Trabalho de Criptografia

Dupla: Larissa Sardinha e Pedro Henrique Moreth

O Trabalho está feito com três algoritmos de criptografias. No primeiro a mensagem é criptografada por criptografia AES. No segundo algoritmo a mensagem está criptografada com DES.No terceiro algoritmo foi usado a criptografia por substituição.
A criptografia AES (Advanced Encryption Standard), também conhecida como Rijndael, é um algoritmo simétrico de criptografia amplamente utilizado para proteger informações confidenciais. Ele foi selecionado pelo Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos como o padrão de criptografia para substituir o antigo padrão DES.
A criptografia por AES opera em blocos de dados fixos de tamanho de 128 bits (16 bytes) e suporta chaves com tamanhos de 128, 192 e 256 bits. O processo de criptografia AES envolve várias etapas:
Chave: Uma chave de criptografia é gerada ou fornecida pelo usuário. O tamanho da chave determina a força da criptografia.
Expansão de Chave: A chave original é expandida em um conjunto de subchaves que serão usadas em diferentes etapas do algoritmo.
Adição de Chave: O bloco de dados a ser criptografado é combinado (bit a bit) com uma subchave inicial.
Rodadas: O algoritmo AES é composto por várias rodadas, dependendo do tamanho da chave. Cada rodada executa uma série de transformações nos dados para torná-los cada vez mais embaralhados e difíceis de serem reconhecidos. Cada rodada consiste em quatro operações principais:
SubBytes: Substituição de cada byte do bloco por um valor correspondente na S-Box (tabela de substituição não linear).
ShiftRows: Desloca as linhas do bloco em diferentes quantidades, aumentando a difusão.
MixColumns: Combinações lineares de cada coluna do bloco, misturando os bytes entre as colunas.
AddRoundKey: Combinação bit a bit dos bytes do bloco com uma subchave correspondente.
Rodada Final: A última rodada executa todas as etapas, exceto a operação MixColumns, para obter o resultado final.
Após passar pelas rodadas, o bloco de dados criptografado é obtido. O mesmo processo pode ser aplicado para descriptografar o bloco de dados usando a chave correspondente.
A criptografia AES é considerada segura e eficiente em termos de desempenho. Ela oferece uma forte proteção para dados sensíveis e é amplamente utilizada em sistemas e protocolos de segurança, como criptografia de arquivos, comunicação segura (por exemplo, HTTPS) e criptografia de dados armazenados.

A criptografia por DES (Data Encryption Standard) é um algoritmo de criptografia simétrica amplamente utilizado que foi desenvolvido nos anos 1970 pelo governo dos Estados Unidos. Embora tenha sido amplamente adotado no passado, o DES é considerado atualmente como um algoritmo de criptografia inseguro para muitos cenários, devido à sua chave de tamanho relativamente curto.

