UNIVERSIDADE DE BRASÍLIA

DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO

CIC0201 - Segurança Computacional - 2023.2 - Turma 01

Projeto 1 - Implementação da Cifra de Vigenère

Gustavo Barbosa de Almeida - 202037589

1.0 Introdução

Neste presente trabalho é nos apresentado a **cifra de vigenère,** que é um método de criptografia que usa uma série de diferentes cifras de César baseadas em letras de uma senha. Trata-se de uma versão simplificada de uma mais geral cifra de substituição polialfabética, inventada por Leon Battista Alberti cerca de 1465. Dito isso, nos foi pedido para implementar duas tarefas, sendo elas:

1.1 Tarefa 1 - cifrador/decifrador:

Onde o cifrador recebe uma senha e uma mensagem que é cifrada segundo a cifra de Vigenère, gerando um criptograma, enquanto o decifrador recebe uma senha e um criptograma que é decifrado segundo a cifra de Vigenère, recuperando uma mensagem.

1.2 Tarefa 2 - ataque de recuperação de senha por análise de frequência:

Serão fornecidas duas mensagens cifradas (uma em português e outra em inglês) com senhas diferentes. Cada uma das mensagens deve ser utilizada para recuperar a senha geradora do keystream usado na cifração e então decifradas.

2 Fundamentação teórica

Numa cifra de César, cada letra do alfabeto é deslocada da sua posição um número fixo de lugares; por exemplo, se tiver um deslocamento de 3, "A" torna-se "D", "B" fica "E", etc. A cifra de Vigenère consiste no uso de várias cifras de César em sequência, com diferentes valores de deslocamento ditados por uma "palavra-chave".

Para cifrar, é usada uma tabela de alfabetos que consiste no alfabeto escrito 26 vezes em diferentes linhas, cada um deslocado ciclicamente do anterior por uma posição. As 26 linhas correspondem às 26 possíveis cifras de César. Uma palavra é escolhida como "palavra-chave", e cada letra desta palavra vai indicar a linha a ser utilizada para cifrar ou decifrar uma letra da mensagem.

Por exemplo, supondo que se quer criptografar o texto:

ATACARBASESUL ("atacar base Sul")

Escolhendo a chave e repetindo-a até ter o comprimento do texto a cifrar, por exemplo, se a chave for "LIMAO":

LIMAOLIMAOLIM

A primeira letra do texto, A, é cifrada usando o alfabeto na linha L, que é a primeira letra da chave. Basta olhar para a letra na linha L e coluna A na grelha de Vigenère, e que é um L. Para a segunda letra do texto, ver a segunda letra da chave: linha I e coluna T , que é B, continuando sempre até obter:

Texto:	**ATACARBASESUL**
Chave:	**LIMAOLIMAOLIM**
Texto cifrado:	**LBMCOCJMSSDCX**

A decriptação é feita inversamente.

3.0 - Metodologia utilizada na implementação

Este programa em C++ implementa a cifra e a decifra usando a Cifra de Vigenère.

A primeira parte do trabalho funciona de forma bem intuitiva com o que foi pedido, cifrar e decifrar usando a cifra de vigenère. O programa começa com a inclusão das bibliotecas necessárias e a declaração do espaço de nomes `std`. Em seguida, ele define duas funções: cipher e decipher.

3.1 Função cipher

A função `cipher` recebe dois parâmetros: `texto` e `chave`. Ela cria uma string vazia `cipherText` para armazenar o texto cifrado. Em seguida, ela repete a chave até que ela tenha o mesmo tamanho que o texto.

A função então entra em um loop que percorre cada caractere do texto. Se o caractere não for uma letra ou um espaço, ele é ignorado.

Se o caractere for uma letra, ele é convertido para maiúsculas e a letra correspondente da chave também é convertida para maiúsculas. A letra cifrada é calculada como o resultado da expressão `((letraTexto - 'A') + (letraChave - 'A')) % 26 + 'A'`. A letra cifrada é então adicionada ao `cipherText`.Finalmente, a função retorna o `cipherText`.

3.2 Função decipher

A função `decipher` é semelhante à função `cipher`, mas decifra o texto em vez de cifrá-lo. Ela recebe dois parâmetros: `cipherText` e `chave`. Ela cria uma string vazia `decipherText` para armazenar o texto decifrado.

A função então entra em um loop que percorre cada caractere do `cipherText`. Se o caractere não for uma letra ou um espaço, ele é ignorado.

Se o caractere for uma letra, ele é convertido para maiúsculas e a letra correspondente da chave também é convertida para maiúsculas. A letra decifrada é calculada como o resultado da expressão `((letterCipher - letterKey  + 26) % 26) + 'A'`. A letra decifrada é então adicionada ao `decipherText`.

Finalmente, a função retorna o `decipherText`.

3.3 Função main

A função `main` é a função de entrada do programa. Ela começa solicitando ao usuário que escolha uma opção: cifrar ou decifrar.

Se a opção escolhida for cifrar, o programa solicita ao usuário que insira o texto e a chave. Em seguida, ele chama a função `cipher` para cifrar o texto e exibe o texto cifrado.

Se a opção escolhida for decifrar, o programa solicita ao usuário que insira o texto cifrado e a chave. Em seguida, ele chama a função `decipher` para decifrar o texto e exibe o texto decifrado.

Se a opção escolhida for inválida, o programa exibe uma mensagem de erro.

Finalmente, a função `main` retorna 0 para indicar que o programa terminou com sucesso.

4 Conclusão

Esse trabalho demonstra a compreensão da cifra de Vigenère e como implementá-la em um programa, no caso, em C++. A cifra de Vigenère é uma técnica clássica de criptografia que, embora não seja tão segura quanto métodos modernos, ainda é um exemplo valioso de criptografia histórica e princípios fundamentais de segurança de dados.

5 Referências

https://www.dcode.fr/vigenere-cipher#q5

https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Frequency-Analysis.html

https://pt.wikipedia.org/wiki/Cifra_de_Vigen%C3%A8re

https://www.youtube.com/watch?v=bgQyLQmylsA

https://www.youtube.com/watch?v=SkJcmCaHqS0

https://www.youtube.com/watch?v=P4z3jAOzT9I

https://pt.wikipedia.org/wiki/Frequ%C3%AAncia_de_letras