UFRRJ
INSTITUTO DE CIÊNCIAS EXATAS
MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL – PROFMAT

DISSERTAÇÃO

A CRIPTOGRAFIA COMO UMA FERRAMENTA PARA O ENSINO DA MATEMÁTICA NO ENSINO MÉDIO.

Rubens Brás de Lucena

2020

UNIVERSIDADE FEDERAL RURAL
DO RIO DE JANEIRO
INSTITUTO DE CIÊNCIAS EXATAS
MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL – PROFMAT

A CRIPTOGRAFIA COMO UMA FERRAMENTA PARA O ENSINO DA MATEMÁTICA NO ENSINO MÉDIO.

RUBENS BRÁS DE LUCENA

Sob a Orientação do Professor

Cláudio Cesar Saccomori Júnior

Dissertação submetida como requisito parcial para obtenção do grau de mestre no Curso de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, Área de Concentração em Matemática.

Seropédica, RJ

Setembro de 2020

Universidade Federal Rural do Rio de Janeiro
Biblioteca Central / Seção de Processamento Técnico

Ficha catalográfica elaborada
com os dados fornecidos pelo(a) autor(a)

Lucena, Rubens Brás de, 1976-
L935c A criptografia como uma ferramenta para o ensino da matemática no ensino médio / Rubens Brás de Lucena. - Seropédica, 2020.
82 f.: il.

Orientador: Cláudio Cesar Saccomori Júnior.
Dissertação(Mestrado). -- Universidade Federal Rural do Rio de Janeiro, Curso de Pós-graduação em Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, 2020.

1. Criptografia. 2. RSA. 3. Ensino de matemática. I. Saccomori Júnior, Cláudio Cesar, 1977-, orient. II Universidade Federal Rural do Rio de Janeiro. Curso de Pós-graduação em Mestrado Profissional em Matemática em Rede Nacional - PROFMAT III. Título.

UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

RUBENS BRÁS DE LUCENA

Dissertação submetida como requisito parcial para a obtenção de grau de **Mestre**, no Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, área de Concentração em Matemática.

DISSERTAÇÃO APROVADA EM 15/09/2020.

Conforme deliberação número 001/2020 da PROPPG, de 30/06/2020, tendo em vista a implementação de trabalho remoto e durante a vigência do período de suspensão das atividades acadêmicas presenciais, em virtude das medidas adotadas para reduzir a propagação da pandemia de Covid-19, nas versões finais das teses e dissertações as assinaturas originais dos membros da banca examinadora poderão ser substituídas por documento(s) com assinaturas eletrônicas. Estas devem ser feitas na própria folha de assinaturas, através do SIPAC, ou do Sistema Eletrônico de Informações (SEI) e neste caso a folha com a assinatura deve constar como anexo ao final da tese / dissertação.

Cláudio Cesar Saccomori Júnior (Dr. Orientador, Presidente da Banca)

André Luiz Martins Pereira. Dr. UFRRJ

Cleber Haubrichs dos Santos. Dr. IFRJ

AGRADECIMENTOS

A Ti, Senhor, agradeço pela proteção e amor. Sou grato pela Tua presença constante que me conduz firme e que tanto me ilumina e protege pelos caminhos da vida.

Aos meus pais que me deram a vida e me ensinaram a vivê-la com dignidade.

À minha esposa, amiga, companheira de vida e maior inspiração, Flávia Fernanda, obrigado por motivar todos os meus planos e sonhos.

Às minhas filhas Ana Clara e Isadora por me fazerem querer ser melhor a cada dia.

À minha família e à família de minha esposa pelo apoio, companheirismo, amor fraterno e compreensão da minha ausência em decorrência da premissa de tempo que o mestrado exige.

Aos meus amigos da turma PROFMAT/UFRRJ 2018 pelo companheirismo e ajuda e, em especial, agradeço imensamente aos grandes amigos Leonardo Bueno e Alan Rangel por formarem comigo um grupo de estudos e serem tão generosos em compartilhar seus conhecimentos. Muita sorte ingressar no mestrado justamente nessa turma e com esses amigos que levarei para a vida.

Aos professores e tutores do PROFMAT/UFRRJ por todos os ensinamentos transmitidos e, em especial, agradeço ao professor Dr. Cláudio Cesar Saccomori Júnior pela orientação, paciência, dedicação e profissionalismo.

Aos meus alunos e ex alunos que, com certeza, a cada aula, contribuíram em minha formação e me fizeram aprender ensinando.

Aos meus amigos, colegas de profissão e, em especial, ao professor Carlos Augusto.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de financiamento 001.

This study was financed in party by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance code 001.

RESUMO

LUCENA, Rubens Brás de. **A CRIPTOGRAFIA COMO UMA FERRAMENTA PARA O ENSINO DA MATEMÁTICA NO ENSINO MÉDIO.** 2020. 82p. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT). Instituto de Ciências Exatas, Universidade Federal Rural do Rio de Janeiro, Seropédica, RJ, 2020.

O presente trabalho é pautado na investigação da influência que o uso da criptografia causa no processo de ensino-aprendizagem dos alunos do ensino médio. A criptografia traz consigo temas relevantes para dar significado aos conceitos matemáticos estudados no ensino médio, fazendo conexões com conteúdos de séries anteriores e abordando pré-requisitos que são fundamentais para diminuir as dificuldades dos mesmos frente às avaliações internas e externas. Nesse sentido, este trabalho tem como objetivo verificar os avanços em relação aos conteúdos de matrizes e teoria dos números tratados com a turma. A pesquisa foi desenvolvida com 25 alunos do terceiro ano do ensino médio em uma escola estadual, localizada na cidade de Japeri - RJ e dividida em sete aulas de cinquenta minutos cada. Inicialmente apresenta-se um breve histórico sobre o desenvolvimento da criptografia, desde sua origem até o sistema RSA, e os fundamentos matemáticos básicos necessários para compreender os processos criptográficos propostos. Em seguida são aplicadas três atividades com a turma dividida em grupos com o objetivo de criptografar e descriptografar mensagens. Com base nos resultados obtidos por comparação das notas dos alunos em avaliações internas e externas, aplicadas antes e após a realização do trabalho, é possível observar uma melhora de rendimento da turma. O que demonstra que, de fato, a criptografia tem potencial para ser uma boa ferramenta para o ensino da matemática no ensino médio e que não é um conceito exclusivo de filmes de espionagem.

Palavras-chave: criptografia; sistema RSA; ensino de matemática.

ABSTRACT

LUCENA, Rubens Brás de. **CRYPTOGRAPHY AS A TOOL FOR TEACHING MATHEMATICS IN HIGH SCHOOL .** 2020. 82 pages. Dissertation (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT). Instituto de Ciências Exatas, Universidade Federal Rural do Rio de Janeiro, Seropédica, RJ, 2020.

The current study is based on the investigation of the influence that the use of cryptography causes in the teaching-learning process of high school students. Cryptography brings with it relevant themes to give meaning to the mathematical concepts studied in high school, making connections with content from previous grades and addressing prerequisites that are essential to reduce their difficulties in the face of internal and external evaluations. In this sense, this study aims to verify the advances in relation to the contents of matrices and number theory treated with the classes. The research was developed with 25 students of the last year of high school in a state school, located in the city of Japeri - RJ and divided into seven classes of fifty minutes each. Initially, a brief history of the development of cryptography is presented, from its origin to the RSA system, and the basic mathematical foundations necessary to understand the proposed cryptographic processes. Then, three activities were applied with the class divided into groups in order to encrypt and decrypt messages. Based on the results obtained by comparing students' grades in internal and external evaluations applied before and after the work is done, it is possible to observe an improvement in class performance. Which demonstrates that, in fact, cryptography has the potential to be a good educational tool for teaching mathematics in high school and that is not an exclusive concept of spy films.

Keywords: cryptography; RSA system; mathematics teaching.

Lista de figuras

SUMÁRIO

1. INTRODUÇÃO

Este trabalho é dedicado a detalhar atividades de aplicação da criptografia em sala de aula, apresentando ao aluno o contexto histórico, revisando vários conceitos, dando significado ao que é estudado e mostrando que a mesma é uma ferramenta de segurança amplamente utilizada nos meios de comunicação e nas transações via internet e consiste basicamente na transformação de determinado dado ou mensagem a fim de ocultar seu real significado.

Ensinar matemática pelo caminho da repetição de procedimentos, fazendo cálculos desprovidos de utilidade e representatividade, provoca a desmotivação dos alunos e aumenta a dificuldade de aprendizado. Nesse sentido, o presente trabalho é produto da reflexão à busca de um tema com potencial de abordar conteúdos matemáticos do ensino que seja significativo ao aluno.

A criptografia surge como um tema que, além de estar relacionado com assuntos do ensino médio, também resgata vários pré-requisitos importantes de séries anteriores.

Assim, temos como objetivo neste trabalho, estimular o aluno do ensino médio ao estudo da matemática mostrando o funcionamento da criptografia e como ela está presente em nosso dia a dia.

Esta pesquisa é composta por cinco capítulos, onde o primeiro está desenvolvido neste texto introdutório.

O segundo capítulo aborda a matemática que está ligada, direta ou indiretamente, aos métodos criptográficos aplicados em sala de aula de modo que seja possível compreender os mistérios da criptografia e também explicar o funcionamento e a segurança dos mesmos. O material de apoio para o estudo de conceitos relacionados à teoria dos números e à compreensão dos métodos criptográficos foi formado principalmente pelas referências Coutinho (2005) e Hefez (2006).

O terceiro capítulo traz um breve histórico sobre os números primos e a criptografia, desde as cifras de substituição até os métodos de chaves assimétricas. Para uma melhor compreensão do presente, faz-se necessário conhecer características do passado.

O quarto capítulo é dedicado à aplicação da criptografia em sala de aula, dando exemplos de como a criptografia é abordada nos livros didáticos e em vestibulares e, principalmente, detalhando as atividades desenvolvidas numa turma de terceiro ano do ensino médio de uma escola estadual localizada no município de Japeri-RJ.

Encerramos com algumas considerações finais e relatando os impactos gerados pelo trabalho no processo de ensino aprendizagem e na relação professor-aluno.

1.1 MOTIVAÇÃO.

Lecionar é algo que aumenta o próprio conhecimento, germina a independência, a liberdade de consciência, a percepção dos limites e de possibilidades, aumenta o grau de autonomia, de atualização, de investigação, de compreensão, de pensamento como uma busca de melhorar o mundo, como um desafio.

A situação de aula é uma busca de conhecer o que se passa na cabeça dos alunos, de lhes proporcionar descobertas próprias, de gerar mudanças em cada um, de acolhimento, de aceitação das pessoas, de aprender com elas. É uma busca de desenvolver e multiplicar ideias. Um movimento inteiro, interno e externo, emocional e intelectual, numa relação de reciprocidade mútua entre professor-aluno.

Ensinar matemática fazendo cálculos desprovidos de utilidade, contextualização e representatividade, ocasiona um problema na relação professor-aluno. Nesse sentido, o tema criptografia foi escolhido por ser muito rico e estar relacionado aos conteúdos do ensino médio, tornando-se uma excelente forma de mostrar ao aluno as aplicações daquilo que se aprende em sala de aula, dando significado ao conteúdo.

Nos Parâmetros Curriculares Nacionais (PCNs) temos que:

> "–A matemática é componente importante na construção da cidadania na medida em que a sociedade se utiliza cada vez mais de conhecimentos científicos e recursos tecnológicos dos quais os cidadãos devem se apropriar.
> – A matemática precisa estar ao alcance de todos e a democratização do seu ensino deve ser prioritária do trabalho docente.
> – A atividade matemática escolar não é "olhar para coisas prontas e definitivas" mas a construção e a apropriação de um conhecimento pelo aluno, que se servirá dele para compreender e transformar sua realidade.

> – No ensino da matemática, destacam-se dois aspectos básicos: um consiste em relacionar observações do mundo real com representações (esquemas, tabelas, figuras); outro consiste em relacionar essas representações com princípios e conceitos matemáticos. Nesse processo a comunicação tem grande importância e deve ser estimulada levando-se o aluno a "falar" e a "escrever" sobre matemática... ." (BRASIL,1997,p.15)

Um grande problema enfrentado pelos professores de matemática, em relação aos alunos, é a falta de pré-requisitos necessários para o bom entendimento do conteúdo. Existe, infelizmente, uma enorme defasagem entre os conceitos matemáticos que o aluno do ensino médio deveria dominar e os conceitos que, de fato, ele domina. Com base nisso, há uma demanda, por parte dos alunos, de um tema capaz de dar uma vertente mais prática ao conteúdo matemático e, ao mesmo tempo, resgatar conteúdos anteriores de forma harmônica com os conteúdos da série vigente.

Os PCNs para o ensino médio reforçam:

> "A aprendizagem em matemática está ligada à compreensão, isto é, à apreensão do significado; apreender o significado de um objeto ou acontecimento pressupõe vê-lo em suas relações com outros objetos e acontecimentos. Assim, o tratamento dos conteúdos em compartimentos estanques e numa rígida sucessão linear deve dar lugar a uma abordagem em que as conexões sejam favorecidas e destacadas. O significado da matemática para o aluno resulta das conexões que ele estabelece entre ela e as demais disciplinas, entre ela e seu cotidiano e das conexões que ele estabelece entre os diferentes temas matemáticos"(BRASIL,1997,p.19).

A aplicação em sala de aula de técnicas de criptografia com a utilização de operações com matrizes, critérios de divisibilidade, congruência, entre outros assuntos, torna possível a visualização desses conteúdos em situações reais e estimula a aprendizagem. As técnicas de criptografia utilizadas se mostram como excelentes meios para a concretização desses saberes.

Este trabalho visa um resultado quali-quantitativo, através de atividades teóricas e práticas, no intuito de uma melhoria no rendimento dos alunos envolvidos. Neste processo buscamos conexões entre a matemática que se aprende em sala de aula e o cotidiano do aluno dando significado ao que é aprendido.

As atividades foram aplicadas entre abril e agosto de 2019 em uma turma com 25 alunos, entre 17 e 19 anos, do 3º ano do ensino médio, que estudam em tempo integral em uma escola estadual situada no município de Japeri - RJ.

Este trabalho baseia-se na busca do desenvolvimento de um procedimento metodológico que possa facilitar o processo ensino/aprendizagem da matemática da série vigente dos alunos, fazendo conexões com conteúdos adormecidos ou nunca por eles aprendidos, de forma dinâmica e desafiadora. Para isso, ocorreu a busca de um tema que atendesse à essas demandas e a criptografia se mostrou um tema bastante promissor.

2. FUNDAMENTOS MATEMÁTICOS.

Antes de descrevermos como a criptografia pode ser abordada em sala de aula com os alunos, estabeleceremos alguns resultados que serão usados para entender os seus mistérios e também para explicar como o método RSA funciona. As demonstrações desses resultados são baseadas naquelas encontradas em Hefez (2006) e em Coutinho (2005).

2.1 MATRIZES.

Temos indícios de que os chineses resolveram alguns problemas cujos cálculos eram feitos em formas de quadros que sugerem a ideia de matrizes. Em 1790 Joseph Louis Lagrange (1736-1813) apresenta o primeiro uso da noção desses quadros ou tabelas. Ele utilizou essas tabelas para o estudo de máximos e mínimos de funções reais de várias variáveis. Em 1850, James Joseph Sylvester (1814-1897) chamou essa representação de matriz, nome utilizado até os dias atuais.

Uma matriz de tipo m x n, onde m, $n \geq 1$ é uma tabela formada por mn elementos dispostos em m linhas e n colunas; se $n = 1$, a matriz é dita matriz coluna; se $m = 1$, matriz linha; se $m = n$, matriz quadrada de ordem n.

Em uma matriz quadrada A de ordem n, os elementos a_{ij} tais que $i = j$ formam a diagonal principal e os elementos a_{ij} tais que $i + j = n + 1$ formam a diagonal secundária.

Quando os elementos da diagonal principal de uma matriz quadrada são iguais a 1 e os demais elementos iguais a zero, temos uma matriz chamada matriz identidade. A matriz I_n é o elemento neutro da multiplicação de matrizes quadradas de mesma ordem.

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, I_n = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}.$$

2.1.1 PRODUTO DE MATRIZES.

Dada uma matriz $A = (a_{ij})$ de tipo m x n, e uma matriz $B = (b_{jk})$, de tipo n x p, chama-se produto de A por B (indica-se AB) a matriz $C = (c_{ik})$, de tipo m x p, onde

$$c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk} = a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{in}b_{nk}\,.$$

2.1.2 MATRIZES INVERTÍVEIS.

Uma matriz quadrada A de ordem n se diz invertível se existe uma matriz B tal que $AB = BA = I_n$. A matriz B se diz inversa de A e se indica por A^{-1}.

Observe que, se A é invertível, então a sua inversa é única : com efeito, se B e B' são inversas de A, temos

$B = BI_n = B\,(AB') = (BA)B' = I_nB' = B'$

Logo $B = B'$, ou seja a inversa é única!

Proposição: Se A é invertível, então a sua inversa é invertível e $(A^{-1})^{-1} = A$. Se A e B são invertíveis, o produto é invertível e $(AB)^{-1} = B^{-1} \cdot A^{-1}$.

Demonstração: A primeira parte é imediata. O leitor deve observar, na segunda parte, que a inversa do produto é igual ao produto das inversas na ordem contrária (compare com a transposta do produto). Para provar, sejam $C = AB$ e $D = B^{-1}\ A^{-1}$. Então

$CD = (AB)\,(B^{-1}\,A^{-1}) = A\,(B\,B^{-1})\,A^{-1} = A\,I\,A^{-1} = A\,A^{-1} = I.$

Da mesma forma $DC = I$. Portanto D é inversa de C.

■

Iremos, agora, caracterizar as matrizes invertíveis.

Consideraremos o conjunto das matrizes quadradas de elementos reais. Seja *A* uma matriz de ordem *n, com* $n \leq 3$, desse conjunto. Chamamos determinante da matriz *A* o número que podemos obter operando com os elementos de *A* da seguinte forma:

i. Se *A* é de ordem *n* = 1, então det *A* é o único elemento de *A*.

$A = [\ a_{11}\ ] \rightarrow \det A = a_{11}$.

ii. Se *A* é de ordem *n* = 2, o produto dos elementos da diagonal principal menos o produto dos elementos da diagonal secundária.

