

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

```
C:\Users\Alexandre\Documents\UnB\SC\Trabalhos\Cifra Vigenere> ./main
Bem vindo a Cifra de Vigenere. O que voce deseja?
1. Cifrar mensagem
2. Decifrar mensagem
3. Atacar uma mensagem cifrada
4. Sair
```

Mensagem cifrada pela opção 01

```
nteyo beibw fluqtau ac hgdiw mjpmi mspma kiowrema ninw pnuvamiqo kg xcpq nri, uars g, ae lazge gu pnuucmtw lqsi
pa ws e oqndm umvwm. sgbwqxq w uoa dspir oqry gqueymz ninw nwekgggvtk, pcyw ewnoulcvcckoe uc pgdanmu y efwtwd l
: m xpmominm m oyg mu jmw qsw xrbzgeomnpg ck ewbon pmdypbo, ima sq fmfqzbm ewbon, bipe scei m kyqri fku wsxtw b
i sce k qaavkbo bukyvki aoeqk qcqs cmtyrvm e imqq rqdo. iaqgiu, yua fikfgu ckzbmy c auw ywpvg, vak m xmw pw iijf
cjo: zuncvgvcw dibmeil azbpi gata xgtvq m o lqvrevmuya. lgxq qspa, mvtkzee ma byca hkdiq hc banpm bi wua oqfre-h
momwvw da 1869, zi kmppa xqty gjicwdi bi eitqyig. xkvhw gvq wgasazby i scapdw yrqa, revwq i rzoobmpsu, mrw ewjxg
zae fm tnqhcrrws yavrsu m fqu iasoxajtibs cw cayqritgo laz mrbm aiuomw. qvza mugkqa! vadlyhg m qqq vys jwurq kyv
a. ygtmsyq ysi eporui ÔÇô nîpminmdu yoi cdgdgrji megly, xtqspq m aspatwzbc, xcw ckzarepbe a fim xtqspq, ysi nmvk
kmio pi spvqmw twpe c qnpgzaenir aeby ipoejtwqe kleem vm hkacqdam uwm pnancvkc a xqqpe fm mezpy ggda: ÔÇô ÔÇôfraa
atae, ucyu aejtwpiu, doo bwbika delmp gguica ysi c vapgzcdc xanqkc iuban opmvcvdk m xcvfi indmnetivax lc yo loo
ktadm q uwm tay pmrtidk m psqcvizmlc. iube wd amqdzik, qareu oopma bs emu, wcccpc nqhmllw gacqdiq uwm cknzcq q iz
i hcnadmm, xwlo eeam i c lon ozse g ua mgm jlg zoe m vyxwzevm iq qcqs ezbgqca ejfzyrjis; pglm muao a gu qydtiiq
```

Mensagem decifrada pela opção 02

```
it looked like rain. the sky was gray. it was almost noon, but the sun was hidden by a gray blanket. it was cool. there
birds flying anywhere. a couple of birds sat on the telephone wire. bob was standing outside talking to bill. they both
eir hands in their pockets. they knew that it was probably going to rain shortly. a sudden breeze blew some leaves off a
nto the sidewalk. a young woman wearing a dark blue coat and jeans walked by. she was walking a small dog. it was pure wh
d pretty. it sniffed at a tree trunk. the woman waited patiently. finally, the dog lifted its leg. bob said that he liked
```

Opções de ataque da opção 03.

```
Realizar ataque:
1. Encontrar tamanho da chave
2. Encontrar chave
3. Voltar
```

Opções disponíveis para ajudar a encontrar o tamanho da chave

```
Encontrar tamanho de chave:
1. Definir tamanho de blocos: 4
2. Visualizar lista de blocos
3. Visualizar por frequencias
4. Voltar
Opcao:
```

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

```
1. Definir L1 :
2. Definir L2 :
3. Definir L3 :
4. Definir L4 :
5. Definir L5 :
0. Voltar

Opcao:
```

Opções de deslocamento para encontrar a letra correta

Texto		Ingles	
a (4%)		a (8.167%)	
b (0%)		b (1.492%)	
c (4%)		c (2.782%)	
d (3%)		d (4.253%)	
e (3%)		e (12.702%)	
f (7%)		f (2.228%)	
g (9%)		g (2.015%)	
h (0%)		h (6.094%)	
i (4%)		i (6.966%)	
j (2%)		j (0.153%)	
k (4%)		k (0.772%)	
l (0%)		l (4.025%)	
m (6%)		m (2.406%)	
n (4%)		n (6.749%)	
o (0%)		o (7.507%)	
p (4%)		p (1.929%)	
q (7%)		q (0.095%)	
r (1%)		r (5.987%)	
s (1%)		s (6.327%)	
t (4%)		t (9.056%)	
u (4%)		u (2.758%)	
v (6%)		v (0.978%)	
w (3%)		w (2.36%)	
x (3%)		x (0.15%)	
y (3%)		y (1.974%)	
z (2%)		z (0.074%)	
1. Deslocar para cima			
2. Deslocar para baixo			
3. Definir letra			
0. voltar			
Opcao: <input type="text"/>			