Comparação de Métodos de Criptografia: Cifra de César, Cifra da Espartilho (Scytale Cipher) e Cifra de Vigenère

O objetivo desta tarefa é comparar o desempenho e a segurança de diferentes métodos de criptografia, incluindo a Cifra de César, a Cifra da Espartilho (Scytale Cipher) e a Cifra de Vigenère. Ao implementar e analisar esses métodos, os alunos ganharão uma compreensão prática da criptografia clássica e suas características.

Instruções:

Redija um texto contemplando os seguintes aspectos:

1. Introdução:

a. Forneça uma breve introdução sobre criptografia e sua importância na segurança da informação.
b. Explique o conceito de criptografia simétrica e a diferença entre cifração e decifração.
c. Discuta a importância da segurança dos métodos de criptografia e as limitações dos métodos clássicos.

2. Cifra de César:

a. Apresente o método da Cifra de César, que é um método de substituição simples.
b. Explique o processo de cifração e decifração utilizando um deslocamento fixo do alfabeto.
c. Discuta as limitações da Cifra de César e sua vulnerabilidade a ataques de força bruta.

3. Cifra da Espartilho (Scytale Cipher):

a. Apresente a Cifra da Espartilho, um método de criptografia transposicional.
b. Explique o processo de cifração e decifração usando um cilindro com uma fita enrolada nele.
c. Discuta as características únicas da Cifra da Espartilho e sua resistência a ataques de força bruta.

4. Cifra de Vigenère:

a. Introduza a Cifra de Vigenère, um método de criptografia polialfabética.
b. Explique o conceito de palavra-chave e seu uso para gerar uma série de deslocamentos do alfabeto.
c. Destaque as vantagens da Cifra de Vigenère em relação à Cifra de César e discuta suas limitações.

5. Cálculo de Medidas de Teoria da Informação:

a. Explique o conceito de entropia e como ela quantifica a incerteza ou aleatoriedade de uma mensagem.
b. Calcule a entropia das mensagens originais em texto simples e dos textos cifrados obtidos por ambas as cifras.
c. Calcule a informação mútua entre o texto simples e o texto cifrado para cada cifra, destacando sua relevância na mensuração do vazamento de informação.
d. Para realizar os cálculos anteriores, utilize como base uma mensagem de texto suficientemente longa para que tais análises sejam significativas.

6. Técnicas de Criptoanálise:

a. Apresente técnicas básicas de criptoanálise, como análise de frequência e métodos estatísticos aplicáveis às cifras deste trabalho.
b. Analise as mensagens cifradas pelas três cifras usando análise de frequência para identificar padrões ou vulnerabilidades.
c. Realize ataques de texto escolhido para avaliar a resistência de cada cifra. Tente desvendar o texto cifrado conhecendo uma parte do texto original. Explore padrões, características linguísticas ou outras informações disponíveis para quebrar a cifra e recuperar o texto original.

Prática

7. Implementação e Testes:

a. Implementem os algoritmos da Cifra de César, Cifra da Espartilho e Cifra de Vigenère usando MATLAB/Octave.
b. Testem os algoritmos com diferentes mensagens e chaves para verificar a corretude das implementações.
c. Realize a cifração e decifração de mensagens utilizando cada método e comparem os resultados obtidos.
d. Façam testes trocando mensagens cifradas com os colegas, certificando assim a interoperabilidade possíveis diferentes implementações realizadas por cada um dos alunos.

8. Análise Comparativa:

a. Compararem os três métodos de criptografia com base em critérios como segurança, facilidade de implementação e desempenho.
b. Analise as vantagens e desvantagens de cada método em termos de resistência a ataques e praticidade de uso.
c. Discutam os resultados obtidos, comparando a eficácia dos métodos em diferentes cenários e contextos de aplicação.

Conclusão

9. Conclusão:

a. Resuma as conclusões da análise comparativa dos métodos de criptografia.

b. Destaque as principais características de cada método e sua relevância na segurança da informação.
c. Reflitam sobre a importância de selecionar o método de criptografia adequado com base nos requisitos de segurança e praticidade.

Observação: Para as implementações dos métodos, considere apenas textos e chaves com caracteres maiúsculos A-Z, remova todos espaços, sinais pontuação ou qualquer outro caractere diferente dos caracteres A-Z. Converta os caracteres minúsculos em caracteres maiúsculos. Documente o código de implementação, análises, resultados e observações ao longo da tarefa. Apresentem suas descobertas por meio de tabelas, gráficos e explicações claras. A citação adequada de quaisquer fontes externas utilizadas na tarefa é essencial.