


A CIFRA DE HILL COMO APLICAÇÃO LÚDICA NO ENSINO DE MATRIZES NO ENSINO MÉDIO

 <https://doi.org/10.22533/at.ed.531112414105>

Data de aceite: 08/11/2024

Wesley Vieira de Araujo

Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Parnaíba – PI
<https://orcid.org/0009-0000-6786-7248>

Jamisson Ferreira dos Santos

Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Cocal – PI
<https://orcid.org/0009-0001-5136-6956>

Kécia Silva Araujo

Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Cocal – PI
<https://orcid.org/0009-0004-6719-4126>

Kristian Pessoa dos Santos

Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Parnaíba – PI
<https://orcid.org/0000-0002-8305-8122>

Davi Ribeiro dos Santos

Universidade Vale do Acaraú, Sobral – CE
<https://orcid.org/0000-0002-1505-9051>

RESUMO: Este artigo apresenta os resultados de uma pesquisa do tipo bibliográfica sobre criptografia, com foco na Cifra de Hill e na sua utilização como ferramenta lúdica no ensino de matrizes. A criptografia, amplamente utilizada na proteção de dados e informações

nos dias de hoje, assim como qualquer outra invenção do homem, passou por diversas mudanças ao longo do tempo. Desde as cifras de substituição, utilizadas principalmente pelo imperador Júlio Cesar, até a criptografia quântica, especialmente usada pelos serviços de inteligência, foram inúmeras cifras criadas e utilizadas no decorrer dos séculos. Uma facilmente quebráveis, outras extremamente seguras – mérito da matemática – todas as cifras já criadas revelam o fascinante mundo da criptografia, riquíssimo histórica e matematicamente. A cifra de Hill se mostra uma boa ferramenta para a abordagem do conteúdo de matrizes no ensino médio, utilizando-a como ferramenta lúdica, e diferente da tradicional associação feita com tabelas. Neste trabalho serão expostos alguns resultados de Aritmética modular e álgebra, em especial, resultados como congruências, relações de equivalência classes de equivalência e operações matriciais em \mathbb{Z}_{26} . Tal exposição tem como objetivo dar fundamento ao funcionamento do método criptográfico conhecido como Cifra de Hill, objeto de estudo desse artigo.

PALAVRAS-CHAVE: matemática; criptografia; cifra de hill; matrizes.

HILL'S CIPHER AS A PLAYFUL APPLICATION IN TEACHING MATRICES IN SECONDARY EDUCATION

ABSTRACT: This article presents the results of a bibliographic research on cryptography, focusing on the Hill Cipher and its use as a playful tool in the teaching of matrices. Encryption, widely used in data and information protection today, as well as any other invention of man, has undergone several changes over time. From the substitution ciphers, used mainly by Emperor Julius Caesar, to quantum cryptography, especially used by intelligence services, numerous ciphers have been created and used over the centuries. Some easily breakable, others extremely secure – merit of mathematics – all the ciphers already created reveal the fascinating world of cryptography, rich historically and mathematically. Hill's cipher proves to be a good tool for addressing the content of matrices in high school, using it as a playful tool, and different from the traditional association made with tables. In this work will be exposed some results of modular arithmetic and algebra, in particular, results such as congruences, equivalence relationships equivalence classes and matrix operations in \mathbb{Z}_{26} . This exhibition aims to support the functioning of the cryptographic method known as Hill Cipher, the object of study of this article.

Keywords: math; cryptography; hill cipher; matrices.

INTRODUÇÃO

O ensino da matemática, de uma forma geral, baseia-se nas possibilidades de uso do que se estuda, tendo como princípio a adequação das regras matemáticas para o uso no cotidiano. O ensino da matemática no ensino médio, mais especificamente, busca estreitar as relações dos conteúdos abordados em sala com o seu uso no dia a dia, uma vez que a associação com a matemática pura, somente, não oferece benefícios para o aprendizado do aluno. “Mover-se da referência à matemática pura para a referência a vida real pode resultar em reflexões sobre a matemática e suas aplicações”. (Skovsmose, 2000, p. 1).

Os objetivos do Ensino Médio em cada área do conhecimento devem envolver, de forma combinada, o desenvolvimento de conhecimentos práticos, contextualizados, que respondam às necessidades da vida contemporânea, e o desenvolvimento de conhecimentos mais amplos e abstratos, que correspondam a uma cultura geral a uma visão de mundo. [...] (Brasil, 1999, p. 6).

Ainda sobre o pensamento, Brasil (1999, p. 40) diz que:

No que diz respeito ao caráter instrumental da Matemática no Ensino Médio, ela deve ser vista pelo aluno como um conjunto de técnicas e estratégias para serem aplicadas a outras áreas do conhecimento, assim como para a atividade profissional. Não se trata de os alunos possuírem muitas e sofisticadas estratégias, mas sim de desenvolverem a iniciativa e a segurança para adaptá-las a diferentes contextos, usando-as adequadamente no momento oportuno.

Por outro lado, a inserção de temas ligados à tecnologia ainda no âmbito escolar favorece para um desenvolvimento educacional mais satisfatório, pois propicia a utilização de tecnologias no processo de ensino, desencadeia a curiosidade pelos processos usados no funcionamento das tecnologias atuais, além de oferecer novas possibilidades de formação superior e/ou qualificação para o mercado de trabalho.

O impacto da tecnologia na vida de cada indivíduo vai exigir competências que vão além do simples lidar com as máquinas. A velocidade do surgimento e renovação de saberes e de formas de fazer em todas as atividades humanas tornarão rapidamente ultrapassadas a maior parte das competências adquiridas por uma pessoa ao início de sua vida profissional. (Brasil, 1999, p. 41).

Outro ponto a ser abordado é a utilização de ferramentas lúdicas no processo de ensino. A utilização de tais ferramentas tem como objetivo auxiliar no entendimento da teoria através de jogos e dinâmicas, tirando o peso da matemática pura e trabalhando sua aplicabilidade.

A Matemática lúdica é uma ferramenta essencial pronta a atender à necessidade de elaborar pedagogicamente aulas com maior aproveitamento e entretenimento, ajudando o aluno a analisar, compreender e elaborar situações que possam resolver determinados problemas que sejam propostos pelo professor permitindo a análise e compreensão da proposição exposta pelo aluno – o resultado – e assim adquirir conhecimento, interpretar e articular métodos para argumentar e concretizar problemas. (Da Cunha; Da Silva, 2012, p. 2).

