

VINICIUS ROBERTO GOMES DOMINGUES

CRIPTOGRAFIA NO ENSINO MÉDIO

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação do Mestrado Profissional em Matemática em Rede Nacional, para obtenção do título de *Magister Scientiae*.

VIÇOSA
MINAS GERAIS - BRASIL
2017

**Ficha catalográfica preparada pela Biblioteca Central da Universidade
Federal de Viçosa - Câmpus Viçosa**

T

D671c Domingues, Vinícius Roberto Gomes, 1988-
2017 Criptografia no Ensino Médio / Vinícius Roberto Gomes
Domingues. – Viçosa, MG, 2017.
viii, 98f. : il. ; 29 cm.

Inclui apêndices.

Orientador: Mercio Botelho Faria.

Dissertação (mestrado) - Universidade Federal de Viçosa.

Referências bibliográficas: f83-84.

1. Aritmética. 2. Matrizes (Matemática). 3. Criptografia -
Ensino médio. I. Universidade Federal de Viçosa. Departamento
de Matemática. Programa de Pós-graduação em Matemática.
II. Título.

CDD 22 ed. 513

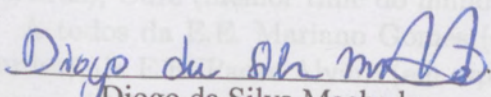
VINÍCIUS ROBERTO GOMES DOMINGUES

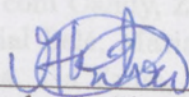
Agradecimentos

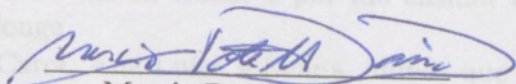
CRIPTOGRAFIA NO ENSINO MÉDIO

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós Graduação do Mestrado Profissional em Matemática em Rede Nacional, para obtenção do título de *Magister Scientiae*.

OVADA: 09 de fevereiro de 2017.


Diogo da Silva Machado


Anderson Tiago da Silva


Mercio Botelho Faria
(Orientador)

Resumo

DOMINGUES, Vinícius Roberto Gomes, M.Sc., Universidade Federal de Viçosa, fevereiro de 2017. **Criptografia no Ensino Médio**. Orientador: Mercio Botelho Faria.

Este trabalho trata aos conceitos de Aritmética Modular e Matrizes que são utilizados na Criptografia. Foram abordados fatos históricos para mostrar a importância da Criptografia. Apresentamos conteúdos que podem ser facilmente trabalhados em aula do Ensino Médio. Demonstramos dois métodos distintos de se criptografar mensagens utilizando tais conceitos, com sugestões de como podem ser utilizados.

Abstract

DOMINGUES, Vinícius Roberto Gomes, M.Sc., Universidade Federal de Viçosa, February, 2017. **Cryptography in High School**. Advisor: Mercio Botelho Faria.

2	Contexto Histórico	5
This work is related to concepts of modular arithmetic and matrices, which are used in cryptography. Historical facts have been approached to show the importance of cryptography. We present contents that can be easily applied in high school classes. We demonstrate two distinct methods of how to encrypt messages using these concepts, with suggestions on how they can be used.		
3.1	Critérios Selecionatórios Gerais e Todas as Áreas	24
3.2	Princípios e critérios de avaliação para a Área de Matemática	25
3.3	Crerérios eliminatórios específicos para Matemática	26
3.4	A escolha dos livros	27
3.4.1	Livro 1	28
3.4.2	Livro 2	29
3.4.3	Livro 3	31
4	A base Matemática do método RSA	33
4.1	Aritmética Modular	34
4.2	Propriedades da congruência modular	35
4.3	Resíduos	36
4.4	Inversos Modulares	39
4.5	Algoritmo do Resto Chinês	40
4.6	Potências	42
5	O Método RSA	43
5.1	Codificar	44
5.2	Decodificar	47
6	Um pouco de Matrizes e Determinantes	51
6.1	Fila, Linha, Coluna	53
6.2	Algumas Matrizes Especiais	55
6.2.1	Matriz Transposta	56