UNIVERSIDADE FEDERAL DO TOCANTINS
CAMPUS DE ARAGUAÍNA
CURSO DE LICENCIATURA EM MATEMÁTICA

ARIANE ANDRESSA NORONHA DE SOUSA MIRANDA

UMA OFICINA DE MATEMÁTICA NO ENSINO BÁSICO POR MEIO DA CRIPTOGRAFIA

ARAGUAÍNA
2020

ARIANE ANDRESSA NORONHA DE SOUSA MIRANDA

UMA OFICINA DE MATEMÁTICA NO ENSINO BÁSICO POR MEIO DA CRIPTOGRAFIA

Monografia apresentada ao curso de Licenciatura em Matemática da Universidade Federal do Tocantins, como requisito parcial para a obtenção de título de Licenciada em Matemática.
Orientadora: Prof. Dra. Fernanda Vital de Paula.

ARAGUAÍNA
2020

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

M672o Miranda, Ariane Andressa Noronha de Sousa.
UMA OFICINA DE MATEMÁTICA NO ENSINO BÁSICO POR MEIO DA CRIPTOGRAFIA. / Ariane Andressa Noronha de Sousa Miranda. – Araguaína, TO, 2020.
46 f.

Monografia Graduação - Universidade Federal do Tocantins – Câmpus Universitário de Araguaína - Curso de Matemática, 2020.
Orientadora : Fernanda Vital de Paula

1. Matrizes e Funções. 2. História da criptografia. 3. Conceitos básicos da criptografia. 4. Oficina e discussão de resultados. I. Título

CDD 510

Elaborado pelo sistema de geração automática de ficha catalográfica da UFT com os dados fornecidos pelo(a) autor(a).

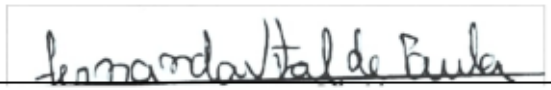
ARIANE ANDRESSA NORONHA DE SOUSA MIRANDA

UMA OFICINA DE MATEMÁTICA NO ENSINO BÁSICO POR MEIO DA CRIPTOGRAFIA

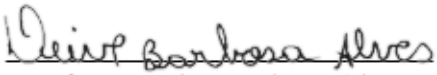
Monografia apresentada ao curso de Licenciatura em Matemática da Universidade Federal do Tocantins, como requisito parcial para a obtenção de título de Licenciada em Matemática.
Orientadora: Prof. Dra. Fernanda Vital de Paula.

Aprovada em: 18/ 08/ 2020.

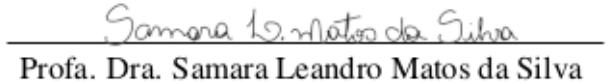
BANCA EXAMINADORA



Profa. Dra. Fernanda Vital de Paula (orientadora)



Prof. Dr. Deive Barbosa Alves



Profa. Dra. Samara Leandro Matos da Silva

AGRADECIMENTOS

À minha família, pelo incentivo e apoio durante toda elaboração deste trabalho e por estar presente em minha vida. Essencialmente, à Alzerina, que é a base de toda a minha formação como pessoa e Amanda, que colaborou pessoalmente na monografia.

Aos colegas da Licenciatura em Matemática da UFT, pelos anos maravilhosos, em especial aos meus amigos: Ana Gabrielly, Ancelmo, Bruno, Carlos, Diogo, Elissama, Hentony, Larisse, Leandro, Márcya, Surama e Werik, pela parceria, noites de jogos e estudos, amizade e participação em todas as etapas ao decorrer do curso.

Ao Prof. Me. André Ortiz, pela instrução inicial que propiciou o alcance dos objetivos desse trabalho.

Aos preceptores Marinete Duarte e Gildemberg da Cunha, respectivamente, professores da Escola Estadual Jorge Amado e do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO), pelo auxílio dado na oficina proposta neste trabalho e pelas suas contribuições no meu preparo como futura docente.

Ao Prof. Dr. Deive Barbosa, supervisor do programa Residência Pedagógica, por todo apoio e monitoração durante o programa.

Por fim, à minha orientadora Profa. Dra. Fernanda Vital, pela paciência e instrução nesse trabalho.

“Ensinar não é transferir conhecimento, mas criar as possibilidades para a sua própria produção ou a sua construção.”

Paulo Freire

RESUMO

A presente monografia aborda a criptografia e sua aplicação no Ensino Fundamental e Médio, por meio da proposição e desenvolvimento de uma oficina. Tendo em vista a importância da criptografia na manutenção da segurança e privacidade em todas as operações tecnológicas do cotidiano, o tema é abordado como possibilitador da associação entre teoria e realidade, com o objetivo de ampliar o conhecimento do aluno e motivá-lo a compreender conteúdos matemáticos, culminando assim, em um aprendizado mais didático. Dessa forma, serão exibidos métodos criptográficos praticáveis no Ensino Básico, utilizando funções e matrizes, uma breve recapitulação acerca da sua história e seu funcionamento por intermédio de chaves. Posteriormente, a oficina é apresentada por meio da metodologia utilizada para sua organização, que consiste de três momentos distintos: abordagem histórica, exemplificação/revisão de conteúdo e prática. Por fim, os resultados obtidos por meio de questionário e relato pessoal, após sua execução em duas turmas do Ensino Básico, são exibidos.
Palavras-chave: Criptografia. Ensino Básico. Oficina.

ABSTRACT

This monograph addresses cryptography and its application in elementary and high school, through the proposition of a workshop. In view of the importance of cryptography in maintaining security and privacy in all technological operations of everyday life, the theme is approached as enabling the association between theory and reality, in order to expand the student's knowledge and motivate him to understand contents mathematicians, thus culminating in more didactic learning. In this way, practicable cryptographic methods in Basic Education will be displayed, using functions and matrices, a brief recap about their history and their operation through keys. Finally, the activity developed is presented and the results obtained after the execution in two classes of Basic Education are displayed.
Keywords: Cryptography. Basic education. Workshop.

Lista de Figuras

Sumário

Capítulo 1

Introdução

O educador pode buscar formas de interligar o conhecimento matemático com situações reais. Isso reforça e desenvolve a habilidade de raciocínio do aluno e, portanto, competências como: capacidade de resolver problemas, criatividade e a liberdade no processo de aprendizagem que convergem para um pensamento lógico. Advindo dessa percepção, esse trabalho se baseia na criptografia, a partir do pensamento de que a matemática deve ser ensinada de forma a produzir significado para o aluno, usando situações que remetem a realidade.

No cotidiano, todos têm alguma informação que por vários motivos preferem manter no sigilo e/ou disponível para acesso de poucos, sejam elas conversas em aplicativos de mensagens, pastas, contas, e-mails, informações militares, transações bancárias, dados de clientes e outras. Dessa deficiência, nasceu a criptografia, desenvolvida em períodos de guerra, oriunda da necessidade de ocultar dados para garantir a segurança. Neste sentido, "o objetivo dos sistemas criptográficos não é esconder a existência de uma mensagem, mas evitar que uma pessoa desautorizada compreenda o seu significado, mesmo que tenha acesso às informações cifradas." (MENEZES, 2013, p. 16).

A palavra criptografia vem do grego kriptos (escondido) e grapho (escrita), ou seja, é um mecanismo de codificação da escrita. O objetivo é que um certo comunicado seja recebido apenas pelo seu destinatário legítimo e esse, com o uso de uma chave específica, possa ter acesso a ela.

Destaca-se que a ideia de abordar esse tema, neste trabalho, foi motivado pelo programa Residência Pedagógica, do qual fui bolsista de agosto de 2018 a dezembro de 2019. Em uma atividade desenvolvida em uma escola de Ensino Médio, foram apresentados aspectos históricos do uso da criptografia na segunda guerra mundial e os alunos tiveram a oportunidade de criar suas próprias mensagens criptografadas, utilizando matrizes como chaves criptográficas.

Dessa forma, este trabalho foi norteado a partir do seguinte ponto: como a criptografia pode ser inserida na matemática vista no ensino básico por meio do conteúdo de função afim? Com o intuito de responder essa pergunta, uma oficina é proposta objetivando o ensino e

aprendizagem de função afim por meio da criptografia.

A ideia da oficina é utilizar função afim para codificar e decodificar mensagens, entendendo o funcionamento e importância da criptografia de uma maneira simples, embora na prática, a criptografia utilizes técnicas e conceitos complexos. A escolha da oficina como ferramenta de ensino, deu-se a fim de colaborar com a desmistificação da matemática como uma matéria que apresenta dificuldade de assimilação, explorando uma possibilidade de ensino e aprendizagem diferente do ensino tradicional. A mesma foi desenvolvida em duas turmas, uma do 9º ano do Ensino Fundamental e outra do 3º ano do Ensino Médio e foi avaliada por meio da aplicação de questionários aos alunos participantes e os resultados obtidos serão exibidos e analisados ao decorrer deste trabalho.

No que diz respeito à organização deste trabalho, o mesmo se apresenta do seguinte modo: no Capítulo 2 serão apresentados conceitos, propriedades e definições sobre matrizes e funções, conteúdos necessários para o desenvolvimento e entendimento da oficina proposta bem como para o processo de codificação e decodificação de mensagens nos exemplos que serão exibidos. No Capítulo 3, os principais fatos históricos no desenvolvimento da criptografia assim como os conceitos abarcados pelo tema como chaves e métodos criptográficos são descritos. Para finalizar, o quarto capítulo apresenta a oficina proposta de uma maneira pormenorizada, os resultados dos questionários aplicados, evidenciando a percepção do aluno e também da aplicadora, sobre a oficina na prática.

Capítulo 2

Preliminares Matemáticas

Para compreensão acerca da ordenação deste trabalho e de como chegou-se as oficinas, neste capitulo haverá uma breve apresentação de todo o conteúdo matemático que foi aplicado. As definições, propriedades e teoremas estão de acordo com as obras de Iezzi e Murakami (1983), Iezzi e Hazzan (1983) e Anton e Busby (2008). As demonstrações dos teoremas serão omitidas, visto que as mesmas são dispensáveis para os objetivos deste trabalho. Para consultá-las, os autores nos quais este capítulo se baseia, podem ser consultados.

2.1 Matrizes

Matriz é uma tabela de elementos dispostas em linhas e colunas, o termo é utilizado para denotar qualquer arranjo retangular de números. As entradas ou elementos se encontram no cruzamento entre linhas e colunas. Uma matriz de m linhas e n colunas é dita de tamanho $m \times n$. Em geral, utilizamos letras maiúsculas para representar matrizes e minusculas para denotar entradas. A matriz A é representada abaixo, a fim de exemplificação.

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{am} & a_{m2} & \dots & a_{mn} \end{bmatrix}.$$

Quando queremos uma notação mais compacta, podem ser utilizadas as notações $A = [a_{ij}]_{m\times n}$ ou como $A = [a_{ij}]$. A primeira é utilizada quando é necessário informar o tamanho da matriz e a segunda, quando essa informação é irrelevante. Também utilizamos o símbolo $[A_{ij}]$ para a entrada na linha i e coluna j da matriz A.

