add40b2666bdb00750e6f7f05a80d170
a0d95bdf93177ae7f6d34c8c3a92e353f9941ac6378d545e059e3b248701644f5094494d3f3410b220eb461f8df5b8b05fef45fd2042147alaba27b69c1cd
0060af2e8098dfcddb504ec4d00114e0d083ddb160b85d484cf1c3167964df1952ecb5ab2ff0f7f7ad229bbc53a02ef71cf0a7315ea7975892d0924a381f6
1c654c344fe9d36bf7158d6cd76feb376eee4f1253c1f49f6c86141a556eb147a6f7915aefcf0f9f53f1216a3266aaa020dc2dbb71b528ba21d499f7f7d77
89f86571f915ba879c28e83116e5bc62d07991dc032b85698e24e5a47e67c027b38509d9182f7358e7eb155543cd3952e4f590da402431ac17d4df9629ce2
722f55adbdb97736474fb134d5285847231c33493a20fc0db5356cd0d4cc8fd18a922b967798fa8cca4361acc3c79bbae7dbd0fa8fe8c327b8a87672937e2
5ec66ed34db365e30799c4fc008ea6d3350db8c96b94af7d3320e0387b025590078313cdf61ef0d9ced035780dd3250b5549a6d4fe5a9879fb284d62250d
6a8e05c9157e66e90ed2ee34338e257a8465c5b93aea031cba96d25b3ee9a91e9c217201e807a1b0708143dfa4fdecc14062e2dae215207d342d58b0cb
d0ad80f87944526fa0f9a92c837b04b8b15bc39b11a507705b060efe151a2c0e78b0aa81e7bee9d99c633dbc5fa15359f698602b12f3f039c1eb3971c2187
14dd23bac5962148d4754c
Chave: qLpC7kftDZNVHViQ
Numero de rodadas: 10
Mensagem descryptografada: o que eu bebi por voce da pra encher um navio e nao teve barril que me fez esquecer o que eu bebi
por voce nunca artista bebeu nem pirata bebeu nem ninguém vai beber o que eu bebi por voce quase sempre era ruim e bem antes
do fim eu ja tava a merce o que eu bebi por voce me fazia tao mal que ja era normal acordar no bide cada dono de boteco e cat
ador de lata agora te sorri agradecido se seu plano era contra o meu figado meu bem, voce foi bem sucedido parabens pra voce
cada dono de boteco e catador de lata agora te sorri agradecido se seu plano era contra o meu figado meu bem, voce foi bem su
cedido parabens pra voce.
```

Figura 2. Resultado Decifração

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=cae0d5bfeafddc8able89306c2be733&pid=1-s2.0-S1875389212005822-main.pdf>
- [5] Criptografia e Segurança de Dados - AES (Advanced Encryption Standard)
<https://youtu.be/-lybDqNi-bM?si=aNNE16qeMnYcwcqh>