Sobre a temática, Da Silva (2013, p. 5) diz que:

Os objetivos da implantação da Matemática lúdica no ensino é trazer o aluno para a sala de aula disposto a aprender se divertindo. O incentivo para participação das aulas lúdicas, não quer dizer que o aluno tem que ir à escola somente brincar, o aluno tem que ver a aula de Matemática como uma prazerosa atividade de aprendizagem e não como ainda é vista em alguns ambientes educacionais, como aula de repetição e memorização, e logo após a prova o assunto que foi transmitido durante as aulas seja esquecido.

O uso de meios lúdicos no ensino de matrizes busca oferecer novas abordagens para um conteúdo que, geralmente, é visto como difícil e pouco utilizado no cotidiano do aluno. Comumente associado à análise de tabelas, o conteúdo de matrizes torna-se enfadonho, já que pouco oferece ao aluno na perspectiva de utilização.

A utilização de um método criptográfico como ferramenta lúdica abre possibilidade para a inserção de temas atuais em sala de aula que são utilizados em diversas áreas. A mais óbvia é a utilização da criptografia nos meios de comunicação, em especial as redes sociais. Utilizar essa narrativa em sala faz com que os alunos tenham interesse do que acontece durante o funcionamento dos meios que são mais utilizados hoje em dia. Abre espaço também para a abordagem de outros métodos criptográficos, além de uma análise do contexto histórico atrelado às diversas cifras existentes.

Um dos principais aspectos que explicam a evolução humana no decorrer da história é o desenvolvimento da comunicação e da transmissão de conhecimento. Junto a esse desenvolvimento humano, sempre houve a necessidade de se manter em segredo determinadas informações, sejam elas mensagens de amor ou planos de guerra.

Antes mesmo da existência da criptografia, já se fazia necessário esconder determinadas informações, e tal ação era feita utilizando a esteganografia. Do grego *esteganos*, coberto, e *graphein*, escrever, nada mais é do que ocultar a existência de uma determinada mensagem. Com o passar do tempo, os métodos esteganográficos foram se tornando populares e, conseqüentemente, inúteis. Partindo da necessidade de se obter novas formas de se comunicar de forma secreta e usando como base o desenvolvimento de novas ideias e das ciências (em especial, a matemática), deu-se origem a criptografia, do grego *kriptos*, oculto, e *graphein*, escrever, que se difere da esteganografia no objetivo. Segundo Singh (2003, p. 22), “O objetivo da criptografia não é ocultar a existência de uma mensagem, e sim esconder o seu significado”.

A criptografia, assim como diversas outras coisas que utilizamos no cotidiano, teve seu desenvolvimento ligado com o desenrolar de guerras e batalhas. Numa guerra, dois lados que se confrontam sempre buscam estar um passo à frente de seu inimigo, daí entra a criptografia, utilizada na comunicação entre aliados que buscavam esconder seus planos de inimigos. Para Singh (2003, p. 11), “Foi a ameaça da interceptação pelo inimigo que motivou o desenvolvimento de códigos e cifras, técnicas para mascarar uma mensagem de modo que só o destinatário possa ler o conteúdo”.

Nas seções a seguir veremos alguns conceitos importantes para o desenvolvimento e entendimento da cifra de Hill.

TEORIA DOS NÚMEROS

Aqui estão descritos alguns tópicos de teoria dos números que são necessários na compreensão e desenvolvimento da cifra de Hill. Para um estudo aprofundado desses e de outros tópicos relacionados à aritmética modular, recomendo a leitura de (Alencar Filho, 1981), (Burton, 2016) e (Santos, 2015).

Congruência

Definição 2.1 Seja n um número inteiro positivo dado. Diz-se que os inteiros a e b são *congruentes módulo n* , simbolizando por

$$a \equiv b(\text{mod } n)$$

se n divide a diferença $a-b$, ou seja, desde que $a-b=kn$ para algum inteiro k . Quando $n \nmid (a-b)$, dizemos que a é *incongruente a b módulo n* , e neste caso escrevemos $a \not\equiv b(\text{mod } n)$.

Exemplo 2.1 Pela definição, temos

- a. $31 \equiv 1 \pmod{10}$, pois $10 \mid (31-1)$;
- b. $15 \not\equiv 2 \pmod{7}$, pois $7 \nmid (15-2)$.

Teorema 2.1 Para inteiros arbitrários a e b , $a \equiv b \pmod{n}$ se, e somente se, a e b deixam o mesmo resto quando divididos por n .

Demonstração: Uma solução para o Teorema acima pode ser encontrada em (Alencar Filho, 1981).

Exemplo 2.2 Podemos comprovar o item a) do exemplo anterior utilizando tal Teorema, já que 31 e 1 deixam o mesmo resto quando divididos por 10, o que notamos utilizando o algoritmo da divisão

$$31 = 10 \cdot 3 + 1 \text{ e } 1 = 10 \cdot 0 + 1.$$

ÁLGEBRA

Abaixo são listados alguns resultados importantes que são utilizados no funcionamento da cifra de Hill. Para um melhor entendimento sobre esses resultados, incido o estudo de (Boldrini, 1980), (Domingues, 2003), (Gonçalves, 2013), (Iezzi; Hazzan, 1977) e (Leon, 2014).

Relação de equivalência

Definição 3.1 Uma relação R sobre um conjunto E não vazio é chamado *relação de equivalência* sobre E se, e somente se, R é reflexiva, simétrica e transitiva. Ou seja, R deve cumprir, respectivamente, as seguintes propriedades:

- I. **Reflexiva:** Se $x \in E$, então xRx ;
- II. **Simétrica:** Se $x, y \in E$ e xRy , então yRx ;
- III. **Transitiva:** Se $x, y, z \in E$ e xRy e yRz , então xRz .