$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \rightarrow \det = a_{11}a_{22} - a_{21}a_{12}$.

iii. Se *A* é de ordem *n* = 3, isto é,

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix},$$

definimos det $A = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12}$.

Existe uma definição geral de determinante que pode ser vista em (HEFEZ, 2016, p.188)

Proposição: A matriz quadrada *A* é invertível se, e somente se, det $A \neq 0$.
A demonstração pode ser encontrada em (IEZZI, 2004, p.123).

Exemplo: Dadas as matrizes

$A = \begin{pmatrix} 2 & 6 \\ 1 & 3 \end{pmatrix}$ e $B = \begin{pmatrix} 2 & 4 \\ 1 & 4 \end{pmatrix}$.

Temos que, det A = 2 . 3 - 1 . 6 = 0, ou seja a matriz A não é invertível.

E det B = 2 . 4 - 1 . 4 = 4 e, como det $B \neq 0$, podemos dizer que B é invertível. Para determinar a matriz inversa de B, usamos a equação:

$\begin{pmatrix} 2 & 4 \\ 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, que resultará nos sistemas de equações:

1) $\begin{cases} 2a + 4c = 1 \\ 1a + 4c = 0 \end{cases}$ e 2) $\begin{cases} 2b + 4d = 0 \\ b + 4d = 1 \end{cases}$.

Resolvendo os sistemas, obtemos:

1)	2)
a = 1 (subtraindo as linhas)	b = -1
2.1 + 4c = 1 (substituindo o valor encontrado)	-1 + 4d =1
4c = -1	4d = 2
$c = \frac{-1}{4}$	$d = \frac{1}{2}$

Assim, $B^{-1} = \begin{pmatrix} 1 & -1 \\ \frac{-1}{4} & \frac{1}{2} \end{pmatrix}$.

2.2 NOÇÕES DE TEORIA DOS NÚMEROS.

Apresentamos nesta seção os fundamentos matemáticos em aritmética necessários para justificar o funcionamento dos sistemas criptográficos utilizados. Em teoria dos números, os conceitos são muito abstratos e geralmente de difícil compreensão sem exemplos, por conta disso, esta seção contará com exemplos para facilitar o entendimento.

2.2.1 DIVISIBILIDADE.

Dados dois números inteiros a e b, diremos que a *divide* b, escrevendo $a \mid b$, quando existir $c \in \mathbb{Z}$ tal que $b = ca$. Nesse caso, diremos também que a é um *divisor* ou um fator de b ou, ainda, que b é um múltiplo de a ou que b é *divisível* por a.

A notação $a \mid b$ não representa nenhuma operação em $\mathbb{Z}$, nem representa uma fração. Trata-se de uma sentença que diz ser verdade que existe *c* inteiro tal que *b* = *ca*. A negação dessa sentença é representada por $a \nmid b$, significando que não existe nenhum número inteiro *c* tal que *b* = *ca*.

Exemplos

É fácil mostrar pela definição que:

i) $0 \mid 0$, $\pm 1 \mid 0$, $\pm 2 \mid 0$, $\pm 3 \mid 0$, de forma geral, $z \mid 0$ para todo $z \in \mathbb{Z}$.

ii) $\pm 1 \mid 8$ $\pm 2 \mid 8$ $\pm 4 \mid 8$ $\pm 8 \mid 8$

iii) $0 \nmid 8$ $\pm 3 \nmid 8$ $\pm 5 \nmid 8$ $\pm 6 \nmid 8$ $\pm 7 \nmid 8$

2.2.2 DIVISÃO EUCLIDIANA.

Teorema: Sejam *a* e *b* dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros *q* e *r* tais que

$$a = bq + r, \text{ com } 0 \leq r < |b|.$$

Demonstração:
Considere o conjunto

$$S = \{x = a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\}).$$

Existência: Pela propriedade Arquimediana, existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, logo $a - nb > 0$, o que mostra que *S* é não vazio. O conjunto *S* é limitado inferiormente por 0, logo, pelo Princípio da Boa Ordenação, temos que *S* possui um menor elemento *r*. Suponhamos então que $r = a - bq$. Sabemos que $r \geq 0$. Mostraremos que $r < |b|$. Suponhamos por absurdo que $r \geq |b|$. Portanto, existe *s*

$\in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, logo $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de S, pois $s = a - (q \pm 1)b \in S$, com $s < r$.

Unicidade: Suponha que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < |b|$ e $0 \leq r' < |b|$. Assim, temos que $-|b| < -r \leq r' - r \leq r' < |b|$. Logo, $|r' - r| < |b|$. Por outro lado, $b(q - q') = r' - r$, o que implica que

$$|b||q - q'| = |r' - r| < |b|,$$

o que só é possível se $q = q'$ e consequentemente, $r = r'$.

■

Nas condições do teorema acima, os números q e r são chamados, respectivamente, de *quociente* e de *resto* da divisão de a por b.

Da divisão euclidiana, temos que o resto da divisão de a por b é zero se, e somente se, b divide a.

Exemplos.

1) O quociente e o resto da divisão de 17 por 3 são $q = 5$ e $r = 2$. O quociente e o resto da divisão de -17 por 3 são $q = -6$ e $r = 1$.

2) Determinaremos o número de múltiplos de 7 que se encontram entre 1 e 353.

Pelo algoritmo da divisão temos que

$$353 = 7 \cdot 50 + 3,$$

ou seja, o maior múltiplo de 7 que cabe em 353 é 7.50, onde 50 é o quociente da divisão de 353 por 7. Portanto, os múltiplos de 7 entre 1 e 353 são

$$1 \cdot 7, 2 \cdot 7, 3 \cdot 7, ..., 50 \cdot 7$$

e, consequentemente, são em número de 50.

2.2.3 MÁXIMO DIVISOR COMUM.

Sejam dois inteiros *a* e *b*, distintos ou não. Um número inteiro *d* será dito um divisor comum de *a* e *b* se $d \mid a$ e $d \mid b$.

Por exemplo, os números $\pm 1, \pm 2, \pm 4, \pm 8$ são os divisores comuns de 16 e 24.

A definição dada a seguir é essencialmente a definição dada por Euclides nos *Elementos* e constitui-se em um dos pilares de sua aritmética.

Diremos que um número inteiro $d \geq 0$ é um *máximo divisor comum* (mdc) de *a* e *b*, se possuir as seguintes propriedades:

i) *d* é um divisor comum de *a* e *b*, e

ii) *d* é divisível por todo divisor comum de *a* e *b*.

Neste caso, denotaremos $d = (a,b)$.

Concluindo o exemplo, o mdc de 16 e 24 é 8.

2.2.4 ALGORITMO DE EUCLIDES

A seguir, apresentaremos o método chamado *Algoritmo de Euclides,* um primor do ponto de vista computacional e pouco conseguiu-se aperfeiçoá-lo em mais de dois milênios.

Dados $a, b \in \mathbb{N}$, podemos supor $b \leq a$. Se $b = 1$ ou $b = a$, ou ainda $b \mid a$, já vimos que $(a,b) = b$. Suponhamos, então, que $1 < b < a$ e que $b \nmid a$. Logo, pela divisão euclidiana, podemos escrever

$$a = bq_1 + r_1, \text{ com } 0 < r_1 < b.$$

O algoritmo pode ser sintetizado e realizado na prática como mostramos a seguir.

Inicialmente, efetuamos a divisão $a = bq_1 + r_1$ e colocamos os números envolvidos no seguinte diagrama:

	q_1	
a	b	
r_1		

A seguir, continuamos efetuando a divisão $b = r_1q_2 + r_2$ e colocamos os números envolvidos no diagrama

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Prosseguindo, enquanto for possível dividir r_i por r_{i+1}, teremos

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	$r_n = (a,b)$
r_1	r_2	r_3	r_4	$\cdots$	r_n		

Pode-se demonstrar que o último resto não nulo é justamente o mdc entre a e b.

Exemplo

Calculemos o mdc de 6180 e 5200.

	1	5	3	3	1	
6180	5200	980	300	80	60	20
980	300	80	60	20		

Observe que, no exemplo acima, o algoritmo de Euclides fornece-nos:

20 = 80 - 1 . 60
60 = 300 - 3 . 80
80 = 980 - 3 . 300
300 = 5200 - 5 . 980,
Donde se segue que:
20 = 80 - 1 . 60
= 80 - 1 . (300 - 3 . 80)
= 4 . 80 - 300
= 4 . (980 - 3 . 300) - 300
= 4 . 980 - 13 . 300
= 4 . 980 - 13 . (5200 - 5 . 980)
= 69 . 980 -13 . 5200.
= 69 . (6180 - 1 . 5200) - 13. 5200
= 69 . 6180 + (-82) . 5200
Temos, então, que
(6180,5200) = 20 = 69 . 6180 + (-82) . 5200.

Conseguimos, através do algoritmo de Euclides de trás pra frente, escrever 20 = (6180,5200) como um múltiplo de 6180 mais um múltiplo de 5200.

Quando utilizarmos o Algoritmo de Euclides para expressar (a,b) na forma $ma + nb$, com m,$n \in \mathbb{Z}$, como no exemplo acima, referir-nos-emos a ele como *Algoritmo de Euclides Estendido.*

O leitor pode encontrar a demonstração do porquê este algoritmo de fato nos fornecer o mdc (a,b) em Hefez (2013, p.77).

2.2.5 NÚMEROS PRIMOS.

O interesse pelos números primos aumentou significativamente nas últimas décadas e o seu uso em criptografia RSA teve grande contribuição para isso. O teste de primalidade, que é usado para garantir que um dado número natural é primo, passou a ter uma importância de valor econômico significativo. Isto porque a

segurança do sistema RSA reside na dificuldade de fatorar $n = p \cdot q$ quando p e q são primos com dezenas de algarismos.

Definição: Um número natural maior do que 1 que só possui como divisores positivos 1 e ele próprio é chamado de número *primo*.

Dados dois números primos p e q e um número inteiro a qualquer, decorrem da definição acima os seguintes fatos:

i. Se $p \mid q$, então $p = q$. De fato, como $p \mid q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$.

ii. Se $p \nmid a$, então $(p,a) = 1$.

De fato, se $(p,a) = d$, temos que $d \mid p$ *e* $d \mid a$. Portanto, $d = p$ *ou* $d = 1$. *Mas* $d \neq p$, *pois* $p \nmid a$ *e,* consequentemente, $d = 1$.

Um número maior do que 1 e que não é primo será dito *composto*. Portanto, se um número natural $n > 1$ é composto, existirá um divisor natural n_1 de n tal que $1 < n_1 < n$. Logo, existirá um número natural n_2 tal que

$n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$.

Exemplo:

2, 3, 5, 7, 11, 13, 1009, são números primos, enquanto que 4, 6, 8, 9, 10, 1024, são compostos.

Hefez (2013, p.122) escreveu que "do ponto de vista da estrutura multiplicativa dos naturais, os números primos são os mais simples e ao mesmo tempo são suficientes para gerar todos os números naturais"

Lema de Gauss*:*

Sejam a, b *e* c números inteiros. *Se* $a \mid bc$ e $(a,b) = 1$, então $a \mid c$.

A demonstração pode ser encontrada em (HEFEZ, 2013, p.83).

Lema de Euclides.

Sejam *a, b, p* ∈ ℤ, com *p* primo**.** Se *p* | *ab*, então *p* | *a ou p* | *b.*

Demonstração:

Basta provar que, se *p* | *ab* e *p*∤*a, então p* | *b*. Mas, se *p*∤*a, temos que (p,a) = 1,* e o resultado segue-se do lema de Gauss*.*

■

Corolário.

Se *p*, p_1, ... ,p_n são números primos e, se *p* | $p_1 ... p_n$, então *p* = p_i para algum *i* = 1, ..., *n.*

A demonstração pode ser encontrada em (HEFEZ, 2013, p.123).

Teorema fundamental da Aritmética.

Teorema: Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.

Demonstração:

Usaremos a segunda forma do Princípio de indução. Se *n* = 2, o resultado é obviamente verificado.

Suponhamos o resultado válido para todo número natural menor do que *n* e vamos provar que vale para *n*. Se o número *n* é primo, nada temos a demonstrar. Suponhamos, então, que *n* seja composto. Logo, existem números naturais n_1 *e* n_2 tais que *n* = $n_1 n_2$, com 1< n_1 < *n* e 1< n_2 < *n*. Pela hipótese de indução, temos que existem números primos p_1 , ..., p_r e q_1 , ..., q_s tais que $n_1 = p_1 ... p_r$ e $n_2 = q_1 ... q_s$. Portanto, *n* = $p_1 ... p_r q_1 ... q_s$.

Provaremos, agora, a unicidade da escrita. Suponha que tenhamos *n* = $p_1 ... p_r = q_1 ... q_s$, onde os p_i e os q_j são números primos. Como $p_1 | q_1 ... q_s$, pelo corolário acima, temos que $p_1 = q_j$ para algum *j*, que, após reordenamento de q_1 , ..., q_s, podemos supor que seja q_1. Portanto,

$p_2 \cdots p_r = q_2 \cdots q_s$.

Como $p_2 \cdots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares.

■

Teorema: Existem infinitos números primos.

Demonstração: Suponha, por absurdo, que exista um número finito de primos $p_1 p_2 \cdots p_r$.

Tomemos o número natural $n = p_1 p_2 \cdots p_r + 1$. Pelo teorema fundamental da aritmética, *n* possui, ao menos, um fator primo *p*, que deve ser algum p_i, com $1 \leq i \leq r$. Como $p_i \mid p_1 p_2 \cdots p_r$ e $p_i \mid n$, então $p_i \mid 1$, o que é absurdo, pois 1 não tem divisores maiores que ele mesmo. Logo, existem infinitos números primos.

■

2.2.6 TESTE DE PRIMALIDADE.

Com o surgimento da criptografia de chave pública, a partir da década de 1960, apareceram várias tentativas de obter um método eficiente para verificar a primalidade de um número natural. A importância desse problema cresce a cada ano devido à crescente utilização de números primos nos algoritmos de criptografia. O ponto chave da segurança do sistema de criptografia RSA é a enorme dificuldade de se fatorar um número muito grande.

Na atualidade, para que o sistema RSA seja considerado seguro, é necessário que o número escolhido para a chave contenha dois primos *p* e *q* com aproximadamente 100 algarismos cada. O grande desafio do método consiste em ter certeza que os números escolhidos sejam realmente primos.

Usaremos o crivo de Eratóstenes como exemplo de teste de primalidade, ele é utilizado para encontrar os números primos ou determinar se um número é primo, esse método baseia-se na eliminação dos múltiplos dos primos anteriores ao número que se deseja verificar se é primo ou não. Para simplificar o método, basta listar todos os números de 2 até *n*, em seguida retirar os múltiplos dos números

primos cujo quadrado não supere o número que desejamos testar a primalidade, com base na seguinte proposição.

Proposição: Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leq n$, então ele é primo.

Demonstração: Suponha, por absurdo, que n não seja primo. Seja q o menor primo que divide n, então $n = qk$ e $q \leq k$. Daí, $q^2 = q \cdot q \leq q \cdot k = n \Rightarrow q^2 \leq n$, o que é absurdo,pois n é divisível por um primo q tal que $q^2 \leq n$. Logo, n é primo.

■

Mostraremos como funciona o processo calculando todos os primos menores que 300. Primeiro escrevemos todos os números de 2 até 300. Como 2 é primo, riscamos todos os números múltiplos de 2, maiores que 2, depois riscamos todos os múltiplos de 3, maiores que 3. Depois, riscamos todos os múltiplos de 5, maiores que 5. Depois, riscamos todos os múltiplos de 7, maiores que 7. Depois, riscamos todos os múltiplos de 11, maiores que 11. Depois, riscamos todos os múltiplos de 13, maiores que 13. E, por fim, riscamos todos os múltiplos de 17, maiores que 17. Como o próximo número primo é 19 e $19^2 = 361 > 300$, paramos o processo no número primo 17. Assim, todos os números da lista que não foram riscados são todos os primos menores que 300.

	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100	101	102	103	104	105
106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132	133	134	135
136	137	138	139	140	141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160	161	162	163	164	165
166	167	168	169	170	171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190	191	192	193	194	195
196	197	198	199	200	201	202	203	204	205	206	207	208	209	210
211	212	213	214	215	216	217	218	219	220	221	222	223	224	225
226	227	228	229	230	231	232	233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248	249	250	251	252	253	254	255
256	257	258	259	260	261	262	263	264	265	266	267	268	269	270
271	272	273	274	275	276	277	278	279	280	281	282	283	284	285
286	287	288	289	290	291	292	293	294	295	296	297	298	299	300

Os números realçados em amarelo são os primos de 2 até 300.

O maior número primo descoberto atualmente, anunciado em 21 de dezembro de 2018, tem 24.862.048 dígitos, mais de 1,5 milhão de dígitos a mais do que o número primo recorde descoberto em 2017. Ele pode ser expresso como $2^{82589933}$ - 1 e foi chamado de M82589933. Pertencente à classe especial de números primos raros, conhecidos como primos de Mersenne, este é o 51° primo de Mersenne descoberto.

De acordo com a publicação no site do IMPA em 15 de janeiro de 2019, Patrick Laroche é o "pai" do M82589933, ele é um profissional de TI e sua caça ao número primo de verdade durou cerca de 4 meses.

A tabela apresenta os maiores números primos conhecidos. M_p é um número de Mersenne primo com expoente *p* e que satisfaz a relação $M_p = 2^p - 1$.

Figura 1 - Maiores primos conhecidos.

