Universidade de Brasília,
Departamento de Ciência Da Computação,
Segurança computacional

Aluno: Eduardo Afonso da Silva Inácio
Matrícula: 221033920

Cifra de Vigenère

Brasília, Outubro de 2023

1 Introdução

Este relatório descreve a implementação de um código em Python para a cifra de Vigenère e um ataque por análise de frequência para descriptografar mensagens cifradas. A cifra de Vigenère é um método de criptografia que utiliza uma chave para cifrar e decifrar mensagens de texto. O ataque por análise de frequência é uma técnica para quebrar cifras quando a chave é desconhecida.

2 Implementação da Cifra de Vigenère

O código implementa duas funções principais: `cifrar_vigenere` e `decifrar_vigenere`.

- `cifrar_vigenere`: Esta função recebe uma mensagem e uma chave como entrada e retorna a mensagem cifrada usando a cifra de Vigenère. Ela repetirá a chave para coincidir com o tamanho da mensagem e, em seguida, cifrará cada caractere da mensagem com base na chave.
- `decifrar_vigenere`: Esta função recebe um criptograma e uma chave como entrada e retorna a mensagem original decifrada. Ela também repete a chave para coincidir com o tamanho do criptograma e decifra cada caractere com base na chave.

3 Análise de Frequência

O código também inclui funções para calcular frequências de letras em mensagens e para calcular a correlação entre as frequências das letras na mensagem decifrada e as frequências esperadas em português ou inglês.

- `calcular_frequencias`: Esta função calcula as frequências das letras em uma mensagem, desconsiderando caracteres não alfabéticos.
- `calcular_correlacao`: Esta função calcula a correlação entre as frequências das letras na mensagem decifrada e as frequências esperadas em português ou inglês.

4 Ataque por Análise de Frequência

O código inclui uma função `ataque_analise_frequencia` que realiza um ataque por análise de frequência em um criptograma. A função tenta todas as possíveis chaves e calcula a correlação entre as frequências das letras na mensagem decifrada e as frequências esperadas. A chave que resulta na maior correlação é considerada a chave correta.

5 Testes

Foram realizados testes para cifrar e decifrar mensagens simples em português e inglês. Além disso, testes de ataque por análise de frequência foram realizados para recuperar a chave e decifrar mensagens cifradas.

6 Conclusão

O código implementa a cifra de Vigenère e um ataque por análise de frequência para quebrar mensagens cifradas. Ele demonstra a importância da análise de frequência na quebra de cifras e como a escolha de uma chave segura é essencial para a segurança das mensagens criptografadas.