Exemplo 3.1 Verificamos que a relação R em \mathbb{Z} definida por

$$aRb \Leftrightarrow a \equiv b \pmod{m}$$

é uma relação de equivalência analisando os três itens:

- I. Reflexiva: vemos que $aRa, \forall a \in \mathbb{Z}$, pois

$$a - a = 0 = m \cdot 0 \Rightarrow a \equiv a \pmod{m}.$$

- II. Simétrica: tomando $a, b \in \mathbb{Z}$ tais que aRb , temos

$$\begin{aligned} a \equiv b \pmod{m} &\Rightarrow a - b = mk, k \in \mathbb{Z} \\ &\Rightarrow -(b - a) = mk \\ &\Rightarrow b - a = -mk \end{aligned}$$

$$\begin{aligned}\Rightarrow b - a &= m \cdot (-k), -k \in \mathbb{Z} \\ \Rightarrow b &\equiv a \pmod{m}.\end{aligned}$$

III. Transitiva: tomando $a, b, c \in \mathbb{Z}$ tais que aRb e bRc , temos

$$\begin{aligned}a \equiv b \pmod{m} &\Leftrightarrow a - b = k_1 m, k_1 \in \mathbb{Z} (*) \\ b \equiv c \pmod{m} &\Leftrightarrow b - c = k_2 m, k_2 \in \mathbb{Z} (**).\end{aligned}$$

Somando (*) e (**), temos

$$\begin{aligned}(a - b) + (b - c) &= k_1 m + k_2 m \\ a - c &= (k_1 + k_2)m, k_1 + k_2 \in \mathbb{Z} \\ \Rightarrow a &\equiv c \pmod{m}.\end{aligned}$$

Classe de equivalência

Definição 3.2 Seja R uma determinada relação de equivalência sobre E . Dado a , com $a \in E$, chama-se *classe de equivalência* determinada por a , módulo R , o subconjunto \bar{a} de E constituído pelos elementos x tais que xRa . Em símbolos:

$$\bar{a} = \{x \in E | xRa\}.$$

Proposição 3.1 Seja \sim uma relação de equivalência em um conjunto A e sejam $x, y \in A$. Então

1. $\bar{x} = \bar{y} \Leftrightarrow x \sim y$.
2. $\bar{x} \neq \bar{y} \Leftrightarrow \bar{x} \cap \bar{y} = \emptyset$.
3. $\bigcup_{x \in A} \bar{x} = A$.

Demonstração: A demonstração da proposição acima pode ser encontrada em (Gonçalves, 2013).

Conjunto quociente

Definição 3.3 O conjunto das classes de equivalência módulo R será indicado por E/R e chamado de *conjunto quociente* de E por R . Ou seja,

$$E/R = \{\bar{a} | a \in E\}.$$

Durante todo o artigo resumiremos à utilização do conjunto quociente de \mathbb{Z} pela relação R definida no exemplo 3.1, o qual será denotado aqui por \mathbb{Z}_m .

A proposição a seguir trata do número de classes contidas em \mathbb{Z}_m .

Proposição 3.2 Se $n \in \mathbb{N} - \{0\}$ então $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ é um conjunto contendo exatamente n classes de equivalência.

Demonstração: Tal demonstração pode ser encontrada em (Gonçalves, 2013).

Exemplo 3.2 Pela proposição, o conjunto \mathbb{Z}_{26} contém 26 classes de equivalência, que podem ser escritas da forma

$$\bar{n} = \{a \in \mathbb{Z} | a \equiv n \pmod{26}\} = \{n + 26k, k \in \mathbb{Z}\}.$$

Pelas proposições 3.1 e 3.2, podemos descrever \mathbb{Z}_{26} como

$$\mathbb{Z}_{26} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{25}\}.$$

A partir de agora, iremos considerar elementos de uma mesma classe como sendo iguais, sem a necessidade de utilizar a barra usual de uma classe de equivalência. Tal decisão tem como objetivo não carregar muitas notações no decorrer do artigo, e não representa um risco de eventuais erros.

Outra estratégia que adotaremos é, sempre que necessário, considerar o representante de uma determinada classe como sendo um número entre 0 e 25, também sem risco de erros, e com o objetivo de facilitar o funcionamento da cifra de Hill mais adiante.

Matrizes em \mathbb{Z}_{26}

Nesta seção trataremos apenas de matrizes quadradas, matrizes linha e matrizes coluna, cujos elementos são classes em \mathbb{Z}_{26} , que serão as utilizadas no funcionamento da cifra de Hill. Isto é, iremos tratar de matrizes na forma

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}, a_{ij} \in \mathbb{Z}_{26}.$$

Definição 3.4 (Igualdade). Duas matrizes A e B , de mesma ordem, são ditas *iguais* se $a_{ij} = b_{ij}$ em \mathbb{Z}_{26} , $\forall i, j$.

Exemplo 3.3 As matrizes $A = \begin{bmatrix} 1 & 4 \\ 2 & 7 \end{bmatrix}$ e $B = \begin{bmatrix} 27 & 82 \\ -24 & 33 \end{bmatrix}$ são ditas iguais em \mathbb{Z}_{26} e escrevemos

$$A = \begin{bmatrix} 1 & 4 \\ 2 & 7 \end{bmatrix} = \begin{bmatrix} 27 & 82 \\ -24 & 33 \end{bmatrix} = B,$$

pois $1=27$, $4=84$, $2=-24$ e $7=33$ em \mathbb{Z}_{26} .

Definição 3.5 (Multiplicação por escalar). Se A é uma matriz e $\alpha \in \mathbb{Z}_{26}$ um escalar, então αA é a matriz cujo elemento da i -ésima linha e j -ésima coluna é αa_{ij} .

Exemplo 3.4 Sendo $\alpha = 5$ e $A = \begin{bmatrix} 4 & 9 \\ 8 & -2 \end{bmatrix}$, temos

$$\alpha A = 5 \cdot \begin{bmatrix} 4 & 9 \\ 8 & -2 \end{bmatrix} = \begin{bmatrix} 20 & 45 \\ 40 & -10 \end{bmatrix} = \begin{bmatrix} 20 & 19 \\ 14 & 16 \end{bmatrix}.$$

Definição 3.4 (Adição). Se $A = (a_{ij})$ e $B = (b_{ij})$ são duas matrizes de mesma ordem, então a **soma** $A+B$ é a de ordem igual a ordem de A e B , cujo elemento da i -ésima linha e j -ésima coluna é $a_{ij} + b_{ij}$.