Nome M_n	Data de descoberta	Primo M_q	Número de algarismos	Processador
M_{35}	13 de novembro de 1996	$M_{1398269}$	420.921	Pentium (90 MHz)
M_{36}	24 de agosto de 1997	$M_{2976221}$	895.932	Pentium (100 MHz)
M_{37}	27 de janeiro de 1998	$M_{3021377}$	909.526	Pentium (200 MHz)
M_{38}	1 de junho de 1999	$M_{6972593}$	2.098.960	Pentium (350 MHz)
M_{39}	14 de novembro de 2001	$M_{13466917}$	4.053.946	AMD T-Bird (800 MHz)
M_{40}	17 de novembro de 2003	$M_{20996011}$	6.320.430	Pentium (2 GHz)
M_{41}	15 de maio de 2004	$M_{24036583}$	7.235.733	Pentium 4 (2.4 GHz)
M_{42}	18 de fevereiro de 2005	$M_{25964951}$	7.816.230	Pentium 4 (2.4 GHz)
M_{43}	15 de dezembro de 2005	$M_{30402457}$	9.152.052	Pentium 4 (2 GHz overclocked para 3 GHz)
M_{44}	4 de setembro 2006	$M_{32582657}$	9.808.358	Pentium 4 (3 GHz)
M_{45} [*]	6 de setembro de 2008	$M_{37156667}$	11.185.272	
M_{46} [*]	12 de abril de 2009	$M_{42643801}$	12.837.064	Intel Core 2 Duo (3 GHz)
M_{47} [*]	23 de agosto de 2008	$M_{43112609}$	12.978.189	Intel Core 2 Duo E6600 CPU (2.4 GHz)
M_{48} [*]	25 de janeiro de 2013	$M_{57885161}$	17.425.170	Intel Core 2 Duo E8400 @ 3.00GHz
M_{49} [*]	7 de janeiro de 2016	$M_{74207281}$ [**]	22.338.618	Intel Core i7-4790
M_{50}	3 de janeiro de 2018	$M_{77232917}$	23.249.425	Intel Core i5-6600 Quad-Core
M_{51}	21 de dezembro de 2018	$M_{82589933}$	24.862.048	Intel Core i5-4590T

Fonte: Wikipedia.org.maior número primo conhecido

Veremos outros exemplos de testes de primalidade no estudo das congruências.

2.2.7 CONGRUÊNCIA.

O sistema criptográfico RSA usa essencialmente a aritmética dos restos, tanto para justificar porque o RSA funciona como para realizar os testes de primalidade.

Definição. Seja *m* um número natural. Diremos que dois números inteiros *a* e *b* são congruentes módulo *m* se os restos de sua divisão euclidiana por *m* são iguais. Quando os inteiros *a* e *b* são congruentes módulo *m*, escreve-se

$$a \equiv b \bmod m.$$

Quando a relação $a \equiv b \bmod m$ for falsa, diremos que *a e b* não são congruentes e denotaremos:

$$a \not\equiv b \bmod m.$$

Proposição. Suponha que *a, b, m* ∈ ℤ, com *m* > 1. Tem-se que *a* ≡ *b mod m se,* e somente se, *m* | *b - a.*

Demonstração: Sejam *a* = *mq* + *r*, com 0 ≤ *r* < *m* e *b* = *mq'* + *r'*, com 0 ≤ *r'* < *m*, as divisões euclidianas de *a* e *b* por *m*, respectivamente. Logo,

$$b - a = m(q' - q) + (r' - r).$$

Portanto, *a* ≡ *b mod m,* se, e somente se*, r* = *r',* o que, em vista da igualdade acima, é equivalente a dizer que *m* | *b - a*, já que $|r - r'| < m.$

■

Proposição 2. Seja *m* ∈ ℕ, *m* > 0. Para todos *a, b, c* ∈ ℤ, tem-se que

i. a ≡ *a mod m,*

ii. se a ≡ *b mod m,* então *b* ≡ *a mod m,*

iii. se a ≡ *b mod m e b* ≡ *c mod m,então a* ≡ *c mod m.*

Demonstrações:

i. *m* | *0, ou seja, m* | *a - a, o* que implica que *a* ≡ *a mod m.*

ii. se *a* ≡ *b mod m, então b - a = qm, com q* ∈ ℤ*.*

$$a - b = -qm = (-q)m \Rightarrow b \equiv a \mod m.$$

iii. se *a* ≡ *b mod m e b* ≡ *c mod m,* então existem inteiros q_1 e q_2 tais que

$$b - a = q_1 m \text{ e } c - b = q_2 m.$$

Portanto,

$$c - a = (b + q_2 m) - (b - q_1 m) = q_2 m + q_1 m = (q_2 + q_1)m$$

e isto significa que $a \equiv c \mod m$.

■

Proposição 3. Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.

i. se $a \equiv b \mod m$ e $c \equiv d \mod m$, então $a + c \equiv b + d \mod m$.

ii. se $a \equiv b \mod m$ e $c \equiv d \mod m$, então $a\,c \equiv b\,d \mod m$.

Demonstração: Suponhamos que $a \equiv b \mod m$ e $c \equiv d \mod m$. *Logo,* temos que $m \mid b - a$ e $m \mid d - c$.

i. basta observar que $m \mid (b - a) + (d - c)$ e, portanto, $m \mid (b + d) - (a + c)$, o que prova essa parte do resultado.

ii. basta notar que

$bd - ac = d\,(b - a) + a\,(d - c)$

e concluir que $m \mid bd - ac$.

■

Proposição 4. Para todos $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, se $a \equiv b \mod m$, então tem-se que

$$a^n \equiv b^n \mod m.$$

Demonstração: Provaremos por indução. A proposição é verdadeira para $n = 1$ e suponha que seja verdadeira para qualquer natural k. Desta forma temos:

$a^k \equiv b^k \bmod m \quad e \quad a \equiv b \bmod m$

portanto, pela proposição 3 acima

$a^k . a \equiv b^k . b \bmod m$, *e como* $a^k . a = a^{k+1}$ e $b^k . b = b^{k+1}$, temos:

$a^{k+1} \equiv b^{k+1} \bmod m$,

isto é, a proposição é verdadeira para o natural *k* + 1. Logo, a proposição é verdadeira para todo natural *n*.

■

Como exemplo de aplicação de congruência resolveremos o sistema:

$X \equiv 2 \bmod 11$, $X \equiv 4 \bmod 12$ e $X \equiv 5 \bmod 13$.

$$\begin{cases} X \equiv 2\ mod\ 11 & (equação\ 1) \\ X \equiv 4\ mod\ 12 & (equação\ 2) \\ X \equiv 5\ mod\ 13 & (equação\ 3) \end{cases}$$

Da equação 3 $\exists\ a \in \mathbb{Z}$ tal que $X = 13a + 5$. Como $X \equiv 4\ mod\ 12$, temos:

$13a + 5 \equiv 4 \bmod 12$. Mas, $13 \equiv 1 \bmod 12$. Logo,

$a + 5 - 5 \equiv 4 - 5 \bmod 12$ (subtraindo 5 em ambos os lados)

$a \equiv -1 \bmod 12$. Portanto, $a \equiv 11 \bmod 12$, então $\exists\ b \in \mathbb{Z}$ tal que $a = 12b + 11$.

Fazendo $a = 12b + 11$ em $13a + 5$, temos:

$X = 13 (12b + 11) + 5$, ou seja, $X = 156b + 148$.

Da equação 1 temos: $X \equiv 2\ mod\ 11$ e como $X = 156b + 148$, temos:

$156b + 148 \equiv 2 \bmod 11$ e (como $156 \equiv 2 \bmod 11$ e $148 \equiv 5 \bmod 11$), temos:

$2b + 5 \equiv 2 \bmod 11$, que equivale a $2b \equiv -3 \bmod 11$, que por sua vez equivale a

$2b \equiv 8 \bmod 11$ (multiplicando ambos os lados por 6), obtemos $12b \equiv 48 \bmod 11$,

logo $b \equiv 4 \bmod 11$, então $\exists\ c \in \mathbb{Z}$ tal que $b = 11c + 4$.

Fazendo $b = 11c + 4$ em $156b + 48$, temos $X = 156\,(11c + 4) + 148$, ou seja,

$X = 1716c + 624 + 148$, que equivale a $X = 1716c + 772$, logo a solução do sistema é: $X \equiv 772 \bmod 1716$.

E como $772 \equiv 2 \bmod 11$, $772 \equiv 4 \bmod 12$ e $772 \equiv 5 \bmod 13$, temos que *X,* de fato, é uma solução.

2.2.8 TEOREMA DE WILSON:

O fatorial de um número natural representado por (!) indica o produto deste número por todos os seus anteriores, assim, para calcular *n*! faremos,

$n! = n \,.\, (n\text{-}1) \,.\, (n\text{-}2) \,.\, (n - 3) \,.\, \ldots\, 3 \,.\, 2 \,.\, 1.$

Para complementar a seção 2.2.6 teste de primalidade, usaremos a recíproca do Teorema de Wilson como uma boa forma de verificar em aula se um número é primo.

Proposição: *p* é um número primo se, e somente se,

$$(p - 1)! \equiv -1 \bmod p.$$

A demonstração pode ser encontrada em (HEFEZ, 2013, p.206).

A proposição acima nos dá um critério de primalidade, porém esse método não é muito útil para números muito grandes, exemplo:

Para verificar se o número 109 é primo, tenho que calcular (109 - 1)! + 1 e verificar se esse número é divisível por 109. O método torna-se eficiente na aplicação em sala de aula, pois são utilizados números bem menores.

2.2.9 FUNÇÃO φ DE EULER:

A função φ de Euler de um número natural *n é* definida como o número de naturais menores ou iguais a *n* que são relativamente primos com *n*, ou seja,

$\varphi(n) = \#\{1 \leq m \leq n \,/\, (m,n) = 1\}$.

Quando n é primo, $\varphi(n) = n - 1$.

Proposição: Sejam $a, b \in \mathbb{N}$**,** primos e distintos. Então $\varphi(ab) = \varphi(a)\,\varphi(b)$.

Demonstração: Temos que $\varphi(p) = (p - 1)$ e $\varphi(q) = (q - 1)$, pois p e q são primos. Faça, sem perda de generalidade, $p < q$. Considere o conjunto dos naturais que vão de 1 até $p.q$ e dele vamos descartar todos os números que são divisíveis por p e os que são divisíveis por q.

Os números divisíveis por p são: $p.1$, $p.2$, ..., $p.q$. E os divisíveis por q são: $q.1$, $q.2$, ... ,$p.q$. Observe que $p.q$ aparece nos dois conjuntos, então devemos repor um elemento. Daí:

$$\varphi(p.q) = p.q - p - q + 1 = p(q - 1) - (q - 1) = (p - 1)\,(q - 1) = \varphi(p)\,\varphi(q).$$

■

Teorema (Euler): Se n é um inteiro positivo e a é um inteiro tal que $(a,n) = 1$, então $a^{\varphi(n)} \equiv 1 \bmod n$.

Demonstração: Temos que todo inteiro b que é primo com n tem um inverso módulo n. De fato, pelo *Algoritmo de Euclides Estendido*, se $(b,n) = 1$, então existem inteiros s e t tais que $sb + tn = 1$; assim, $1 - sb = tn \equiv 0 \bmod n$, ou seja, $sb \equiv 1 \bmod n$, como queríamos.

Sejam $1 = a_1 < a_2 < \cdots < a_{\varphi(n)} \leq n - 1$ os $\varphi(n)$ inteiros entre 1 e n que tem mdc igual a 1 com n. Pelo Teorema Fundamental da Aritmética, $(a_1.\, a_2 \cdots a_{\varphi(n)}, n) = 1$. Daí, $a_1.\, a_2 \cdots a_{\varphi(n)}$ tem inverso módulo n, que denotaremos por α. Seja agora a um inteiro qualquer com $(a,n) = 1$. Para cada $i = 1, 2, \cdots, \varphi(n)$, temos que $(a.a_i, n) = 1$. Segue que $a.a_i \equiv a_j \bmod n$ para algum j. Além disso, se $a.a_r \equiv a.a_s \bmod n$, multiplicando ambos os lados da congruência pelo inverso de a módulo n, temos que $a_r \equiv a_s \bmod n$, o que só é possível para $a_r = a_s$. Podemos concluir que cada inteiro do conjunto $\{a.a_1, \cdots, a.\, a_{\varphi(n)}\}$ é congruente a um único inteiro do conjunto $\{a_1, \cdots, a_{\varphi(n)}\}$.

Portanto, pela propriedade multiplicativa das congruências:

$$[(a.a_1). \cdots .(a.\, a_{\varphi(n)})] \equiv a_1 \cdots a_{\varphi(n)} \text{ mod } n.$$

Assim, $[a^{\varphi(n)}.(\, a_1 \cdots a_{\varphi(n)})] \equiv a_1 \cdots a_{\varphi(n)}$ mod *n*. Multiplicando os dois lados da congruência por α, obtemos $a^{\varphi(n)} \equiv 1$ mod *n*.

■

Como exemplo de aplicação do Teorema de Euler encontraremos o resto da divisão de 3^{100} por 26.

Note que

$$\varphi(26) = \varphi(2 \,.\, 13) = (2 - 1) \,.\, (13 - 1) = 1 \,.\, 12 = 12.$$

Pelo Teorema de Euler, temos que $3^{12} \equiv 1$ mod 26, logo,

$$3^{100} = 3^{12\,.\,8+4} \equiv 3^4 \equiv 3 \text{ mod } 26.$$

Portanto, 3 é o resto da divisão de 3^{100} por 26.

2.3 DESCRIÇÃO DO MÉTODO RSA.

Nesta seção estudaremos as características de funcionamento do sistema RSA.

Segundo Coutinho (2003), a primeira etapa do método é a pré-codificação que consiste em converter a mensagem desejada em uma sequência de números, supondo que a mensagem original é um texto onde não há números, apenas palavras.

Cada letra do alfabeto deve estar associada a um valor numérico, além de uma numeração específica para o espaço entre as palavras . Esta associação é feita de acordo com a escolha de quem deseja criptografar a mensagem.

Tabela - Conversão de letras em números

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
10	11	12	13	14	15	16	17	18	19	20	21	22
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
23	24	25	26	27	28	29	30	31	32	33	34	35

Fonte: o autor

O número 36 aparecerá representando um espaço entre duas palavras. Observe que só usamos números naturais de dois algarismos: 10, 11, ..., 36. A escolha se dá dessa forma para evitar o seguinte problema. Se tivéssemos escolhido valores de 1 ao 27 não saberíamos se 21 corresponde à letra U ou à sílaba BA.

Usando a tabela de conversão, suponha, para fins de exemplo, que queremos codificar a mensagem VALORIZE O PROFESSOR, a frase seria convertida no número 31102124271835143624362527241514282824 27 e teríamos a pré-codificação da mensagem.

Para obter as chaves de encriptação e decriptação é necessário escolher dois números primos p e q (com $p \neq q$); uma parte é obtida pela multiplicação dos primos p e q ($n = p.q$). Outra parte da chave de encriptação é obtida pela função φ de Euler de n. Assim:

$\varphi(n) = \varphi(p.q) = \varphi(p)\ \varphi(q) = (p - 1)\ (q - 1)$, pois mdc$(p,q) = 1$.

Após calcularmos $\varphi(n)$ devemos escolher um número e, que faz parte da chave pública, de forma que mdc$(e, \varphi(n)) = 1$ e $1 < e < \varphi(n)$. Desta forma, a chave será o par (n,e). Obtida a chave, utilizamos o sistema de congruências para encriptar a mensagem.

Resolvendo a congruência $ed \equiv 1 \pmod{\varphi(n)}$ encontra-se d, ou seja, d é o inverso multiplicativo de e módulo $\varphi(n)$. E d faz parte da chave privada.

A mensagem numérica obtida na pré-codificação é composta por único bloco que será dividida em blocos A, de forma que $1 \leq A < n$.

De posse da chave pública (e,n) criptografa-se os blocos A de acordo com a congruência $A^e \equiv R \bmod n$, onde R é a mensagem criptografada.

De posse da chave privada (*d,n*) descriptografa-se de acordo com a congruência: $R^d \equiv A \bmod n$, onde *A* é a mensagem descriptografada, $1 \leq A < n$. O usuário do sistema RSA publica a chave de codificação (*e,n*) e mantém em segredo a chave de decodificação (*d,n*).

A segurança do sistema RSA é baseada na enorme dificuldade de se fatorar um número muito grande rapidamente e é necessária a fatoração de *n* para calcular $\varphi(n)$.

Nesse sentido, por meio do algoritmo Schroeppel e usando um computador capaz de efetuar uma multiplicação em um microssegundo (10^{-6} segundo), o tempo para "quebrar" o RSA em função do número de algarismos de *n*, é dado pela tabela:

Tabela- "Quebra" do RSA por meio do algoritmo Schroeppel

Número de algarismos de n	Tempo necessário para "quebrar" o RSA
50	3,9 horas
75	104 dias
100	74 anos
200	3,8 . 10^7 séculos
300	4,9 . 10^{13} séculos
500	4,2 . 10^{23} séculos

Criptografia e a importância das suas aplicações. RPM 12

Como exemplo de aplicação do sistema RSA, podemos voltar à mensagem VALORIZE O PROFESSOR, que já foi pré-codificada para o número 31102124271835143624362527241514282824 27.

Agora, escolhemos dois números primos distintos. Usaremos os números 7 e 11, para facilitar os cálculos (sabendo que na aplicação real, os números escolhidos são muito grandes), temos *p* = 7 e *q* = 11, daí *n* = 7 . 11 = 77 e $\varphi(n)$ = (7 - 1) (11 - 1) = 6 . 10 = 60 e podemos tomar *e* = 7, visto que $1 < 7 < \varphi(n)$ e mdc(7, 60) = 1.

O próximo passo é dividir a mensagem pré-codificada acima em blocos com números menores que 77, que é o valor de *n*, obtemos, por exemplo:

31 - 10 - 21 - 24 - 27 - 18 - 35 - 14 - 36 - 24 - 36 - 25 - 27 - 24 - 15 - 14 - 28 - 28 - 24 - 27.

Aplicamos em cada bloco a congruência $A^e \equiv R$ mod *n, ou seja,* $A^7 \equiv R$ mod *77.* Desta forma, temos:

$31^7 \equiv$ 59 mod 77.
$10^7 \equiv$ 10 mod 77.
$21^7 \equiv$ 21 mod 77.
$24^7 \equiv$ 73 mod 77.
$27^7 \equiv$ 69 mod 77.
$18^7 \equiv$ 39 mod 77.
$35^7 \equiv$ 7 mod 77.
$14^7 \equiv$ 42 mod 77.
$36^7 \equiv$ 64 mod 77.
$25^7 \equiv$ 53 mod 77.
$15^7 \equiv$ 71 mod 77.
$28^7 \equiv$ 63 mod 77.