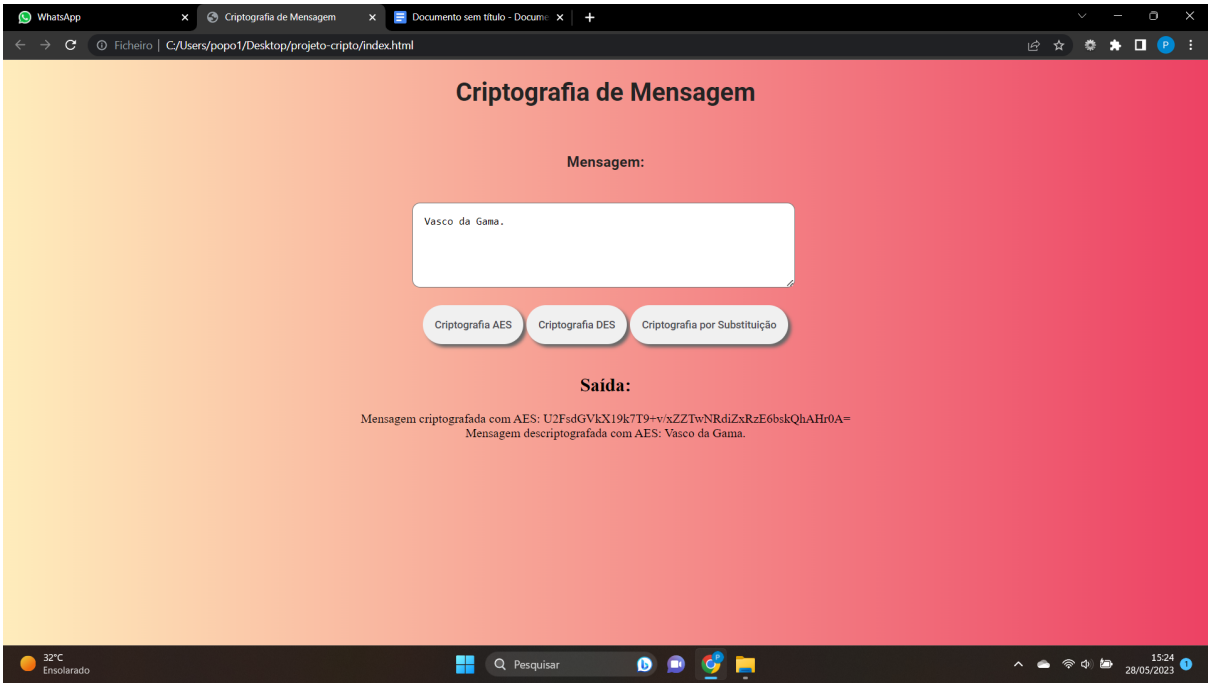
A criptografia DES opera em blocos de dados fixos de 64 bits (8 bytes) e utiliza uma chave de 56 bits para a criptografia. O processo de criptografia DES envolve as seguintes etapas:
Chave: Uma chave de criptografia de 56 bits é gerada ou fornecida pelo usuário. Posteriormente, essa chave é expandida em um conjunto de subchaves a serem usadas nas diferentes etapas do algoritmo.
Permutação Inicial: O bloco de dados a ser criptografado passa por uma permutação inicial para rearranjar os bits.
Rodadas: O algoritmo DES consiste em uma série de rodadas que são repetidas várias vezes. Cada rodada executa uma combinação de substituições, permutações e operações lógicas nos dados.
Substituição: Cada bloco de 48 bits do bloco de dados é substituído por um novo valor de 32 bits, usando uma tabela de substituição chamada S-Box. As substituições ajudam a difundir os bits e aumentar a segurança.
Permutação: Os bits do bloco de dados são rearranjados por meio de permutações para obter um novo arranjo.
Operações Lógicas: Operações lógicas, como XOR (OU exclusivo), são realizadas entre os bits do bloco de dados e as subchaves correspondentes.
Rodada Final: A última rodada executa as mesmas etapas que as rodadas anteriores, mas sem a operação de permutação.
Após passar pelas rodadas, o bloco de dados criptografado é obtido. O mesmo processo pode ser aplicado para descriptografar o bloco de dados usando a mesma chave, mas em ordem inversa, ou seja, as subchaves são usadas na ordem reversa.
Embora o DES tenha sido amplamente utilizado no passado, seu tamanho de chave relativamente curto tornou-o vulnerável a ataques de força bruta. Como resultado, o algoritmo foi substituído pelo AES (Advanced Encryption Standard), que oferece uma segurança mais forte e é amplamente adotado atualmente.