Exemplo 2.1. *Considere a matriz A dada por:*

$$\mathbf{A} = \begin{bmatrix} 5 & 3 & 7 \\ 0 & 2 & 1 \\ 9 & 6 & 0 \end{bmatrix},$$

tem-se:

$$a_{11} = 5, a_{12} = 3, a_{13} = 7, a_{21} = 0, a_{22} = 2, a_{23} = 1, a_{31} = 9, a_{32} = 6, a_{33} = 0.$$

Exemplo 2.2. *Considere a matriz A dada por:*

$$\mathbf{A} = \begin{bmatrix} 5 & 3 & 7 \\ 0 & 2 & 1 \\ 9 & 6 & 0 \end{bmatrix},$$

tem-se:

$$a_{11} = 5, a_{12} = 3, a_{13} = 7, a_{21} = 0, a_{22} = 2, a_{23} = 1, a_{31} = 9, a_{32} = 6, a_{33} = 0.$$

2.1.1 Matrizes Especiais

- **Matriz Quadrada.** É uma matriz com m linhas e n colunas, quando $m = n$, é dita matriz quadrada. Nesse caso, as entradas $a_{11}, a_{12}, \ldots, a_{mm}$ forma a diagonal principal da matriz. A outra diagonal é denominada secundária.

  Uma propriedade interessante das matrizes quadradas é que, em sua diagonal principal $i = j$ e, em sua diagonal secundária, $i + j = n + 1$.

  Exemplo 2.3. *Considerando a matriz quadrada A, de ordem 2,*

  $$\mathbf{A} = \begin{bmatrix} 2 & 4 \\ 6 & 8 \end{bmatrix},$$

  tem-se $a_{11} = 2$ e $a_{22} = 8$ como elementos da diagonal principal e $a_{12} = 4$ e $a_{21} = 6$ como elementos da diagonal secundária.

- **Matriz Identidade.** A matriz quadrada cujas entradas da diagonal principal são iguais a 1 e $a_{ij} = 0$ para $i \neq j$ é denominada matriz identidade. Utiliza-se a notação I_n, onde n é a ordem da matriz.

  Exemplo 2.4. *As matrizes identidade de ordem 2 e 3 são dadas por*

  $$\mathbf{I_2} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ e } \mathbf{I_3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

2.1.2 Multiplicação de Matrizes

Se A é uma matriz $m \times n$ e **x** é um vetor-coluna $n \times 1$, então o produto $A\mathbf{x}$ é o vetor $m \times 1$ que resulta formando a combinação linear dos vetores-coluna de A tendo entradas de **x** como coeficientes. Mais precisamente, se os vetores-coluna de A são $a_1, a_2, \ldots, a_n$, então:

$$A\mathbf{x} = [a_1 \ a_2 \ \ldots \ a_n] \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = [x_1 a_1 + x_2 a_2 + \ldots + x_n a_n].$$

Exemplo 2.5. *Seja* $\mathbf{A} = \begin{bmatrix} 2 & 3 & -1 \\ 4 & 1 & 0 \end{bmatrix}$ *e* $\mathbf{B} = \begin{bmatrix} -3 \\ 1 \\ 2 \end{bmatrix}$. *Tem-se*

$$A.B = \begin{bmatrix} 2 & 3 & -1 \\ 4 & 1 & 0 \end{bmatrix} \begin{bmatrix} -3 \\ 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 2(-3) + 3 \cdot 1 + (-1) \cdot 2 \\ 4(-3) + 1 \cdot 1 + 0 \cdot 2 \end{bmatrix} = \begin{bmatrix} -5 \\ -11 \end{bmatrix}.$$

Teorema 1. *Se A é uma matriz $m \times n$, então as seguintes relações valem para quaisquer vetores-coluna u e v em R_n e qualquer escalar r:*

a. $A(ru) = r(Au)$.

b. $A(u + v) = Au + Av$.

2.1.3 Determinante

O determinante da matriz quadrada M é o número obtido operando com os elementos de M da seguinte forma:

1. Se M tem ordem 1, então **det M** é o único elemento de M.

   $$M = [a_{11}] \Rightarrow \textbf{det M} = a_{11}.$$

   No que se refere à notação, **det M** também poderá ser indicado por $|M|$, ou seja, colocando uma barra vertical de cada lado de M.

2. Se M é de ordem 2, **det M** é dado pela soma do produto dos elementos da diagonal principal e o oposto do produto dos elementos da diagonal secundária, conforme segue.

   $$\textbf{det M} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}.a_{22} - a_{12}.a_{21}.$$

3. Se M é de ordem $n = 3$, isto é, $\mathbf{M} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$, definimos

$$\textbf{det M} = a_{11}\cdot a_{22}\cdot a_{33} + a_{12}\cdot a_{23}\cdot a_{31} + a_{13}\cdot a_{21}\cdot a_{32} - a_{13}\cdot a_{22}\cdot a_{31} - a_{11}\cdot a_{23}\cdot a_{33} - a_{12}\cdot a_{21}\cdot a_{33}.$$

Para o caso em que a ordem da matriz é 3, o cálculo do determinante é facilitado pela regra de Sarrus, que funciona da seguinte forma:

(a) Repete-se ao lado da matriz, as duas primeiras colunas.

(b) Os termos obtidos multiplicando-se os elementos da diagonal principal e de suas diagonais paralelas que contêm três elementos são precedidos pelo sinal $+$.

(c) Os termos obtidos multiplicando-se todos os elementos da diagonal secundária e de suas diagonais paralelas que contêm três elementos são precedidos pelo sinal $-$.

(d) Soma-se todos os resultados obtidos.

Exemplo 2.6. *Calcule o determinante da matriz* $\mathbf{M} = \begin{bmatrix} 3 & 4 & 3 \\ 7 & 5 & -3 \\ 5 & 2 & 1 \end{bmatrix}$.

Pela regra de Sarrus, tem-se

$$\textbf{\textit{det M}} = \begin{vmatrix} 3 & 4 & 3 \\ 7 & 5 & -3 \\ 5 & 2 & 1 \end{vmatrix} \begin{matrix} 3 & 4 \\ 7 & 5 \\ 5 & 2 \end{matrix} = [15 + (-60) + 28] - [28 + (-18) + 50] = -77.$$

É possível calcular o determinante para matrizes de ordens superiores, porém, a fim de atingir os objetivos deste trabalho, o cálculo de determinante até a ordem 3 é suficiente. Para um maior aprofundamento, indica-se Iezzi e Hazzan (p. 75, 1983).

2.1.4 Sistemas Lineares

Uma coleção finita de equações lineares é denominada um sistema linear. As variáveis de um sistema linear são denominadas incógnitas.

Um sistema linear geral de m equações e n incógnitas $x_1, x_2, \ldots, x_n$ é exibido a seguir, a título de exemplificação.

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = b_n. \end{cases}$$

Uma solução de um sistema linear nas incógnitas $x_1, x_2, \ldots, x_n$ é uma sequência de n números $s_1, s_2, \ldots, s_n$ tais que, sendo substituídos nos lugares de $x_1, x_2, \ldots, x_n$, respectivamente, tornam verdadeira cada equação do sistema.

Exemplo 2.7. *Considere o seguinte sistema nas incógnitas x e y.*

$$\begin{cases} x + y = 7 \\ 2x + y = 11, \end{cases}$$

aqui, $x = 4$ e $y = 3$ é solução desse sistema, dado que satisfaz ambas as equações, ou seja, $S = \{(4, 3)\}$.

2.1.5 Matriz Inversa

Cada número não-nulo a tem um recíproco ou inverso multiplicativo a^{-1}, onde $a^{-1} = \frac{1}{a}$. Conforme as propriedades conhecidas dos números reais, tem-se $a.a^{-1} = a^{-1}.a = 1$.

Se A é uma matriz quadrada e se existe uma matriz B de mesmo tamanho que A tal que $AB = BA = I$, dizemos que A é invertível ou não-singular e que B é uma inversa de A. Destaca-se que I se refere à matriz identidade já apresentada anteriormente. Se não existir uma matriz B com essa propriedade, dizemos que A é não-invertível ou singular.

Exemplo 2.8. *Considere as matrizes A e B de modo que*

$$\mathbf{A} = \begin{bmatrix} 1 & 3 \\ 5 & 7 \end{bmatrix} \text{ e } \mathbf{B} = \begin{bmatrix} -\frac{7}{8} & \frac{3}{8} \\ \frac{5}{8} & -\frac{1}{8} \end{bmatrix}.$$

Tem-se:

$$\mathbf{AB} = \begin{bmatrix} 1 & 3 \\ 5 & 7 \end{bmatrix} \begin{bmatrix} -\frac{7}{8} & \frac{3}{8} \\ \frac{5}{8} & -\frac{1}{8} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

e

$$\mathbf{BA} = \begin{bmatrix} -\frac{7}{8} & \frac{3}{8} \\ \frac{5}{8} & -\frac{1}{8} \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 5 & 7 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I.$$

Assim, A e B são invertíveis e cada uma é inversa da outra.

Propriedade 2.9. *Se A é uma matriz invertível e se B e C são ambas inversas de A então $B = C$, ou seja, uma matriz invertível tem uma única inversa.*

Teorema 2. *A matriz A de tamanho 2×2 dada por*

$$\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

é invertível se e somente se, $ad - bc \neq 0$ e, nesse caso, a inversa é dada pela fórmula:

$$A^{-1} = \frac{1}{(ad - bc)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}. \tag{2.1}$$

Teorema 3. *Se A e B são matrizes invertíveis de mesmo tamanho, então AB é invertível e*

$$(AB)^{-1} = B^{-1}A^{-1},$$

que é o inverso do produto e o produto de inversas na ordem oposta.

Teorema 4. *Se A é invertível, k um escalar e n é um inteiro não-negativo, então:*

(a)A^{-1} é invertível;

(b)A^n é invertível e $(A^n)^{-1} = A^{-n} = (A^{-1})^n$;

(c) kA é invertível para qualquer escalar não-nulo k e $(kA)^{-1} = k^{-1}A^{-1} = \frac{1}{k}A^{-1}$.

2.2 Relações

Dados dois conjuntos A e B, não vazios, chama-se relação de A em B um conjunto formado por pares ordenados (a, b) em que $a \in A$ e $b \in B$.

Exemplo 2.10. *Sejam $A = \{1, 2, 3, 4\}$ e $B = \{a, b, c\}$. Alguns exemplos de relações de A em B são dados por:*

$$R_1 = \{1, a\}, R_2 = \{(1, a), (2, b), (3, c), (4, c)\} \text{ e } R_3 = \{(1, a), (2, b), (3, a), (4, c)\}.$$

2.2.1 Relações Inversas

Cada relação R de A para B tem uma relação inversa R^{-1} de B para A que é definida por:

$$R^{-1} = \{(y, x) \in B \times A | (x, y) \in R\}.$$

Como R^{-1} é subconjunto de $B \times A$, então R^{-1} é uma relação de B em A à qual é chamada de relação inversa de R. De modo geral,

$$(y, x) \in R^{-1} \Leftrightarrow (x, y) \in R.$$

Exemplo 2.11. *Sejam $A = \{2, 4\}$ e $B = \{a, b\}$ e a relação dada por $R = \{(2, a), (4, b)\}$ de A em B. Nesse caso, a relação inversa de R é $R^{-1} = \{(a, 2), (b, 4)\}$.*

2.2.2 Domínio e Imagem de uma Relação

Seja R uma relação de A em B, isto é, seja R um subconjunto de $A \times B$. O domínio D da relação R é o conjunto de todos os primeiros elementos dos pares ordenados em R.

$$x \in D \Leftrightarrow \exists y, \text{ com } y \in B \text{ , tal que } (x, y) \in R.$$

A imagem de R é o conjunto Im de todos os segundos elementos dos pares ordenados pertencentes a R.

$$y \in Im \Leftrightarrow \exists x, \text{ com } x \in A, \text{ tal que } (x, y) \in R.$$

Exemplo 2.12. *Dados os conjuntos* $A = \{2, 5, 7, 11, 13\}$ *e* $B = \{4, 10, 14, 22, 26\}$ *e a relação* $R = \{(x, y) \in A \times B | y = 2x\}$*, determine* $D(R)$ *e* $Im(R)$*. Escrevendo os elementos da relação, tem-se:*

$$R = \{(2, 4), (5, 10), (7, 14), (11, 22), (13, 26)\}.$$

Assim,

$$D(R) = \{2, 5, 7, 11, 13\} \text{ e } Im(R) = \{4, 10, 14, 22, 26\}.$$

2.3 Funções

Dados dois conjuntos A e B contidos em $\mathbb{R}$, não vazios, uma relação f de A em B recebe o nome de aplicação de A em B ou função definida em A com imagens em B se, e somente se, para todo $x \in A$ existe um só $y \in B$ tal que $(x, y) \in f$, isto é,

$$f \text{ é função de } A \text{ em } B \Leftrightarrow \forall\, x \in A,\ \exists |\ y\ \in B \text{ tal que } (x, y) \in f,$$

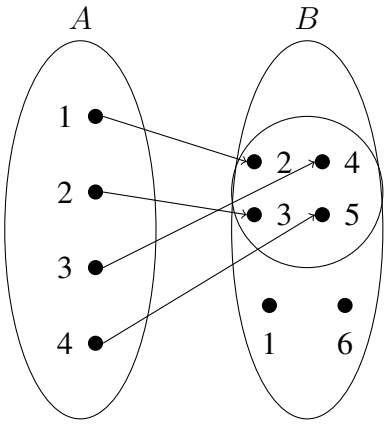
sendo A chamado de domínio de f, indicado por $D(f)$, B é o contra domínio de f, representado por $CD(f)$ e o conjunto de B, determinado por f, é chamado de imagem de f e denotado por $Im(f)$.

