Documentação do Algoritmo de Criptografia AES

Nome: João Vítor de Oliveira Souza - 6° ADS

1. Introdução ao AES

AES (Advanced Encryption Standard) é um algoritmo de criptografia simétrica, o que significa que utiliza a mesma chave para criptografar e descriptografar dados. AES foi desenvolvido para substituir o DES (Data Encryption Standard), oferecendo maior segurança e desempenho. O algoritmo AES é amplamente utilizado em aplicações de segurança de dados, incluindo comunicações seguras e armazenamento de informações confidenciais.

2. Principais Características

- Tipo de Algoritmo: Criptografia simétrica.
- Tamanho do Bloco: 128 bits (16 bytes).
- Tamanhos de Chave Suportados: 128, 192, ou 256 bits.
- Segurança: AES é considerado extremamente seguro quando aplicado com tamanhos de chave de 192 ou 256 bits.

3. Funcionamento do Algoritmo AES

AES opera em blocos de 128 bits (ou 16 bytes), aplicando uma série de transformações matemáticas aos dados para garantir que a mensagem original fique irreconhecível sem a chave correta. A criptografia ocorre em várias etapas ou 'rodadas', que dependem do tamanho da chave:

- Chave de 128 bits: 10 rodadas
- Chave de 192 bits: 12 rodadas
- Chave de 256 bits: 14 rodadas

Cada rodada inclui quatro operações principais:
1. SubBytes: Substituição de cada byte do bloco por outro byte, de acordo com uma tabela de substituição (S-box).
2. ShiftRows: Deslocamento das linhas do bloco, criando uma nova ordem dos bytes.
3. MixColumns: Mistura dos bytes em cada coluna do bloco.
4. AddRoundKey: Combinação do bloco de dados com a chave da rodada atual.

Na última rodada, a operação MixColumns é omitida.

4. Criptografia e Descriptografia com AES

1. Criptografia: A mensagem é dividida em blocos de 128 bits. Cada bloco passa pelas rodadas de transformação, gerando um bloco criptografado. Esse processo usa uma chave

de criptografia que deve ser mantida secreta.
2. Descriptografia: É o processo inverso da criptografia. Utilizando a mesma chave, os blocos são transformados de volta para seus valores originais, reconstituindo a mensagem original.

5. Implementação em JavaScript

Na implementação fornecida, utilizamos a biblioteca CryptoJS para realizar a criptografia e descriptografia AES. O algoritmo divide a mensagem em blocos e utiliza a chave definida pelo usuário para criptografar o texto. O processo de descriptografia reconstrói o texto original a partir do texto criptografado, assumindo que a chave fornecida está correta.

Exemplo de Uso:

- Criptografia: Ao fornecer uma mensagem e uma chave, o algoritmo criptografa a mensagem e exibe o texto cifrado.
- Descriptografia: O usuário insere o texto cifrado e a chave usada para criptografá-lo, e o algoritmo retorna o texto original.

6. Benefícios do AES

- Segurança Alta: AES é confiável e resiste a ataques de força bruta.
- Desempenho Eficiente: Otimizado para processamento rápido em hardware e software.
- Ampla Adoção: Utilizado em várias indústrias para proteger dados sensíveis.