Exemplo 3.5 Dadas as matrizes $A = \begin{bmatrix} 1 \\ 12 \end{bmatrix}$ e $B = \begin{bmatrix} -5 \\ 13 \end{bmatrix}$, temos

$$A + B = \begin{bmatrix} 1 + (-5) \\ 12 + 13 \end{bmatrix} = \begin{bmatrix} -4 \\ 25 \end{bmatrix} = \begin{bmatrix} 22 \\ 25 \end{bmatrix}.$$

Definição 3.5 (Multiplicação de matriz). Se $A=(a_{ij})$ é uma matriz $m \times n$ e $B=(b_{ij})$ é uma matriz $n \times r$, então o produto $AB=C=(c_{ij})$ é a matriz $m \times r$ cujos elementos são definidos por

$$c_{ij} = [a_{i1} \quad \dots \quad a_{in}] \cdot \begin{bmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{bmatrix} = \sum_{k=1}^n a_{ik} b_{kj}.$$

Exemplo 3.6 Sejam $A = \begin{bmatrix} 4 & 7 \\ 3 & 1 \end{bmatrix}$ e $B = \begin{bmatrix} 15 \\ 2 \end{bmatrix}$, temos

$$AB = \begin{bmatrix} 4 & 7 \\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 15 \\ 2 \end{bmatrix} = \begin{bmatrix} 74 \\ 47 \end{bmatrix} = \begin{bmatrix} 22 \\ 21 \end{bmatrix}.$$

Exemplo 3.7 Sejam $C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ e $D = \begin{bmatrix} 3 & 7 \\ 4 & 2 \\ 2 & 1 \end{bmatrix}$, temos

$$CD = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 3 & 7 \\ 4 & 2 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 3+0+0 & 7+0+0 \\ 0+4+0 & 0+2+0 \\ 0+0+2 & 0+0+1 \end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 4 & 2 \\ 2 & 1 \end{bmatrix}.$$

Definição 3.6 (Transposta). A transposta de uma matriz $A_{m \times n}$ é uma matriz $B_{n \times m}$ definida por

$$b_{ji} = a_{ij}.$$

para $j=1,2,\dots,m$ e $i=1,2,\dots,n$. A transposta de A é denotada como A^T .

Exemplo 3.8 Dada $A = \begin{bmatrix} 12 & 8 \\ 15 & 3 \end{bmatrix}$, temos

$$A^T = \begin{bmatrix} 12 & 15 \\ 8 & 3 \end{bmatrix}.$$

Definição 3.7 (Inversão de matriz). Uma matriz quadrada de ordem n é dita *invertível* se existe uma matriz B tal que $AB=BA=I$, onde I é a matriz identidade. A matriz B é dita a *inversa* de A e denotada por A^{-1} .

Exemplo 3.9 As matrizes $A = \begin{bmatrix} 3 & 5 \\ 15 & 10 \end{bmatrix}$ e $B = \begin{bmatrix} 20 & 3 \\ 9 & 19 \end{bmatrix}$ são inversas, já que

$$AB = \begin{bmatrix} 3 & 5 \\ 15 & 10 \end{bmatrix} \cdot \begin{bmatrix} 20 & 3 \\ 9 & 19 \end{bmatrix} = \begin{bmatrix} 105 & 104 \\ 390 & 235 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

e

$$BA = \begin{bmatrix} 20 & 3 \\ 9 & 19 \end{bmatrix} \cdot \begin{bmatrix} 3 & 5 \\ 15 & 10 \end{bmatrix} = \begin{bmatrix} 105 & 130 \\ 312 & 235 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Definição 3.8 (Determinante ($n \leq 3$)). Seja A uma matriz de ordem n . Chamamos *determinante* da matriz A (e indicamos por $\det A$) o número que podemos obter operando com os elementos de A da seguinte forma:

1. Se A é de ordem $n=1$, então $\det A$ é o único elemento de A . $A=(a_{11}) \Rightarrow \det A = a_{11}$.

2. Se A é de ordem $n=2$, então $\det A$ é o produto dos elementos da diagonal principal menos o produto dos elementos da diagonal secundária.

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \Rightarrow \det A = a_{11} \cdot a_{22} - a_{12} \cdot a_{21}.$$

3. Se A é de ordem $n=3$, isto é,

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

definimos:

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

Definição 3.9 Seja A uma matriz quadrada de ordem n e seja a matriz M_{ij} de ordem $(n-1)$ obtida de A eliminando-se a linha e a coluna contendo a_{ij} . Definimos o *cofator* Δ_{ij} de a_{ij} por

$$\Delta_{ij} = (-1)^{i+j} \det M_{ij}.$$

Definição 3.10 Seja A uma matriz quadrada de ordem n , chamaremos de *matriz dos cofatores de A* , e denotaremos por \bar{A} , a matriz obtida com a substituição de cada elemento por seu cofator. Ou seja,

$$\bar{A} = \begin{bmatrix} \Delta_{11} & \cdots & \Delta_{1n} \\ \vdots & \ddots & \vdots \\ \Delta_{n1} & \cdots & \Delta_{nn} \end{bmatrix},$$

onde Δ_{ij} é o cofator de a_{ij} da matriz A .

A transposta de \bar{A} é chamada de *matriz adjunta de A* e denotada por $\text{adj}A$. Isto é,

$$\text{adj}A = \begin{bmatrix} \Delta_{11} & \cdots & \Delta_{n1} \\ \vdots & \ddots & \vdots \\ \Delta_{1n} & \cdots & \Delta_{nn} \end{bmatrix}$$

Definição 3.11 (Determinante (caso geral)). O *determinante* de uma matriz A de ordem n , denotado por $\det A$, é um escalar associado à matriz A que é definido indutivamente por

$$\det A = \begin{cases} a_{11}, & \text{se } n = 1 \\ a_{11}\Delta_{11} + a_{12}\Delta_{12} + \cdots + a_{1n}\Delta_{1n}, & \text{se } n > 1 \end{cases}$$

na qual

$$\Delta_{1j} = (-1)^{1+j} \det M_{1j}, j = 1, 2, \dots, n.$$

Teorema 3.1 Se M é uma matriz quadrada de ordem n e $\det M \neq 0$, então a inversa de M é

$$M^{-1} = (\det M)^{-1} \cdot \text{adj}M.$$

Demonstração: Uma solução para o Teorema pode ser encontrada em (Boldrini, 1980).