Exemplo 2.13. *Seja* $A = \{1, 3, 5, 9\}$ *e* $R_1 = \{(1, 3), (3, 5), (5, 9), (9, 1)\}$*. Nesse caso,* R_1 *é uma função, pois cada* $a \in A$ *aparece como o primeiro elemento em um, e somente um, par ordenado em* R_1*.*

Exemplo 2.14. *Sejam* $A = \{1, 2, 3, 4\}, B = \{1, 2, 3, 4, 5, 6\}$ *e a função* $f : A \to B$*, onde* $f(x) = x + 1$*. O conjunto* A *é o domínio,* B *é o contradomínio e os elementos de* B *que estão relacionados a elementos em* A *formam o conjunto denominado imagem de* f*. A Figura 2.1 ilustra* f *por meio de diagrama.*

$$\begin{aligned} f &= \{(1, 2), (2, 3), (3, 4), (4, 5)\}, \\ D(f) &= \{1, 2, 3, 4\}, \\ CD(f) &= \{1, 2, 3, 4, 5, 6\}, \\ Im(f) &= \{2, 3, 4, 5\}. \end{aligned}$$

Figura 2.1: Representação de f por meio de diagrama.



2.3.1 Funções bijetoras

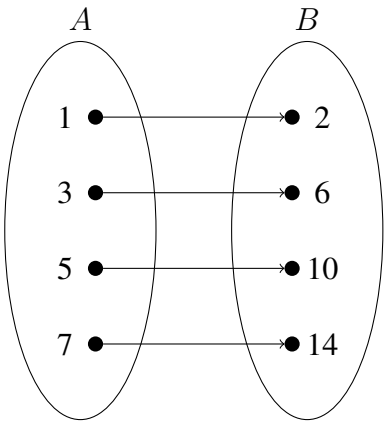
A função $f : A \to B$ é bijetora se, e somente se, f é sobrejetora e injetora.

- Função Injetora

  Uma função $f : A \to B$ é injetora se, e somente se, quaisquer que sejam x_1 e x_2 pertencentes a A de modo que $x_1 \neq x_2$ então $f(x_1) \neq f(x_2)$.

  Exemplo 2.15. *A função $f : A \to B$, $A = \{1, 3, 5, 7\}$, tal que $f(x) = 2x$ é injetora, visto que para quaisquer dois elementos distintos de A tem-se imagens distintas.*

Figura 2.2: Função injetora f

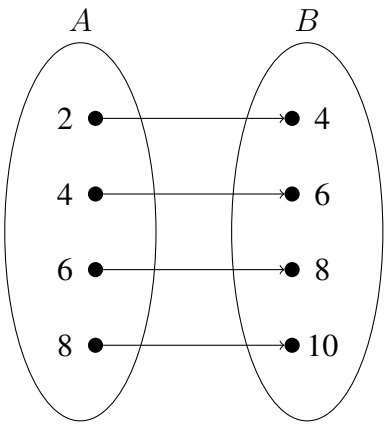


- Função Sobrejetora

  Uma função $g : A \to B$ é sobrejetora se, e somente se, para todo y pertencente a B existe um elemento x pertencente a A tal que, $g(x) = y$. Nesse caso, a imagem e contradomínio de funções sobrejetoras são iguais.

  Exemplo 2.16. *A função $g : A \to B$, em que $A = \{2, 4, 6, 8\}$, definida por $g(x) = x + 2$, é sobrejetora pois $Im(g) = CD(g)$.*

Figura 2.3: Função sobrejetora g

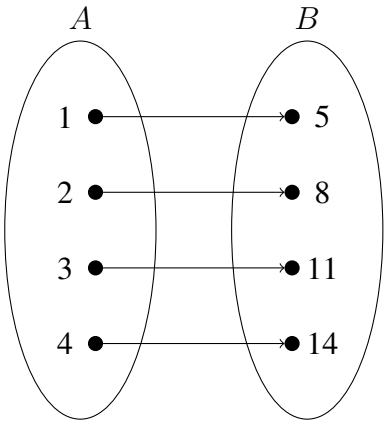


Portanto, uma função $f : A \to B$ é bijetora se, e somente se, para qualquer elemento y pertencente a B existe um único elemento x pertencente a A tal que $f(x) = y$.

$$f \text{ é bijetora} \Leftrightarrow \forall\, y, y \in B,\ \exists |\ x \in A \text{ tal que } f(x) = y.$$

Exemplo 2.17. *Sejam os conjuntos* $A = \{1, 2, 3, 4\}$ *e* $B = \{5, 8, 11, 14\}$ *e a função* f *definida por* $f(x) = 3x + 2$. f *é ilustrada pela Figura 2.4.*

Figura 2.4: Função f



Tem-se que f *é bijetora, de modo que* $D(f) = \{1, 2, 3, 4\}$, $CD(f) = \{5, 8, 11, 14\}$ *e* $Im(f) = \{5, 8, 11, 14\}$.

2.3.2 Função Inversa

Seja f uma função biunívoca de A em B. Nesse caso, a função inversa de f, de B em A, é indicada por f^{-1}, isto é, $f^{-1} : B \to A$.

Observação 2.3.2.1. *Sendo* f^{-1} *a função inversa de* f*, temos as seguintes propriedades:*

(a) $D(f^{-1}) = B = Im(f)$;

(b) $Im(f^{-1}) = A = D(f)$;

(c) $(b, a) \in f^{-1} \Leftrightarrow (a, b) \in f$;

(d) o gráfico de f^{-1} *é simétrico do gráfico de* f *em relação á reta* $f(x) = x$.

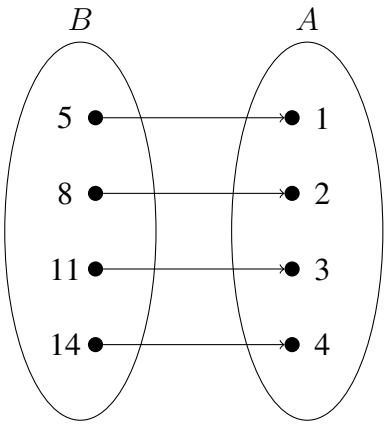
Dada a função inversível $f : A \to B$, definida pela lei $y = f(x)$, procede-se da seguinte maneira para obter-se a lei que define f^{-1}:

1. A expressão $y = f(x)$ é transformada algebricamente de maneira que x seja expresso em função de y:
$$x = f^{-1}(y).$$
2. Troca-se x por y e vice-versa, obtendo a lei $y = f^{-1}(x)$.

Exemplo 2.18. *Seja* $f : \mathbb{R} \to \mathbb{R}$, *dada por* $f(x) = y = 2x + 5$. *A fim de obter a inversa de* f, *troca-se* x *por* y *e vice-versa,*
$$x = 2y + 5.$$
Isolando y, *obtém-se* $y = \frac{x-5}{2}$. *Portanto,* $f^{-1}(x) = \frac{x-5}{2}$.

Exemplo 2.19. *A Figura 2.4 trata-se de um diagrama de uma função bijetora, logo admite uma função inversa* f^{-1}. *Invertendo os elementos correspondentes, obtém o diagrama da Figura 2.5.*

Figura 2.5: Função inversa $f^{-1} : B \to A$



Capítulo 3

História e Conceitos

Menezes (2003, p. 15) diz que “[...] a ameaça de interceptação de mensagens por espiões motivou não apenas o desenvolvimento de métodos para torná-las ininteligíveis, mas também o aparecimento de técnicas para ocultá-las”. A ação de criptografar funciona como um sistema de algoritmos embaralhando o conteúdo, possuindo as fases de codificação e decodificação. Codificar é converter os componentes de uma mensagem em símbolos secretos. O processo também é chamado de encriptação ou ciframento que consiste em transformar certa informação usando um algoritmo. Posteriormente, o remetente recebe e o decodifica. A seguir serão abordados alguns dos métodos utilizados ao longo do tempo, e respectivamente, suas melhorias e seu papel decisivo nas guerras.

Sobre seu início Galdino (2014, p. 5) destaca ”Uma das primeiras informações data de Heródoto no ano de 480 a.C., o qual escreveu sobre os conflitos entre Grécia e a Pérsia”. As principais ocorrências em seu desenvolvimento e concretização serão apresentadas adiante.

3.1 História

Com a necessidade de ocultar e/ou direcionar uma certa informação, nasceu o que hoje é chamado de criptografia, anterior à segurança de bancos e aplicativos; Fundamental em meio as guerras, manter a privacidade foi primordial para garantir estratégias, vantagens e segurança de vidas, tesouros e terras.

O primeiro sistema criptografado usado para fins militares, datada em 487 a.C., é a Cítala, exibida na Figura 3.1. Para muitos pesquisadores, o sistema não passa de mito, para outros, ele era utilizado pelos soldados espartanos. Para seu uso, enrolava-se uma tira de tecido sobre um bastão e, sobre tal tira, escrevia-se um recado. Terminando-o, desenrolava-se a tira e a enviava como um cinto por um mensageiro. No destino, ela precisava ser enrolada em um bastão com a mesma largura do original, como resultado, era revelada a mensagem.

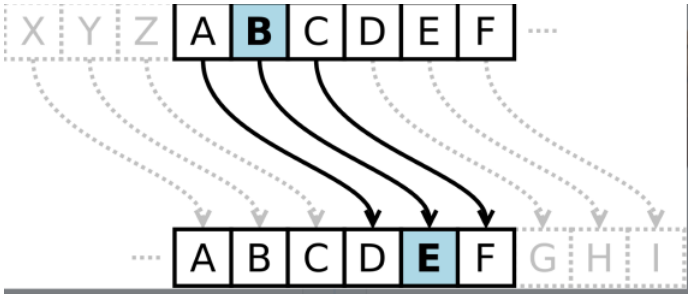
Figura 3.1: Cítala espartana usada para envio de mensagens

Fonte: MEDEIROS (2015)

O imperador Júlio César em aproximadamente 50 a.C., usou um método para confabular com os seus generais, esse consistia na troca de todas as letras dos seus comunicados, assim mesmo que interceptados pelos inimigos iriam parecer sem significado. A técnica consistia em transpor as letras do alfabeto que eram substituídas por outras que estavam localizadas em posições à frente desse alfabeto. A Figura 3.2 é um exemplo dessa transposição.

