Revista ARACÊ
ISSN: 2358-2472

O USO DA CRIPTOGRAFIA COMO FERRAMENTA PEDAGÓGICA

THE USE OF CRYPTOGRAPHY AS AN EDUCATIONAL TOOL

EL USO DE LA CRIPTOGRAFÍA COMO HERRAMIENTA PEDAGÓGICA

https://doi.org/10.56238/arev7n12-112

Data de submissão: 11/11/2025 **Data de publicação:** 11/12/2025

Valéria C. Brum
Doutora em Matemática
Instituição: Universidade Federal de Santa Maria (UFSM)
E-mail: valeriacardosobrum@gmail.com
Orcid: https://orcid.org/0000-0003-2766-4598
Lattes: https://lattes.cnpq.br/7057570207918370

Igor Godoy Borges
Mestre em Matemática
Instituição: Colégio Estadual Coronel Pilar de Santa Maria
E-mail: igorgodoy@yahoo.com.br
Orcid: https://orcid.org/0009-0007-6793-1714
Lattes: https//lattes.cnpq.br/1688699076561554

RESUMO
O presente artigo trata da aplicação de uma sequência didática inovadora sobre criptografia, com a turma 312 do Colégio Estadual Coronel Pilar de Santa Maria, e as suas relações com a Matemática. Buscamos desenvolver atividades usando conceitos matemáticos, tais como, operações com matrizes, matriz in- versa, determinantes e aritmética modular. A crescente relevância da criptografia no mundo digital contemporâneo motiva a necessidade de sua inclusão nos currículos escolares, preparando os alunos para os desafios da segurança de informação. O objetivo central é tornar o conceito de criptografia acessível e estimulador para os alunos, promovendo o desenvolvimento do pensamento crítico e habilidades na resolução de problemas.

Palavras-chave: Matrizes. Criptografia. Ensino Médio.

ABSTRACT
This article discusses the application of an innovative teaching sequence on cryptography with class 312 at Colégio Estadual Coronel Pilar de Santa Maria, and its relationship with mathematics. We sought to develop activities using mathematical concepts such as matrix operations, inverse matrices, determinants, and modular arithmetic. The growing relevance of cryptography in the contemporary digital world motivates the need for its inclusion in school curricula, preparing students for the challenges of information security. The central objective is to make the concept of cryptography accessible and stimulating for students, promoting the development of critical thinking and problem-solving skills.

Keywords: Matrices. Cryptography. High School.

Revista ARACÊ
ISSN: 2358-2472

RESUMEN
El presente artículo trata sobre la aplicación de una secuencia didáctica innovadora sobre criptografía, con la clase 312 del Colegio Estatal Coronel Pilar de Santa Maria, y sus relaciones con las matemáticas. Buscamos desarrollar actividades utilizando conceptos matemáticos, tales como operaciones con matrices, matriz inversa, determinantes y aritmética modular. La creciente relevancia de la criptografía en el mundo digital contemporáneo motiva la necesidad de su inclusión en los planes de estudio escolares, preparando a los alumnos para los retos de la seguridad de la información. El objetivo central es hacer que el concepto de criptografía sea accesible y estimulante para los alumnos, promoviendo el desarrollo del pensamiento crítico y las habilidades para la resolución de problemas.

Palabras clave: Matrices. Criptografía. Educación Secundaria.

Revista ARACÊ
ISSN: 2358-2472

1 INTRODUÇÃO

Um dos grandes desafios do professor de matemática e tornar suas aulas atrativas de maneira que o aluno compreenda conceitos abstratos que podem ser difíceis de entender sem uma base sólida no pensamento crítico e analítico. O uso da Criptografia como ferramenta pedagógica no ensino de Álgebra Linear no ensino médio pode ser uma abordagem inovadora e atrativa, pois consegue aguçar o interesse e a curiosidade dos alunos. Os alunos têm a oportunidade de ver aplicações práticas da Álgebra Linear em segurança e tecnologia que fazem parte da vida cotidiana moderna, além disso desenvolvem habilidades na resolução de problemas, já que muitos problemas criptográficos exigem um alto grau de raciocínio lógico e habilidade analítica. Este trabalho foi aplicado com a turma 312 do Colégio Estadual Coronel Pilar de Santa Maria.