Nossa mensagem criptografada será:

59 - 10 - 21 - 73 - 69 - 39 - 7 - 42 - 64 - 73 - 64 - 53 - 69 - 73 - 71 - 42 - 63 - 63 - 73 - 69.

Para encontrarmos o valor de *d*, temos que resolver a congruência $7d \equiv 1$ mod 60, ou seja, *d* é o inverso multiplicativo de 7 módulo 60 e, pelo Algoritmo Euclidiano Estendido, temos 1 = 7.43 - 5 . 60, e a chave privada será (43,77).

Segundo Coutinho (2003), para que o sistema RSA possa manter-se seguro é necessário escolher números primos *p* e *q* que não estejam próximos um do outro, senão, ambos os primos estarão próximos de $\sqrt{n}$ e daí, é possível mostrar que *n* pode ser fatorado de forma muito mais fácil através do Algoritmo de Fermat.

Os métodos de fatoração existentes e a velocidade de processamento dos computadores atuais ainda não são capazes de fatorar em tempo razoável números inteiros tão grandes quanto os utilizados no sistema RSA, por isso, esse sistema criptográfico é largamente utilizado e extremamente seguro.

Um exemplo do uso do sistema RSA são as mensagens via WhatsApp que são criptografadas de ponta a ponta de forma que o conteúdo só possa ser acessado pelos dois extremos da comunicação.

Figura 2 - Criptografia de ponta a ponta.

Fonte: o autor

3. NÚMEROS PRIMOS E A HISTÓRIA DA CRIPTOGRAFIA.

Os registros mais antigos de um estudo acerca dos números primos remetem aos gregos. Os elementos de Euclides (cerca de 300 a.C) contêm teoremas importantes sobre os números primos, incluindo a demonstração de sua infinitude e o teorema fundamental da aritmética.

Os números primos possuem grande importância na composição dos números inteiros e sempre exerceram enorme fascínio sobre os matemáticos. É possível que a escola pitagórica tenha sido precursora na descoberta sobre esses números fantásticos.

Os números primos desempenham papel fundamental e a eles estão associados muitos problemas famosos cujas soluções têm resistido aos esforços de várias gerações de matemáticos. Afinal, o que é um número primo? Um número natural maior do que 1 que só possui como divisores positivos 1 e ele próprio.

Sautoy (2007, p.13) escreveu que "os primos são as pérolas que adornam a vastidão infinita do universo de números que os matemáticos exploraram ao longo dos séculos".

3.1 AS ORIGENS DA CRIPTOGRAFIA.

A palavra criptografia deriva-se do grego, onde *kriptos* significa "secreto" ou "oculto" e "*graphia*" quer dizer escrita e, portanto, a palavra criptografia significa "escrita secreta". Para Singh (2005) a criptografia não pretende ocultar a existência de uma mensagem mas esconder seu significado, processo o qual é chamado encriptação. Encriptar é alterar um texto de acordo com uma regra conhecida apenas pelo emissor e pelo receptor.

Ao contrário do que se pensa, a criptografia não é uma técnica moderna, pois existem relatos bem antigos de sua utilização, como os hieróglifos que formam um sistema extremamente complexo onde há caracteres ideográficos, caracteres silábicos e caracteres determinativos que servem para distinguir homônimos. Um marco na decifração de códigos foi a descoberta da *pedra de Roseta,* que é um bloco de basalto negro que contém uma mesma inscrição escrita em hieróglifos, demótico e grego.

Figura 3- Pedra de Roseta (196 a.C)

(Museu Britânico)

"Em 1799, durante a campanha funesta de Napoleão no Egito, engenheiros franceses que escavavam o solo, perto do braço de Roseta do delta do Nilo, para as fundações de um forte, encontraram um fragmento basáltico polido que iria propiciar a decifração dos caracteres hieroglíficos e demóticos. Essa pedra, que mede três pés e sete polegadas por dois pés e seis polegadas, contém inscrições como uma mensagem repetida em hieróglifos egípcios, em caracteres demóticos egípcios e em grego. Tomando o grego como chave foi possível decifrar a escrita egípcia antiga. O autor desse feito foi o sábio francês Jean François Champollion (1790-1832). A pedra (conhecida como pedra de Roseta) foi gravada em 196 a.C e, como resultado do tratado de capitulação, quando a França foi derrotada pela Inglaterra, encontra-se agora no Museu Britânico." EVES (2004, p.70)

Os espartanos usavam o *bastão de Licurgo* para transmitir mensagens secretas. Consiste de uma cifra de transposição envolta por uma tira de couro. A mensagem era escrita no sentido do seu comprimento, em seguida desenrolava-se a tira de couro para o envio ao destinatário, que, ao recebê-la, enrolava a tira num bastão idêntico e decodificava a mensagem.

Figura 4- Bastão de Licurgo

Fonte:https://pt.wikipedia.org/wiki/Cítala

A história narrada por Heródoto mostra uma das primeiras técnicas para trazer privacidade a uma troca de informações, a esteganografia. A esteganografia consiste em esconder a mensagem. A segurança da informação vem da tática de simplesmente esconder a mensagem. É uma ciência considerada irmã da criptografia. Diversas técnicas esteganográficas surgiram ao longo dos anos. Um exemplo é o microponto, que consiste em reduzir uma foto de um texto até transformá-la em um ponto. O microponto era então oculto sobre o ponto final de uma carta aparentemente inofensiva. Tal técnica foi praticada pelos alemães durante a 2ª guerra mundial (Singh, 2011). Mas a esteganografia sofre de uma fraqueza fundamental. Se a mensagem for descoberta, então o conteúdo da comunicação secreta é imediatamente revelado.

3.2 CIFRAS DE SUBSTITUIÇÃO

Os códigos secretos, como os usados pela maioria das pessoas quando criança, consiste em substituir uma letra por outra, transladando o alfabeto, usando uma determinada ordem de substituição que somente o emissor e o receptor sabem. De forma semelhante César usou essas cifras de substituição para comunicar-se com as legiões em combate pela Europa. A Cifra de César é um caso específico que será estudado na subseção 3.2.1. As cifras de substituição podem ser monoalfabéticas ou polialfabéticas. César foi um líder militar e político romano nascido em 100 a.C. viveu até 44 a.C.

O sistema monoalfabético substitui cada caractere de um texto por outros caracteres de acordo com uma tabela pré existente que é a tabela cifrante.

> Daí em diante, mesmo ficando explicita a vulnerabilidade do método da substituição monoalfabética diante da análise de frequências, durante toda a Idade Média, a Europa ainda utilizava esta técnica de criptografia. Na realidade, o avanço científico nesta época foi moroso, sendo que grande parte do conhecimento sobre criptografia era considerado magia negra. A criação da criptoanálise como ciência, a partir da definição do método da análise de frequências, deu início a uma permanente luta entre os criadores e os quebradores de códigos, o que, desde aquela época, vem beneficiando ambas as partes (SANTOS, 2013, p.20).

O sistema polialfabético pode utilizar dois ou mais cifrantes e é uma combinação ordenada de diversos sistemas monoalfabéticos. Um bom exemplo é a cifra de Vigenère que será estudada na subseção 3.2.2.

*A chave de um sistema polialfabético é um conjunto de *n* letras: (L_1, L_2, L_3 ..., L_n);

*A mensagem deve ser dividida em blocos de *n* letras: (A_1, A_2, A_3 ..., A_n);

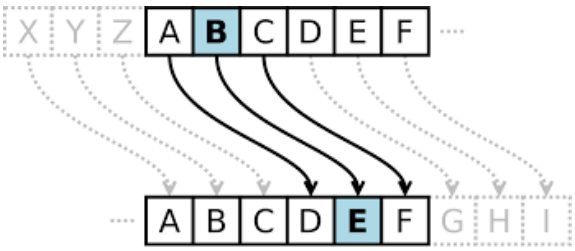
*O texto cifrado *X* é obtido a partir da fórmula:

$X = ((A_1 + L_1) \text{ mod}26, (A_2 + L_2) \text{ mod}26, ..., (A_p + L_p) \text{ mod}26)$.

3.2.1 CIFRA DE CÉSAR

Este provavelmente é o primeiro exemplo de um código secreto de que se tem relatos. A cifra de César era um código de substituição simples, como já foi dito anteriormente, consistia em substituir cada letra da mensagem original por outra letra deslocando três posições à frente.

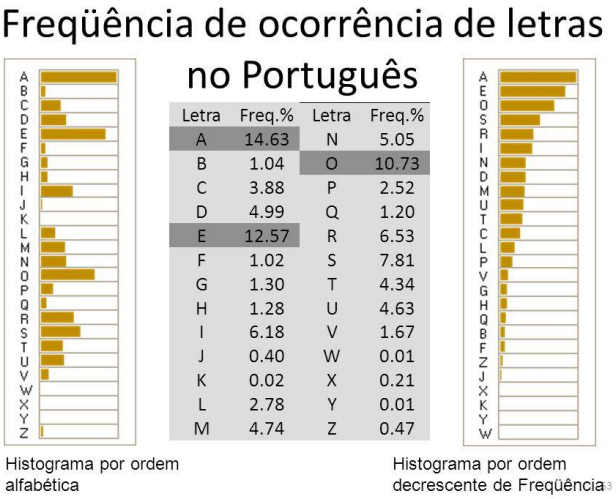
Figura 5 - A cifra de César



Fonte:canaltech.com.br/o-que-e/protecao-de-dados/o-que-e-criptografia-e-por-que-voce-deveria-usa-la/

O maior problema é que códigos como o de César são muito fáceis de quebrar. Na verdade, qualquer código que envolva substituição sistemática de uma letra por outra ou por um símbolo sofrem do mesmo mal. Isto se deve ao fato de que, geralmente, os símbolos mais frequentes do texto cifrado representam as letras mais comuns do idioma mesmo não estando em ordem. Um texto cifrado na língua portuguesa, por exemplo, deverá conter mais símbolos que representem as letras A, E e O, pois são as mais frequentes em nossa língua.

Figura 6 - Frequência de ocorrência de letras no Português



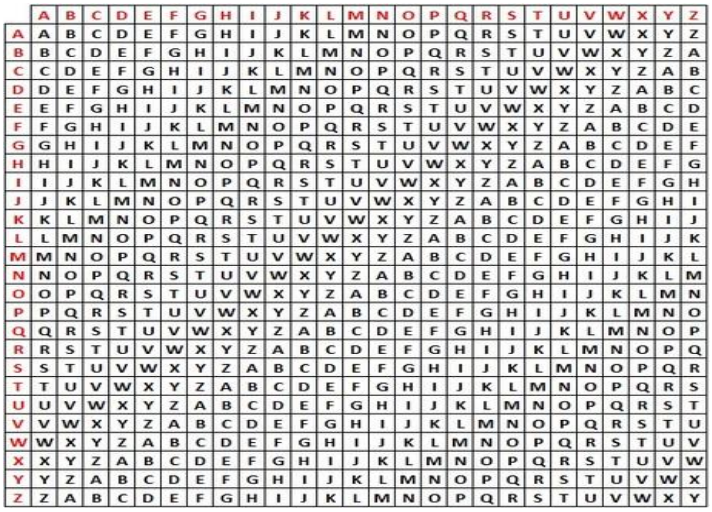
UESC SINFORM 2011 César Bravo

Após algum tempo passou-se a designar como código de César qualquer cifra onde cada letra da mensagem original fosse substituída por outra deslocada um determinado número de posisões e não necessariamente três como no formato original.

3.2.2 CIFRA DE VIGENÈRE

Vigenère juntou ideias de códigos de substituição e desenvolveu uma cifra que usa vários alfabetos de substituição ao mesmo tempo. Usando o quadrado de Vigenère, precisamos de uma palavra chave que será usada repetidamente para as colunas de cifras de uma frase. Blaise de Vigenère foi um diplomata e criptógrafo francês que viveu de 1523 a 1596.

Figura 7 - Cifra de Vigenère

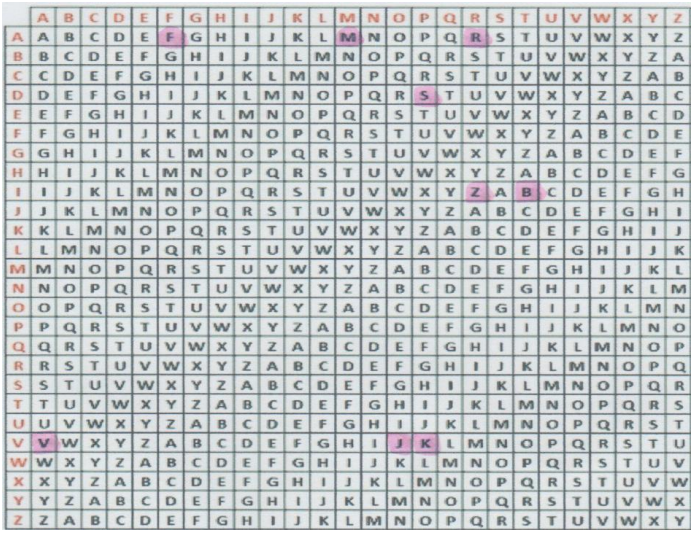


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: https://danieldonda.wordpress.com/2007/10/31/cifradevigenere-le-chiffre-indechiffrable

Como exemplo poderíamos utilizar como palavra chave a palavra PROFMAT para encriptar a frase VIVA A VIDA, assim usamos a coluna P para cifrar a letra V, a coluna R para cifrar a letra I, a coluna O para cifrar a letra V, a coluna F para cifrar a letra A e assim por diante.

Figura 8 - Cifra de Vigenère 2



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: O autor

Até obter KZJF M VBSR como encriptação da frase VIVA A VIDA.

A cifra de Vigenère comparada com a cifra de César, por exemplo, era bem mais segura, pois é fundamentada no uso periódico de uma palavra chave e, quando geradas ao acaso, tornavam a decodificação muito difícil.

3.2.3 CIFRA DE HILL

Conforme Godinho (2011), a cifra de Hill surge por volta de 1929 inventada por Lester S. Hill. Este sistema utiliza a transformação matricial para a substituição e para criptografar uma mensagem. Consiste em relacionar cada letra do alfabeto a um número (tabela) e utiliza como chave de encriptação e decriptação um par de matrizes quadradas (*A* e *B*) inversas uma da outra. Cria-se uma criptografia denominada matriz chave que deve ser multiplicada pela matriz cifrada gerando então uma nova matriz criptografada. Lester S. Hill foi um matemático norte americano que viveu de 1891 a 1961.

Tabela - cifra de Hill

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
1	2	3	4	5	6	7	8	9	10	11	12	13	14
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**.**	**#**
15	16	17	18	19	20	21	22	23	24	25	26	27	28

Fonte: o autor

Como exemplo da cifra de Hill, suponhamos que a mensagem a ser transmitida seja: ESTUDE MAIS.

De acordo com a tabela numérica temos os números: 5, 19, 20, 21, 4, 5, 28, 13, 1, 9, 19, 27.

A sequência de números acima deve ser arrumada em uma matriz *M* de duas linhas:

$$M = \begin{pmatrix} 5 & 19 & 20 & 21 & 4 & 5 \\ 28 & 13 & 1 & 9 & 19 & 27 \end{pmatrix}.$$

Utilizaremos como chave de encriptação qualquer par de matrizes quadradas de ordem 2 inversas entre si. A condição para a escolha da matriz *A* é que ela seja invertível.

Exemplo:

$A = \begin{pmatrix} 2 & 4 \\ 1 & 4 \end{pmatrix}$ e $B = \begin{pmatrix} 1 & -1 \\ -\frac{1}{4} & \frac{1}{2} \end{pmatrix}$.

O remetente utiliza a matriz *A* para criptografar a mensagem fazendo: *N* = *A.M* e, desse modo, obtém a matriz *N*.

$$A.M = \begin{pmatrix} 2 & 4 \\ 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 5 & 19 & 20 & 21 & 4 & 5 \\ 28 & 13 & 1 & 9 & 19 & 27 \end{pmatrix} =$$

$$\begin{pmatrix} 122 & 90 & 44 & 78 & 84 & 118 \\ 117 & 71 & 24 & 57 & 80 & 113 \end{pmatrix} = N.$$

Os elementos de *N* constituem a mensagem cifrada:

122, 90, 44, 78, 84, 118, 117, 71, 24, 57, 80, 113.

Quando a mensagem cifrada chega ao destinatário, ele utiliza a matriz de desencriptação *B* para desfazer os procedimentos anteriores; considerando que:

$B \cdot N = B \cdot A \cdot M = I \cdot M = M$

De posse da mensagem criptografada, o destinatário constrói uma matriz com duas linhas *N* e calcula o produto *B. N*.

$$B.N = \begin{pmatrix} 1 & -1 \\ -\frac{1}{4} & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} 122 & 90 & 44 & 78 & 84 & 118 \\ 117 & 71 & 24 & 57 & 80 & 113 \end{pmatrix} =$$

$$= \begin{pmatrix} 5 & 19 & 20 & 21 & 4 & 5 \\ 28 & 13 & 1 & 9 & 19 & 27 \end{pmatrix} = M.$$

Os elementos da matriz *M* obtida formam a sequencia de números: 5, 19, 20, 21, 4, 5, 28, 13, 1, 9, 19, 27, cuja decriptação é:

5	**19**	**20**	**21**	**4**	**5**	**28**	**13**	**1**	**9**	**19**	**27**
E	**S**	**T**	**U**	**D**	**E**	**#**	**M**	**A**	**I**	**S**	**.**

Com base na proposta da cifra de Hill foi realizada uma atividade em sala de aula que será detalhada no capítulo 4.

3.3 DISCOS DE CIFRAS

Sua concepção básica consiste de dois discos concêntricos de diâmetros distintos com escalas e com o alfabeto gravado. Ao movê-los em torno do mesmo eixo, ocorre uma relação entre eles de modo que permite a mudança de cifras.

Figura 9 - Disco de Alberti

Disponível em:<http://webdehistoria.blogspot.com.br/2014/05/leon-battista-alberti.html>

A invenção desse disco é atribuiída a Leone Battista Alberti, secretário da cúria Romana. O disco de cifras transforma a letra do texto original na letra do texto cifrado, considerando um alfabeto com 26 letras o desvio pode variar de 0 até 25. Isto funciona como a operação de adição em aritmética modular e pode ser representado como:

$$C_i = m_i + p \pmod{26}.$$

Assim, temos um total de 26 chaves possíveis, considerando que o desvio igual a zero reproduz o próprio texto.

