CRIPTOANÁLISE - VIGENERE

Edson Ricardo da Costa [*]
Gabriel Fanto Stundner [**]

RESUMO

Projeto desenvolvido para a disciplina de Sistemas de Segurança da faculdade de Engenharia de Software na universidade da Pontifícia Universidade do Rio grande do Sul. O propósito desse projeto é apresentar uma possível solução para a decodificação de cifras de Vigenére por meio da programação, explicando o processo de implementação.

ABSTRACT

Project developed for the Security Systems course at the Software Engineering faculty at the Pontifical University of Rio Grande do Sul. The purpose of this project is to present a possible solution for the decoding of Vigenére ciphers through programming, explaining the implementation process.

1 INTRODUÇÃO

A cifra de Vigenére é um método de criptografia que usa uma série de tipos de cifra de César baseadas nas letras de uma palavra chave. Para cifrar é utilizado uma tabela de alfabetos escrito 26 vezes em diferentes linhas, cada um é deslocado uma posição de forma controlada, essa tabela é chamada de "Quadrado de Vigenére" onde cada linha é movimentada de forma cíclica para a esquerda comparado com o alfabeto anterior, de forma a corresponder às 26 cifras de César possíveis. Durante o processo de criptografia é utilizado um alfabeto diferente de uma das linhas e o alfabeto a ser utilizado em cada ponto depende da palavra-chave, que é repetida caso a mensagem seja maior que a palavra-chave inicial.

O problema proposto consiste em desenvolver uma aplicação (de livre) capaz de decifrar textos cifrados em Vigenére a partir do tamanho das suas chaves, com a opção de utilização dos métodos Kamiski ou Índice de Coincidência e os testes devem ser realizados através de textos previamente disponibilizados.

2 DESENVOLVIMENTO

A solução para o algoritmo de decifragem foi realizada em Java e conta com apenas uma estrutura de controle e visualização. Inicialmente organizamos a estrutura das principais funções em uma interface para posteriormente serem implementadas. Dentre as funções utilizadas:

readCipherText: Função que processa a entrada de dados no sistema (a partir do caminho de um arquivo de texto (no formato .txt disponibilizados no Moodle pelo professor). A função retorna uma String com o conteúdo.

[*] Estudante de Engenharia de Software – Pontifícia Universidade do Rio Grande do Sul.
[**] Estudante de Engenharia de Software – Pontifícia Universidade do Rio Grande do Sul.

createSequences: Função que recebe um texto cifrado como entrada e cria sequências de caracteres desse texto, com base em diferentes tamanhos de chave possíveis. O objetivo provável é realizar uma análise de índice de coincidência (IOC) em cada sequência gerada para determinar o tamanho provável da chave usada na cifra.

calcIoc: Função para calcular o Índice de Coincidência (IOC) de uma lista de sequências de caracteres. O código realiza os seguintes passos:

- Inicializa uma lista vazia de médias chamada "avgs".
- Para cada sequência de caracteres na lista de sequências de caracteres "sequences":
- Inicializa variáveis de contagem "n" e soma "sum".
- Inicializa um array de contagem de caracteres "values" com 26 posições.
- Calcula o somatório para cada caractere no array "values".
- Calcula a média do Índice de Coincidência (IOC) para a sequência de caracteres atual.
- Calcula a média do Índice de Coincidência (IOC) para todas as sequências.
- Retorna a média do Índice de Coincidência.

findKeyBySize: Função para encontrar a chave de criptografia de um texto cifrado usando a técnica de análise de frequência. O código realiza os seguintes passos:

- Constrói sequências de caracteres a partir do texto cifrado.
- Chama uma função externa "calcProbLetterByIndex" para encontrar a letra mais provável da chave de criptografia para cada sequência de caracteres na lista "sequences".
- Concatena as letras mais prováveis encontradas para cada sequência de caracteres, formando a chave de criptografia.
- Retorna a chave de criptografia encontrada como uma String.

calcProbLetterByIndex: Função que tem como objetivo calcular a probabilidade de uma letra do alfabeto ser a letra mais provável em uma determinada posição de uma chave utilizada na cifra de Vigenére.

decipherByKey: A função recebe como entrada o texto cifrado (cipherText) e a chave (key) que será utilizada para decifrar o texto. O resultado da decifragem é armazenado na variável decipher e é retornado ao final da função.