Exemplo 3.10 Iremos calcular a inversa da matriz $A = \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix}$ utilizando o Teorema 3.1. Inicialmente, verificamos se $\det A \neq 0$, o que, de fato ocorre, já que

$$\det A = 3 \cdot 12 - 5 \cdot 7 = 36 - 35 = 1.$$

Por outro lado, vemos que $(\det A)^{-1} = 1$, uma vez que o inverso de 1 é igual a 1 em \mathbb{Z}_{26} , ou seja, $1 \cdot 1 \equiv 1 \pmod{26}$ (Veja mais sobre o Algoritmo de Euclides em (Alencar Filho, 1981)). A matriz adjunta de A é encontrada calculando a transposta da matriz dos cofatores de A , isto é,

$$\text{Adj}A = (\bar{A})^T = \begin{bmatrix} 12 & -5 \\ -7 & 3 \end{bmatrix}^T = \begin{bmatrix} 12 & 21 \\ 19 & 3 \end{bmatrix}^T = \begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix}.$$

Logo, a matriz inversa de A , segundo o Teorema 3.1, é dada por

$$A^{-1} = 1 \cdot \begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix} = \begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix}.$$

Exemplo 3.11 Devemos calcular a matriz inversa de $A = \begin{bmatrix} 4 & 7 & 9 \\ 5 & 1 & 3 \\ 8 & 7 & 2 \end{bmatrix}$ utilizando o Teorema 3.1.

Primeiramente, calculamos o determinante da matriz dada:

$$\begin{aligned} \det A &= 4 \cdot 1 \cdot 2 + 7 \cdot 3 \cdot 8 + 9 \cdot 5 \cdot 7 - (9 \cdot 1 \cdot 8 + 7 \cdot 5 \cdot 2 + 4 \cdot 7 \cdot 3) \\ &= 8 + 168 + 315 - (72 + 70 + 84) \\ &= 491 - 226 \\ &= 265 \\ &= 5. \end{aligned}$$

Utilizando o Algoritmo de Euclides (ver (Alencar Filho, 1981)), encontramos o inverso do determinante $(\det A)^{-1} = 21$, já que $21 \cdot 5 \equiv 1 \pmod{26}$. Para encontrar a matriz adjunta de A , precisamos primeiro determinar a matriz dos cofatores, ou seja,

$$\begin{aligned} \bar{A} &= \begin{bmatrix} 2 \cdot 1 - 3 \cdot 7 & -(5 \cdot 2 - 3 \cdot 8) & 5 \cdot 7 - 1 \cdot 8 \\ -(7 \cdot 2 - 9 \cdot 7) & 4 \cdot 2 - 9 \cdot 8 & -(4 \cdot 7 - 7 \cdot 8) \\ 7 \cdot 3 - 9 \cdot 1 & -(4 \cdot 3 - 9 \cdot 5) & 4 \cdot 1 - 7 \cdot 5 \end{bmatrix} \\ \bar{A} &= \begin{bmatrix} -19 & 14 & 27 \\ 49 & -64 & 28 \\ 12 & 33 & -31 \end{bmatrix} \\ \bar{A} &= \begin{bmatrix} 7 & 14 & 1 \\ 23 & 14 & 2 \\ 12 & 7 & 21 \end{bmatrix}. \end{aligned}$$

Assim a matriz adjunta, que é a matriz transposta da matriz dos cofatores, é dada por

$$\text{Adj}A = \begin{bmatrix} 7 & 23 & 12 \\ 14 & 14 & 7 \\ 1 & 2 & 21 \end{bmatrix}.$$

Logo, para obter a matriz inversa de A , temos

$$A^{-1} = 21 \cdot \begin{bmatrix} 7 & 23 & 12 \\ 14 & 14 & 7 \\ 1 & 2 & 21 \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} 147 & 483 & 252 \\ 294 & 294 & 147 \\ 21 & 42 & 441 \end{bmatrix}$$

$$A^{-1} = \begin{bmatrix} 17 & 15 & 18 \\ 8 & 8 & 17 \\ 21 & 16 & 25 \end{bmatrix}.$$

CIFRA DE HILL

Nesta seção trataremos do funcionamento da cifra de Hill, importante, porém não tão seguro, método criptográfico para a história da criptografia. Zatti e Beltrame (2006, p. 3) define a cifra de Hill como “uma classe de sistemas poligráficos no qual o texto comum é dividido em conjuntos de n letras, cada um dos quais é substituído por um conjunto de n letras cifradas. As cifras de Hill são baseadas em transformações matriciais”.

Esta cifra foi criada pelo matemático americano Lester Hill, que tinha grande interesse em aplicações matemáticas nas comunicações. Segundo Costa e Caetano (2017, p. 15), a cifra de Hill “contribuiu em larga escala para tornar a criptografia mais algébrica”.



Figura 1 – Lester Hill

Fonte: https://en.wikipedia.org/wiki/Lester_S._Hill

Abaixo será descrito de forma resumida o passo a passo do funcionamento da cifra.

Pré-codificação

Antes da codificação, precisamos fazer a associação das letras no corpo da mensagem com números, que serão agrupados e escritos em forma de matrizes coluna. Essa associação é necessária, pois possibilita os cálculos que faremos mais adiante.

Uma mensagem codificada com uma matriz $n \times n$ é chamada de “ n -cifra de Hill”. Logo, uma mensagem codificada com uma matriz 2×2 é chamada “2-cifra de Hill”. (De Souza, 2017, p. 2)

Para tal associação, utilizaremos a tabela abaixo, que é uma simplificação da tabela ASCII.

LETRA	A	B	C	D	E	F	G	H	I	J	K	L	M
NÚMERO	0	1	2	3	4	5	6	7	8	9	10	11	12
LETRA	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
NÚMERO	13	14	15	16	17	18	19	20	21	22	23	24	25

Tabela 1 – Atribuição de valores

Fonte: (Costa; Caetano, 2017).

Como exemplo, codificaremos a mensagem MATEMATICA. Primeiramente, a dividiremos em grupamentos de duas letras, já que a matriz que será usada como chave de codificação será uma matriz quadrada de ordem 2.

M A – T E – M A – T I – C A

Em seguida, cada letra é substituída pelo número associado a ela na tabela mostrada anteriormente.