A substituição de letras com códigos nesse caso é mais falha, toda língua tem um padrão, quando se percebe a frequência de uma determinada letra fica fácil decifrar as outras, por exemplo, no português o 'A' é a letra de maior repetição, comparando a um texto que estivesse codificado tendo recorrência do 'D', saberíamos que o deslocamento foi de três casas. Mesmo assim essa cifra foi usada por centenas de anos pelos militares depois de César.

Figura 3.2: Cifra de César um código de troca



Fonte: MEDEIROS (2015)

Cada idioma tem uma espécie de impressão digital, para que essa não fosse usada com a finalidade de decodificação por eventuais invasores, foi preciso equiparar a constância que as letras iriam aparecer. A Cifra de Vigenère consiste na utilização da cifra polialfabética, sua encriptação conta com diferentes valores de deslocamento, nessa pratica diferente da cifra de César é usado uma palavra como chave. O Quadrado de Vigenère como mostra a Figura 3.3, tem o alfabeto escrito 26 vezes em diferentes linhas, por esse motivo durante muito tempo ficou conhecida como indecifrável, demorando mais de 300 anos para ser quebrada.

Figura 3.3: Cifra de Vigenère e suas substituições polialfabéticas

	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: MEDEIROS (2015)

Na segunda guerra, foi desenvolvido e memorizado um código que diferente dos anteriores era uma linguagem. A ideia partiu de Philip Johnston que era um veterano da primeira guerra mundial. Em 1942, Johnston sugeriu que os navajos (povo indígena da América do Norte) e outras tribos pudessem ser muito úteis para manter o sigilo das comunicações. Os fuzileiros recrutaram 29 navajos para em duas semanas criarem um código em seu idioma. Eles fizeram uma palavra navajo para cada letra do alfabeto inglês. Como precisavam memorizar usaram coisas familiares como nomes de animais. Este foi o único código oral de guerra que não foi decifrado pelo inimigo. A Figura 3.4 exibe os navajos em operação na guerra.

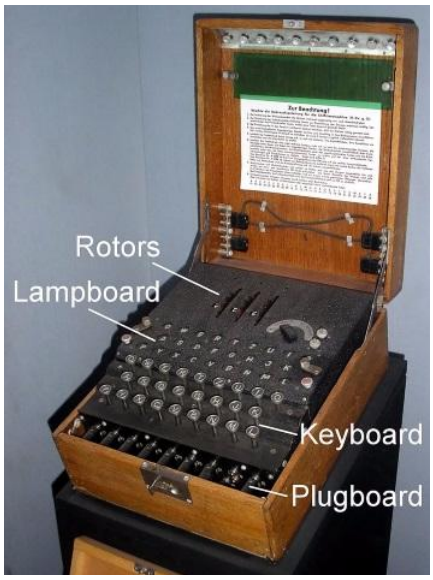
Figura 3.4: Navajos em operação

Fonte: FERNANDES (2012)

A máquina Enigma, feita pelos alemães durante a segunda guerra mundial, foi criada pelo engenheiro alemão Arthur Scherbius no fim da primeira guerra, mas apenas em 1920

o governo usou para fins militares. A criptografia da enigma era simples, mas sua engrenagem gerava milhares de possibilidades, o que tornava humanamente impossível decifrá-la. As possibilidades numéricas chegavam a 6 sextilhões de códigos. A máquina tinha 5 rotores Figura 3.5, mas apenas três eram selecionados, ainda havia várias posições possíveis nos vinte e seis anéis de cada rotor. O operador também precisava saber a posição inicial de uma sequência de três posições, a máquina possibilitava que a Alemanha trocasse informações sobre ataques e localizações.

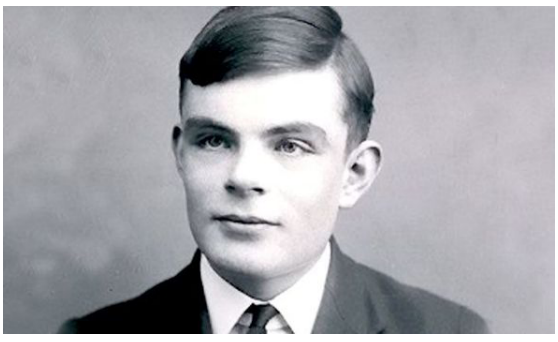
Figura 3.5: Máquina Enigma usada para criptografar e descriptografar códigos de guerra



Fonte: MEDEIROS (2015)

Enigma reinou até que a Bombe fosse criada, sem ela talvez os nazistas tivessem vencido a guerra. A Figura 3.6 mostra Alan Mathison Turing (1912-1954), matemático e inventor da máquina, foi acusado de indecência e submetido à castração química por ser homossexual. Aos 42 anos se suicidou comendo uma maça envenenada, em 2003 a rainha Elizabeth II concedeu a Turing um perdão real póstumo, horando assim seus feitos.

Figura 3.6: Alan Turing matemático e inventor da Bombe



Fonte: MOCHETTI (2016)

Desde jovem ele sempre teve um grande interesse por números, se formou em 1934 pela King's College em Cambridge. Turing junto com um grupo de matemáticos foi convocado em 1939 para trabalhar no Government Code and Cypher School (GC&CS) em Bletchley Park no Reino Unido com o intuito de romper os códigos da enigma. Enquanto a equipe se concentrava em quebrar os códigos diariamente, ele trabalhava em um equipamento que segundo ele decifraria a enigma a todo momento. Assim, nasce a Bombe.

Essa máquina indicada na Figura 3.7 capturava e identificava quando o sinal estava protegido pelo mesmo da enigma, para depois usar um padrão até que se chegava a mensagem verdadeira. Uma curiosidade sobre a máquina é que apesar do fato de que naquele momento eles estavam um passo a frente da Alemanha, era preciso escolher quais ataques iriam impedir, pois não podiam correr o risco de serem descobertos pelos alemães. Dessa maneira, foi desenvolvido um sistema que os ajudava a determinar quando agir, por meio de uma análise estatística, que os fizeram ganhar a guerra.

Figura 3.7: Máquina Bombe auxiliava na decodificação de mensagens secretas alemãs

Fonte: MEDEIROS (2015)

Após o fim da segunda guerra, a equipe não pode se encontrar e a papelada de toda a operação foi destruída. O trabalho de Turing foi uma das inspirações do que hoje é chamado de computador.

3.2 Métodos Criptográficos

Os métodos que permitem cifrar mensagens, chamados de algoritmos, podem ser classificados como: transposições, substituições ou ciframentos compostos. A transposição é gerada com a reorganização das letras e pode ser feita de inúmeras maneiras. O algoritmo de substituição poderá ser monoalfabético (onde cada letra é substituída sempre pela sua correspondente, independente de quantas vezes apareça) e polialfabético (a mesma letra no texto pode ser trocada por variações), já o ciframento composto usa transposição e substituição, sendo este um padrão usado em dados computacionais, como é o caso do DES (Data Encryption Standard).

Tais técnicas criptográficas são possíveis junto a uma chave que permite a encriptação de dados, podendo esta ser simétrica e assimétrica.

Além de serem mostrados alguns dos métodos criptográficos e como se relacionam com suas respectivas chaves nesta seção, os exemplos que serão apresentados são sugeridos para desenvolvimento no Ensino Básico, utilizando como preliminares, os conteúdos abordados no Capítulo 2.

3.2.1 Chaves criptográficas

Uma chave é um objeto de metal que possibilita abrir ou fechar uma porta ou cadeado. Imagine que fosse preciso enviar um baú - com algo dentro que somente o destinatário pudesse ter acesso - e esse trancado por um cadeado que possuísse apenas uma chave. Para isso seria necessário enviar o baú e um mensageiro com a chave do mesmo, porém essa chave poderia ser interceptada. Em uma tentativa de evitar que isso aconteça, o baú poderia ser enviado com um cadeado. Chegando no destinatário, sem ter como abrir o baú, colocaria outro cadeado e o reenviaria ao remetente. Este tiraria o seu cadeado e, novamente, despacharia o baú. Assim, quando chegasse no seu destino, a chave estaria com o recebedor original. Essa ideia é análoga à função da chave no contexto de criptografia, não havendo um utensílio literalmente. Na rede de dados, essa chave será assimétrica ou simétrica.

A assimétrica utiliza-se duas chaves diferentes, uma pública e outra privada, nesta somente a primeira codifica e apenas a segunda decodifica. Acerca do processo, Oliveira (2012, p.3) comenta "[...] as chaves não são apenas senhas, mas arquivos digitais mais complexos (que eventualmente até estão associados a uma senha)". A chave pública pode ser conhecida por diversos usuários, já a privada é de uso exclusivo. Este sistema é utilizado em aplicativos de troca de mensagens.

A vantagem do uso desse processo é que o interceptor teria acesso a chave pública, afinal a mesma é criada visando a possibilidade de que qualquer um possa ter, mas a chave privada é de uso particular do receptor e em nenhum momento precisará ser compartilhada.

Na simétrica, a chave é usada junto com o algoritmo de ciframento que envia uma mensagem cifrada e esta poderá ser decifrada caso o receptor saiba o algoritmo de deciframento correspondente e tenha a mesma chave.

O benefício de usar esse método é a praticidade, sendo possível criptografar uma quantidade maior de dados e em menos tempo. Sua desvantagem é que se algum interceptor conseguir ter acesso a uma das chaves, conseguirá entender a mensagem. Um exemplo de seu uso é no envio de e-mails.

3.2.2 Criptografia RSA

Houve uma evolução gradual pela insuficiência de segurança, até porque as cifras que eram usadas não teriam êxito no contexto tecnológico atual. A criptografia moderna não utiliza as letras na sua codificação, mas sim, números binários dentro de computadores, utilizada principalmente em transações bancárias, senhas de e-mails e redes sociais.

Com os avanços dos computadores e internet, foi preciso reforçar a segurança para conseguir se comunicar. Reis (1989, p.8) cita que "com o aparecimento do computador em cena, surgiram novas aplicações para a criptografia como transferência automática de fundos, [...] proteção de dados em arquivos, etc". Nesse contexto, diversas empresas passaram a investir em ferramentas tecnológicas de segurança utilizando criptografia. Um método muito utilizado por essas empresas é a criptografia RSA.

Esse método é composto por diferentes algoritmos assimétricos resultando em uma encriptação mais segura. Seu funcionamento é baseado em princípios matemáticos, utilizando números primos. "A garantia de segurança está relacionada com a dificuldade na fatoração do produto de dois números primos relativamente grandes" (GALDINO, 2014, p. 61). Por esse motivo a decriptação torna-se inviável até para uma máquina.

Utilizando números primos, o método RSA cria uma chave de codificação. Como os números utilizados são muito grandes, mesmo quem conhece a chave pública não tem acesso a eles, algo que é necessário para decodificar.

No contexto do Ensino Básico, algumas atividades podem ser realizadas usando a criptografia. Acerca dessas, é importante destacar que é possível introduzir o tema junto a conteúdos da base curricular como matrizes e funções. A seguir, serão apresentados alguns exemplos que conectam tais conteúdos à criptografia, utilizando cifras de substituição e de transposição.

3.2.3 Cifra de Hill

A cifra de Hill é um algoritmo de substituição fundamentado na álgebra linear, criada por Lester Hill em 1929.

Pereira et al. (2012, p.4) diz que "o processo de cifras de Hill consiste em transformar pares sucessivos de texto em texto cifrado, através da escolha de uma matriz A de ordem 2×2 e uma tabela com valores numéricos para todas as letras do alfabeto". Outras ordens para A podem ser utilizadas, desde que a matriz seja inversível.

