Universidade de Brasília
Departamento de Ciências da Computação
Segurança Computacional (CIC0201)

Trabalho 1:

Cifra de Vigenère

David Herbert de Souza Brito Mat: 200057405

Professor:
João José Costa Gondim

3 de outubro de 2023

Conteúdo

1 Introdução

A cifra de Vigenère 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.

A invenção da cifra de Vigenère é erradamente atribuída a Blaise de Vigenère encontra-se originalmente descrita por Giovan Battista Bellaso no seu livro datado de 1553 com o título La Cifra del Sig. Giovan Battista Bellaso.

Esta cifra é muito conhecida porque é fácil de perceber e de pôr em prática, parecendo, a quem tem pouca prática, que é inquebrável (indecifrável). Consequentemente, muitos programadores implementaram esquemas de criptografia nas suas aplicações que são no essencial cifras de Vigenère, e que são facilmente quebradas por qualquer criptoanalista.

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.

A cifra de Vigenère pode ser vista algebricamente. Se as letras A–Z forem mapeadas nos números inteiros 0–25, e a adição módulo 26 for aplicada, a criptografia pode ser escrita:

$C_i = P_i + K_i \mod (26)$

e a decriptação,

$P_i = C_i - K_i \mod (26)$

2 Ferramentas Utilizadas

- VS Code
- C++
- GCC 9.4.0
- Google
- WSL 2 - 20.04

Para compilar os códigos basta abrir o terminal e digitar:

```
g++ vigenere.cpp -o arquivo -Wall
```

e para executar:

```
./arquivo
```

3 Implementações

3.1 Cifração de decifração de Vigenère

vigenere.cpp > ...

```cpp
#include <iostream>
#include <string>
#include <cctype>

using namespace std;

// Função para cifrar a cifra de Vigenère
string encryptVigenere(const string &message, const string &key) {
    string encryptedMessage;
    int messageLength = message.length();
    int keyLength = key.length();

    for (int i = 0; i < messageLength; i++) {

        if (isalpha(message[i])) {
            char messageChar = message[i];
            char keyChar = key[i % keyLength];
            char encryptedChar;

            char shift = isupper(messageChar) ? 'A' : 'a';

            encryptedChar = (messageChar + keyChar - 2 * shift) % 26 + shift;

            encryptedMessage += encryptedChar;
        } else {
            encryptedMessage += message[i];
        }
    }

    return encryptedMessage;
}
```

Figura 1: Função para cifrar a mensagem

vigenere.cpp > ...

```cpp
// Função para decifrar a cifra de Vigenère
string decryptVigenere(const string &message, const string &key) {
    string decryptedMessage;
    int messageLength = message.length();
    int keyLength = key.length();

    for (int i = 0; i < messageLength; i++) {
        if (isalpha(message[i])) {
            char messageChar = message[i];
            char keyChar = key[i % keyLength];
            char decryptedChar;

            char shift = isupper(messageChar) ? 'A' : 'a';

            decryptedChar = (messageChar - keyChar + 26) % 26 + shift;

            decryptedMessage += decryptedChar;
        } else {
            decryptedMessage += message[i];
        }
    }

    return decryptedMessage;
}
```

Figura 2: Função para decifrar a mensagem

vigenere.cpp > ...

```cpp
int main() {
    int choice;
    string message, key, result;

    cout << "Escolha uma opção:\n";
    cout << "1. Cifrar\n";
    cout << "2. Decifrar\n";
    cout << "Opção: ";
    cin >> choice;

    cin.ignore(); // Limpa o buffer do teclado

    switch (choice) {
        case 1:
            cout << "Digite a mensagem para cifrar: ";
            getline(cin, message);

            cout << "Digite a chave: ";
            getline(cin, key);

            result = encryptVigenere(message, key);
            cout << "Mensagem cifrada: " << result << endl;
            break;

        case 2:
            cout << "Digite a mensagem para decifrar: ";
            getline(cin, message);

            cout << "Digite a chave: ";
            getline(cin, key);

            result = decryptVigenere(message, key);
            cout << "Mensagem decifrada: " << result << endl;
            break;

        default:
            cout << "Opção inválida!" << endl;
            break;
    }
    return 0;
}
```

Figura 3: Função main

Esse código implementa a cifra de Vigenère, um método de criptografia que usa uma chave para cifrar e decifrar mensagens. Ele permite ao usuário escolher entre cifrar ou decifrar uma mensagem usando a cifra de Vigenère:

A função encryptVigenere cifra uma mensagem de entrada usando uma chave de acordo com a cifra de Vigenère. A função decryptVigenere decifra uma mensagem cifrada usando a mesma chave. O programa principal main oferece um menu onde o usuário pode escolher entre cifrar e decifrar. Após a escolha, o usuário pode inserir a mensagem e a chave. O programa imprime a mensagem cifrada ou decifrada, dependendo da escolha do usuário. Em resumo, este código implementa um programa de linha de comando para cifrar e decifrar mensagens usando a cifra de Vigenère com base na entrada do usuário.

3.2 Recuperação de senha por análise de frequência

Para resumir os passos da criptoanálise da cifra de Vigenère:

Encontrar o tamanho da chave: Identifique padrões de repetição no texto criptografado para determinar o comprimento da chave. Isso envolve encontrar diferenças entre as posições das repetições e encontrar um número que seja um divisor comum para todas essas diferenças.

Fatiar o texto: Divida o texto criptografado em segmentos igualmente espaçados, com base

no tamanho da chave. Isso ajuda a analisar as frequências das letras em cada segmento individualmente.

Análise de Frequência: Realize uma análise de frequência em cada segmento para determinar as letras mais comuns. Isso pode ser feito assumindo que a letra mais comum em um segmento corresponde à letra mais comum no idioma original (por exemplo, 'E' em inglês ou 'A' em português).

Descobrir a chave: Com base nas letras mais comuns em cada segmento, determine a provável chave de deslocamento usada para criptografar cada segmento.

Decifrar o texto: Use a chave descoberta para decifrar o texto criptografado, realizando a operação inversa do deslocamento em cada letra.

Essa parte não foi implementada no código enviado, por conta que ouve alguns problemas nessa parte, com isso preferi não coloca-lá.

4 Referências

[1]Site: `https://pt.wikipedia.org/wiki/Cifra_de_Vigenre`. [2]Site: `http://informatabrasileiro.blogspot.com/2013/04/quebrando-cifra-de-vigenere.html`.