A criptografia por substituição de caracteres é um método de criptografia que opera substituindo cada caractere no texto original por outro caractere, de acordo com uma determinada tabela de substituição. Também conhecida como criptografia de substituição simples, é um tipo de criptografia de substituição monoalfabética, o que significa que cada caractere no texto original é substituído por um único caractere na mensagem criptografada.
O processo de criptografia por substituição de caracteres envolve as seguintes etapas:
Tabela de substituição: É criada uma tabela de substituição que associa cada caractere do alfabeto original a um novo caractere correspondente na mensagem criptografada. Por exemplo, pode-se definir uma tabela em que a letra "A" é substituída pela letra "D", "B" é substituída por "E", e assim por diante. Essa tabela pode ser fixa ou variar de acordo com a preferência do usuário.
Criptografia: Cada caractere no texto original é substituído pelo caractere correspondente na tabela de substituição. Por exemplo, se a tabela de substituição definir que "A" é substituído por "D", então todas as ocorrências de "A" no texto original serão substituídas por "D" na mensagem criptografada. Esse processo é realizado para cada caractere no texto original.
Mensagem criptografada: A mensagem criptografada é formada pelos caracteres resultantes da etapa de criptografia.
Para descriptografar a mensagem, basta realizar o processo inverso:
Tabela de substituição: Utiliza-se a mesma tabela de substituição utilizada na criptografia.
Descriptografia: Cada caractere na mensagem criptografada é substituído pelo caractere correspondente na tabela de substituição reversa. Por exemplo, se "D" é substituído por "A", então todas as ocorrências de "D" na mensagem criptografada serão substituídas por "A" no texto original.

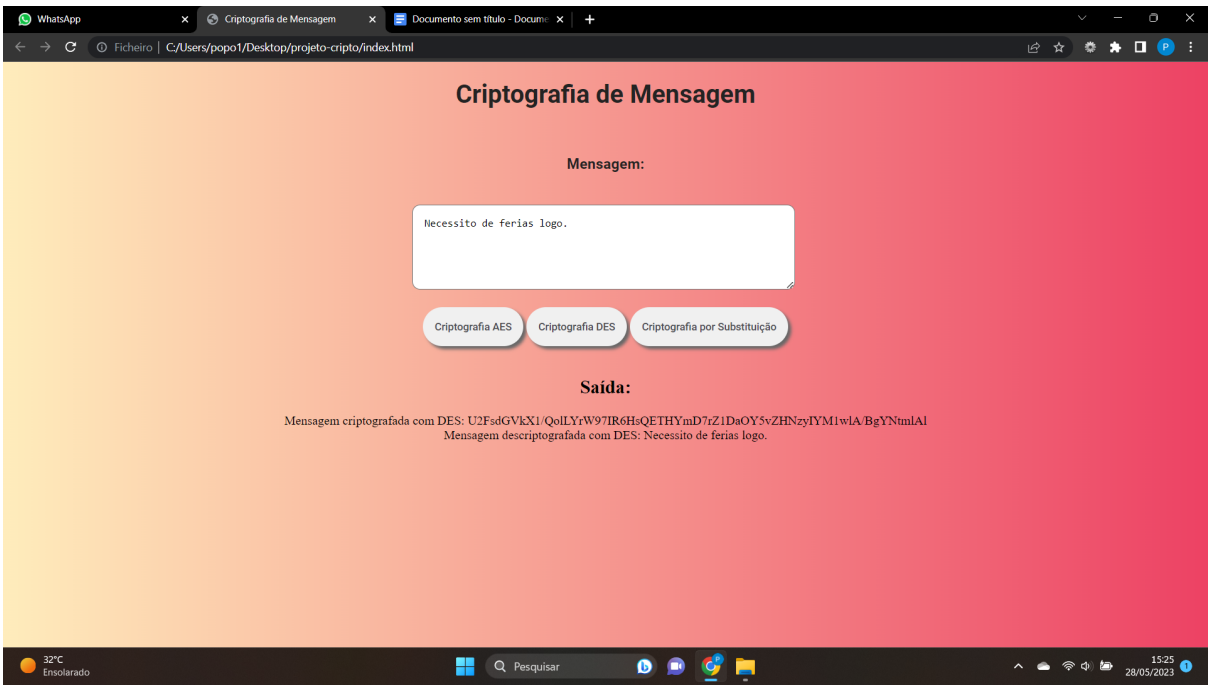
Texto original: O texto original é formado pelos caracteres resultantes da etapa de descriptografia.
A criptografia por substituição de caracteres é um método simples e básico de criptografia, mas possui várias limitações. É facilmente suscetível a análise de frequência, em que os padrões de frequência de letras e símbolos podem revelar informações sobre o texto original. Além disso, como é uma substituição fixa, a mesma letra é sempre substituída pelo mesmo caractere na mensagem criptografada, o que pode levar a padrões e tornar a criptografia mais vulnerável. Portanto, esse método não é adequado para a maioria das aplicações modernas de criptografia, sendo substituído por algoritmos mais robustos e seguros, como AES e RSA.