12 0 – 19 4 – 12 0 – 19 8 – 2 0

Os grupamentos obtidos são organizados em forma de matrizes coluna e estas serão utilizadas na codificação da mensagem, como abaixo

$$\begin{bmatrix} 12 \\ 0 \end{bmatrix}, \begin{bmatrix} 19 \\ 4 \end{bmatrix}, \begin{bmatrix} 12 \\ 0 \end{bmatrix}, \begin{bmatrix} 19 \\ 8 \end{bmatrix} \text{ e } \begin{bmatrix} 2 \\ 0 \end{bmatrix}.$$

Codificação

Aqui se inicia a codificação da mensagem. Para tal processo será utilizada a matriz

$$\begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix},$$

de ordem 2, e que possui inverso em \mathbb{Z}_{26} , ou seja, existe uma matriz também de ordem 2, tal que o produto entre essas matrizes resulta na matriz identidade em \mathbb{Z}_{26} .

Para codificar os blocos obtidos na pré-codificação, multiplicaremos a matriz utilizada como chave de codificação por cada matriz coluna.

$$\begin{aligned} \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 0 \end{bmatrix} &= \begin{bmatrix} 36 \\ 60 \end{bmatrix} = \begin{bmatrix} 10 \\ 8 \end{bmatrix} \\ \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 4 \end{bmatrix} &= \begin{bmatrix} 85 \\ 143 \end{bmatrix} = \begin{bmatrix} 7 \\ 13 \end{bmatrix} \\ \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 0 \end{bmatrix} &= \begin{bmatrix} 36 \\ 60 \end{bmatrix} = \begin{bmatrix} 10 \\ 8 \end{bmatrix} \\ \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 8 \end{bmatrix} &= \begin{bmatrix} 113 \\ 191 \end{bmatrix} = \begin{bmatrix} 9 \\ 9 \end{bmatrix} \\ \begin{bmatrix} 3 & 7 \\ 5 & 12 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 0 \end{bmatrix} &= \begin{bmatrix} 6 \\ 10 \end{bmatrix}. \end{aligned}$$

Ao fim do processo do processo acima, obtemos as matrizes

$$\begin{bmatrix} 10 \\ 8 \end{bmatrix}, \begin{bmatrix} 7 \\ 13 \end{bmatrix}, \begin{bmatrix} 10 \\ 8 \end{bmatrix}, \begin{bmatrix} 9 \\ 9 \end{bmatrix} \text{ e } \begin{bmatrix} 6 \\ 10 \end{bmatrix},$$

que organizadas em blocos e, em seguida, feita a substituição de cada número por sua respectiva letra, de acordo com a tabela anterior. Por fim, os blocos são agrupados e formam a mensagem codificada.

$$\begin{aligned} 10\ 8 - 7\ 13 - 10\ 8 - 9\ 9 - 6\ 10 \\ KI - HN - KI - JJ - GK \\ KIHNKIJJGK \end{aligned}$$

Decodificação

Em posse da mensagem codificada, o destinatário iniciará o processo de decodificação transformando a mensagem recebida em blocos de duas letras e, em seguida, substituindo cada letra por seu representante numérico utilizando, de novo, a tabela anterior. Por fim, os blocos numéricos são escritos em forma de matrizes.

$$\begin{aligned} KIHNKIJJGK \\ KI - HN - KI - JJ - GK \\ 10\ 8 - 7\ 13 - 10\ 8 - 9\ 9 - 6\ 10 \\ \begin{bmatrix} 10 \\ 8 \end{bmatrix}, \begin{bmatrix} 7 \\ 13 \end{bmatrix}, \begin{bmatrix} 10 \\ 8 \end{bmatrix}, \begin{bmatrix} 9 \\ 9 \end{bmatrix} \text{ e } \begin{bmatrix} 6 \\ 10 \end{bmatrix}. \end{aligned}$$

Feito isso, cada matriz acima será multiplicada à esquerda (esta questão de ordem é pelo simples fato de garantir o produto entre as matrizes de codificação e decodificação, as quais são inversas) pela chave de decodificação, que é a matriz

$$\begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix}$$

inversa em \mathbb{Z}_{26} à que foi utilizada como chave de codificação e que foi encontrada utilizando o Teorema 3.1.

$$\begin{aligned} \begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix} \cdot \begin{bmatrix} 10 \\ 8 \end{bmatrix} &= \begin{bmatrix} 272 \\ 234 \end{bmatrix} = \begin{bmatrix} 12 \\ 0 \end{bmatrix} \\ \begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix} \cdot \begin{bmatrix} 7 \\ 13 \end{bmatrix} &= \begin{bmatrix} 331 \\ 186 \end{bmatrix} = \begin{bmatrix} 19 \\ 4 \end{bmatrix} \\ \begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix} \cdot \begin{bmatrix} 10 \\ 8 \end{bmatrix} &= \begin{bmatrix} 272 \\ 234 \end{bmatrix} = \begin{bmatrix} 12 \\ 0 \end{bmatrix} \end{aligned}$$

$$\begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix} \cdot \begin{bmatrix} 9 \\ 9 \end{bmatrix} = \begin{bmatrix} 279 \\ 216 \end{bmatrix} = \begin{bmatrix} 19 \\ 8 \end{bmatrix}$$

$$\begin{bmatrix} 12 & 19 \\ 21 & 3 \end{bmatrix} \cdot \begin{bmatrix} 6 \\ 10 \end{bmatrix} = \begin{bmatrix} 262 \\ 156 \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 12 \\ 0 \end{bmatrix}, \begin{bmatrix} 19 \\ 4 \end{bmatrix}, \begin{bmatrix} 12 \\ 0 \end{bmatrix}, \begin{bmatrix} 19 \\ 8 \end{bmatrix} \text{ e } \begin{bmatrix} 2 \\ 0 \end{bmatrix}$$

$$12\ 0 - 19\ 4 - 12\ 0 - 19\ 8 - 2\ 0$$

M A - T E - M A - T I - C A

MATEMÁTICA.

Mesmo utilizando matrizes de ordem 2 como chaves de codificação e decodificação, os cálculos apresentam um certo trabalho se forem feitos à mão, o que piora conforme a ordem das matrizes escolhidas vai aumentando. Veremos abaixo mais um exemplo do funcionamento da cifra, agora utilizando matrizes de ordem 3 como chaves de codificação e decodificação. As matrizes utilizadas aqui serão as mesmas vistas no exemplo 3.11.

Pré-codificação

Neste exemplo iremos codificar a mensagem ENSINO MÉDIO usando uma 3-cifra de Hill, já que as matrizes usadas como chaves são de ordem três. Não vamos considerar os acentos e espaços presentes na mensagem e, além disso, será adicionado uma letra O no final para que a divisão em blocos de três letras seja feita de forma exata, sem o risco de alterar o sentido da mensagem. Fazendo as alterações, obtemos

ENSINOMEDIOO

E N S - I N O - M E D - I O O.

