Segurança de Sistemas T1

Pâmela Mendonça Barreto

October 1, 2022

1 Introduction

Atualmente utilizamos a criptografia em muitas tarefas do nosso dia-a-dia que requerem mais segurança e confiabilidade dos sistemas. Trocas de mensagens pelo Whatsapp, ou acessar saldo da sua conta de banco, são exemplos comuns e que utilizam das mais diversas tecnologias para garantir a segurança dos dados.

Sendo assim, o presente artigo consiste em desenvolver um sistema que possa ser capaz de transformar uma mensagem criptografada em um texto claro. A criptografia usada na mensagem cifrada deve ser o método de Vigenére.

O algoritmo foi desenvolvido usando a linguagem de programação Python, e os textos usados nos testes de funcionalidade do algoritmo a seguir apresentado, foram todos disponibilizados na plataforma Moodle. .

2 O que é Cifra de Vigenére

É um método polialfabético prático de criptografar uma mensagem. Essa cifra se baseia em um conjunto de cifras de César, as quais usam as letras da senha para criptografia. Se tornou um método comumente usado por ser fácil de entender e colocar em prática. Sendo considerado seguro contra pessoas com pouco ensino linguístico algo quase indecifrável, o que era muito comum em séculos passados.

3 Descobrindo o tamanho da chave

A primeira parte para decifrar o texto é encontrar o tamanho da chave, isso serve para que posteriormente seja possível separar o texto cifrado em blocos e iniciar o processo de descobrimento dos caracteres da chave. Para esta etapa é usado o "Teste de Friedman", o qual usa o Índice de Coincidência de cada língua. Usando de assenta esse índice é possível testar qual das diferentes subtrings do texto cifrado é a mais próxima do índice. As substrings são formadas por partes do texto cifrado, que consistem em pegar seus caracteres a cada N valor de pulo.

3.1 Algoritmo para o Cálculo do Tamanho da Chave

Se inicia supondo que o tamanho da chave é 1. Agora se cria as substrings usando o tamanho da chave suposto como pulo. Então o algoritmo da criação das substrings é o seguinte:

t = tamanho da chave a ser testada

m = texto cifrado original

Sn = strings criadas a partir do pulo t em m

S1 = m1mt + 1m2t + 1... S2 = m2mt + 2m2t + 2...

Assim que temos as substrings, calculamos o índice de frequência, valor o qual sinaliza quando acharmos o possível tamanho da chave. Assim que achamos a lista de substrings que possuem o índice de frequência mais próximo (entre os demais) do índice de coincidência da língua a qual o texto está escrito (para cada texto cifrado já se sabe qual língua ele pertence), verificamos a quantidade de substrings da lista, esse valor será o tamanho da chave.

4 Cálculo da Chave

4.1 Algoritmo da Distância

Usando do valor encontrado para o tamanho da chave na seção anterior e a lista de substrings correspondente e usamos neste algoritmo. Começamos calculando a frequência de aparecimento de cada caractere de cada string da lista. Pegamos o caractere de maior frequência da string e calculamos a distância dele pelo alfabeto até o caractere de maior frequência da língua. O algoritmo do cálculo da distância pode ser representado da seguinte forma:

deslocamento = ASCIILetraCifrada - ASCIILetraMaiorFLingua
ajuste = deslocamento + ASCIILetraA
letraChave = ASCIIAjuste

5 Decifrando a Mensagem

Como nosso último passo para ter o texto cifrado como uma mensagem clara, começamos o algoritmo de decifragem. Nesse algoritmo percorremos cada uma das letras do texto cifrado e aplicamos uma função matemática, a qual resulta na letra original. Essa função é a seguinte:

letraOriginal = ASCII ((ASCIILetraCifrada - ASCIILetraChave + 26) MOD 26)

A letra da chave usada no algoritmo é correspondente com a letra da chave na posição correspondente. Isso ocorre pois para cifrar Vigenére, é usada a chave repetidamente no texto.

6 Resultados

O teste do algoritmo inteiro operou com os arquivos-texto disponibilizados no Moodle, nas línguas inglês e português. Foram feitas em torno de 10 iterações para descobrir o tamanho da chave em inglês, e 17 em português. Para ambos, foi descoberta a chave “meunome”. No texto em português foi necessário implementar uma chamada ao usuário, visando que seja escolhido a letra ”a” ou ”e”. Os textos cifrados ficarão na pasta “Decifrados” a qual é entregue junto com o código.

7 Conclusão

Ao percorrer dos testes, percebi que o algoritmo desenvolvido não conseguiu decifrar corretamente os textos na língua portuguesa. E isso se dá ao fato de nessa língua os caracteres “a” e “e” possuem valores de frequência muito similares. Isso perturba o algoritmo a achar os caracteres corretos da chave, pois é utilizado a frequência no cálculo do mesmo. Exemplo: Digamos que a letra mais frequente na substring seja a letra “p”, o algoritmo não consegue identificar se deve traduzir para “a” ou “e” já que a frequência de aparecimento dessas duas letras nas palavras da língua portuguesa são muito similares.

Deste modo, com o auxílio do professor Avelino implementei uma chamada ao usuário do programa. Essa chamada visava deixar a encargo do usuário a escolha da letra “a” ou “e” para o descobrimento da chave. Assim que o usuário escolher corretamente o texto pode ser lido claramente.