2 OBJETIVOS GERAIS E ESPECIFÍCOS

Esse trabalho tem como objetivo geral capacitar os alunos a compreenderem os conceitos básicos de criptografia e sua importância na segurança de informação e como objetivos específicos introduzir o conceito de criptografia, incluindo o Método de Hill e demonstrar através de exemplos práticos como a criptografia é utilizada na proteção de dados.

3 CRIPTOGRAFIA

Em grego, Cryptos significa secreto oculto. A criptografia estuda métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la.

3.1 UM POUCO DE HISTÓRIA DA CRIPTOGRAFIA

Um dos primeiros registros da criptografia vem de 1900 a.C., quando um escriba substituiu algumas palavras de um hieróglifo a fim de proteger a mensagem de algum ladrão e impedir seu acesso a tesouros escondidos. Por volta de 50 a.C., Júlio César utilizou a cifra de substituição para proteger comunicações governamentais; atualmente, o método é conhecido como Cifra de César. Durante a Idade Média, sistemas de criptografia mais complexos, como a cifra de Vigenère, que utiliza uma chave de repetição para realizar substituições variadas, começaram a surgir. O século XX, no período das guerras mundiais, trouxe avanços significativos com a introdução de máquinas como a Enigma, usada pelas forças alemãs. Em 1929, um matemático americano de nome Lester S. Hill apresentou um dos primeiros exemplos de criptografia baseada em álgebra linear, particularmente utilizando matrizes, o que representou um avanço significativo em relação às técnicas de substituição

Revista ARACÊ
ISSN: 2358-2472

monoalfabética e polialfabéticas até então utilizadas. O cenário da criptografia mudou drasticamente com a chegada dos computadores. O método de cifrar e decifrar evoluiu para técnicas mais avançadas, como o DES (Data Encryption Standard) e o AES (Advanced Encryption Standard).

3.2 CIFRA DE CÉSAR

A cifra de César consiste em substituir cada letra da mensagem original por outra que estivesse 3 posições à frente no mesmo alfabeto, conforme Tabela 1

Tabela 1: Cifra de César

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

Fonte: Elaborada pelos autores.

Assim a mensagem AMO MATEMÁTICA seria codificada como DPRPDWHPD-WLFD.

A cifra de César se enquadra como cifra de substituição monoalfabética e embora simples se tornou indecifrável por séculos.

3.3 CIFRA DE VIGENERE

É uma cifra de substituição polialfabética. Utiliza 26 alfabetos diferentes para cifrar uma mensagem conforme figura 1.

Embora a cifra de Vigenere seja mais difícil de ser decifrada, qualquer código que envolva substituir uma letra sistematicamente por outra é relativamente fácil de ser quebrada. Isso ocorre porque a frequência média com que cada letra aparece em um texto de uma determinada língua e mais ou menos constante. Por exemplo, a frequência média na língua portuguesa da letra A é 14, 64 por cento. Existem várias maneiras de tornar inviável a aplicação de uma contagem de frequência. A mais simples é a Criptografia em Blocos dada a seguir.

Revista ARACÊ
ISSN: 2358-2472

3.4 CRIPTOGRAFIA EM BLOCOS

Esse método consiste em dividirmos uma mensagem em blocos de várias letras e embaralharmos esses blocos. Por exemplo a mensagem AMO MATEMÁTICA pode ser codificada usando os seguintes passos: passo 1. Elimine os espaços entre as palavras e complete a mensagem com A no final, caso tenha uma quantidade ímpar de letras;

AMOMATEMATICAA

Passo 2: divida a mensagem em blocos de 2 letras;

AM-OM-AT-EM-AT-IC-AA

Figura 1: Cifra de Vegenere

	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
01	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
02	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
03	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
04	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
05	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
06	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
07	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
08	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
09	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Fonte: Wikipedia.