Utilizando a notação de matrizes para representar este algoritmo, tem-se:

$$C = AM, \tag{3.1}$$

onde *M* é a matriz com as letras da mensagem original, com n possibilidades $(m_1, m_2, ..., m_n)$, *A* é a matriz chave de ciframento e *C*, a mensagem codificada $(c_1, c_2, ..., c_n)$, isto é,

$$\mathbf{C} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}, \ \mathbf{A} = \begin{bmatrix} a_{11} & \dots & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \text{ e } \mathbf{M} = \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{bmatrix}.$$

Na forma de sistemas lineares, tem-se

$$\begin{cases} c_1 = a_{11}m_1 + \ldots + a_{1n}m_n \\ c_2 = a_{21}m_1 + \ldots + a_{2n}m_n \\ \qquad\qquad \ldots \\ c_n = a_{n1}m_1 + \ldots + a_{nn}m_n \end{cases}.$$

Para decifrar uma mensagem, isto é, obter M, sendo A inversível, faz-se $M = A^{-1}C$.

Exemplo 3.1. *O primeiro passo na utilização do método de Hill é ter uma correspondência de letras e números como a exibida pela Tabela 3.1.*

Tabela 3.1: Conversão de letras em números

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

Acerca da chave, é preciso que ela seja uma matriz inversível. Neste exemplo, a matriz abaixo será a chave.

$$\begin{bmatrix} 1 & 2 \\ 0 & 4 \end{bmatrix}.$$

Aqui, a mensagem SIGILO será cifrada.
Colocando cada número correspondente a sua letra, com a utilização da Tabela 3.1, tem-se:

$$19 \ \ 9 \ \ 7 \ \ 9 \ \ 12 \ \ 15.$$

Fazendo a multiplicação de matrizes, como na Equação 3.1, sendo M a matriz referente a cada um dos blocos SI, GI e LO, isto é, $\begin{bmatrix} 19 \\ 9 \end{bmatrix}$, $\begin{bmatrix} 7 \\ 9 \end{bmatrix}$ *e* $\begin{bmatrix} 12 \\ 15 \end{bmatrix}$, *respectivamente, obtém-se:*

$$\mathbf{C} = \begin{bmatrix} 1 & 2 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} 19 \\ 9 \end{bmatrix} = \begin{bmatrix} 1 \cdot 19 + 2 \cdot 9 \\ 0 \cdot 19 + 4 \cdot 9 \end{bmatrix} = \begin{bmatrix} 37 \\ 36 \end{bmatrix},$$

$$\mathbf{C} = \begin{bmatrix} 1 & 2 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} 7 \\ 9 \end{bmatrix} = \begin{bmatrix} 1 \cdot 7 + 2 \cdot 9 \\ 0 \cdot 19 + 4 \cdot 9 \end{bmatrix} = \begin{bmatrix} 25 \\ 36 \end{bmatrix},$$

$$\mathbf{C} = \begin{bmatrix} 1 & 2 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} 12 \\ 15 \end{bmatrix} = \begin{bmatrix} 1 \cdot 12 + 2 \cdot 15 \\ 0 \cdot 12 + 4 \cdot 15 \end{bmatrix} = \begin{bmatrix} 42 \\ 60 \end{bmatrix}.$$

Logo, a mensagem cifrada, conforme tabela de correspondência numérica e a chave utilizada, é dada por

$$37\ 36\ \ 25\ 36\ \ 42\ 60.$$

Caso seja necessário descobrir a mensagem original, a partir da cifrada, a equação $M = A^{-1}C$ *deve ser utilizada. Para isso, faz-se necessária a obtenção de* A^{-1}*, que pode ser obtida conforme a Equação 2.1, ou seja,*

$$A^{-1} = \frac{1}{1 \cdot 4 - 2 \cdot 0} \begin{bmatrix} 4 & -2 \\ -0 & 1 \end{bmatrix} = \frac{1}{4} \begin{bmatrix} 4 & -2 \\ -0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{1}{4} \end{bmatrix}.$$

Com todos os dados necessários já identificados, finaliza-se aplicando a expressão:

$$\mathbf{M} = \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{1}{4} \end{bmatrix} \begin{bmatrix} 37 \\ 36 \end{bmatrix} = \begin{bmatrix} 1 \cdot 37 + (-\frac{1}{2}) \cdot 36 \\ 0 \cdot 37 + \frac{1}{4} \cdot 36 \end{bmatrix} = \begin{bmatrix} 19 \\ 9 \end{bmatrix},$$

$$\mathbf{M} = \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{1}{4} \end{bmatrix} \begin{bmatrix} 25 \\ 36 \end{bmatrix} = \begin{bmatrix} 1 \cdot 25 + (-\frac{1}{2}) \cdot 366 \\ 0 \cdot 37 + \frac{1}{4} \cdot 36 \end{bmatrix} = \begin{bmatrix} 7 \\ 9 \end{bmatrix},$$

$$\mathbf{M} = \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{1}{4} \end{bmatrix} \begin{bmatrix} 42 \\ 60 \end{bmatrix} = \begin{bmatrix} 1 \cdot 42 + (-\frac{1}{2}) \cdot 60 \\ 0 \cdot 42 + \frac{1}{4} \cdot 60 \end{bmatrix} = \begin{bmatrix} 12 \\ 15 \end{bmatrix}.$$

É possível adaptar a cifra de Hill, utilizando funções inversíveis ao invés de matrizes quadradas.

Exemplo 3.2. *Um grupo de soldados recebe um bilhete de seu general com a mensagem* $78\ \ 358\ \ 58\ \ 62\ \ 2\ \ 74\ \ 2\ \ 22\ \ 358\ \ 18\ \ 54\ \ 78\ \ 18$ *e a chave* $f(x) = 4x - 2$.

A mensagem possui como chave uma função afim. Para decifrá-la, deve-se encontrarar a inversa de f*. Para isto, são necessários três passos simples:*

- *Faz-se* $y = f(x)$ *na expressão de* f*:*

$$y = 4x - 2.$$

- *Troca-se* x *por* y *e vice-versa, obtendo:*

$$x = 4y - 2.$$

- *Isola-se y, obtendo:*

$$y = \frac{x+2}{4}.$$

Obtendo $f^{-1}(x) = \frac{x+2}{4}$, basta substituir x por cada valor numérico que compõe a mensagem.

$$\begin{aligned}
f^{-1}(78) &= \tfrac{78+2}{4} = 20,\\
f^{-1}(358) &= \tfrac{358+2}{4} = 18,\\
f^{-1}(58) &= \tfrac{58+2}{4} = 15,\\
f^{-1}(62) &= \tfrac{62+2}{4} = 16,\\
f^{-1}(2) &= \tfrac{2+2}{4} = 1,\\
f^{-1}(74) &= \tfrac{74+2}{4} = 19,\\
f^{-1}(2) &= \tfrac{2+2}{4} = 1,\\
f^{-1}(22) &= \tfrac{22+2}{4} = 6,\\
f^{-1}(358) &= \tfrac{358+2}{4} = 18,\\
f^{-1}(18) &= \tfrac{18+2}{4} = 5,\\
f^{-1}(54) &= \tfrac{54+2}{4} = 14,\\
f^{-1}(78) &= \tfrac{78+2}{4} = 20,\\
f^{-1}(18) &= \tfrac{18+2}{4} = 5.
\end{aligned}$$

Portanto, a mensagem decifrada é dada por

$$20\ \ 18\ \ 15\ \ 16\ \ 1\ \ 19\ \ 1\ \ 6\ \ 18\ \ 5\ \ 14\ \ 20\ \ 5.$$

Com o amparo da Tabela 3.1, os soldados obtiveram a seguinte mensagem "TROPAS A FRENTE".

Exemplo 3.3. *Suponha agora, que esse mesmo pelotão vai responder ao seu general. No comunicado, estará escrito o seguinte "ATACAREMOS PELA MANHA".*

Para evitar que a mensagem seja interceptada por tropas inimigas, é necessário que a mensagem seja encriptada, iniciando o processo com o auxílio da Tabela 3.1, obtendo a seguinte correspondência

$$1\ \ 20\ \ 1\ \ 3\ \ 1\ \ 18\ \ 5\ \ 13\ \ 15\ \ 19\ \ 16\ \ 5\ \ 12\ \ 1\ \ 13\ \ 1\ \ 14\ \ 8\ \ 1.$$

Os soldados utilizaram, como chave, a função $f(x) = 2^x - 12$.

$$\begin{aligned}
f(1) &= 2^1 - 12 = -10,\\
f(20) &= 2^{20} - 12 = 1048564,\\
f(1) &= 2^1 - 12 = -10,\\
f(3) &= 2^3 - 12 = -4,\\
f(1) &= 2^1 - 12 = -10,\\
f(18) &= 2^{18} - 12 = 262132,\\
f(5) &= 2^5 - 12 = 20,\\
f(13) &= 2^{13} - 12 = 8180.
\end{aligned}$$

$$\begin{aligned}
f(15) &= 2^{15} - 12 = 32756,\\
f(19) &= 2^{19} - 12 = 524276,\\
f(16) &= 2^{16} - 12 = 65524,\\
f(5) &= 2^{5} - 12 = 20,\\
f(12) &= 2^{12} - 12 = 4084,\\
f(1) &= 2^{1} - 12 = -10,\\
f(13) &= 2^{13} - 12 = 8180,\\
f(1) &= 2^{1} - 12 = -10,\\
f(14) &= 2^{14} - 12 = 16372,\\
f(8) &= 2^{8} - 12 = 244,\\
f(1) &= 2^{1} - 12 = -10.
\end{aligned}$$

Portanto, a mensagem cifrada que será enviada ao general é dada por

$$-10\ \ 1048564\ \ -10\ \ -4\ \ -10\ \ 262132\ \ 20\ \ 8180\ \ 32756\ \ 524276\ \ 65524\ \ 20\ \ 4084\ \ -10$$

$$8180\ \ -10\ \ 16372\ \ 244\ \ -10.$$

O general, para decifrar a mensagem, visto que terá que encontrar a inversa da função utilizada como chave pelos soldados, terá que dominar o conteúdo de funções logarítmicas.

3.2.4 Cifras de transposição

Além da possibilidade de cifrar mensagens por meio de substituição, conforme apresentado anteriormente, também é possível fazê-lo por meio de transposição. Dada a simplicidade do método, será exibido apenas um exemplo.

Exemplo 3.4. *Codifique a palavra $DESLOCAMENTO$ usando como chave uma matriz 4×3 e a permutação $3-1-2$ para as colunas.*

$$\begin{array}{ccc} 1 & 2 & 3 \\ D & E & S \\ L & O & C \\ A & M & E \\ N & T & O \end{array} \rightarrow \begin{array}{ccc} 3 & 1 & 2 \\ S & D & E \\ C & L & O \\ E & A & M \\ O & N & T \end{array}$$

Portanto, a palavra cifrada é dada por $SDECLOEAMONT$.

Capítulo 4

Oficina: aplicação, resultados e discussões

A ideia principal desse trabalho é sugerir e mostrar que a criptografia pode ser introduzida na prática de ensino e aprendizagem de Matemática no Ensino Básico. Para tal, uma oficina envolvendo criptografia foi proposta e aplicada em duas turmas. Nesse capítulo, serão descritas as etapas e mostrados os resultados obtidos, a partir da observação em sala de aula e por meio de questionários que foram respondidos pelos alunos.

Essa proposta surgiu da necessidade de realização de projetos no Ensino Básico, pelos participantes do programa Residência Pedagógica. O Programa busca promover um contato mais próximo dos licenciandos com as escolas de Educação Básica, aprimorando os estágios e vivência dos futuros professores.

