Trabalho 1 de Segurança computacional

Gabriel Faustino Lima da Rocha(190013249)
Enzo Yoshio Niho(190027304)

December 2022

1 Introdução

Este projeto foi feito como trabalho 1 de segurança computacional do segundo semestre de 2022 da Universidade de Brasília(UnB), o trabalho foi dividido em duas partes, na primeira era necessário implementar um programa que fizesse os passos para cifrar uma mensagem utilizando uma chave, pelo método da cifra de Vigenère, o programa também deveria, dado um texto cifrado e a chave descifrar a mensagem de volta à original. Já a segunda parte consistia em fazer um programa que dado um texto cifrado pela cifra de Vigenère o programa retornasse a possível chave e o texto original, ou seja criar um programa que quebre a a cifra sem utilizar a chave e retorne a possível chave utilizada.

A cifra de Vigenère consiste em um método de criptografia primeiramente descrito por Giovan Battista Bellaso em 1553, mas a invecção foi atribuida à Blaise de Vigenère por engano, o nome da cifra vem desse erro de atribuição do inventor da cifra. Em 1863 Friedrich Kasiski foi o primeiro a determinar uma maneira de quebrar a cifra através da análise de frequência de caracteres da linguagem em que a mensagem foi codificada, o método descrito por ele foi utilizado para fazer a segunda parte do projeto

2 Objetivos

O trabalho tem como objetivo demonstrar como funciona a cifra de Vigenère, por que um ataque de força bruta não funciona nela e como ficou fácil quebrar uma cifra que já foi considerada "inquebrável" na época que era utilizada, devido aos avanços tecnológicos dos tempos atuais é possível quebrar a cifra em segundos utilizando computadores que podem fazer o trabalho de analisar a cifra em segundos além de entregar diversas possíveis chaves e o texto decifrado com cada uma delas.

O trabalho nos mostra que com o avanço da tecnologia e com melhor conhecimento sobre os métodos criptográficos, quebrar criptografias consideras inquebráveis nos dias atuais, pode ser bem factível em alguns anos.

3 Metodologia

Todos os códigos foram implementados utilizando C++ com a ajuda de algumas de suas bibliotecas padrões como *string, vector, iostream* entre outras, mas não foram utilizadas bibliotecas que já implementavam a cifra. A primeira parte do projeto foi feita utilizando o método padrão para a codificação e decodificação da cifra de Vigenère com algumas adaptações para a implementação no computador.

A segunda parte de quebrar a cifra sem a chave foi feita utilizando o método de Friedrich Kasiski procurando por sequencias de 3 letras que se repetiam durante o texto e salvando a distancia da sequencia anterior e repetindo esse processo até o final do texto, depois era utilizado eram pegos os divisores das distancias e feito um histograma deles, eram então pegos os 3 mais frequentes para definir o tamanho da chave. Com o tamanho definido dividimos o texto em N seções em que N é o tamanho da chave definido, cada seção correspondia a um espaçamento de tamanho N entre as letras do texto , por exemplo, 1, N+1, 2N+1,... para a primeira secção. Após isso o cada secção poderia ser tratada como uma cifra de César, pois era cifrada com a mesma letra toda vez, utilizando da frequência de letras na língua desejada era possível pegar determinar qual a letra utilizada para cifrar através da frequência das letras na secção, por exemplo se na secção a letra C tem uma frequência de 13% e na língua portuguesa a letra A tem uma frequência de 14% uma possibilidade é de que a letra utilizada para cifrar seja a letra B, pois ao cifrar A usando B obtemos C, porém seria preciso analisar as demais letras, pegando as frequências de todas as letras e somando, o valor máximo obtido para essa soma é a resposta para a a cifra.

4 Resultados e limitações

O cifrador e decifrador foram feitos com o alfabeto contido no *ASCII*[1] pelas dificuldades encontradas em ler caracteres fora deste padrão com a linguagem desejada, porém, a implementação foi feita de forma que, caso houvesse uma forma fácil de ler caracteres que não estão na tabela *ASCII*, também seria possível codificar e decodificar a mensagem. Por falta de tempo, não encontramos um método para ler e escrever tais caracteres.

No nosso projeto o cifrador e decifrador funcionou como o esperado, com o alfabeto padrão apenas com as 26 letras do alfabeto português.

5 Desenvolvimento

O projeto foi desenvolvido em C++, utilizando das bibliotecas padrões do C++ e os algoritmos implementados, são os clássicos para a resolução desse problema, como já explicado nas seções anteriores. Por ter sido feito em dupla foi utilizado também o *github*, para manter o projeto sincronizado entre os 2 desenvolvedores,

[1] https://pt.wikipedia.org/wiki/ASCII

e para os 2 poderem desenvolver ao mesmo tempo, além das vantagens do versionamento de código, como a possibilidade de voltar para versões anteriores caso alguma parte do projeto tenha dado errado na versão atual e o desenvolvimento do projeto de várias fontes de forma online e contínua.

6 Conclusão

O projeto demonstrou como era feita a criptografia no tempo antes do computadores, e com menos conhecimento e tecnologia, também demonstrou o porque da segurança/criptografia ser uma área em constante desenvolvimento, pois algo inquebrável ou muito demorado para ser quebrado, pode se tornar trivial e/ou rápido de ser quebrado e revelar os segredos que escondia. O trabalho foi muito interessante de programar, pois treinamos o desenvolvimento de uma aplicação bem elaborada com alguns dos padrões de indústria para o C++.