O disco de cifras de Alberti incentivou algumas outras pessoas a também empregarem o conceito de criptografia assistida. Em 1795, Thomas Jefferson criou uma máquina de encriptação (figura abaixo) que era composta por 25 discos de madeira que giravam em torno de um eixo comum. Em cada disco de madeira as 26 letras do alfabeto eram gravadas de forma aleatória.

Uma vez que os discos foram colocados sobre o eixo na ordem combinada, o remetente roda cada disco para cima e para baixo até que uma mensagem desejada seja explicitada em uma fileira. O destinatário simplesmente tem que organizar os discos na ordem combinada e só é capaz de ler a mensagem que foi cifrada quem souber a perfeita ordem combinada das posições dos discos.

Figura 10 - Máquina de encriptação de Thomas Jefferson

http://www.fazano.pro.br/port79d.html

3.4 A MÁQUINA ENIGMA

Os alemães fizeram na segunda guerra mundial o uso de uma máquina que usava uma chave enorme e sem um padrão que pudesse ser reconhecido. Essa máquina se chamava enigma.

Uma máquina eletromecânica que automatizava e "embaralhava" completamente a troca de alfabeto a cada letra codificada, então mesmo que uma letra como o *A* aparecesse várias vezes pela mensagem ela seria substituída por letras diferentes a cada ocorrência deixando muito mais difícil a descriptografia da mensagem.

A máquina de encriptação enigma era tão eficiente que só quem soubesse quais eram os rolos misturadores usados poderiam recriar a mensagem.

Figura 11 - A máquina Enigma.

Instituto de informática- UFRGS

Alan Turing construiu um dos primeiros computadores, o Bombe, para testar milhões e milhões de combinações de chaves para tentar desvendar a enigma e conseguir ler as mensagens alemães. O filme "O jogo da imitação" de Morten Tyldum, lançado em 2015, conta um pouco sobre Turing e sua máquina. A análise de frequência das letras e de combinações, mais uma vez, deu a chave para os criptoanalístas.

> Descobriram que alguns operadores de rádio alemães, especialmente um homem chamado Walter, estavam a ignorar as instruções e iniciavam as suas máquinas com a mesma chave todos os dias. Calcularam, acertadamente, que as unidades alemães espalhadas por toda a Europa transmitiriam mensagens idênticas pelo aniversário de Führer, em abril de 1940 e deitaram as mãos a uma máquina Enigma atualizada que a marinha britânica obtivera num navio meteorológico alemão capturado ao largo da Groenlândia (Norman, 2008. p.55).

Alan Turing, que atualmente é conhecido como o pai da computação, apesar de toda a sua genialidade e de seus estudos serem a base para a computação moderna, ainda é muito pouco conhecido do grande público. A versão mais conhecida de sua morte é que em seus últimos dias de vida foi condenado à castração química, pelo fato de ser homossexual, tendo cometido suicídio com cianeto aos 41 anos de idade em Winslow na Inglaterra.

Figura 12 - Alan Turing.

(figura obtida em http://horizontes.sbc.org.br/index.php/2016/11/22alan-turing-e-a-enigma/)

Até a década de 1960, a distribuição de chaves tinha um custo enorme para os bancos. Eles gastavam fortunas para distribuir as chaves de segurança pessoalmente pelo mundo de forma extremamente sigilosa até que surgiram as chaves públicas e privadas.

3.5 SISTEMA RSA.

Os métodos para criptografar e descriptografar mensagens podem ser classificados em métodos de chave simétrica e métodos de chave assimétrica.

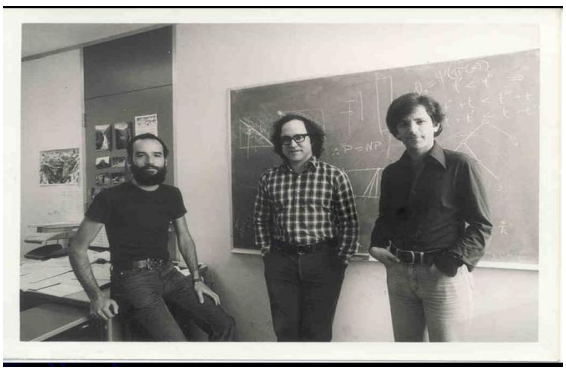
Chaves simétricas: As chaves para criptografar e descriptografar mensagens são conhecidas pelo remetente e pelo destinatário. A chave para encriptar a mensagem é a mesma para desencriptar. Saber encriptar implica em saber desencriptar e necessita de um canal seguro entre remetente e destinatário para combinar a chave de encriptação. Como exemplo temos a Cifra de César.

Chaves assimétricas: Uma chave encripta a mensagem e outra chave desencripta. A chave de encriptação é pública e a chave de desencriptação é privada. Mesmo com os computadores mais avançados é praticamente impossível encontrar a chave de desencriptação. Saber encriptar não implica em saber desencriptar e não precisa de um canal seguro. Como exemplo temos o sistema RSA.

Os métodos de chave assimétrica, introduzidos após a década de 1970, revolucionaram a criptografia e representam o último passo, por enquanto, nessa sequência histórica.

A criptografia RSA foi desenvolvida por Ron L. **R**ivest, Adi **S**hamir e Len **A**dleman em 1978, quando trabalhavam no Massachussets Institute of technology (M.I.T.). Observe que as iniciais dos nomes dos inventores deram origem ao nome do código.

Figura 13 - Adi Shamir, Ronald Rivest e Leonard Adleman



http://www.usc.edu/dept/molecular-science/RSApics.htm

O sistema RSA baseia-se em algoritmos computacionais utilizando a chave assimétrica e dentre os diversos métodos criptográficos, o RSA é um dos mais utilizados, em particular, na internet, através das mensagens de e-mail, mensagens de WhatsApp, comércio eletrônico, entre outros. Com isso, a criptografia RSA é um dos melhores exemplos de aplicações dos números primos no cotidiano das pessoas.

> [...] Hoje em dia nossas chamadas telefônicas saltam entre satélites e nossos e-mails passam por vários computadores. Ambas as formas de comunicação podem ser interceptadas facilmente, ameaçando nossa privacidade. (SINGH,2005,p.12)

Como vimos na seção 2.3 e veremos em aplicações em sala de aula, a segurança do sistema RSA reside na dificuldade de fatorar um número grande em seu fatores primos.

Hefez (2016, p.274) escreveu que "O princípio baseia-se na relativa facilidade em encontrar números primos muito grandes e ao mesmo tempo na enorme dificuldade prática em fatorar o produto de dois desses números".

> O único problema para a segurança da criptografia de chave pública RSA é que, em alguma época no futuro, alguém possa encontrar um modo rápido de fatorar N. É concebível que daqui a uma década, ou mesmo amanhã, alguém possa descobrir um método para a fatoração rápida e aí a RSA se tornará inútil. Contudo, por dois mil anos os matemáticos têm tentado e fracassado em encontrar um atalho, e por enquanto, a fatoração continua sendo um cálculo muito trabalhoso. A maioria dos matemáticos acredita que a fatoração é uma tarefa inerentemente difícil e que existe alguma lei matemática que proíbe a existência de qualquer atalho. Vamos presumir que eles estejam certos: deste modo, a RSA estará segura durante o futuro previsível. (SINGH, 2005, p.303)

4. APLICAÇÕES DA CRIPTOGRAFIA EM SALA DE AULA.

4.1 A CRIPTOGRAFIA NOS LIVROS DIDÁTICOS.

O livro didático é um instrumento fundamental, visto que, na maioria dos casos é o único material pedagógico utilizado pelo professor em suas aulas. No ambiente escolar o livro impresso ainda é o material que melhor atende às necessidades dos professores.

Com o objetivo de verificar se o tema criptografia é abordado nos livros didáticos e de que maneira essa abordagem ocorre, o autor deste trabalho, analisou três coleções aprovadas no Programa Nacional do Livro e do Material Didático (PNLD 2018).

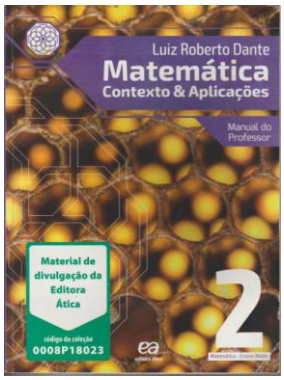
Dentre as coleções de matemática aprovadas pelo PNLD 2018 foram analisadas aquelas que estavam disponíveis na biblioteca da escola onde atua o professor autor deste trabalho, as quais estão descritas de forma detalhada na tabela abaixo e ilustradas em seguida.

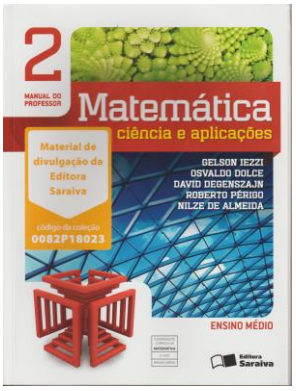
Tabela- Coleções aprovadas pelo PNLD 2018 que foram utilizadas nessa pesquisa.

Título	Autores	Edição	Editora	Cidade	Ano
Matemática- Contexto & Aplicações.	Luiz Roberto Dante.	V.1 - 3° V.2 - 3° V.3 - 3°	Ática	São Paulo	2017
Quadrante.	Eduardo Chavante, Diego Prestes.	V.1 - 1° V.2 - 1° V.3 - 1°	SM	São Paulo	2016
Matemática - Ciência e aplicações.	Gelson Iezzi, Osvaldo Doce, David Degenszajn, Roberto Périgo e Nilze de Almeida.	V.1 - 9° V.2 - 9° V.3 - 9°	Saraiva	São paulo	2017

Fonte: Organizada pelo autor.

Figura 14 - Exemplos de capas dos livros analisados



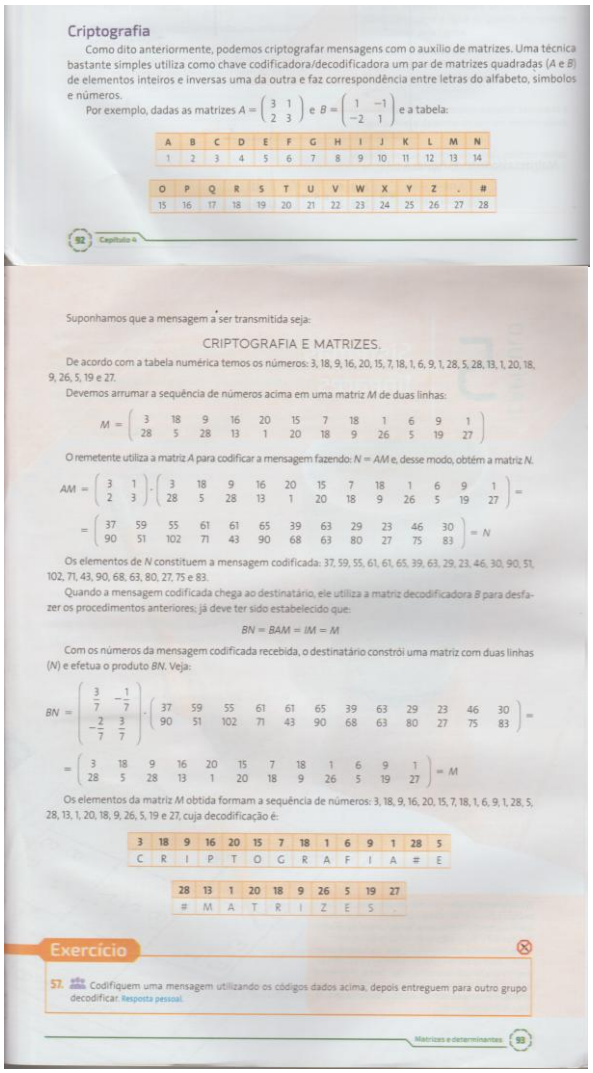


Fonte: O autor.

Das três coleções analisadas encontramos o tema criptografia em duas, são elas: *Matemática- Contexto & Aplicações*, autor: Luiz Roberto Dante, volume 2 e *Quadrante*, autores Eduardo Chavante e Diego Prestes, volume 2. A coleção *Matemática- Ciência e aplicações* não aborda o tema criptografia em nenhum volume.

A coleção *Matemática- Contexto & Aplicações*, autor: Luiz Roberto Dante faz uso do tema criptografia no capítulo 4 do volume 2, mais precisamente no estudo de matrizes, determinantes e sistemas lineares nas páginas 92 e 93, fechando o capítulo e usando o tema criptografia como uma forma de aplicação de operações com matrizes e complementando o conteúdo estudado.

Figura 15 - Matemática-Contexto Contexto & Aplicações, autor: Luiz Roberto Dante, volume 2, páginas 92 e 93.



Criptografia

Como dito anteriormente, podemos criptografar mensagens com o auxílio de matrizes. Uma técnica bastante simples utiliza como chave codificadora/decodificadora um par de matrizes quadradas (A e B) de elementos inteiros e inversas uma da outra e faz correspondência entre letras do alfabeto, símbolos e números.

Por exemplo, dadas as matrizes $A = \begin{pmatrix} 3 & 1 \\ 2 & 3 \end{pmatrix}$ e $B = \begin{pmatrix} 1 & -1 \\ -2 & 1 \end{pmatrix}$ e a tabela:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	2	3	4	5	6	7	8	9	10	11	12	13	14

O	P	Q	R	S	T	U	V	W	X	Y	Z	.	#
15	16	17	18	19	20	21	22	23	24	25	26	27	28

92 Capítulo 4

Suponhamos que a mensagem a ser transmitida seja:

CRIPTOGRAFIA E MATRIZES.

De acordo com a tabela numérica temos os números: 3, 18, 9, 16, 20, 15, 7, 18, 1, 6, 9, 1, 28, 5, 28, 13, 1, 20, 18, 9, 26, 5, 19 e 27.

Devemos arrumar a sequência de números acima em uma matriz M de duas linhas:

$$M = \begin{pmatrix} 3 & 18 & 9 & 16 & 20 & 15 & 7 & 18 & 1 & 6 & 9 & 1 \\ 28 & 5 & 28 & 13 & 1 & 20 & 18 & 9 & 26 & 5 & 19 & 27 \end{pmatrix}$$

O remetente utiliza a matriz A para codificar a mensagem fazendo: $N = AM$ e, desse modo, obtém a matriz N.

$$AM = \begin{pmatrix} 3 & 1 \\ 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 3 & 18 & 9 & 16 & 20 & 15 & 7 & 18 & 1 & 6 & 9 & 1 \\ 28 & 5 & 28 & 13 & 1 & 20 & 18 & 9 & 26 & 5 & 19 & 27 \end{pmatrix} =$$

$$= \begin{pmatrix} 37 & 59 & 55 & 61 & 61 & 65 & 39 & 63 & 29 & 23 & 46 & 30 \\ 90 & 51 & 102 & 71 & 43 & 90 & 68 & 63 & 80 & 27 & 75 & 83 \end{pmatrix} = N$$

Os elementos de N constituem a mensagem codificada: 37, 59, 55, 61, 61, 65, 39, 63, 29, 23, 46, 30, 90, 51, 102, 71, 43, 90, 68, 63, 80, 27, 75 e 83.

Quando a mensagem codificada chega ao destinatário, ele utiliza a matriz decodificadora B para desfazer os procedimentos anteriores; já deve ter sido estabelecido que:

$$BN = BAM = IM = M$$

Com os números da mensagem codificada recebida, o destinatário constrói uma matriz com duas linhas (N) e efetua o produto BN. Veja:

$$BN = \begin{pmatrix} \frac{3}{7} & -\frac{1}{7} \\ -\frac{2}{7} & \frac{3}{7} \end{pmatrix} \cdot \begin{pmatrix} 37 & 59 & 55 & 61 & 61 & 65 & 39 & 63 & 29 & 23 & 46 & 30 \\ 90 & 51 & 102 & 71 & 43 & 90 & 68 & 63 & 80 & 27 & 75 & 83 \end{pmatrix} =$$

$$= \begin{pmatrix} 3 & 18 & 9 & 16 & 20 & 15 & 7 & 18 & 1 & 6 & 9 & 1 \\ 28 & 5 & 28 & 13 & 1 & 20 & 18 & 9 & 26 & 5 & 19 & 27 \end{pmatrix} = M$$

Os elementos da matriz M obtida formam a sequência de números: 3, 18, 9, 16, 20, 15, 7, 18, 1, 6, 9, 1, 28, 5, 28, 13, 1, 20, 18, 9, 26, 5, 19 e 27, cuja decodificação é:

3	18	9	16	20	15	7	18	1	6	9	1	28	5
C	R	I	P	T	O	G	R	A	F	I	A	#	E

28	13	1	20	18	9	26	5	19	27
#	M	A	T	R	I	Z	E	S	.

Exercício

57. Codifiquem uma mensagem utilizando os códigos dados acima, depois entreguem para outro grupo decodificar. Resposta pessoal.

Matrizes e determinantes 93

Fonte: O autor

Este autor usa o tema criptografia apenas como uma aplicação do conteúdo e não faz uma introdução ao estudo de criptografia.

Para exemplificar o processo, o autor propõe a cifragem da mensagem "CRIPTOGRAFIA E MATRIZES" através de uma matriz A quadrada invertível de ordem 2. A matriz A usada como chave para a cifragem será $A = \begin{pmatrix} 3 & 1 \\ 2 & 3 \end{pmatrix}$. Na figura acima observa-se todo o processo de codificação e decodificação da mensagem proposta pelo autor. Esse exemplo enfatiza de forma robusta as operações com matrizes e destaca o conceito de matrizes inversas, porém percebemos que a matriz

decodificadora $B = \begin{pmatrix} 1 & -1 \\ -2 & 1 \end{pmatrix}$ citada pelo autor na página 92 não é a inversa da matriz $A = \begin{pmatrix} 3 & 1 \\ 2 & 3 \end{pmatrix}$, onde o correto seria $B = \begin{pmatrix} \frac{3}{7} & -\frac{1}{7} \\ -\frac{2}{7} & \frac{3}{7} \end{pmatrix}$. O capítulo termina com o autor propondo que os alunos codifiquem uma mensagem criada por eles usando o exemplo.

