Segurança computacional
Trabalho 1 - Cifra de Vigenère - Turma 02

Lucas Amaral de Faria - 211055316

Setembro 2023

1 Introdução

Esse trabalho tem como objetivo realizar a cifração e a decifração de textos por meio da cifra de Vigenère, além disso, é realizada a quebra dessa cifra por meio da análise da frequência das letras do alfabeto da lingua inglesa e da lingua portuguesa.

Para realizar o trabalho foi utilizada a linguagem C++. As principais funções do programa são:

- cifra: Recebe uma mensagem e uma chave e por delas meio retorna a mensagem cifrada.
- decifra: Recebe uma mensagem cifrada e uma chave e por meio delas retorna a mensagem decifrada.
- quebrar_cifra: Recebe somente a mensagem cifrada e por meio dela retorna a chave mais provável de acordo com os métodos utilizados no trabalho

2 Cifra de Vigenère

2.1 Cifração

A cifra de Vigenère é um método de criptografia o qual consiste de uma extensão da fórmula da cifra de César. Essa cifra consiste em escolher uma palavra-chave e aplicar a cifra de César de acordo com os caracteres da palavra-chave. Após escolher a chave, basta repeti-lá para fazer com que ela fique do mesmo tamanho da mensagem. Assim, toda letra da mensagem terá o seu valor incrementado por uma letra da chave a qual esteja na mesma posição.

Além disso, também é necessário decidir como lidar com caracteres especiais. No trabalho foi decidido que os caracteres especiais serão ignorados, ou seja, quando chegar um caracter especial ele será pulado e a chave não irá avançar, assim, a letra da chave que cifraria o caractere especial irá cifrar a próxima letra normal do texto.

Exemplo:
Mensagem: In the first week of June each year he would get a bad attack of hay fever and he would cycle to the office wearing a service gas mask
Chave: teste
Texto cifrado: br lai ymjlx piwd sy nmgi xeua cxej ai psmeh zil t fth smxtgc hj aeq yioij trw lw psnpv vcvpw ms mlw hjymux axejbrz e kxvomux ktw etwd

2.2 Decifração

Dado que possuimos a chave, para realizarmos a decifração do texto basta realizar o processo inverso da cifração, ou seja, repetimos a chave até ela ficar do mesmo tamanho do texto e em vez de incrementar as letras do texto pelas letras em mesma posição na chave, devemos decrementar as letras do texto utilizando a chave. Caracteres especiais também serão ignorados na decifração.

3 Quebra da cifra

Para realizar a quebra da cifra são necessários dois passos principais, descobrir o tamanho da chave e descobrir quais letras compõem essa chave.

3.1 Tamanho da chave

Para descobrir os possíveis tamanhos da chave, o texto cifrado é percorrido a procura de sequências de três letras que se repetem e é guardado a distância entre a sequência que se repetiu. Após isso é verificado qual o múltiplo mais comum da distância das sequências repetidas entre todas as encontradas. O tamanho da chave estará entre os múltiplos mais comuns encontrados. No trabalho são armazenados os cinco tamanhos mais prováveis.

3.2 Descoberta da chave

Após decidir o tamaho da chave, a chave em si será encotrada por meio da análise de frequência das letras. Digamos que a chave possui n letras, devemos agrupar as letras em n grupos. O primeiro grupo irá receber as letras das posições iguais a 0 (mod n), o segundo grupo irá receber as posições iguais a 1 (mod n) e assim por diante.

Exemplo:

Texto cifrado: A R S Q L B L O D M S Y X K M A P W S Y Q P L
Tamanho da chave: 3
Grupo 1: A,Q,L,M,X,A,S,P
Grupo 2: R, L, O , S, P, Y, L
Grupo 3: S, B, D, Y, M, Q

Com esses grupos em mãos basta analisar qual seria a letra da chave que geraria maior similariadade com a frequência das letras da língua em questão.

Vale lembrar que como o texto pode ser tanto em inglês quanto em português, devemos gerar as chaves mais provaveis para o inglês e para o portugês, gerando assim, 10 chaves diferentes ao total ao invés de cinco sendo duas de cada tamanho.

3.3 Escolha da melhor chave

Como foi dito anteriormente, são escolhidos 5 tamanhos prováveis de chave, a partir desses valores serão geradas as melhores chaves para esses tamanhos se baseando em frequência. Entretanto, devemos escolher qual delas será a chave correta, para fazer isso é analisado qual chave gera o texto decifrado com maior similaridade com as línguas em questão. Para escolher entre a melhor chave para a língua portuguêsa e para a língua inglesa, é utilizada a que gera maior grau de similaridade no geral.

4 Conclusão

Durante a elaboração do trabalho não foram encontradas muitas dificuldades. Ficou perceptível o quão vulnerável a cifra de Vigenère é, uma vez que é possível quebra-lá utilizando somente uma análise de frequência básica.