Os testes de decifragem foram realizados via console e interface gráfica, resultando nas seguintes saídas:

File	KeySize	Key	File	KeySize	Key
cipher1.txt	8	CRISTIAN	cipher17.txt	7	MARCELO
cipher2.txt	5	DAVID	cipher18.txt	6	MATEUS
cipher3.txt	10	DIEGODIEGO	cipher19.txt	7	MATHEUS
cipher4.txt	7	EDUARDO	cipher20.txt	7	MATHIAS
cipher5.txt	6	FELIPE	cipher21.txt	10	PAULOPAULO
cipher6.txt	7	GIROTTO	cipher22.txt	6	RITTER
cipher7.txt	7	GREGORY	cipher23.txt	10	COMPANHONI
cipher8.txt	8	HERCILIO	cipher24.txt	7	CADAVAL
cipher9.txt	6	MAURER	cipher25.txt	6	RENATA
cipher10.txt	6	RANGEL	cipher26.t.txt	7	RICARDO
cipher11.txt	9	JERUSALEM	cipher27.txt	7	RODRIGO
cipher12.txt	8	SOFTWARE	cipher28.txt	6	BRANCO
cipher13.txt	8	IGORIGOR	cipher29.txt	10	KROTHKROTH
cipher14.txt	9	JOAOPEDRO	cipher30.txt	9	VIRGILIUS
cipher15.txt	10	STEINSTEIN	cipher31.txt	5	VITOR
cipher16.txt	7	SCHULER			

Tabela 1: Resultados dos textos cifrados.

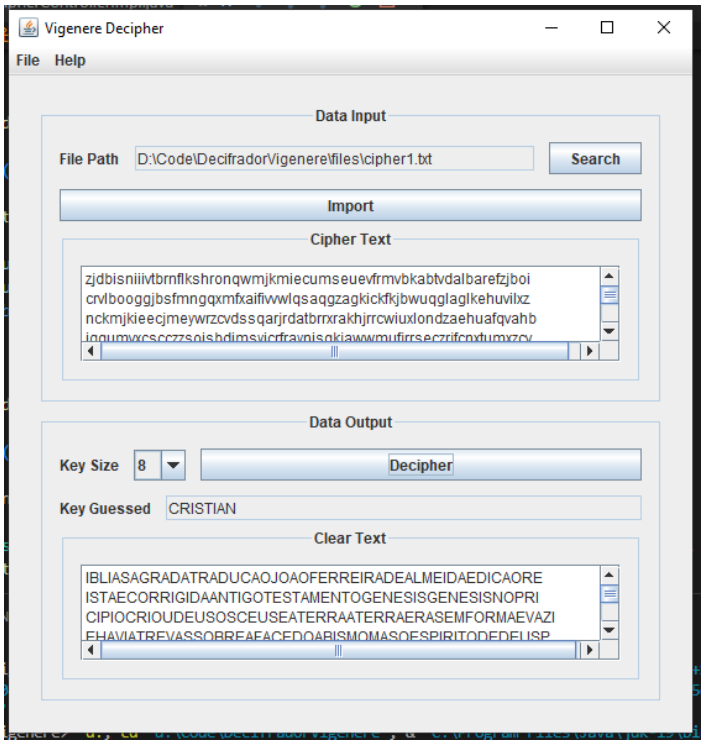

Figura 1: Tela principal da aplicação.

3 CONCLUSÃO

Em conclusão, o artigo descreveu o desenvolvimento de uma aplicação em Java para decifrar textos cifrados em Vigenére, utilizando o método Índice de Coincidência, a partir do tamanho das chaves. Foram implementadas diversas funções, como a leitura do texto cifrado a partir de arquivos, a criação de sequências de caracteres para teste, o cálculo do Índice de Coincidência, a busca da chave pelo tamanho da chave e a decifragem do texto cifrado.

A solução proposta é uma ferramenta útil para decifrar textos cifrados em Vigenére com base no tamanho das chaves, facilitando a análise de criptografias desse tipo em situações reais.

Futuros trabalhos podem incluir a melhoria da interface gráfica, a implementação de outros métodos de criptoanálise e a ampliação das funcionalidades da aplicação.

4 REFERÊNCIAS

CIFRA DE VIGENÉRE. Criptografia - Cifra de Vigenére - Bóson Treinamentos em Ciência e Tecnologia (bosontreinamentos.com.br). Acessado em 11/04/2023.