Utilizando a Tabela 1 para fazer a mudança das letras pelos respectivos números associados, obtemos

$$4\ 13\ 18 - 8\ 13\ 14 - 12\ 4\ 3 - 8\ 14\ 14.$$

Por fim, reescrevendo os blocos numéricos em forma de matrizes, chegamos a

$$\begin{bmatrix} 4 \\ 13 \\ 18 \end{bmatrix}, \begin{bmatrix} 8 \\ 13 \\ 14 \end{bmatrix}, \begin{bmatrix} 12 \\ 4 \\ 3 \end{bmatrix} \text{ e } \begin{bmatrix} 8 \\ 14 \\ 14 \end{bmatrix}.$$

Concluimos então a pré-codificação.

Codificação

Usaremos aqui a matriz $\begin{bmatrix} 4 & 7 & 9 \\ 5 & 1 & 3 \\ 8 & 7 & 2 \end{bmatrix}$ como chave de codificação, multiplicando-a por cada matriz obtida no processo de pré-codificação. No final, consideraremos o representante de cada classe como sendo um entre 0 e 25, como já mencionado anteriormente.

$$\begin{bmatrix} 4 & 7 & 9 \\ 5 & 1 & 3 \\ 8 & 7 & 2 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 13 \\ 18 \end{bmatrix} = \begin{bmatrix} 269 \\ 87 \\ 159 \end{bmatrix} = \begin{bmatrix} 9 \\ 9 \\ 3 \end{bmatrix}$$

$$\begin{bmatrix} 4 & 7 & 9 \\ 5 & 1 & 3 \\ 8 & 7 & 2 \end{bmatrix} \cdot \begin{bmatrix} 8 \\ 13 \\ 14 \end{bmatrix} = \begin{bmatrix} 249 \\ 95 \\ 183 \end{bmatrix} = \begin{bmatrix} 15 \\ 17 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 4 & 7 & 9 \\ 5 & 1 & 3 \\ 8 & 7 & 2 \end{bmatrix} \cdot \begin{bmatrix} 12 \\ 4 \\ 3 \end{bmatrix} = \begin{bmatrix} 103 \\ 73 \\ 130 \end{bmatrix} = \begin{bmatrix} 25 \\ 21 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 4 & 7 & 9 \\ 5 & 1 & 3 \\ 8 & 7 & 2 \end{bmatrix} \cdot \begin{bmatrix} 8 \\ 14 \\ 14 \end{bmatrix} = \begin{bmatrix} 256 \\ 96 \\ 190 \end{bmatrix} = \begin{bmatrix} 22 \\ 18 \\ 8 \end{bmatrix}$$

Ao fim dos cálculos, obtemos então as matrizes

$$\begin{bmatrix} 9 \\ 9 \\ 3 \end{bmatrix}, \begin{bmatrix} 15 \\ 17 \\ 1 \end{bmatrix}, \begin{bmatrix} 25 \\ 21 \\ 0 \end{bmatrix} \text{ e } \begin{bmatrix} 22 \\ 18 \\ 8 \end{bmatrix}.$$

Estas são reescritas em formas de blocos numéricos e, em seguida, convertidos em letras utilizando a Tabela 1. Por fim, os blocos são reunidos, formando a mensagem codificada, pronta para ser transmitida.

9 9 3 – 15 17 1 – 25 21 0 – 22 18 8
 J J D – P R B – Z V A – W S I
 JJDPRBZVAWSI.

Decodificação

Ao receber a mensagem, o destinatário deve estar em posse da chave de decodificação. Tal chave é a matriz $\begin{bmatrix} 17 & 15 & 18 \\ 8 & 8 & 17 \\ 21 & 16 & 25 \end{bmatrix}$, inversa da matriz utilizada na codificação.

Sabendo que se trata de uma 3-cifra de Hill, o destinatário deve iniciar a decodificação dividindo a mensagem codificada em blocos de três letras e substituindo cada letra pelo representante numérico, de acordo com a Tabela 1.

JJDPRBZVAWSI
 J J D – P R B – Z V A – W S I
 9 9 3 – 15 17 1 – 25 21 0 – 22 18 8.

Os blocos obtidos são reescritos como matrizes, e estas serão multiplicadas pela chave de decodificação.

$$\begin{bmatrix} 9 \\ 9 \\ 3 \end{bmatrix}, \begin{bmatrix} 15 \\ 17 \\ 1 \end{bmatrix}, \begin{bmatrix} 25 \\ 21 \\ 0 \end{bmatrix} \text{ e } \begin{bmatrix} 22 \\ 18 \\ 8 \end{bmatrix}.$$

$$\begin{bmatrix} 17 & 15 & 18 \\ 8 & 8 & 17 \\ 21 & 16 & 25 \end{bmatrix} \cdot \begin{bmatrix} 9 \\ 9 \\ 3 \end{bmatrix} = \begin{bmatrix} 342 \\ 195 \\ 408 \end{bmatrix} = \begin{bmatrix} 4 \\ 13 \\ 18 \end{bmatrix}$$

$$\begin{bmatrix} 17 & 15 & 18 \\ 8 & 8 & 17 \\ 21 & 16 & 25 \end{bmatrix} \cdot \begin{bmatrix} 15 \\ 17 \\ 1 \end{bmatrix} = \begin{bmatrix} 528 \\ 273 \\ 612 \end{bmatrix} = \begin{bmatrix} 8 \\ 13 \\ 14 \end{bmatrix}$$

$$\begin{bmatrix} 17 & 15 & 18 \\ 8 & 8 & 17 \\ 21 & 16 & 25 \end{bmatrix} \cdot \begin{bmatrix} 25 \\ 21 \\ 0 \end{bmatrix} = \begin{bmatrix} 740 \\ 368 \\ 861 \end{bmatrix} = \begin{bmatrix} 12 \\ 4 \\ 3 \end{bmatrix}$$

$$\begin{bmatrix} 17 & 15 & 18 \\ 8 & 8 & 17 \\ 21 & 16 & 25 \end{bmatrix} \cdot \begin{bmatrix} 22 \\ 18 \\ 8 \end{bmatrix} = \begin{bmatrix} 788 \\ 456 \\ 950 \end{bmatrix} = \begin{bmatrix} 8 \\ 14 \\ 14 \end{bmatrix}.$$

Obtém-se, então, as matrizes

$$\begin{bmatrix} 4 \\ 13 \\ 18 \end{bmatrix}, \begin{bmatrix} 8 \\ 13 \\ 14 \end{bmatrix}, \begin{bmatrix} 12 \\ 4 \\ 3 \end{bmatrix} \text{ e } \begin{bmatrix} 8 \\ 14 \\ 14 \end{bmatrix},$$

que são reorganizadas em forma de blocos numéricos, convertidos em letras seguindo a Tabela 1 e reunidas, formando a mensagem original.

