Universidade de Brasília

FACULDADE DE TECNOLOGIA

Trabalho de Implementação 2

Cifra de Bloco e Modos de Operação

AUTORES:

João Vitor de Almeida Lima – 170079813
Álvaro Marçal de Araújo – 202066858

2025

Contents

1 Introdução

A segurança da informação é um tema crucial na era digital, sendo a criptografia uma ferramenta indispensável para garantir a confidencialidade, integridade e autenticidade dos dados. Este trabalho tem como foco a cifra AES (Advanced Encryption Standard), uma das mais seguras e amplamente utilizadas no mundo, e os modos de operação ECB (Electronic Codebook) e GCM (Galois/Counter Mode).Nesta etapa do trabalho, foi realizada a implementação da cifra AES, abordando sua estrutura interna e as operações envolvidas.

2 Objetivos

O principal objetivo desta etapa é implementar a cifra AES, configurável para diferentes números de rodadas, e documentar suas características e funcionalidades. Além disso, é apresentado um estudo teórico dos modos de operação ECB e GCM.

3 Fundamentação Teórica

3.1 Cifra AES

3.1.1 Estrutura Geral

A cifra AES (Advanced Encryption Standard) é uma cifra de bloco que opera em blocos de 128 bits, utilizando chaves de 128, 192 ou 256 bits. Sua estrutura baseia-se em rodadas que incluem as operações SubBytes, ShiftRows, MixColumns e AddRoundKey, projetadas para garantir a segurança contra ataques como análise diferencial e linear.

3.1.2 Operações Principais

As principais operações da AES incluem:

- **SubBytes:** Substitui cada byte do bloco por um valor correspondente na tabela S-Box, introduzindo não-linearidade.
- **ShiftRows:** Desloca os bytes das linhas do bloco para a esquerda, misturando os dados horizontalmente.
- **MixColumns:** Combina os bytes de cada coluna utilizando operações no campo finito GF(2^8), garantindo mistura vertical.
- **AddRoundKey:** Aplica uma chave de rodada ao bloco por meio de uma operação XOR.

3.2 Modos de Operação

3.2.1 Modo ECB (Electronic Codebook)

O modo ECB é o mais simples entre os modos de operação. Ele divide o texto plano em blocos de tamanho fixo (geralmente 128 bits) e cifra cada bloco independentemente utilizando a mesma chave. Apesar de sua simplicidade, o ECB apresenta uma falha significativa: blocos de texto plano idênticos resultam em blocos de texto cifrado idênticos.

Isso significa que padrões no texto plano podem ser facilmente detectados no texto cifrado, tornando o modo inadequado para a maioria das aplicações práticas, especialmente aquelas que envolvem grandes volumes de dados ou dados repetitivos.

Esse modo é utilizado principalmente em cenários onde a confidencialidade básica é suficiente e não há necessidade de ocultar padrões, como em certos sistemas de armazenamento local de dados. No entanto, devido às suas limitações, o uso do ECB é geralmente desaconselhado em sistemas que exigem alta segurança.

3.2.2 Modo GCM (Galois/Counter Mode)

O modo GCM é um modo de operação avançado que combina cifração e autenticação de dados. Ele utiliza o modo CTR (Counter Mode) como base para a cifração e um algoritmo de autenticação baseado no campo finito Galois para garantir a integridade dos dados. Cada bloco é cifrado utilizando um contador único, que é incrementado para cada bloco, garantindo que blocos idênticos de texto plano resultem em textos cifrados diferentes.

Além da cifração, o GCM gera um código de autenticação (tag) que pode ser utilizado para verificar a integridade e autenticidade dos dados cifrados. Isso o torna ideal para aplicações como comunicações seguras (e.g., HTTPS), VPNs e sistemas que exigem alta segurança e confiabilidade.

O GCM é amplamente adotado devido à sua eficiência e segurança. Ele é capaz de realizar cifração e autenticação simultaneamente, tornando-o uma escolha preferida para sistemas modernos que necessitam de proteção robusta contra ataques.

4 Implementação

4.1 Estrutura do Código

Nesta etapa, foi realizada a implementação da cifra AES, configurada para operar com chaves de 128 bits. As funções implementadas incluem:

- **Cifração:** Aplicação das operações SubBytes, ShiftRows, MixColumns e AddRoundKey em cada rodada.
- **Decifração:** Reversão do texto cifrado para o texto original utilizando as operações inversas.
- **Expansão de Chaves:** Geração de subchaves para cada rodada a partir da chave principal.

5 Conclusão

Neste trabalho, foi realizada a implementação da cifra AES, destacando suas operações fundamentais como SubBytes, ShiftRows, MixColumns e AddRoundKey. A cifra foi configurada para chaves de 128 bits, oferecendo um equilíbrio entre segurança e desempenho. Além disso, foram analisados os modos de operação ECB e GCM, evidenciando suas diferenças em termos de segurança. O modo ECB, apesar de simples, apresenta vulnerabilidades devido à repetição de padrões no texto cifrado, enquanto o GCM se destaca por combinar criptografia com autenticação de dados, tornando-o mais seguro para aplicações que exigem integridade e autenticidade.

A implementação da cifra AES e o estudo dos modos de operação fornecem uma base sólida para compreender a importância da escolha adequada de algoritmos e modos em sistemas de segurança. A AES, aliada ao GCM, oferece uma solução robusta para garantir a confidencialidade, integridade e autenticidade dos dados em diversos contextos de aplicação, como em comunicações seguras e armazenamento de dados sensíveis.

6 Referências

- Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer.
- Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson.
- FIPS PUB 197 (2001). *Advanced Encryption Standard (AES)*. National Institute of Standards and Technology (NIST).