Segurança Computacional
Alexandre Souza Costa Oliveira
170098168
Universidade de Brasília - UnB

Trabalho 01:

1. Compilação e utilização:

A implementação do código para Cifra de Vigenere foi feito em **C++** com gcc 10.3.0 em ambiente Windows (versão 10).

Para compilação do arquivo, basta entrar na pasta dele com o cmd ou powershell e digite a linha de comando:

`g++ main.cpp -o main -Wall`

O texto cifrado ou o texto que deseja cifrar, deve ser colocado no arquivo texto.txt e a senha deve ser colocada no arquivo key.txt.

Para executar o programa, digite no cmd ou powershell estando dentro da pasta do arquivo main.cpp:

`./main`

2. Código:

O código ficou relativamente pequeno, se não fosse por conta das mensagens a serem demonstradas para o usuário, ficaria menor ainda. As funções de cifrar e decifrar ficaram relativamente simples e não houve muita dificuldade em fazê-las, já as funções de atacar uma cifra foram um pouco mais difíceis de serem feitas e o tamanho delas ficaram significativamente maiores.

Função que irá cifrar um texto em cifra de vigenere:

```
string cifrar(string textKey, string texto, vector<vector<int>> campo){
    string cifrado;

    for(unsigned int i = 0; i < texto.size(); i++){
        if(texto[i] >= 'a' && texto[i] <= 'z'){
            int x, y;

            x = texto[i] - 'a';
            y = textKey[i] - 'a';

            cifrado.push_back((char) (campo[y][x] + 'a' - 1));
        }
        else{cifrado.push_back(texto[i]);}
    }
    return cifrado;
}
```

Função que irá decifrar uma cifra de vigenere:

```
string decifrar(string textKey, string texto, vector<vector<int>> campo){
    string decifrado;

    for(unsigned int i = 0; i < texto.size(); i++){
        if(texto[i] >= 'a' && texto[i] <= 'z'){
            unsigned int x, y;

            y = textKey[i] - 'a';

            for(unsigned int j = 0; j < 26; j ++){
                if(campo[y][j] == texto[i] - 'a' + 1)
                    x = j;
            }
            decifrado.push_back((char) (campo[0][x] + 'a' - 1));
        }
        else{decifrado.push_back(texto[i]);}
    }
    return decifrado;
}
```

Em ambos os casos o vetor campo passado como parâmetro é a matriz alfabética de vigenere usada para cifrar ou decifrar uma mensagem.

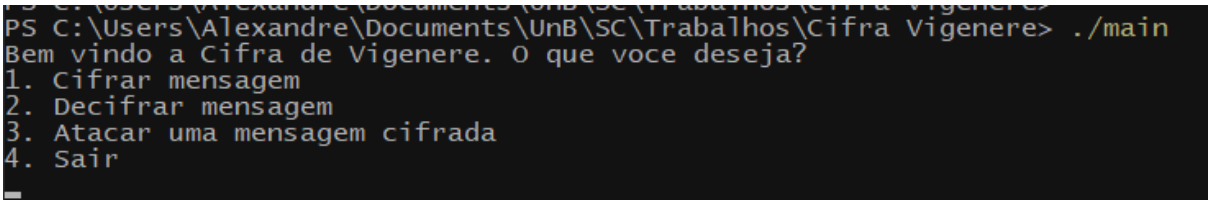
Já as funções de ataque a cifra, como a encontrarTamanhoKey, não são totalmente automatizadas e o usuário precisará tomar decisões, como avaliar as possibilidades de tamanho de chave com base nos cálculos feitos pelo programa. Foi programado para que o usuário possa escolher entre avaliar por blocos de repetição (avaliando a frequência em que uma sequência de caracteres aparece e calculando a distância entre essas sequências), mostrando uma matriz de possibilidades ou por frequências (calculando aqueles que obtiveram um MDC igual para todas as distâncias calculadas e ordenado com base na frequência). Assim, o usuário estará apto a visualizar essas possíveis chaves e escolher a que lhe parece mais óbvia.

