Trabalho de Segurança Computacional

Luis Fernando Lamellas - 19/0016841
Universidade de Brasília

***Abstract*—O presente estudo tem como objetivo descrever o processo de implementação de diversas funções e algoritmos empregados no campo da segurança computacional, visando a aquisição de conhecimento tanto no âmbito do curso em questão.**

I. Introdução

A cifra de Vigenère é uma técnica clássica de criptografia que adiciona uma camada de complexidade ao simples código de César. Desenvolvida por Blaise de Vigenère no século XVI, essa cifra utiliza uma palavra-chave para criar uma sequência de deslocamentos variáveis, tornando a mensagem codificada mais resistente às técnicas de quebra de código. Cada letra da mensagem é deslocada de acordo com a letra correspondente na palavra-chave, criando um padrão aparentemente aleatório. A força dessa cifra reside na sua capacidade de quebrar padrões linguísticos comuns, dificultando a análise estatística. Apesar de ter sido desafiadora em sua época, a cifra de Vigenère é agora vulnerável a métodos mais avançados de criptoanálise, mas seu legado persiste como um marco na história da criptografia.

II. Metodologia

A. Parte 01

A primeira função implementada neste estudo é denominada ”encryption”, cujo propósito é codificar uma mensagem por meio da cifra de Vigenère. Essa função recebe dois argumentos iniciais: uma mensagem a ser codificada e uma palavra-chave a qual guiará o processo de cifração.

Nesse processo, cada letra da mensagem é deslocada de acordo com a letra correspondente na palavra-chave. O algoritmo implementado soma o valor numérico do caractere correspondente da mensagem original com o caractere correspondente da palavra chave. Em seguida, é realizada a operação de módulo para garantir que o valor encontrado esteja dentro dos 26 símbolos do alfabeto.

Ao término da execução da função é retornada como resultado a mensagem cifrada.

A primeira função implementada neste estudo é denominada ”decryption”, cujo propósito é decodificar uma cifra por meio de sua palavra chave. Essa função recebe dois argumentos iniciais: uma crifra a ser decodificada e uma palavra-chave a qual guiará o processo de decodificação.

Nesse processo, cada letra da mensagem é deslocada de acordo com a letra correspondente na palavra-chave, executando o processo inverso da cifração. O algoritmo implementado subtrai o valor numérico do caractere correspondente da cifra do caractere correspondente da palavra chave. Em seguida, é somado 26 para evitarmos valores negativos e a operação de módulo é feita para garantir que o valor encontrado esteja dentro dos 26 símbolos do alfabeto.

Ao término da execução da função é retornada como resultado a mensagem original.

B. Parte 02

A quebra da cifra de Vigenère geralmente envolve a aplicação de técnicas de análise de frequência e índice de coincidências.

Inicialmente, a frequência de letras na cifra é analisada para identificar padrões. Como a cifra de Vigenère envolve deslocamentos diferentes para cada posição na palavra-chave, a frequência de letras pode variar em intervalos regulares. No entanto, o uso de uma palavra-chave torna mais desafiadora a aplicação direta da análise de frequência.

O índice de coincidências é outra ferramenta crucial. Quando uma única letra é cifrada por uma letra correspondente na palavra-chave, pode ocorrer um aumento temporário no índice de coincidências. Detectar esses picos no índice pode revelar o comprimento da palavra-chave.

Após identificar o comprimento da palavra-chave, segmentos da mensagem cifrada podem ser agrupados de acordo com esse comprimento, e cada grupo é tratado como uma cifra de César separada. A análise de frequência pode ser aplicada a cada grupo, facilitando a descoberta das letras mais comuns e, consequentemente, os deslocamentos correspondentes.

Por fim, com os deslocamentos correspondentes de cada grupo descoberto, é possível encontrar a palavra chave da cifra. Nesse estudo utilizamos a fórmula $X^2 = \frac{(F-f_i)^2}{F}$ para aproximação das frequências, onde F é a probabilidade da ocorrência de uma respectiva letra no português ou inglês e f_i é a probabilidade de ocorrer uma letra na cifra daquele grupo.

Assim, torna-se possível descobrir a palavra-chave para decodificação da cifra.

III. Resultados

A. Parte 01

A implementação das funções encryption e decryption proporcionou resultados satisfatórios no processamento da mensagem e da cifra.

Primeiramente executou-se o processamento de uma mensagem com os seguintes parâmetros: a mensagem ”ATTACKATDAWN” e a palavra-chave ”LEMON”. Encontrou-se como resultado a string ”LXFOPVEFRNHR”, mostrando o funcionamento correto do processo de codificação.

Em seguida, executou-se o processamento da cifra obtida com os seguintes parâmetros: a cifra ”LXFOPVEFRNHR” e

a palavra-chave ”LEMON”. Encontrou-se como resultado a string ”ATTACKATDAWN”, aferindo o funcionamento adequado do processo de decodificação.

É importante ressaltar que todos os testes feitos foram com strings somente com letras maiúsculas, sem espaços ou caracteres especiais.

B. Parte 02

Executando-se a quebra da cifra foram feitos dois testes, ambos com strings com aproximadamente 400 caracteres e palavras-chaves com menos de 10 caracteres.

A primeira quebra foi feita de uma cifra de uma mensagem em inglês. A cifra que foi quebrada é a seguinte string:

”PZEPHCIZYOYMBAPGIDLZMQEMAOCTRQOHGSD...”

Encontrou-se a palavra-chave correta ”**POLITICS**”, consequentemente o tamanho da palavra-chave também. A string resultante da decodificação foi:

”ALTHOUGHJANEISNOTPARTICULARLYIMPRES...”

A segunda quebra foi feita de uma cifra de uma mensagem em português. A cifra que foi quebrada é a seguinte string:

”VKEMVXFKMISMGYDEYQFGOTCMIIRWYIEGDIY...”

Encontrou-se a palavra-chave correta ”**VINEGERE**”, consequentemente o tamanho da palavra-chave também. A string resultante da decodificação foi:

”ACRIPTOGRAFIAUMADISCIPLINAESSENCIAL...”

IV. Conclusões

A. Questão 01

As funções apresentaram funcionamento ideal. Vale ressaltar que o formato de entrada é limitado e é necessário que contenha somente letras maiúsculas.

B. Questão 02

A quebra da cifra funcionou de maneira satisfatória para entradas em inglês mas demonstrou algumas falhas quanto a entrada em português. Tais falhas ocorreram pela ocorrência de caracteres fora do padrão como letras que possuem acento.

Em ambos os casos a palavra-chave foi corretamente encontrada. Vale ressaltar que o formato de entrada é limitado e é necessário que contenha somente letras maiúsculas.