A coleção *Quadrante*, autores Eduardo Chavante e Diego Prestes, faz uso do tema criptografia no capítulo 5 do volume 2, mais precisamente no estudo de matrizes na página 146. A seção utilizada para tratar o tema criptografia é a "Valores em ação" (figura abaixo), que, segundo o autor, é um espaço onde o aluno é convidado a refletir a respeito de diversos temas.

Figura 16 - Quadrante, autores Eduardo Chavante e Diego Prestes, volume 2, página 146.

Fonte: O autor.

Este livro introduz o tema para o aluno, explicando as origens da criptografia e sua importância na segurança das transmissões de mensagens na internet e , com o

uso de uma linha do tempo, mostrando seus avanços desde a esteganografia usada por Heródoto até o moderno sistema RSA.

Ao final, o autor propõe um questionário sobre o texto e pede ao aluno para determinar a inversa de uma matriz fazendo uma referência às chaves codificadora e decodificadora.

Como vimos, o tema criptografia, nos dois livros analisados, foi relacionado à matrizes e, de forma mais específica, à matriz inversa. O que parece ser uma tendência, visto que, os dois exemplos de questões de vestibulares que fazem o uso de criptografia, também a relacionam com matrizes.

Exemplos de questões com o tema criptografia cobradas em vestibulares:

Exemplo1: (UEL-PR) Uma das formas de se enviar uma mensagem secreta é por meio de códigos matemáticos, seguindo os passos:

1) Tanto o destinatário quanto o remetente possuem uma matriz chave *C*;

2) O destinatário recebe do remetente uma matriz *P*, tal que *MC* = *P*, em que *M* é a matriz mensagem a ser decodificada;

3) Cada número da matriz *M* corresponde a uma letra do alfabeto: 1 = *a*, 2 = *b*, 3 = *c*, ..., 23 = *z*;

4) Consideremos o alfabeto com 23 letras, excluindo as letras k, w e y;

5) O número zero corresponde ao ponto de exclamação;

6) A mensagem é lida, encontrando a matriz *M*, fazendo a correspondência número/letra e ordenando as letras por linhas da matriz conforme segue: $m_{11}m_{12}m_{13}m_{21}m_{22}m_{23}m_{31}m_{32}m_{33}$.

Considere as matrizes; $C = \begin{bmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 2 & 1 \end{bmatrix}$ e $P = \begin{bmatrix} 2 & -10 & 1 \\ 18 & 38 & 17 \\ 19 & 14 & 0 \end{bmatrix}$.

Com base nos conhecimentos e nas informações descritas, assinale a alternativa que apresenta a mensagem que foi enviada por meio da matriz *M*.

a) Boasorte!

b) Boaprova!

c) Boatarde!

d) Ajudeme!

e) Socorro!

Resolução:

Seja $M = \begin{bmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{bmatrix}$

Como $M.C = P$, temos:

$$\begin{bmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{bmatrix} . \begin{bmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & 2 & 1 \end{bmatrix} = \begin{bmatrix} 2 & -10 & 1 \\ 18 & 38 & 17 \\ 19 & 14 & 0 \end{bmatrix}.$$

$$\Longrightarrow \begin{bmatrix} m_{11} & m_{11} - m_{12} + 2m_{13} & m_{13} \\ m_{21} & m_{21} - m_{22} + 2m_{23} & m_{23} \\ m_{31} & m_{31} - m_{32} + 2m_{33} & m_{33} \end{bmatrix} = \begin{bmatrix} 2 & -10 & 1 \\ 18 & 38 & 17 \\ 19 & 14 & 0 \end{bmatrix}.$$

Com isso, obtemos:

$m_{11} = 2$, $m_{21} = 18$, $m_{31} = 19$, $m_{13} = 1$, $m_{23} = 17$, $m_{33} = 0$

$2 - m_{12} + 2.1 = -10 \Longrightarrow m_{12} = 14$

$18 - m_{22} + 2.17 = 38 \Longrightarrow m_{22} = 14$

$19 - m_{32} + 2.0 = 14 \Longrightarrow m_{32} = 5$

Finalmente, temos que $M = \begin{bmatrix} 2 & 14 & 1 \\ 18 & 14 & 17 \\ 19 & 5 & 0 \end{bmatrix}$.

Logo, a mensagem codificada é "Boasorte!"

O exemplo 1 resolvido acima consta na seção "Desafio" do livro Quadrante, autores Eduardo Chavante e Diego Prestes, volume 2, página 145.

Exemplo 2: (UFAM) Para criptografar uma palavra de quatro letras um aluno de Matemática a representou como uma matriz 4 x 1 substituindo cada letra da palavra por números conforme o quadro a seguir.

A→1	B→2	C→3	Ç→4	D→5	E→6
F→7	G→8	H→9	I→10	J→11	K→12
L→13	M→14	N→15	O→16	P→17	Q→18
R→19	S→20	T→21	U→22	V→23	W→24
X→25	Y→26	Z→27	Ã→28	Õ→29	É→30

Em seguida multiplicou essa matriz pela matriz

$A = \begin{bmatrix} \frac{1}{21} & 0 & 0 & 0 \\ 0 & \frac{1}{11} & 0 & 0 \\ 0 & 0 & \frac{3}{5} & 0 \\ 0 & 0 & 0 & \frac{1}{4} \end{bmatrix}$, obtendo como resultado a matriz $B = \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix}$.

Para descriptografar a palavra deve-se fazer o produto da matriz *B* pela matriz inversa de *A*. Então a palavra originalmente era:

a) UFAM

b) MAÇÃ

c) HEXA

d) TUDO

e) AMOR

Resolução:

O primeiro passo é determinar a inversa da matriz *A*.

$$\begin{bmatrix} \frac{1}{21} & 0 & 0 & 0 \\ 0 & \frac{1}{11} & 0 & 0 \\ 0 & 0 & \frac{3}{5} & 0 \\ 0 & 0 & 0 & \frac{1}{4} \end{bmatrix} \cdot \begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} \frac{1}{21}a & \frac{1}{21}b & \frac{1}{21}c & \frac{1}{21}d \\ \frac{1}{11}e & \frac{1}{11}f & \frac{1}{11}g & \frac{1}{11}h \\ \frac{3}{5}i & \frac{3}{5}j & \frac{3}{5}k & \frac{3}{5}l \\ \frac{1}{4}m & \frac{1}{4}n & \frac{1}{4}o & \frac{1}{4}p \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Com isso, obtemos:

$a = 21$, $b = 0$, $c = 0$, $d = 0$

$f = 11$, $e = 0$, $g = 0$, $h = 0$

$k = \frac{5}{3}$, $i = 0$, $j = 0$, $l = 0$

$p = 4$, $m = 0$, $n = 0$ e $o = 0$.

Logo, $A^{-1} = \begin{bmatrix} 21 & 0 & 0 & 0 \\ 0 & 11 & 0 & 0 \\ 0 & 0 & \frac{5}{3} & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}$.

Finalmente, para descriptografar a palavra, multiplicamos a inversa de *A* pela matriz *B.*

$$\begin{bmatrix} 21 & 0 & 0 & 0 \\ 0 & 11 & 0 & 0 \\ 0 & 0 & \frac{5}{3} & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 21 \\ 22 \\ 5 \\ 16 \end{bmatrix}.$$

E como T→21, U→22, D→5 e O→16

A palavra originalmente era TUDO.

O exemplo 2 resolvido acima consta na seção "Estudo para o ENEM" do livro Dom Bosco - Sistema de Ensino, Pré-vestibular semiextensivo, volume 2, página 95.

Após a análise dos livros citados, da pesquisa de questões de vestibulares e de relatos de outros professores, percebemos que o tema criptografia não é abordado de forma significativa, nunca como parte de algum programa, na maioria das vezes, apenas como uma curiosidade e, sobretudo, como aplicação de matrizes. Considerando a forte presença da criptografia em atividades do cotidiano como transações bancárias, mensagens via internet, bem como o vínculo com fatos

políticos, consideramos que uma implantação adequada do tema pode ser positiva no processo de ensino e aprendizagem dos alunos.

4.2 PROCEDIMENTOS METODOLÓGICOS.

A escola onde as atividades foram aplicadas conta com uma sala exclusiva para aulas de matemática, com todos os materiais necessários para realização do trabalho, como calculadora, cartolina e materiais de pintura. As carteiras da sala são dispostas de modo a facilitar o trabalho em equipes.

Figura 17 - Sala de Matemática da escola

Fonte: O autor.

Antes de iniciarmos as atividades e, no decorrer delas, foram resgatados conteúdos de matemática de séries anteriores que são fundamentais para o bom entendimento das atividades, como: divisão, números primos, operações com frações, potenciação, radiciação e operações com matrizes.

Como introdução à criptografia e como uma forma de despertar o interesse do aluno sobre o tema, iniciamos a aplicação em sala de aula assistindo ao filme "O jogo da imitação", que relata a história do matemático Alan Turing e como a criptografia foi importante nos desdobramentos da Segunda Guerra Mundial.

Figura 18 - Filme "O jogo da imitação"

Título: O jogo da imitação

Diretor: Morten Tyldum

Distribuidor: Diamond Films

Produção: Nora Grossman, Ido Ostrowski e Teddy Schwarzman

Lançado em : 05 de fevereiro de 2015

Nacionalidade: EUA e Reino Unido

Gênero: Drama/Biografia

Duração: 1h55min

Sinopse:

Durante a Segunda Guerra Mundial, o governo britânico monta uma equipe que tem por objetivo quebrar o Enigma, o famoso código que os alemães usam para enviar mensagens aos submarinos. Um de seus integrantes é Alan Turing (Benedict Cumberbatch), um matemático de 27 anos estritamente lógico e focado no trabalho, que tem problemas de relacionamento com praticamente todos à sua volta. Não demora muito para que Turing, apesar de sua intransigência, lidere a equipe. Seu grande projeto é construir uma máquina que permita analisar todas as possibilidades de codificação do Enigma em apenas 18 horas, de forma que os ingleses conheçam as ordens enviadas antes que elas sejam executadas. Entretanto, para que o projeto dê certo, Turing terá que aprender a trabalhar em equipe e tem Joan Clarke (Keira Knightley) sua grande incentivadora.

O filme, além de ser uma excelente forma de introduzir o tema criptografia em sala de aula, ainda funciona muito bem para debater a importância do trabalho em equipe as relações interpessoais.

As atividades foram desenvolvidas em sete aulas (encontros) de dois tempos de cinquenta minutos cada, durante os tempos das disciplinas de matemática e letramento em matemática ministradas pelo autor do trabalho.

A divisão da turma em grupos foi baseada na teoria de Vygotsky que defende que o aprendizado será produzido do externo para o interno, ou seja, através das relações sociais com as outras pessoas e com o meio para futura interiorização do conhecimento.

> Desta forma, a escola seria o lugar onde a intervenção pedagógica intencional desencadearia o processo ensino-aprendizagem. O professor deveria provocar avanços nos alunos interferindo na sua Zona de Desenvolvimento Proximal ZPD. Outro fator relevante para educação, decorrente das teorias de Vygotsky, seria a importância da atuação dos outros membros do grupo social na mediação entre a cultura e o indivíduo, visto que o aluno não seja um mero sujeito da aprendizagem, mas aquele que é capaz de aprender, junto ao outro, o que seu grupo social produz, como: valores, linguagem e próprio conhecimento. Ao observar a zona proximal, o educador poderia orientar o aluno no sentido de adiantar o seu desenvolvimento potencial, tornando-o real. O relacionamento estabelecido entre a criança e os seus colegas seria, também de importância vital. Vigotsky defendeu a utilização de uma criança mais desenvolvida para ajudar a outra menos desenvolvida (Sutherland, 1996, p.73).

Os grupos foram criados de modo a serem o mais heterogêneos possível, com alunos em vários níveis de desenvolvimento para que ocorra a colaboração mútua em prol de alcançar os objetivos. A figura abaixo mostra a turma dividida em grupos realizando uma das atividades.

Figura 19 - Realização da tarefa em sala de aula

Fonte: O autor

4.3 DETALHAMENTO DAS ATIVIDADES.

4.3.1 CRIPTOGRAFANDO COM DISCO DE CIFRAS

Os discos de cifras podem ser utilizados, pela sua simplicidade em relação a outros métodos de criptografia, como uma boa forma de iniciar o aluno no processo de codificação e decodificação de mensagens. Começar utlizando um processo mais simples faz com que o aluno se interesse pelo tema e fique curioso em descobrir novos métodos para cifrar mensagens.

O primeiro passo da atividade é a confecção do disco de cifras por cada grupo para que o mesmo seja utilizado na codificação e decodificação das mensagens. O disco é composto por dois círculos concêntricos, divididos em 26 setores, de modo que o círculo central gira no sentido anti-horário, usando a letra A como origem, tantas casas quantas forem utilizadas para gerar a chave de codificação.

Figura 20 - Discos de cifras

Fonte: O autor

Esta atividade é fundamentada nas cifras de substituição que são detalhadas na seção 3.2 e inspirada no exercício da OBMEP descrito abaixo:

(OBMEP 2007 - 2ª fase) Um antigo método para codificar palavras consiste em escolher um número de 1 a 26, chamado chave do código, e girar o disco interno do aparelho ilustrado na figura até que essa chave corresponda à letra A. Depois disso, as letras da palavra são substituídas pelos números correspondentes, separados por tracinhos. Por exemplo, na figura ao lado a chave é 5 e a palavra PAI é codificada como 20-5-13.

a) Usando a chave indicada na figura, descubra qual palavra foi codificada como 23-25-7-25-22-13.

b) Codifique OBMEP usando a chave 20.

c) Chicó codificou uma palavra de 4 letras com a chave 20, mas esqueceu-se de colocar os tracinhos e escreveu 2620138. Ajude Chicó colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele codificou.

d) Em uma outra chave, a soma dos números que representam as letras A, B e C é 52. Qual é essa chave?

Respostas:

a) Usando a chave 5, temos: 23 = S, 25 = U, 7 = C, 25 = U, 22 = R e 13 = I, logo a palavra é SUCURI.

b) Usando a chave 20, temos: O = 8, B = 21, M = 6, E = 24 e P = 9, logo OBMEP = 8-21-6-24-9.

c) Com os tracinhos ficaria 26-20-13-8 e como 26 = G, 20 = A, 13 = T e 8 = O, a palavra é GATO.

d) Como 52 não é divisível por três e o disco é dividido em 26 setores, a chave será 25. A = 25, B = 26 e C = 1.

A questão detalhada acima foi resolvida em sala de aula com os alunos que, utilizando os conhecimentos adquiridos e o disco construído por eles, resolveram a seguinte atividade:

ATIVIDADE: Utilizando o disco construído por vocês e os procedimentos da atividade anterior, resolva:

a) Codifique a palavra ENEM usando a chave 25.

b) Sabendo que a chave usada foi 17, descubra qual palavra foi codificada como 19-17-4-21-10-17.

c) Usando o método que achar conveniente e de posse do disco de cifras, tente decifrar a mensagem: "H THALTHAPJH L H YHPUOH KHZ JPLUJPHZ"

Respostas:

a) Girando o disco de cifras até que o número 25 esteja alinhado com a letra A, temos: E = 3, N = 12, E = 3 e M = 11 e, de forma codificada 3-12-3-11.

b) Girando o disco de cifras até que o número 17 esteja alinhado com a letra A, temos: 19 = C, 17 = A, 4 = N, 21 = E, 10 = T e 17 = A. Formando a palavra CANETA.

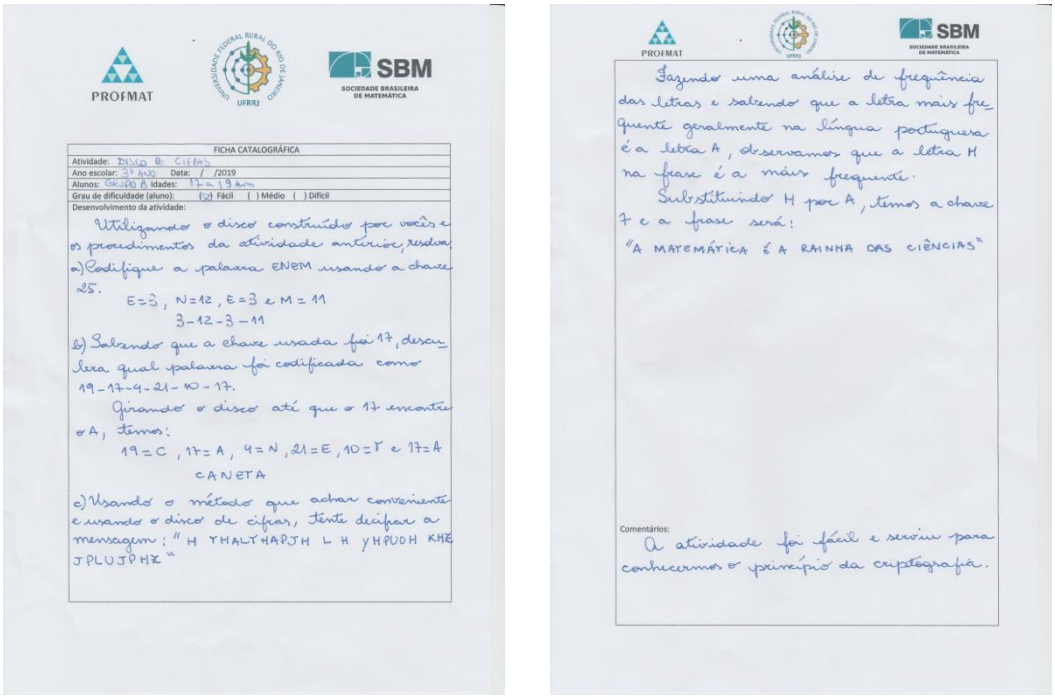
c) Usando a tabela de frequência de ocorrência de letras na língua portuguesa da seção 3.2.1 para fazer uma análise de frequência das letras da frase, observamos que a letra com maior frequência na frase criptografada é o H.

Tomando o H como possível deslocamento da letra A, temos a chave 7, substituindo todas as outras letras da frase criptografada com essa chave, verificamos que a frase faz sentido e é:

"A MATEMÁTICA É A RAINHA DAS CIÊNCIAS"

A seguir, temos um exemplo de atividade realizada por um grupo e seu comentário a respeito da atividade.