A oficina partiu de um experimento denominado *Mensagens Secretas com Matrizes*, disponível no site da coleção Matemática Multimídia da Universidade Estadual de Campinas (UNICAMP). Contudo, ao invés de utilizar matrizes como conteúdo, o experimento foi adaptado para a abordagem de funções. Além disso, a oficina foi implementada pela história da criptografia, a fim de trabalhar todas as dinâmicas apresentadas envolvendo seu contexto histórico.

A oficina foi realizada no Colégio Estadual Jorge Amado, localizado no Setor Noroeste em Araguaína-TO. As informações em relação às turmas constam no Quadro 4.1.

Quadro 4.1: Dados das turmas

Ano	Etapa	N° de alunos	Tempo de duração
9°	Fundamental	11	1 hora e 40 minutos
3°	Médio	12	1 hora e 40 minutos

4.1 Oficina

A oficina, no que se refere a aspectos metodológicos, foi dividida em três momentos, conforme descritos a seguir.

1º Momento

Inicialmente os alunos conheceram o contexto histórico da criptografia, detalhes do seu uso em guerras e principalmente, o funcionamento da cifra de César. Sobre a última, foi colocado um desafio expresso na Figura 4.1, para que usando a transposição, eles chegassem à frase "matemática genial".

Figura 4.1: Exemplo da Cifra de César

OCVGOCVKEC IGPKCN

MATEMÁTICA GENIAL

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

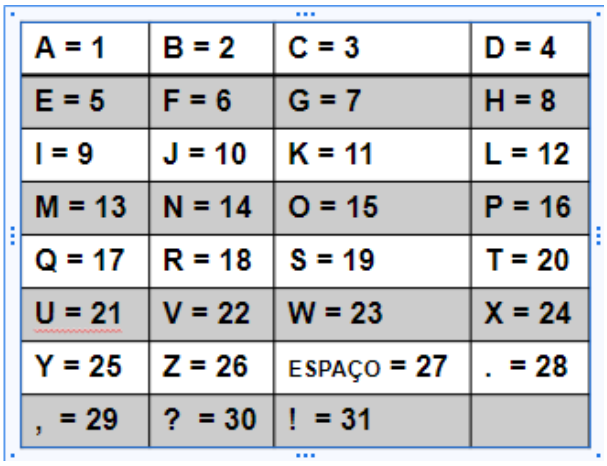
Fonte: Autor

A cifra de César serviu como embasamento para o que viria adiante. A ideia foi que os alunos entendessem o funcionamento da transposição, como método que permite cifrar mensagens, sem o uso da matemática, a princípio.

2º Momento

Aos alunos foi apresentada a Figura 4.2, que continha o alfabeto e seu símbolo correspondente, essa será aproveitada no 3° momento da aula para a pré-codificação (processo de troca da letra pelo seu equivalente em símbolos).

Figura 4.2: Tabela de pré-codificação



A = 1	B = 2	C = 3	D = 4
E = 5	F = 6	G = 7	H = 8
I = 9	J = 10	K = 11	L = 12
M = 13	N = 14	O = 15	P = 16
Q = 17	R = 18	S = 19	T = 20
U = 21	V = 22	W = 23	X = 24
Y = 25	Z = 26	ESPAÇO = 27	. = 28
, = 29	? = 30	! = 31	

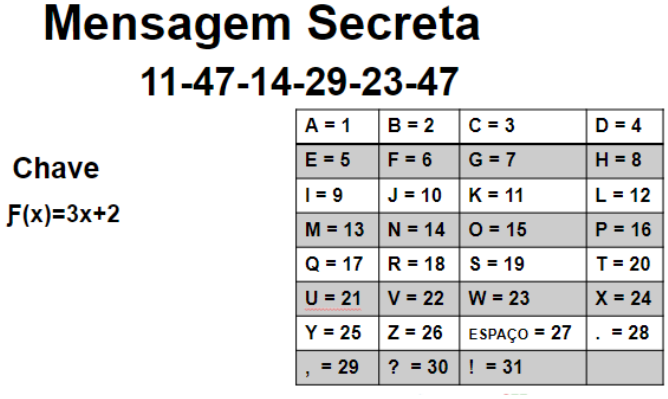
Fonte: Autor

Logo após, a decodificação de uma mensagem secreta foi sugerida como exemplo, essa exibida na Figura 4.3. A priori foi proposto que os estudantes tentassem desvendar/decifrar essa mensagem, todavia isso foi pensado para que eles não tivessem sucesso, para instigar o interesse deles na atividade.

Objetivando o sucesso, foi realizado uma revisão conceitual, com realização de exemplos, do conteúdo de funções e de como chegar a sua inversa, para que assim não houvessem dúvidas sobre a matéria que seria operada.

Após encerrar a parte da fundamentação, voltamos a Figura 4.3 que contém uma correspondência das letras do alfabeto com seus respectivos símbolos numéricos, junto com uma chave de decodificação.

Figura 4.3: Mensagem para decodificação



Mensagem Secreta

11-47-14-29-23-47

Chave

F(x)=3x+2

A = 1	B = 2	C = 3	D = 4
E = 5	F = 6	G = 7	H = 8
I = 9	J = 10	K = 11	L = 12
M = 13	N = 14	O = 15	P = 16
Q = 17	R = 18	S = 19	T = 20
U = 21	V = 22	W = 23	X = 24
Y = 25	Z = 26	ESPAÇO = 27	. = 28
, = 29	? = 30	! = 31	

Fonte: Autor

O esperado dos alunos, extraindo os dados da Figura 4.3, era que procedessem como descrito a seguir.

A mensagem original foi codificada por meio de uma função afim cifradora, que con-

forme a Figura 4.3, é dada por $f(x) = 3x+2$. Para decodificar a mensagem secreta, é necessário que o recebedor calcule as imagens de f^{-1}, onde $D(f) = Im(f^{-1})$ e $D(f^{-1}) = Im(f)$, conforme visto.

Inicialmente, encontra-se a função inversa de f. Para isso, a partir da função $f(x) = y = 3x + 2$, troca-se x por y e vice-versa, obtendo $x = 3y + 2$.

Posteriormente, isola-se a variável y, chegando assim a f^{-1}.

$$x - 2 = 3y \Rightarrow \frac{x-2}{3} = y \Rightarrow f^{-1}(x) = \frac{x-2}{3}.$$

Agora, utiliza-se $f^{-1}(x) = \frac{x-2}{3}$ para descriptografar a mensagem, calculando a imagem de cada número codificado, isto é, basta substituir os valores da sequência $11 - 47 - 14 - 29 - 23 - 47$ por x. Assim,

$$f^{-1}(11) = \frac{11-2}{3} = 3,$$

$$f^{-1}(47) = \frac{47-2}{3} = 15,$$

$$f^{-1}(14) = \frac{14-2}{3} = 4,$$

$$f^{-1}(29) = \frac{29-2}{3} = 9,$$

$$f^{-1}(23) = \frac{23-2}{3} = 7.$$

Obtém-se a sequência $3 - 15 - 4 - 9 - 7 - 15$. Para obter a mensagem, basta fazer uma substituição usando a Figura 4.3, alterando os números da sequência obtida pelas letras e símbolos correspondentes, chegando a palavra “CODIGO”.

Para que não restasse dúvidas, foi mostrado aos alunos como o recado foi criptografado. Destacou-se que cifrar é um processo relativamente mais simples. Inicialmente, escolhe-se a mensagem, que no caso foi CODIGO, e depois, substitui-se cada letra pelo número correspondente, conforme a Figura 4.2, obtendo $3 - 15 - 4 - 9 - 7 - 15$, sendo essa nosso recado pré-codificado.

A mensagem codificada é o resultado do cálculo pré-codificado com a chave, que aqui, trata-se da função $f(x) = 3x + 2$.

É importante ressaltar que essa função precisa ser invertível, ou seja, bijetora. Destaca-se que, com exceção das funções constantes, toda função afim é inversível.

Codificando a mensagem de acordo com f, tem-se

$$f(3) = 3x + 2 = 11,$$

$$f(15) = 3x + 2 = 47,$$

$$f(4) = 3x + 2 = 14,$$

$$f(9) = 3x + 2 = 29,$$

$$f(7) = 3x + 2 = 23.$$

Dessa forma, obtém-se a mensagem que fora decodificada inicialmente.

3º Momento

Na terceira fase, depois de solucionar o desafio junto com os alunos, a sala foi dividida em grupos e as equipes escolhiam uma mensagem para ser codificada. Posteriormente, uns criptografavam enquanto outros descriptografavam, a divisão foi escolhida de forma aleatória.

4.2 Análise de resultados e discussões

A oficina foi avaliada por meio de um questionário contendo perguntas abertas e fechadas. Dessa forma, algumas questões não restringiam os respondentes, de maneira que eles estavam livres para argumentar. Outras eram dicotômicas, isto é, as alternativas de respostas eram restritas a sim ou não.

O objetivo das questões foi entender como os alunos reagem a aulas que englobam história, teoria e prática.

O questionário foi aplicado em cada uma das duas turmas e os resultados obtidos são apresentados separadamente para cada um delas. Toda pergunta realizada será comentada de acordo com as respostas dos alunos, sendo divididas em tópicos para facilitar o entendimento do leitor.

4.2.1 Uso de oficinas nas aulas de Matemática

A primeira questão colocada foi: *O uso de oficinas contribui para o seu conhecimento?*.

Oficinas são ferramentas que podem ser utilizadas pelos docentes como apoio pedagógico e têm como intuito fazer com que a aula não seja puramente uma transferência de informações, gerando uma construção coletiva de conhecimento e sendo uma troca entre os próprios alunos.

Com relação ao retorno dos alunos à oficina proposta, as turmas se mostraram bem confortáveis com a inclusão de uma metodologia fora do tradicional. Isso é notório com o fato de todos os alunos terem respondido “Sim” à pergunta. Quanto à prática, a cooperação e assimilação entre eles foi satisfatória. No final da atividade, todos conseguiram codificar e decodificar suas respectivas mensagens.

Apesar da questão ser dissertativa, poucas respostas foram argumentadas. As que tiveram justificativas foram exibidas no Quadro 4.2.

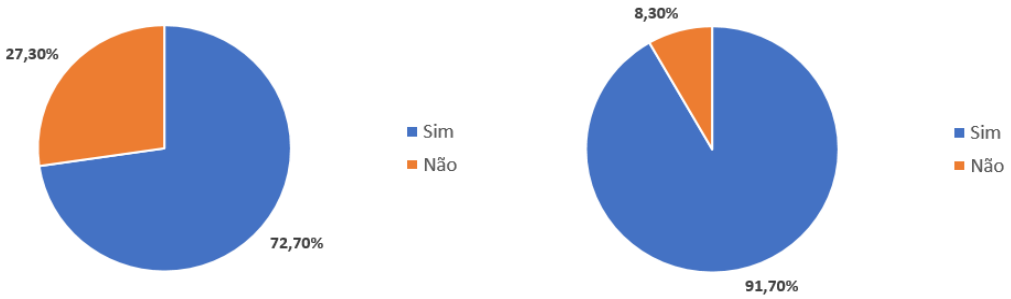
Quadro 4.2: Respostas justificadas da 1° questão

9° ano
Sim, eu pude me aprofundar no assunto e pude entender mais.
Sim, aprendemos a descobrir mensagens e codificar.
3° ano
Sim, é uma forma mais divertida de aprendizado e o entendimento é melhor.
Sim, é bastante interessante para o aprofundamento da aprendizagem.
Sim, é muito legal colocar a mente para trabalhar o seu conhecimento.
Sim, contribuiu para o meu aprendizado.

