Segurança Computacional Trabalho 1

João Viktor de Carvalho Mota - 160127823

1

1. Explicando como foi feito e como rodar

Primeiramente o código foi feita usando CLion da JetBrains no Windows. Foi rodado com o compilador MinGW-w64 e foi feita em C++20 . É tudo feito no próprio terminal , logo para escrever o texto precisa de CLTR-C CLTR-V porém texto com pula linha(ou enter) no meio dele pode não funcionar.

Para rodar pode usar:
g++ cifrador.cpp
g++ decifrador.cpp
g++ quebra.cpp

Foi usado como bibliografia os links:
http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-vigenere-cipher/
http://practicalcryptography.com/cryptanalysis/text-characterisation/chi-squared-statistic/

2. Parte 1 - Cifrador

Primeiramente foi feita com biblioteca vector uma matriz com a Tabela de Vigenere.
Depois pede pro usuário escrever a mensagem e depois a senha.
O código chamada a função cifrador e então transforma toda a mensagem e a senha em maiúsculo, salva o elemento e a posição de todos os elementos do texto que não são letras.
Depois apaga todos esses elementos que não são letras e junta todas as letras .
Pega a chave e copia até ter o mesmo tamanho que o texto.
Então vá percorrer o texto e pegando cada letra como a posição da coluna da matriz da Tabela de Vigenere e então a letra da senha na mesma posição e com ela consegue a posição da linha da matriz.
Após tudo isso, percorre a resposta(mensagem cifrada) e coloque todos os elementos salvos que não são letras em suas respectivas posições.

3. Parte 2 - Decifrador

É praticamente o inverso da parte 1 - cifrador . Primeira é feita a matriz da Tabela de Vigener.
Depois pede pro usuário escrever a mensagem cifrada e depois a senha.
O código chamada a função cifrador e então transforma toda a mensagem e a senha em maiúsculo, salva o elemento e a posição de todos os elementos do texto que não são letras.
Depois apaga todos esses elementos que não são letras e junta todas as letras .

Pega a chave e copia até ter o mesmo tamanho que o texto.
Então vá percorrer a mensagem cifrada e pegando cada letra como a posição da coluna da matriz da Tabela de Vigenere e então percorra a coluna até chegar na linha com a letra da senha na mesma posição. Então olhe em qual linha está esta letra e com isso consiga a letra da mensagem decifrada.
Após tudo isso, percorre a resposta(mensagem cifrada) e coloque todos os elementos salvos que não são letras em suas respectivas posições.

4. Parte 3 - Ataque/Quebra

Primeiramente se obteve a mensagem cifrada pelo usuário.
Depois foi preciso calcular o provável tamanho da senha, com isso foi usada o Índice de Coincidência(IC).
A mensagem foi divida em N colunas sendo que N foi de 1 até 10(podendo mudar esse valor no código) e então se calculou o IC de cada coluna após dividir a mensagem e então calculou a média de todas as colunas.
O maior valor obtido foi considerado o tamanho da chave.
Depois pegou o texto divido com o tamanho da chave e então achou a chave com a estatística Chi-squared(chi quadrado).
Esta estatística funciona da seguinte forma:
Pegou cada coluna da mensagem dividida e decifrou ela em todas as 26 letras possíveis separadamente(com isso se obteve 26 mensagens decifradas), ao decifrar em cada letra ,é calculada o chi-quadrado de toda e cada mensagem decifrada usando a estatística da frequência de letras de inglês e português e da contagem das letras da mensagem.
Ao somar todos os chi-quadrado das 26 letras possíveis da mensagem decifrada é obtido um valor para cada uma das 26 letras em que a mensagem foi decifrada.
A letra em que a mensagem decifrada obteve o menor valor da soma dos chi-quadrado é a letra da chave.
Após fazer isso em todas as colunas é obtida a possível chave.