Figura 21 - Exemplo de resposta dos alunos



Fonte - O autor

Comentários do grupo: *"A atividade foi fácil e serviu para conhecermos o princípio da criptografia"*

4.3.2 CRIPTOGRAFANDO COM MATRIZES

A proposta desta atividade é aplicar os conceitos de operações com matrizes, resgatando conteúdos de séries anteriores, dando significado ao estudo de matrizes e seus conceitos.

Aplicando o conceito de criptografia que consiste em enviar mensagens utilizando chaves pré-estabelecidas entre as partes envolvidas, essa atividade é

inspirada na cifra de Hill (ver seção 3.2.3) e desenvolvida como uma forma de se trocar mensagens usando matrizes como chaves de codificação e decodificação.

Consiste em relacionar cada letra do alfabeto a um número (tabela) e utiliza como chave codificadora/decodificadora um par de matrizes quadradas (*A* e *B*) inversas uma da outra. Cria-se um código denominado matriz chave que deve ser multiplicada pela matriz cifrada gerando então uma nova matriz codificada.

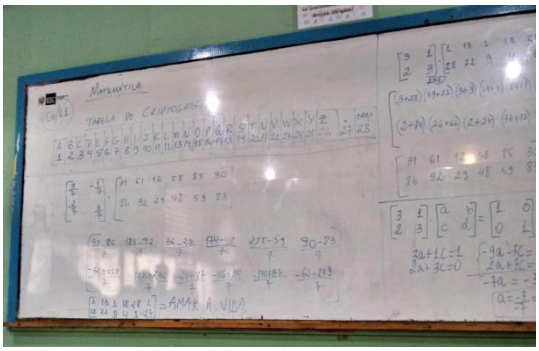
Tabela - cifra de Hill

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
1	2	3	4	5	6	7	8	9	10	11	12	13	14
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**.**	**#**
15	16	17	18	19	20	21	22	23	24	25	26	27	28

Fonte: o autor

A tabela acima é exposta no quadro aos alunos que são orientados a escolherem uma mensagem curta e durante a atividade os alunos usaram calculadora científica cedida pelo professor ou a própria calculadora de seus celulares.

Figura 22 - Exemplo no quadro



Fonte: O autor

Como exemplo de aplicação em sala de aula, suponhamos que a mensagem a ser transmitida seja: AMAR A VIDA.

De acordo com a tabela numérica temos os números: 1, 13, 1, 18, 28, 1, 28, 22, 9, 4, 1, 27.

A sequência de números acima deve ser arrumada em uma matriz *M* de duas linhas:

$M = \begin{pmatrix} 1 & 13 & 1 & 18 & 28 & 1 \\ 28 & 22 & 9 & 4 & 1 & 27 \end{pmatrix}$.

Utilizaremos como chave codificadora/decodificadora as matrizes:

$A = \begin{pmatrix} 3 & 1 \\ 2 & 3 \end{pmatrix}$ e $B = \begin{pmatrix} \frac{3}{7} & -\frac{1}{7} \\ -\frac{2}{7} & \frac{3}{7} \end{pmatrix}$.

O remetente utiliza a matriz *A* para codificar a mensagem fazendo: *N = A.M* e, desse modo, obtém a matriz *N*.

$A.M = \begin{pmatrix} 3 & 1 \\ 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 13 & 1 & 18 & 28 & 1 \\ 28 & 22 & 9 & 4 & 1 & 27 \end{pmatrix} =$

$\begin{pmatrix} 31 & 61 & 12 & 58 & 85 & 30 \\ 86 & 92 & 29 & 48 & 59 & 83 \end{pmatrix} = N.$

Os elementos de *N* constituem a mensagem cifrada:

31, 61, 12, 58, 85, 30, 86, 92, 29, 48, 59, 83.

Quando a mensagem cifrada chega ao destinatário, ele utiliza a matriz decodificadora *B* para desfazer os procedimentos anteriores; considerando que:

B . N = B . A . M = I . M = M. De posse da mensagem codificada, o destinatário constrói uma matriz com duas linhas *N* e calcula o produto *B. N*.

$B.N = \begin{pmatrix} \frac{3}{7} & -\frac{1}{7} \\ -\frac{2}{7} & \frac{3}{7} \end{pmatrix} \cdot \begin{pmatrix} 31 & 61 & 12 & 58 & 85 & 30 \\ 86 & 92 & 29 & 48 & 59 & 83 \end{pmatrix} =$

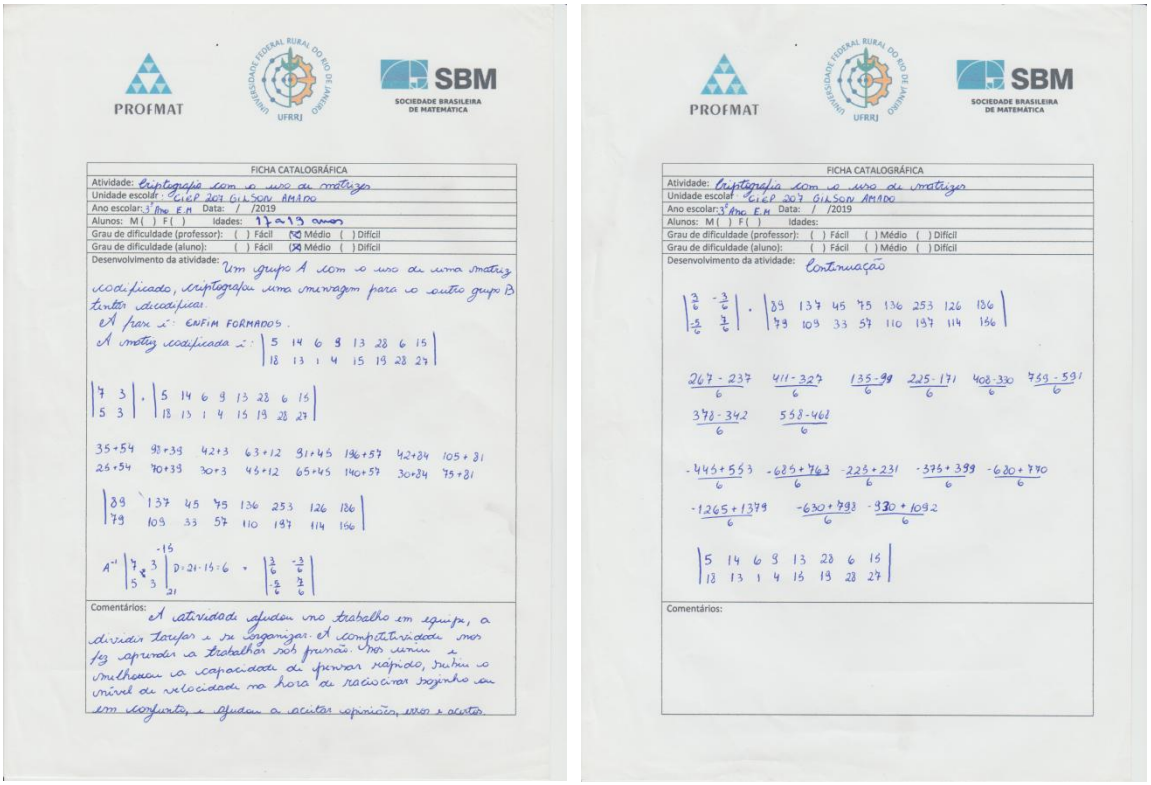
$= \begin{pmatrix} 1 & 13 & 1 & 18 & 28 & 1 \\ 28 & 22 & 9 & 4 & 1 & 27 \end{pmatrix} = M.$

Os elementos da matriz *M* obtida formam a sequência de números: 1, 13, 1, 18, 28, 1, 28, 22, 9, 4, 1, 27, cuja decodificação é:

1	**13**	**1**	**18**	**28**	**1**	**28**	**22**	**9**	**4**	**1**	**27**
A	**M**	**A**	**R**	**#**	**A**	**#**	**V**	**I**	**D**	**A**	**.**

A seguir, temos um exemplo de atividade realizada por um grupo e seu comentário a respeito da atividade.

Figura 23 - Exemplo de resposta dos alunos



Fonte: O autor

Comentário do grupo: "*A atividade ajudou no trabalho em equipe, a dividir tarefas e se organizar. A competitividade nos fez aprender a trabalhar sob pressão, nos uniu e melhorou a capacidade de pensar rápido, subiu o nível de velocidade na hora de raciocinar sozinho ou em conjunto e ajudou a aceitar opiniões, erros e acertos*".

Figura 24 - Grupo comemorando a descoberta da mensagem

Fonte: O autor

4.3.3 CRIPTOGRAFANDO NO SISTEMA RSA.

O exemplo da seção 2.3 foi feito passo a passo com a turma após termos resgatado em aulas anteriores alguns pré-requisitos necessários para o bom entendimento do assunto, como números primos, mmc, mdc e potenciação. A turma então foi dividida em dois grupos A e B, onde o grupo A, com o uso do sistema RSA criptografa uma mensagem para o grupo B decodificar.

Por questões de tempo de duração da atividade e para não torná-la excessivamente trabalhosa, fazendo com que os alunos perdessem o interesse, a mensagem codificada era composta apenas de uma palavra e os números primos escolhidos foram pequenos. Fazendo a atividade com apenas uma palavra codificada e números primos pequenos já é possível mostrar aos alunos a enorme dificuldade de decodificar mensagens extensas com primos muito grandes como os que são usados no RSA hoje em dia.

Para a escolha dos números primos e para realizar testes de primalidade os alunos construíram um crivo de Eratóstenes e para realizar as operações usamos o modelo de calculadora representado abaixo que foi disponibilizado pelo professor.

Figura 25 - Crivo de Eratóstenes e calculadora utilizada

Fonte: O autor

A palavra a ser codificada e os números primos *p* e *q* foram escolhidos pelos alunos e a atividade é detalhada a seguir:

O grupo A, usando o sistema RSA, criptografa uma palavra para o grupo B decodificar usando o exemplo da seção 2.3 resolvido pelo professor em aula.

Passo 1 ⇒ Escolher a palavra e realizar a sua pré-codificação.

A palavra escolhida é SORTE, resultando na sequência 2824272914.

Passo 2 ⇒ Escolher os números primos *p* e *q* e determinar a chave de cifragem *n.*

Os números escolhidos foram *p* = 5 e *q* = 7 ⇒ *n* = 35.

Passo 3 ⇒ Calcular o valor de $\varphi(n)$, o aluno teve uma introdução ao conceito e noções básicas para aplicar na atividade e como o valor de *n* é obtido a partir de dois números primos pequenos, o cálculo de $\varphi(n)$ se torna bem simples.

$\varphi(n) = \varphi(p.q) = (p - 1) . (q - 1) = (5 - 1) . (7 - 1) = 24.$

Passo 4 ⇒ Determinar o parâmetro *e*, onde $(e, \varphi(n)) = 1$.

O parâmetro escolhido foi *e* = 7.

Passo 5 ⇒ Quebrar a mensagem em blocos de tamanho *A*, com $A < n.$

Blocos: 28 24 27 29 14

Passo 6 ⇒ Codificar a mensagem usando a relação: $A^e \equiv R \bmod n.$

Bloco 28

$28^2 \equiv 14 \bmod 35$

$(28^2)^3 \equiv 14^3 \bmod 35$

$(28^2)^3 . 28 \equiv 14^3 . 28 \bmod 35$

$28^7 \equiv 14 . 28 \bmod 35$

$28^7 \equiv 7 \bmod 35$

Bloco 24

$24^2 \equiv 16 \bmod 35$

$(24^2)^3 \equiv 16^3 \bmod 35$

$(24^2)^3 . 24 \equiv 16^3 . 24 \bmod 35$

$24^7 \equiv 1 . 24 \bmod 35$

$24^7 \equiv 24 \bmod 35$

Bloco 27

$27^2 \equiv 29 \bmod 35$

$(27^2)^3 \equiv 29^3 \bmod 35$

$(27^2)^3 . 27 \equiv 29^3 . 27 \bmod 35$

$27^7 \equiv 29.\ 27 \bmod 35$

$27^7 \equiv 13 \bmod 35$

Bloco 29

$29^2 \equiv 1 \bmod 35$

$(29^2)^3 \equiv 1^3 \bmod 35$

$(29^2)^3.29 \equiv 1\ .\ 29 \bmod 35$

$29^7 \equiv\ 29 \bmod 35$

Bloco 14

$14^2 \equiv 21 \bmod 35$

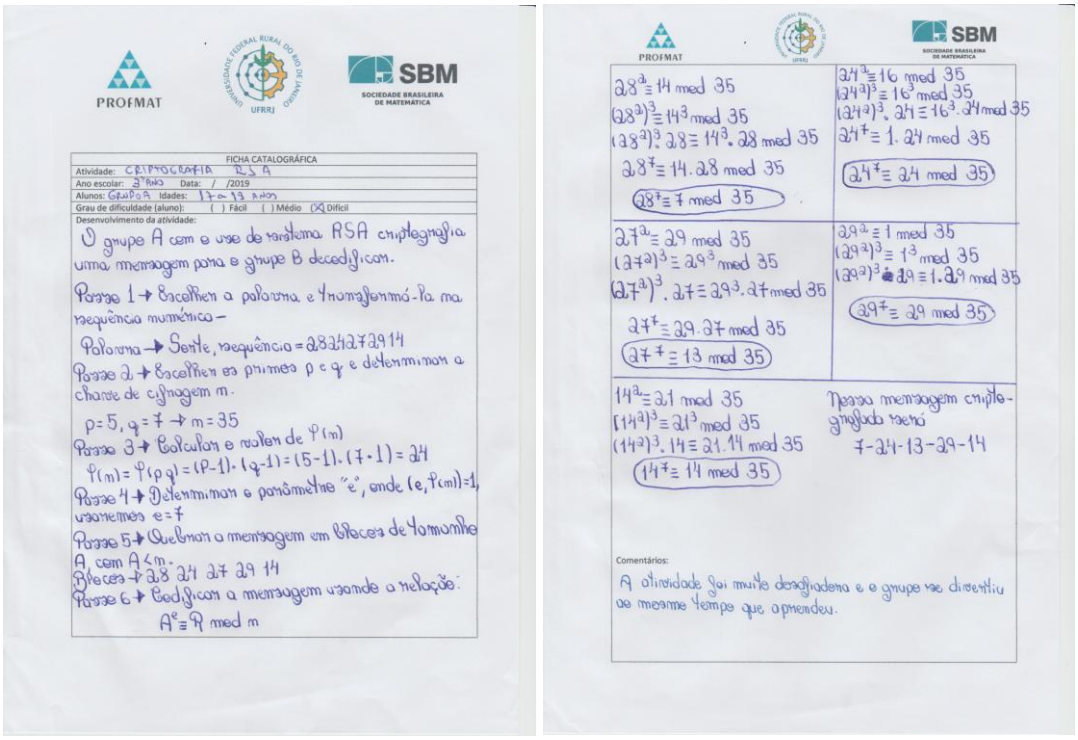
$(14^2)^3 \equiv 21^3 \bmod 35$

$(14^2)^3.14 \equiv\ 21.\ 14 \bmod 35$

$14^7 \equiv 14 \bmod 35$

Assim, a mensagem criptografada será 7-24-13-29-14.

Figura 26 - Atividade RSA do grupo A



Fonte: O autor

Comentário do grupo: "*A atividade foi muito desafiadora e o grupo se divertiu ao mesmo tempo que aprendeu".*

O grupo B de posse da chave de codificação (*e* , *n*) = (7 , 35) RSA cedida pelo grupo A, decodifica a mensagem codificada pelo grupo A 7-24-13-29-14

Passo 1 ⇒ Determinar *d*, o inverso multiplicativo de *e* mod $\varphi(n)$.

$7d \equiv 1 \bmod 24$

como $49 \equiv 1 \bmod 24$

d = 7, pois 7 . 7 = 49.

e a chave privada será (7,35).

Passo 2 ⇒ Decodificar a palavra de acordo com a relação: $R^d \equiv B \bmod n$.

$7^2 \equiv 14 \bmod 35$

$(7^2)^3 \equiv 14^3 \bmod 35$

$(7^2)^3 . 7 \equiv 14^3 . 7 \bmod 35$

$7^7 \equiv 14. 7 \bmod 35$

$7^7 \equiv 28 \bmod 35$

$24^2 \equiv 16 \bmod 35$

$(24^2)^3 \equiv 16^3 \bmod 35$

$(24^2)^3 . 24 \equiv 1 . 24 \bmod 35$

$24^7 \equiv 24 \bmod 35$

$13^2 \equiv 29 \bmod 35$

$(13^2)^3 \equiv 29^3 \bmod 35$

$(13^2)^3 . 13 \equiv 29 . 13 \bmod 35$

$13^7 \equiv 27 \bmod 35$

$29^2 \equiv 1 \bmod 35$

$(29^2)^3 \equiv 1^3 \bmod 35$

$(29^2)^3 . 29 \equiv 1 . 29 \bmod 35$

$29^7 \equiv 29 \mod 35$

$14^2 \equiv 21 \mod 35$

$(14^2)^3 \equiv 21^3 \mod 35$

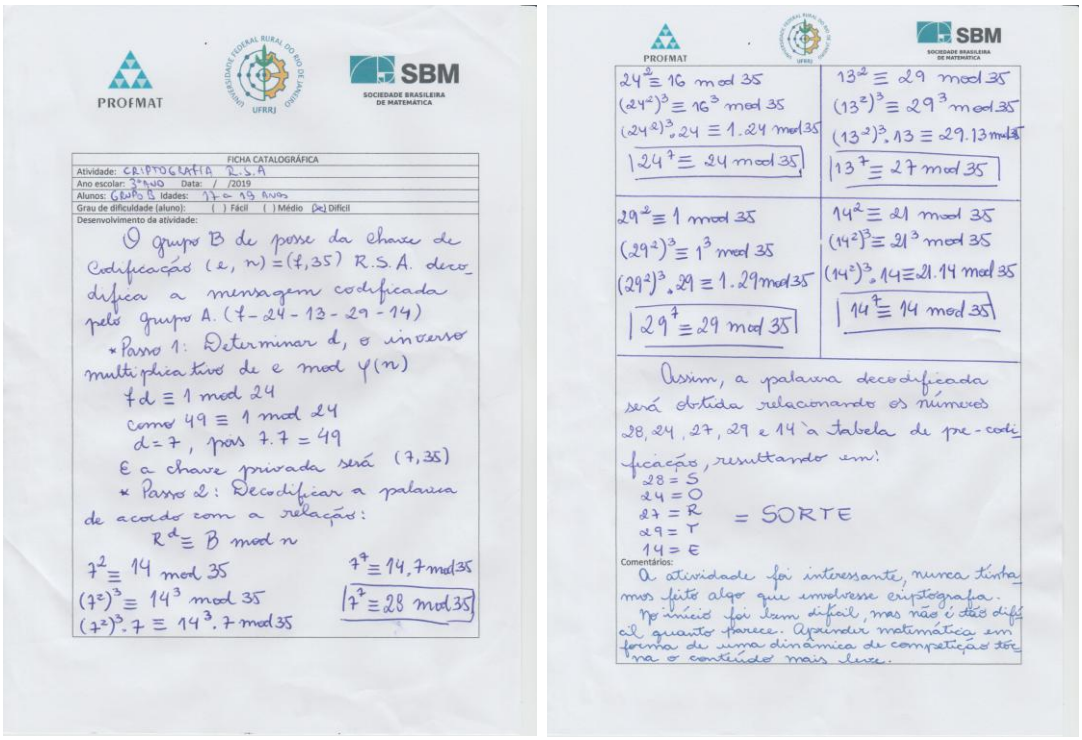
$(14^2)^3 . 14 \equiv 21 \, . \, 14 \mod 35$

$14^7 \equiv 14 \mod 35$

Assim, a palavra decodificada será obtida relacionando os números 28, 24, 27, 29 e 14 à tabela de pré-codificação, resultando em:

28 = S, 24 = O, 27 = R, 29 = T, 14 = E e a palavra é SORTE.

