**CRIPTOANÁLISE - VIGENERE**

Edson Ricardo da Costa [[1]](#footnote-2)\*

Gabriel Fanto Stundner [[2]](#footnote-3)\*\*

**RESUMO**

Projeto desenvolvido na cadeira de Sistemas de Segurança da faculdade de Engenharia de Software na universidade da Pontifica Universidade do Rio grande do Sul. O propósito desse projeto é apresentar como funciona a cifra de codificação e decodificação de Vigenere utilizando a programação moderna, onde iremos explicar os passos de como a cifra funciona e como foi implementada.

**ABSTRACT**

Project developed in the chair of Security Systems of the Faculty of Software Engineering at the University of Pontificia Universidade do Rio Grande do Sul. The purpose of this project is to present how the Vigenère encoding and decoding cipher works using modern programming, where we will explain the steps of how the cipher works and how it was implemented.

**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 ás 26 cifras de César possiveis. 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.

**2 DESENVOLVIMENTO**

**3 CONCLUSÃO**

**REFERÊNCIAS**

CIFRA DE VIGENÉRE. [Criptografia - Cifra de Vigenère - Bóson Treinamentos em Ciência e Tecnologia (bosontreinamentos.com.br)](http://www.bosontreinamentos.com.br/seguranca/criptografia-cifra-de-vigenere/). Acessado em 11/04/2023.

1. \* Estudante de Engenharia de Software – Pontificia Universidade do Rio Grande do Sul. [↑](#footnote-ref-2)
2. **\*\*** Estudante de Engenharia de Software – Pontificia Universidade do Rio Grande do Sul. [↑](#footnote-ref-3)