4.2.2 Interesse dos alunos pela história da Matemática

A segunda pergunta realizada aos alunos foi a seguinte: *Você gosta quando se é trabalhado história da matemática?*. Os resultados obtidos são exibidos na Figura 4.4.

Figura 4.4: Nível de interesse pela história da Matemática



(a) 9° ano (b) 3° ano

A Matemática nasceu da necessidade dos povos ao decorrer de toda a história, entretanto, hoje ela chega na sala de aula lapidada com suas definições, teoremas, propriedades e axiomas. Roque (2012, p. 20) afirma “em vez de partirmos do modo como um conceito matemático foi desenvolvido, mostrando as perguntas às quais ele responde, tomamos esse conceito como algo pronto”. Ao aluno cabe absorver o que já existe, sendo que nem sempre esse sabe o porquê da sua existência ou a sua importância. Quando se associa o que está estudando a algo concreto ou que pelo menos tenha uma contextualização, abrem-se novas possibilidades de entendimento da disciplina.

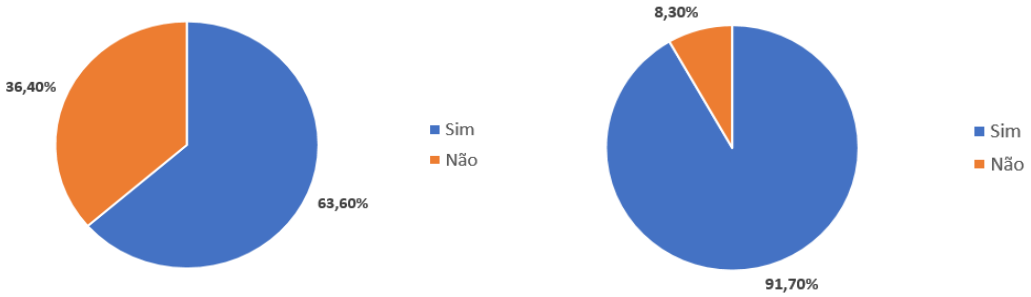
Na oficina proposta, a história da criptografia foi introduzida a fim de que o estudante conseguisse entender o porquê da criação de códigos e como eles funcionavam antes da linguagem computacional. Apesar do foco ter sido a criptografia, a oficina relacionou-se com o conteúdo de funções, mostrando que é possível transformar as definições abstratas em algo operacional. De acordo com a Figura 4.4, o grau de aceitação de oficinas, como metodologia de ensino e aprendizagem, é bem alto, principalmente, com a turma do 3° ano.

4.2.3 A presença da criptografia no cotidiano

A oficina teve o objetivo de explicitar a aplicação e o conceito da criptografia, já que muitos conheciam apenas a palavra. Foi solicitado, inclusive, que houvesse mais aulas práticas deste tipo.

Neste sentido, a terceira pergunta era: *Em algum momento você já tinha ouvido falar em criptografia?*. A Figura 4.5 exibe as respostas obtidas.

Figura 4.5: Conhecimento prévio acerca da criptografia



(a) 9° ano (b) 3° ano

A criptografia, como foi mostrado no decorrer desse trabalho, tem contribuições fundamentais para a segurança de informações desde a Grécia antiga, quando foi criada com a finalidade de ser uma artimanha em meio a conflitos. Hinz (2000, p.12) escreve “a criptografia continua tendo uma importância militar muito grande, entretanto ela é usada também nas mais diversas áreas onde a transmissão de dados necessita de segurança”.

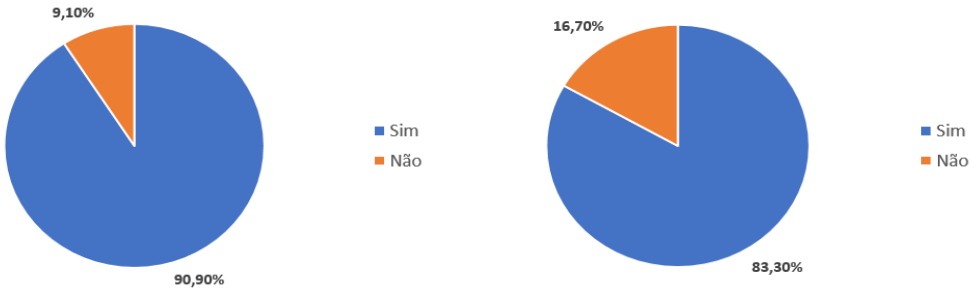
Pode-se observar na Figura 4.5 que a palavra não é desconhecida, principalmente pela turma do 3º ano. Notou-se, entre os alunos que previamente conheciam a criptografia, que tal conhecimento estava relacionado ao aplicativo *WhatsApp*. Quando perguntados em sala sobre o assunto, isso antes de iniciar a exposição, não houve consenso de como funcionava, apenas que se tratava de códigos. Para esse entendimento, a oficina foi de grande auxílio.

4.2.4 Interesse pela criptografia

A criptografia é usada em todas as redes sociais, e-mails e senhas de banco. Dessa forma, embora de forma implícita, é utilizada rotineiramente pelos alunos. Com a oficina, buscou-se destacar a grande presença da criptografia na vida cotidiana, fornecendo uma base para um aprofundamento mais complexo no assunto, motivando que o aluno tivesse o interesse em expandir seu conhecimento. Neste sentido, "O que o aluno aprende passa para além da sala de aula, o que confere ao trabalho do professor o peso de sua contribuição aos indivíduos"(HAGEMEYER, 2004, p. 81).

Neste contexto, a quarta pergunta era: *A oficina despertou algum interesse para se aprofundar no assunto?*. As respostas obtidas estão na Figura 4.6.

Figura 4.6: Interesse pela criptografia.



(a) 9° ano (b) 3° ano

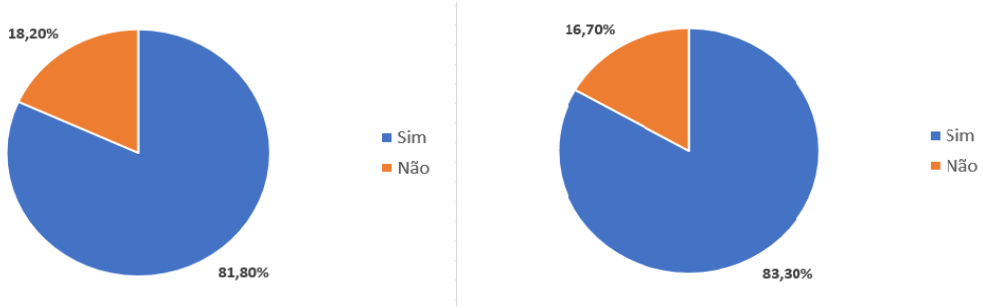
Conforme o resultado exibido na Figura 4.6 e comparando ao número de alunos que já conheciam segundo a Figura 4.5 da resposta anterior, percebe-se que os alunos do 9° ano mostraram maior interesse pela continuidade de seus estudos acerca da criptografia após a oficina. Destaca-se que, esses alunos também possuíam menor conhecimento sobre o assunto preliminarmente. Já os alunos do 3° ano apresentaram menor interesse em dar continuidade aos seus estudos acerca da criptografia, tendo em vista que os mesmos possuíam um maior conhecimento sobre criptografia, antes da realização da oficina.

Embora o conhecimento acerca da criptografia seja pertinente ao nosso cotidiano, ele é negligenciado, muitas vezes, pelo desinteresse. Apesar da maioria dos alunos ter acesso a toda e qualquer informação, isso não significa, necessariamente, um acesso ao conhecimento. Isso pode ocorrer pela falta de uma educação digital.

4.2.5 Conclusões dos alunos sobre a criptografia

A última pergunta fora a seguinte: *Sua concepção sobre o que é criptografia e de como funciona mudou ao final da oficina? Justifique*. A questão permitia comentários e explicações.

Figura 4.7: Parecer dos alunos sobre o quanto aprenderam na oficina



(a) 9° ano (b) 3° ano

Considerando a Figura 4.7, constata-se que houve uma paridade entre os grupos. Assim apurou-se que a criptografia foi entendida pelos alunos e mais esclarecida aos mesmos, de modo geral.

O Quadro 4.3 contém recortes das repostas feitas pelos alunos.

Quadro 4.3: Recorte de respostas afirmativas relativas à 5° questão

Respostas do 9° ano
Sim, a criptografia é bem mais interessante e divertida do que parece ser.
Sim, não sabia o que era criptografia e foi bom, porque é mais um conhecimento.
Sim, as funções que foram passadas nos ajudam a realizar exercícios em sala de aula.
Respostas do 3° ano
Sim, eu já tinha um pouco de conhecimento sobre o assunto, mas oficina melhorou.
Sim, despertou-me ainda mais interesse sobre o assunto.
Sim, porquê com a criação das mensagens o conteúdo ficou bem mais interessante.

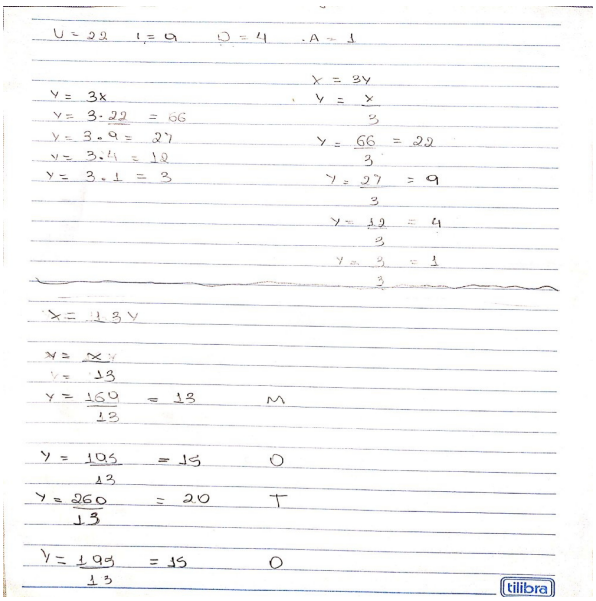
A respeito do 9° ano, as respostas foram positivas. Mesmo aqueles que disseram não, pontuaram que a oficina contribuiu para o seu conhecimento. Os estudantes que responderam sim, indicaram que o tema pode ser divertido e interessante. Com relação ao 3° ano, uma resposta negativa, segundo o aluno, devia-se ao fato dele ter conhecimento prévio sobre o assunto e já conhecer o funcionamento da criptografia.

4.2.6 Comentários sobre a experiência no processo de aplicação

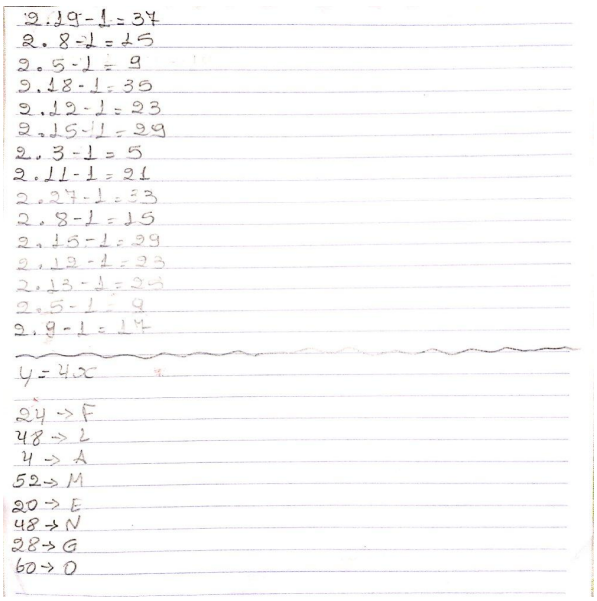
Grande parte dos estudantes consideram as aulas de matemática monótonas. Não é fácil construir projetos em cima de interesses individuais, afinal cada um tem suas singularidades. O desafio de um educador é conseguir que o aluno tenha a capacidade de gerar ideias, de comunicá-las e colocá-las em prática.