Termos de uso

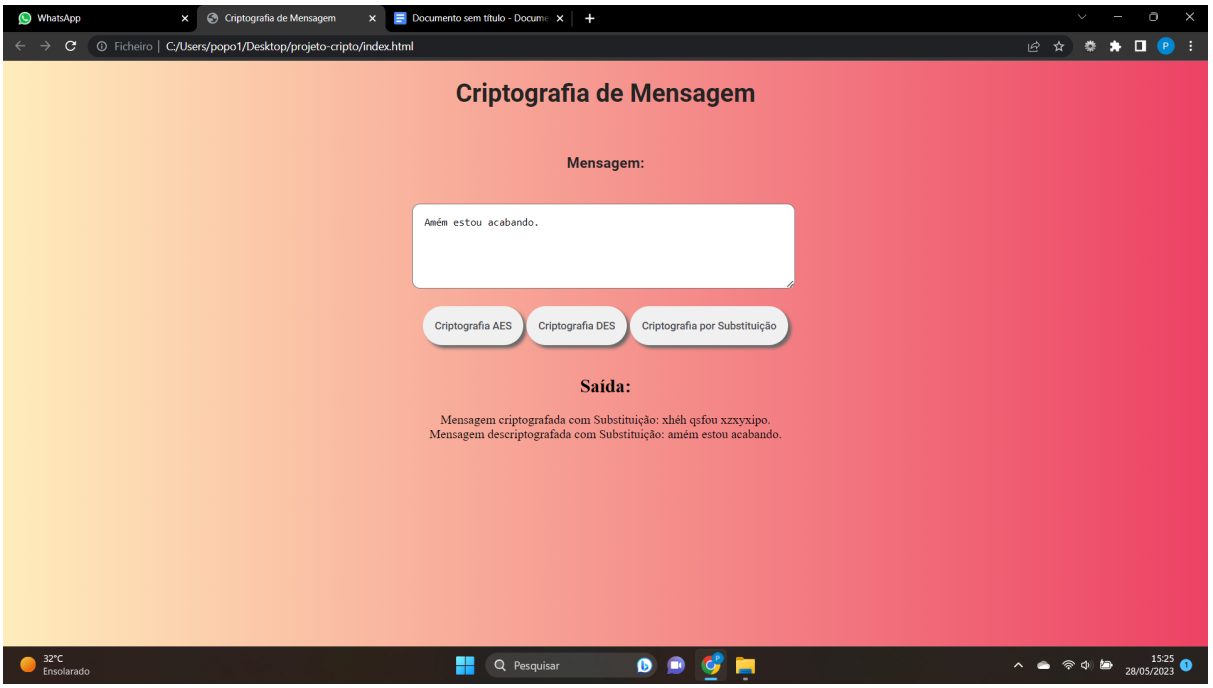
Está feita uma aplicação web.
Para usar a aplicação é necessário abrir o index.html e digitar a mensagem de texto na caixa de mensagem.
Clique no botão no qual deseja criptografar a mensagem.



Caso 1: Mensagem criptografada por AES.



Caso 2: Mensagem criptografada com DES.



Caso 3 : Mensagem criptografada com Substituição.