Figura 27 - Atividade RSA do grupo B



Fonte: O autor

Comentário do grupo: *"A atividade foi interessante, nunca tínhamos feito algo que envolvesse criptografia. No início foi bem difícil, mas não é tão difícil quanto parece. Aprender matemática em forma de uma dinâmica de competição torna o conteúdo mais leve".*

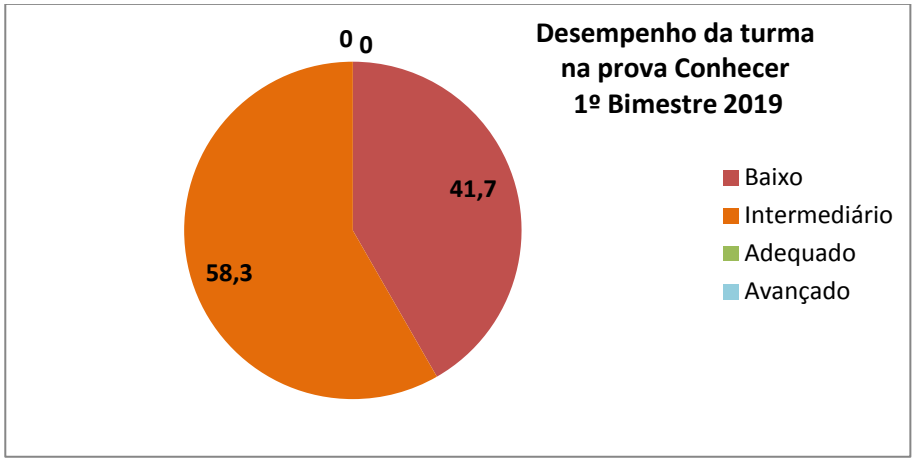
Concluímos a atividade sobre criptografia RSA conversando com os alunos sobre a ética de não utilizar indevidamente senhas de propriedade alheia, sistemas

de criptografia tão robustos só são necessários porque algumas pessoas agem com desonestidade. Uma boa reflexão seria pensar como seria a evolução da criptografia ao longo do tempo caso as pessoas fossem inteiramente honestas.

4.4 RESULTADOS OBTIDOS.

As atividades desenvolvidas foram registradas pelos alunos em fichas catalográficas onde os mesmos apresentaram suas conclusões, que foram utilizadas como um dos parâmetros de avaliação dos objetivos alcançados.

No primeiro bimestre de 2019 foi aplicada a prova conhecer[1] em todas as turmas de terceiro ano do ensino médio das escolas estaduais do Rio de Janeiro que gerou uma ferramenta de análise de testes que apontou o desempenho dos alunos em vários conteúdos.



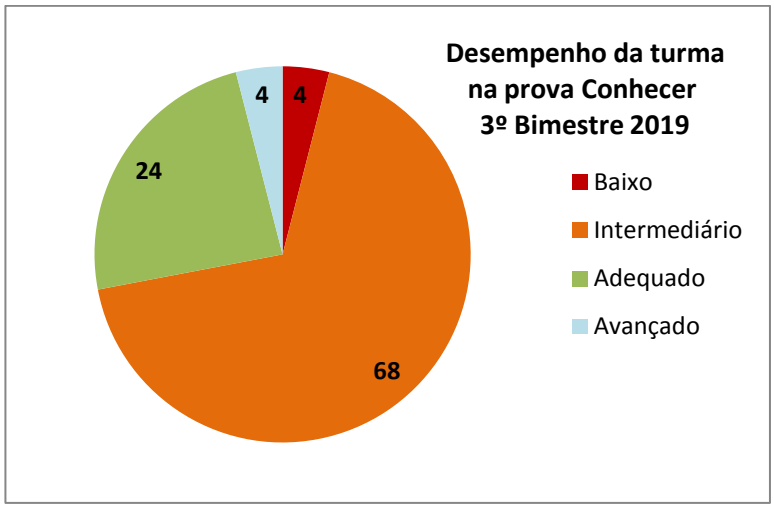
Baixo	Intermediário	Adequado	Avançado
(Até 25%) Os estudantes que apresentam este padrão de desempenho revelam ter desenvolvido competências e habilidades muito aquém do que seria esperado para o período de escolarização em que se encontram. Por isso, esse grupo de alunos necessita de uma intervenção focada, para que possam progredir com sucesso em seu processo de escolarização.	(Acima de 25% até 50%) Os estudantes que apresentam este padrão de desempenho demonstram já terem começado um processo de sistematização e domínio das habilidades consideradas básicas e essenciais ao período de escolarização em que se encontram. Para esse grupo de estudantes, é importante o investimento de esforços, para que possam desenvolver habilidades mais elaboradas.	(Acima de 50% até 75%) Neste padrão de desempenho, os alunos demonstram ter ampliado o leque de habilidades tanto no que diz respeito à quantidade quanto no que se refere à complexidade dessas habilidades, as quais exigem um maior refinamento dos processos cognitivos nelas envolvidos.	(Acima de 75%) Neste padrão de desempenho, os estudantes revelam ser capazes de realizar tarefas que exigem habilidades mais sofisticadas, que superam aquelas esperadas para o período de escolaridade em que se encontram.

Dados da Secretaria de Educação do Estado do Rio de Janeiro

[1] A prova Conhecer é uma avaliação externa diagnóstica desenvolvida pela SEEDUC-RJ com o objetivo de identificar as necessidades pontuais de cada escola e criar um histórico de resultados para o planejamento de ações, visando a melhoria da qualidade do ensino no estado do Rio de janeiro.

O desempenho médio da turma em matemática na prova Conhecer saltou de 25,6% no primeiro bimestre para 45,1% no terceiro bimestre, um aumento de 76,2%.

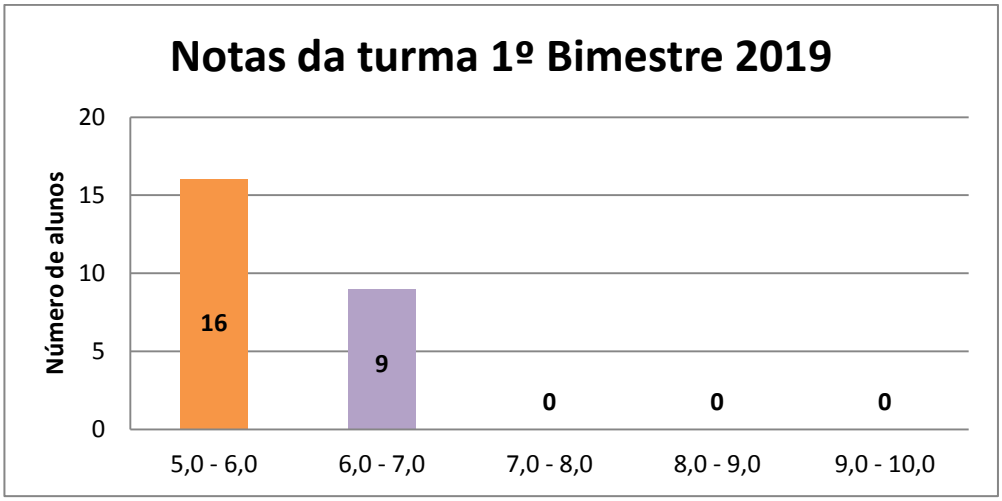
De acordo com a Superintendência de Avaliação e Acompanhamento do Desempenho Escolar- SUPAA, o objetivo da prova conhecer é promover o processo avaliativo com vistas a identificar as habilidades em Matemática não consolidadas ou pouco desenvolvidas, subsidiando às unidades escolares o desenvolvimento de ações pedagógicas direcionadas a corrigir lacunas de aprendizagem.



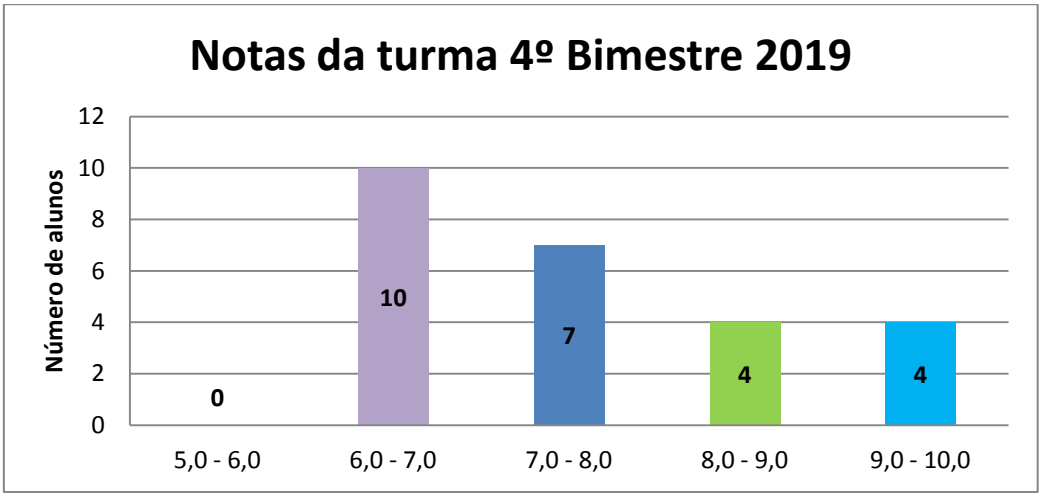
Dados da Secretaria de Educação do Estado do Rio de Janeiro

A Primeira prova Conhecer foi aplicada em abril, no primeiro bimestre letivo de 2019 e a segunda prova Conhecer foi aplicada em agosto, no terceiro bimestre letivo de 2019 e, entre elas, foram desenvolvidas as aulas de introdução ao tema criptografia, foram resgatados conteúdos que eram pré-requisitos para a aplicação das atividades e foram desenvolvidas as atividades 1 e 2 do trabalho.

Outro parâmetro utilizado na análise dos resultados foram as notas bimestrais de matemática dos alunos, fazendo uma comparação entre o primeiro e o quarto bimestres.



Dados coletados no site docente online da SEEDUC-RJ



Dados coletados no site docente online da SEEDUC-RJ

A média bimestral da turma saltou de 5,98 no primeiro bimestre para 7,96 no quarto bimestre.

Comparando os dados apresentados nos gráficos acima, os comentários dos alunos e a avaliação do próprio professor autor do trabalho, percebemos que o trabalho alcançou objetivos, porém é necessário destacar que esses resultados não se devem apenas à aplicação das atividades de criptografia, mas também a outros fatores como: turma com número reduzido de alunos, comprometimento e grau de colaboração dos alunos envolvidos e participação ativa dos alunos nas atividades propostas.

5. CONSIDERAÇÕES FINAIS.

É fundamental que o professor busque constantemente ferramentas que possam auxiliar sua prática em sala de aula, fugindo da mecanização e repetição de exercícios que são institucionalizadas no ensino da matemática. É necessário que se valorize a construção do conhecimento acreditando ser possível encurtar a distância entre a matemática acadêmica e a matemática do dia a dia focando no aluno e o estimulando a pensar.

Este trabalho objetivou investigar como os elementos da teoria dos números e de matrizes poderiam ser aplicados em criptografia com o propósito de fazer uma conexão entre a matemática teórica e a matemática aplicada, estudando alguns métodos de criptografia e mostrando sua importância atual na segurança dos dados transmitidos via rede mundial de computadores.

A utilização da criptografia como ferramenta de ensino mostrou-se bem favorável como recurso didático. A apresentação de filmes sobre o tema, a apresentação do contexto histórico, a confecção do disco de cifras e do crivo Eratóstenes e, sobretudo, as atividades em grupo onde, em clima de competição, os alunos criaram e desvendaram enigmas, serviram para prender a atenção dos mesmos e inserí-los num universo, até então, por eles desconhecido. Propiciando aos discentes o crescimento nas suas próprias ideias e pensamentos.

Os alunos conseguiram codificar e decodificar as mensagens, analisaram os resultados obtidos e tiraram suas próprias conclusões tendo o professor como mediador. As atividades serviram para aguçar a curiosidade e o interesse dos alunos, fazendo evoluir formalmente seus saberes e habilidades matemáticas.

A melhora no rendimento da turma nas avaliações internas e externas também indicou a relevância da aplicação da criptografia como uma boa ferramenta na relação ensino-aprendizagem.

Frente a uma realidade político-econômica e social em que a atividade do magistério pouco é valorizada, mal remunerada e que nem motivação encontra na maioria das vezes na classe estudantil, encontrar mecanismos que facilitem a relação professor-aluno, despertem o interesse e mostrem bons resultados, nos energizam e nos fazem seguir apesar desses dissabores externos.

REFERÊNCIAS.

BEZERRA, D. de J.; MALAGUTTI, P. L.; RODRIGUES, V. C. da S. **Aprendendo Criptologia de forma Divertida**. 1. ed. Rio de Janeiro, 2010.

BOYER, C. B. **História da Matemática**. 3. ed. São Paulo: Blucher, 2010.

BRASIL. Ministério da Educação. Parâmetros Curriculares Nacionais: Matemática (1ª a 4ª séries). Brasília: MEC/SEF, 1997.

BRASIL. Ministério da Educação. Parâmetros Curriculares Nacionais: Matemática (5ª a 8ª séries). Brasília: MEC/SEF, 1997.

BRASIL.Ministério da Educação.Parâmetros Curriculares nacionais: Ensino Médio. Brasília: Ministério da Educação, 1997.

BRASIL, Guia PNLD Literário 2018. Ministério da Educação. Brasília. 2018.

COUTINHO, S. **Números inteiros e criptografia RSA**. 2 ed. Rio de Janeiro: IMPA, 2005.

COUTINHO, S. Introdução à Criptografia I. In: **Aritmética I**, material de disciplina do Mestrado Profissional em Matemática em Rede Nacional.

CHAVANTE, Eduardo; PRESTES, Diego. **Quadrante.** 1 ed. São Paulo: SM, 2016.

DANTE, Luiz Roberto. **Matemática-Contexto** & **Aplicações**. 3 ed. São Paulo: Ática, 2017.

DOMINGUES, H. H. **Fundamentos de Aritmética**. Florianópolis: Ed. da UFSC, 2009.

EVES, Howard. **Introdução à História da Matemática**. Campinas- SP: Editora Unicamp, 2004.

GODINHO, D. S. **Criptografia: a importância da álgebra linear para decifrá-la**. revista iTEC, v.II, nº 2, 2011.

HEFEZ, A. **Aritmética**. 1 ed. Rio de Janeiro: SBM, 2014. (Coleção PROFMAT).

HEFEZ, A. **Aritmética**. 2 ed. Rio de Janeiro: SBM, 2016. (Coleção PROFMAT).

HEFEZ, A. **Elementos de Aritmética**. Sociedade Brasileira de Matemática, Textos Universitários, 2006.

HEFEZ, A.; FERNANDEZ, C. **Introdução à algebra linear**. 2 ed. Rio de Janeiro: SBM, 2016. (Coleção PROFMAT).

IEZZI, G.; DOLCE, O.; DEGENSZAJN, D.; PÉRIGO, R.; ALMEIDA, N. **Matemática: Ciência e Aplicações**. 9 ed. São Paulo: Saraiva, 2017.

IEZZI, G. **Fundamentos de Matemática Elementar**, Vol. 1, 8 ed, São Paulo: Atual, 2004.

LIMA, Elon Lages. **Números e Funções Reais**. Rio de Janeiro: SBM, 2013.

NORMAN, D. **A Europa em guerra (1939-1945)**. Lisboa: Edições 70, 2008.

SANTOS, J. L. **A arte de cifrar, criptografar, esconder e salvaguardar como fontes motivadoras para atividades de matemática básica**. 2013. (Dissertação de Mestrado PROFMAT-UFBA). Salvador-BA

SAUTOY, M. **A Música dos números Primos: a história de um problema não resolvido na matemática**. Rio de Janeiro: Jorge Zahar, 2007.

SINGH, S. **O livro dos códigos**. 2. ed. Rio de Janeiro: Record, 2005.

SINGH, S. **O livro dos códigos: A ciência do sigilo - do antigo Egito à criptografia quântica**. 9. ed. Rio de Janeiro: Record, 2011.

SUTHERLAND, P. **O desenvolvimento cognitivo actual**. Lisboa: Instituto Piaget.

TERADA, R. **Criptografia e a importância das suas aplicações**. Revista do professor de matemática, volume 12. SBM, 1988.