PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL

ESCOLA POLITÉCNICA

CURSO DE BACHARELADO EM ENGENHARIA DE SOFTWARE

Segurança de Sistemas

Pedro Maia Rogoski

2022

Resumo

Este artigo tem como objetivo descrever como foi a experiência do aluno no desenvolvimento de um algoritmo capaz de transformar um texto cifrado em Viegenere para texto claro utilizando das diversas técnicas apresentadas em sala de aula e posteriormente aplicadas no projeto abaixo.

Introdução

Com o início das aulas do ano de 2022/01, o professor Avelino Francisco introduziu para a turma os diversos conceitos da criptografia e segurança de sistemas, sendo os primeiro módulo de estudos focados na Criptografia Clássica de Vigènere. Com isso para desafiar e expandir o conhecimento dos alunos foi proposto como trabalho T1 da disciplina um projeto com objetivo da criação de um programa que dado um texto cidrada encontre o texto claro.

Criptoanálise

Passos

A primeiro etapa do projeto não foi a codificação em si, mas sim compreender quais serão os passos necessários para criar um algoritmo capaz de transformar um texto cifrado em texto claro, já neste primeiro requisito é possível identificar um grande grau de complexidade, e para tentar reduzir esta dificuldade de implementação criei etapas para o desenvolvimento mais simples da solução.

Etapas de implantação

1. Descobrir qual o tamanho da chave;
2. Descobrir qual a palavra da chave;
3. Descriptografar o texto cifrado.

Descobrir qual o tamanho da chave

O cálculo do tamanho inicial da chave poderiam ser executados de 2 formas, via Kasinski ou pelo método do índice de coincidência, para nossa solução foi utilizado o índice de coincidência por conveniência e mais praticidade na hora da implementação.
Nosso método vai basicamente calcular o índice de coincidência para um tamanho de chave, encontrando o índice para o tamanho da chave vamos comparar com o índice de coincidência da língua inglesa e caso o índice do tamanho da chave sejá próximo ao índice da língua inglesa então o tamanho de chave que estamos testando é o tamanho correto baseado no incide.

Descobrir qual a palavra da chave

Como nosso projeto será executado para a língua inglesa, para descobrir a chave precisaremos satisfazer duas condições, 1º é ter o tamanho da chave descoberto e 2º ter a letra mais frequente da língua inglesa, satisfazendo estas duas condições nosso método vai primeiro achar a letra mais frequente de nosso texto cifrado, após encontrarmos a letra mais frequente vamos comparar com a letra mais frequente da língua inglesa e aplicar o cálculo da distância para descobrir qual a letra da nossa chave e após todas as interações descobrimos, qual a palavra-chave.

Descriptografar o texto cifrado

Agora que já temos o tamanho da chave e a chave descoberta podemos avançar para a etapa de descriptografar o texto cifrado, e para isso vamos basicamente pegar o carácter do texto Cifrado menos o carácter da chave descoberta fazer um cast para char e concatenar o resultado em uma string e assim chegamos no texto descriptografado.

Conclusão

O projeto foi muito desafiador visto que ele é composto de diversas etapas que deve ser quebradas em etapas menores, assim facilitando a compreensão dos passos a serem seguidos.
A única divergência que encontrei no resultado do desenvolvimento foi na hora de descobrir a chave, pois o valor que encontramos para a chave descoberta foi "*meunomt"* que na verdade deveria ser "*meunome"*. Essa diferença resultou em um texto claro com as letras da posição 7 da chave como divergentes do que deveria ser para termos um texto claro completamente legível.
Mesmo com as difi culdades encontradas no desenvolvimento do projeto, foi possível passar por todas as etapas propostas e chegar de forma muito aproximada no *output* esperado como retorno da cifra de Viegenere.

Referências

[8.4. Determining the Key Length using Index of Coincidence]
https://www.ime.usp.br/~kellyrb/mac2166_2015/tabela_ascii.html
https://www.youtube.com/watch?v=Tc--MPir6rI