Apesar do resultado ter sido parecido nas respostas do questionário, em aula, o comportamento em cada turma foi distinto. Os alunos do 9° ano mostraram-se mais participativos e abertos para a experiência e antes do tempo estipulado, conseguiram finalizar todas as atividades propostas. A Figura 4.8 mostra algumas das mensagens criptografadas por eles.

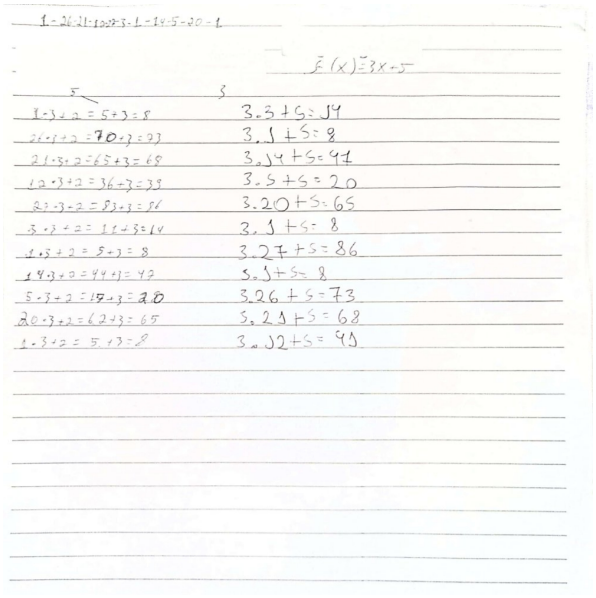
Figura 4.8: Arquivos da pesquisa



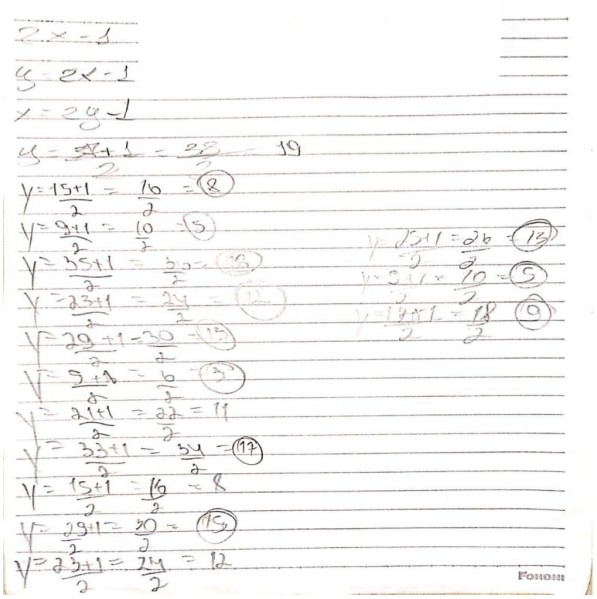
(a) 9° ano



(b) 9° ano



(c) 3° ano



(d) 3° ano

No início da oficina, a turma do 3° ano estava desatenta e o reflexo disso foi visto durante a produção das mensagens e, principalmente, na sua decodificação. Alguns alunos entregaram a tarefa no tempo limite.

A ideia da atividade era introduzir o conceito de criptografia e fixar o conteúdo de função

afim, além de observar a forma que lidariam com o fato de criar e resolver problemas. “Quando o aluno estuda técnicas para criptografar mensagens [...] através de permutações, funções, matrizes, entre outros, ele visualiza situações reais e consegue chegar mais facilmente a um resultado” (HINZ, 2000, p.23). Neste sentido, a maioria dos estudantes concordaram que as oficinas ajudavam na assimilação do conteúdo matemático e inclusive, foi pedido pelas turmas que ocorressem mais aulas deste tipo. A permanência em sala de aula diariamente, pode se converter em algo maçante, porém, com a inclusão de projetos, a experiência pode ser tornar mais animadora.

Para o estudante de licenciatura, o exercício da regência é o momento de executar a proposta educacional vista na graduação, contudo, ela deixa de ser teórica e passa a ser prática, auxiliando assim no desenvolvimento profissional. Como participante do programa Residência Pedagógica, que tem uma carga horária destinada a projetos superior a de um estagio supervisionado, foi possibilitada a oportunidade de ensinar com formas alternativas, fugindo um pouco da maneira tradicional. Por meio de atividades realizadas durante todo o programa, pudemos observar que os alunos absorviam os conteúdos de uma maneira mais natural ao lançar mão de ferramentas de ensino como oficinas.

De modo geral, o questionário realizado após a oficina, mostrou que o assunto foi entendido, não havendo o interesse de todos em aprofundar-se no conteúdo. O termo criptografia causou um espanto natural a muitos dos alunos, no início, porém, com o desenvolver da oficina, eles puderam perceber que o seu funcionamento pode ser entendido. Foi assimilado pelos alunos que a criptografia trata-se de um sistema de algoritmos existente há muitos anos, que funciona como um embaralhamento e que com o passar do tempo, desembaralhar mensagens criptografadas tornou-se uma missão cada vez mais difícil tendo em vista o avanço da tecnologia e implementação de ferramentas matemáticas.

Capítulo 5

Considerações Finais

A escolha da criptografia como assunto a ser abordado no desenvolvimento da oficina foi efetuado com o intuito de despertar entusiasmo nos alunos, já que o tema é bastante atual e presente no cotidiano. Neste sentido, diversas pesquisas na área da Educação Matemática e Matemática debruçam-se nesse tema.

As chaves de segurança pública baseiam-se em conceitos matemáticos como a fatoração de números primos que tornam complexa a decodificação de mensagens até para computadores. No entanto, o propósito da oficina foi mostrar a sua aplicação no cotidiano por meio de um exemplo simples.

Visando um maior envolvimento dos alunos em atividades que envolvam criptografia, é interessante que o professor faça a inserção da história, conceitos e aplicações para que o seu desenvolvimento convirja em uma aprendizagem significativa.

Com base nas respostas obtidas por meio do questionário aplicado, pode-se concluir que o objetivo de fazer com que o aluno pudesse assimilar o conceito de criptografia, sua forma de funcionamento e seu papel histórico para a humanidade foram alcançados.

De modo geral, no que concerne ao propósito deste trabalho, concluiu-se que a criptografia pode ser inserida na matemática vista no ensino básico por meio da função afim, via realização de oficinas que contemplem história, conteúdo e prática.

Como indicação de trabalhos futuros, seria interessante adaptar a oficina realizada para a abordagem de outros conteúdos matemáticos. Matrizes e outros tipos de funções podem ser utilizados como chaves de codificação e decodificação de mensagens. Além disso, adaptar a oficina proposta utilizando softwares também seria bastante válido.

Por fim, espera-se que este trabalho auxilie e inspire docentes em suas aulas, tendo em vista que a criptografia pode ser um grande aproximador de teoria e realidade, podendo ser uma grande aliada no sucesso do ensino e aprendizagem de diversos conteúdos da Matemática.

Referências

[1] ANTON, Howard; BUSBY, Robert C. **Álgebra linear contemporânea**. Porto Alegre: Bookman, 2008. 610 p.

[2] BAGNO, M. **Pesquisa na escola: o que é, como se faz**. 25. ed. São Paulo: Edições Loyola, 2012.

[3] IEZZI, Gelson; MURAKAMI, Carlos. **Fundamentos da Matemática Elementar: conjuntos funções**. São Paulo: Atual, 1983.

[4] IEZZI, Gelson; HAZZAN, Samuel. **Fundamentos da Matemática Elementar: sequências matrizes determinantes sistemas**. 2. ed. São Paulo: Atual, 1983. 119 p.

[5] LIPSHUTZ, Seymour.**Teoria dos Conjuntos. Brooklyn: Megraw-hill**, 1963. 337 p.

[6] MENEZES, Rosilene de.**Criptografia e Álgebra**. 2013. 66 f. TCC (Graduação) - Curso de Matemática, Universidade Federal de Minas Gerais, Belo Horizonte, 2003.

[7] PEREIRA, E. et al. **Criptografia de Dados Utilizando Matrizes**. 25. ed. São Paulo: Edições Loyola, 2012.

[8] REIS, Verônica Lagrange Moutinho dos. **Criptografia, Segurança de Dados e Privacidade - Até que ponto pode-se confiar na discrição dos computadores?** 1989. 139 f. Tese (Doutorado) - Curso de Engenharia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 1989.

[9] **Manual de Normatização para elaboração de Trabalhos acadêmico-científicos da Universidade Federal do Tocantins**. Palmas: UFT, 2017, 102 p.

[10] GALDINO, Uelder Alves. **Teoria dos números e Criptografia com Aplicações Básicas**. TESE (MESTRADO PROFISSIONAL-PROFMAT/CCT/UEPB) -PARAÍBA: UEPB, 2014, 77 p.

[11] OLIVEIRA, Ronielton Rezende. **Criptografia simétrica e assimétrica: os principais algoritmos de cifragem**. 2012. Disponível em:

<http://www.ronielton.eti.br/blog/2012/06/02/artigo-revista-segurana-digital/>. Acesso em: 07 abr. 2020.

[12] BARICHELLO, Leonardo; FIRER, Marcelo; TOREZZAN, Cristiano. **Mensagens Secretas com Matrizes**. Disponível em: <https://m3.ime.unicamp.br/recursos/1020>. Acesso em: 22 ago. 2019.

[13] SOARES, Pedro Henrique; CHIREIA, Rodrigo; GUIMARÃES, Alex Sandro; BORGES, Felipe. **História da Criptografia: A importância da criptografia na segurança da informação. importância da criptografia na segurança da informação**. Disponível em: <https://www.sutori.com/story/historia-da-criptografia–BuExbZLfWYYYbgNaXQ33if51>. Acesso em: 08 abr. 2020.

[14] MOCHETTI, Karina. **Alan Turing e a Enigma**. 2016. Disponível em: <http://horizontes.sbc.org.br/index.php/2016/11/22/alan-turing-e-a-enigma/>. Acesso em: 10 abr. 2020.

[15] MEDEIROS, Flavio. **Uma breve história sobre Criptografia**. 2015. Disponível em: <https://cryptoid.com.br/banco-de-noticias/a-historia-da-criptografia/>. Acesso em: 09 abr. 2020.

[16] FERNANDES, Cor Cruz. **O Lendário Código Navajo**. 2012. Disponível em: <https://historiadastransmissoes.wordpress.com/2012/07/13/o-lendario-codigo-navajo/>. Acesso em: 01 mai. 2020.

[17] LOUREIRO, Flávio Ornellas. **Tópicos de criptografia para o ensino médio**. 2014. 43 f. Dissertação (Mestrado) - Curso de Matemática, Universidade Estadual do Norte Fluminense Darcy Ribeiro, Campos dos Goytacazes - Rj, 2014.

[18] ROQUE, Tatiana.**História da matemática**. Editora Schwarcz-Companhia das Letras, 2012.

[19] HINZ, Marco A. M. **Um estudo descritivo de novos algoritmos de criptografia**. Pelótas: UFP, 2000.

[20] HAGEMEYER, R. C. de C. **Dilemas e desafios da função docente na sociedade atual: os sentidos da mudança**. Educar, Curitiba, n. 24, p. 67-85, 2004. Editora UFPR.

[21] MOTTA, Sergio. **Top 5 programas gratuitos para criptografar arquivos.** Disponível em: <https://www.topfreewares.com.br/top-5-programas-gratuitos-criptografia-arquivos/>. Acesso em: 22 ago. 2020.