Após o usuário ter uma provável certeza do tamanho da chave, ele estará apto agora a tentar descobrir a chave em si. Assim, ao entrar na opção de encontrar chave, ele terá que escolher entre inglês e português. E, após isto, o programa dará a ele a opção de tentar descobrir todas as letras da chave e as frequências de letras mais usadas em ambos os idiomas. O usuário poderá então, deslocar as letras para encontrar uma compatibilidade entre as frequências da cifra e as frequências das letras em cada idioma. Isto pode ser visualizado melhor nas imagens no tópico de Interface.

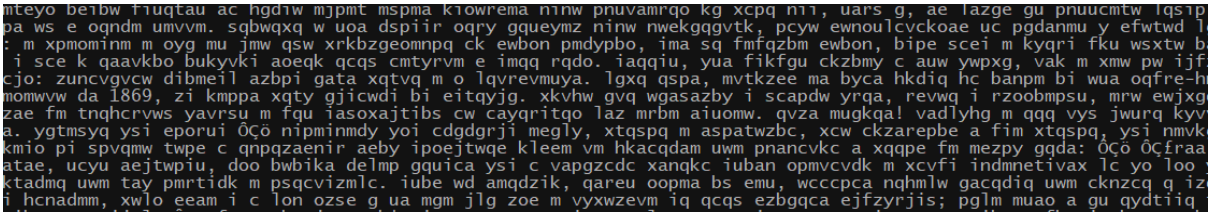
3. Interface:

A interface inicial conta com 4 opções, sendo uma de cifrar uma mensagem, outra para decifrar e outra para realizar um ataque para descobrir a chave utilizada para cifrar uma mensagem.

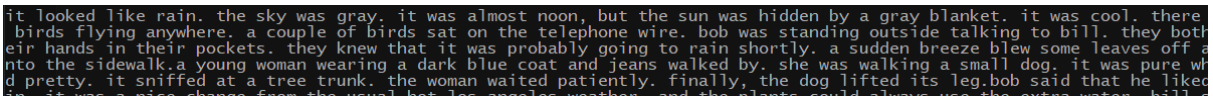
Interface inicial



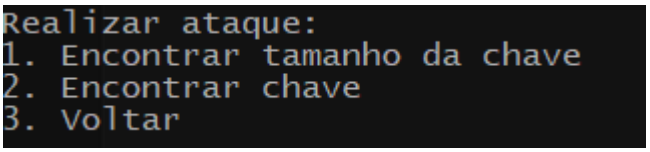
Mensagem cifrada pela opção 01



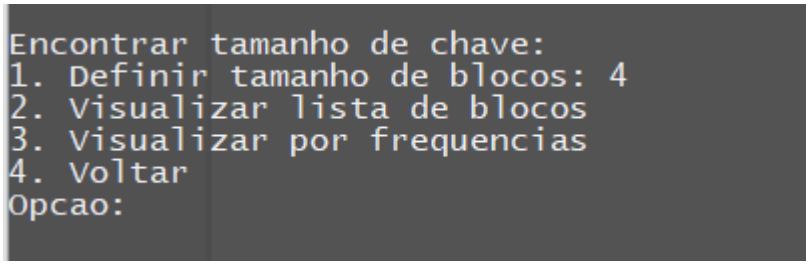
Mensagem decifrada pela opção 02



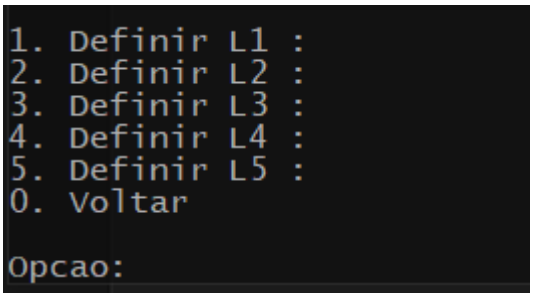
Opções de ataque da opção 03.



Opções disponíveis para ajudar a encontrar o tamanho da chave



Opções após encontrar o tamanho da chave e quiser encontrar a própria chave



Opções de deslocamento para encontrar a letra correta