4 13 18 – 8 13 14 – 12 4 3 – 8 14 14
 E N S – I N O – M E D – I O O
 ENSINOMEDIOO.

Apesar do relativo trabalho, a cifra de Hill hoje não apresenta um satisfatório nível de segurança, principalmente contra ataques computacionais. Neste artigo não trataremos da quebra dessa cifra, esse tema pode ser visto em (Stallings, 2015).

CONSIDERAÇÕES FINAIS

É importante procurar meios para que o ensino da matemática, independentemente do nível de ensino, seja feito de modo que o aluno veja com bons olhos o que é apresentado. O uso de abordagens alternativas torna o ensino mais produtivo, fazendo com que a absorção dos conceitos por parte dos alunos seja mais satisfatória.

A cifra de Hill demonstra o quão variado pode ser a utilização matemática em métodos criptográficos. A álgebra e teoria dos números, apesar de ramos distintos, são facilmente abordados em conjunto, abrindo espaço também para as adaptações que venham a ser necessárias para a abordagem da cifra em sala de aula.

Cada vez mais utilizada em meios digitais, a criptografia se torna mais importante a cada dia que passa, e um estudo sobre ela ainda durante o ensino fundamental e médio se faz necessário para que se crie uma familiaridade com a temática, oferecendo novas possibilidades de abordagem de diversos conteúdos e a interdisciplinaridade.

A produção deste artigo possibilitou um estudo mais aprofundado sobre a matemática por trás do funcionamento da cifra de Hill, além do estudo sobre o ensino de matrizes e seus desafios. Do ponto de vista acadêmico, agregou mais conhecimento sobre a área abordada. Do ponto de vista pessoal, enriqueceu a vivência no campo da produção científica, oferecendo novas possibilidades de crescimento como profissional da educação.

REFERÊNCIAS

- ALENCAR FILHO, Edgar de. Teoria elementar dos números. São Paulo: Nobel, 1981.
- BOLDRINI, José Luiz *et al.* Álgebra linear. 3. ed. São Paulo: Harper & Row do Brasil, 1980.
- BRASIL, Ministério da Educação, Secretaria de Educação Média e tecnológica. Parâmetros Curriculares Nacionais: ensino médio. Brasília: Ministério da Educação, 1999.
- BURTON, David M. Teoria elementar dos números. Tradução: Gabriela dos Santos Barbosa. 7. ed. Rio de Janeiro: LTC, 2016. ISBN 978-85-216-2925-2.
- COSTA, Edson Marques; CAETANO, Natalia Gonçalves. Criptografia com Utilização de Cifra de Hill e Cifra Afim. Matemática e Estatística em Foco. v. 5. p. 14 – 21. jul. 2017.
- DA CUNHA, Jussileno Souza; DA SILVA, José Adgerson Victor. A importância das atividades lúdicas no ensino da Matemática. 2012. Disponível em: https://www.ufsm.br/app/uploads/sites/534/2020/03/RE_Cunha_Jussileno.pdf. Acesso em 23 mai. 2022.
- DASILVA, Jonas Laranjeira Saraiva *et al.* Matemática lúdica ensino fundamental e médio. 2013. Disponível em: http://portal.unisepe.com.br/unifia/wp-content/uploads/sites/10001/2018/06/3matematica_ludica.pdf. Acesso em 23 mai. 2022.
- DE SOUZA, Maycon Pereira. Cifra de Hill. Revista CTS IFG. v. 1, n. 2, 2017. Disponível em: http://cts.luziania.ifg.edu.br/index.php/CTS1/article/view/100/pdf_30. Acesso em 16 mai. 2022.
- DOMINGUES, Hygino H.; IEZZI, Gelson. Álgebra moderna. 4. ed. São Paulo: Atual, 2003. ISBN 978-85-357-0401-3.
- GONÇALVES, Adilson. Introdução à álgebra. 5. ed. Rio de Janeiro: IMPA, 2013. ISBN 978-85-0108-4.
- IEZZI, Gelson; HAZZAN, Samuel. Fundamentos de matemática elementar. v. 4. 2. ed. São Paulo: Atual, 1977.
- LEON, Steven J. Álgebra linear com aplicações. Tradução: Sérgio Gilberto Taboada. 8. ed. Rio de Janeiro: LTC, 2014 ISBN 978-85-216-1769-3.
- SANTOS, José Plínio de Oliveira. Introdução à Teoria dos Números. 3. ed. Rio de Janeiro: IMPA, 2015. ISBN 978-85-244-0142-8.
- SINGH, Simon. O livro dos códigos: A ciência do Sigilo – do antigo Egito à criptografia quântica. Tradução: Jorge Calife. 3. ed. Rio de Janeiro: Record, 2003. ISBN 85-01-05598-0.
- SKOVSMOSE, Ole. Cenários para investigação. Bolema-Boletim de Educação Matemática, v. 13, n. 14, p. 66-91, 2000. Disponível em: <https://www.periodicos.rc.biblioteca.unesp.br/index.php/bolema/article/view/10635>. Acesso em 22 mai. 2022.
- STALLINGS, Willian. Criptografia e segurança de redes. Tradução: Daniel Vieira. 6. ed. São Paulo: Pearson Education do Brasil, 2015. ISBN 978-85-430-1450-0.
- ZATTI, Sandra Beatriz; BELTRAME, Ana Maria. A presença da álgebra linear e teoria dos números na criptografia. 2009. Disponível em: <https://docplayer.com.br/4947507-A-presenca-da-algebra-linear-e-teoria-dos-numeros-na-criptografia-sandra-beatris-zatti-1-ana-maria-beltrame-2.html>. Acesso em 14 mai. 2022.