Trabalho 1 - Segurança Computacional

Isabelle Alex dos Santos Basílio Caldas - 170105636
Universidade de Brasília - UnB

1. Compilação:

Para compilar o arquivo basta digitar o comando abaixo no terminal aberto na pasta que se encontra o arquivo:
g++ vigenere.cpp -o vigenere -Wall

Para executar o arquivo basta digitar o comando abaixo no terminal aberto na pasta que se encontra o arquivo:
./vigenere

No documento *texto.txt* deve ser colocado o texto que se deseja cifrar, ou então o texto a ser decifrado. Já no documento *chave.txt* deve ser colocada a senha para decifrar o texto.

2. Código Cifrador/Decifrador:

Primeiramente pegamos o texto e a senha que estão nos arquivos txt e colocamos todos em letras minúsculas. Depois criamos a chave do texto, onde repetimos a senha várias vezes até ficar do tamanho do texto a ser cifrado/decifrado. Abaixo estão os códigos da cifra e decifra dos textos. A forma que adotei para tratar números e caracteres especiais foi simplesmente ignorar eles e continuar até achar a próxima letra.

Código da cifra:

```
string cifrar(string chaveTexto, 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 = chaveTexto[i] - 'a';

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

    return cifrado;
}
```

Código da decifra:

```
string decifrar(string chaveTexto, 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 = chaveTexto[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;
}
```

O texto cifrado ou decifrado será exibido na tela ao final da execução do código.

3. Código do Ataque

Para fazer o ataque primeiro pegamos o texto que está criptografado e retiramos todos os caracteres especiais dele. Em seguida perguntamos ao usuário qual é a linguagem da cifra (Português ou Inglês) e se o usuário sabe o tamanho da senha. Se não souber, o programa vai criar um grupo de três letras usando a cifra para verificar a frequência de espaçamento que esse grupo se repete. Depois de fazer isso para todos os grupos, analisarmos em qual espaçamento os grupos mais se repetem e retornamos isso como sendo o tamanho da nossa chave.

Depois que temos o tamanho da chave é mostrado uma tabela com a frequência de vezes que a letra aparece e ao lado a frequência de vezes da letra no idioma selecionado, então devemos alinhar as duas colunas para assim descobrir as letras da senha.