Revista ARACÊ
ISSN: 2358-2472

Passo 3: em cada bloco permute as letras de lugar;

MA-MO-TA-ME-TA-CI-AA

Passo 4: fixe os blocos pares e permute os blocos impares, trocando o primeiro pelo último, o terceiro pelo penúltimo e assim sucessivamente.

AA-MO-TA-ME-TA-CI-MA

O que nos dá a mensagem AAMOTAMETACIMA

Existe um m´método de criptografia chamado Cifra de Hill que são baseados em transformações matriciais. Esse m´método foi inventado pelo matemático norte americano Lester S. Hill em 1929. Uma mensagem codificada com uma matriz *nxn* é denominada *n*− cifra de Hill.

Para estudarmos esse método, vamos primeiramente rever alguns conceitos matemáticos, tais como matrizes, matrizes invertíveis e aritmética modular.

3.5 FUNDAMENTAÇÃO MATEMÁTICA

3.5.1 Matriz

Definição 1: Chama-se matriz *m* por *n* com entradas nos números reais, toda tabela *A* formada por números reais distribuidos em *m* linhas e *n* colunas. Usamos a seguinte notação A_{mxn}

$$A_{mxn} = \begin{pmatrix} a_{11} & a_{12} \dots & a_{1n} \\ a_{21} & a_{22} \dots & a_{2n} \\ a_{m1} & a_{m2} \dots & a_{mn} \end{pmatrix} = [a_{ij}]_{mxn} \quad (1)$$

Revista ARACÊ
ISSN: 2358-2472

Definição 2: Uma matriz cujo o número de linhas é igual ao número de colunas chama-se Matriz Quadrada.

$$A_{nxn} = \begin{pmatrix} a_{11} & a_{12} \dots & a_{1n} \\ a_{21} & a_{22} \dots & a_{2n} \\ a_{n1} & a_{n2} \dots & a_{nn} \end{pmatrix} \quad (2)$$

Definição 3: Uma matriz quadrada onde $a_{ij} = 0 \text{ para } i \neq j$ é denominada Matriz Diagonal

$$A_{nxn} = \begin{pmatrix} a_{11} & 0 \dots & 0 \\ 0 & a_{22} \dots & 0 \\ 0 & 0 \dots & a_{nn} \end{pmatrix} \quad (3)$$

Definição 4: Uma matriz quadrada de ordem nxn onde$a_{ij} = 0 \text{ para } i \neq j$ e $a_{ij} = 1 \text{ para } i = j$ é denominada Matriz Identidade denotada por I_n

$$I_n = \begin{pmatrix} 1 & 0 \dots & 0 \\ 0 & 1 \dots & 0 \\ 0 & 0 \dots & 1 \end{pmatrix} \quad (4)$$

3.5.2 Operações com matrizes

3.5.2.1 Adição

Definição 5: Dadas duas matrizes $A = [a_{ij}]_{mxn}$ e $B = [b_{ij}]_{mxn}$ Chama-se soma $A + B$ a matriz $C = [c_{ij}]_{mxn}$, onde $c_{ij} = a_{ij} + b_{ij}$

Exemplo: Sejam as matrizes

$$A = \begin{pmatrix} 2 & -1 \\ 1 & 3 \end{pmatrix} \text{ e } B = \begin{pmatrix} 0 & 3 \\ -2 & 1 \end{pmatrix}. \quad (5)$$

Revista ARACÊ
ISSN: 2358-2472

Então a matrix $C = A + B$ é dada por $C = \begin{pmatrix} 2 & 2 \\ -1 & 4 \end{pmatrix}$ (6)

3.5.2.1 Multiplicação por um escalar:

Definição 6: Sejam $A = [a_{ij}]_{mxn}$ e $K \in \mathbb{R}$. Definimos o produto kA como a matriz $B = [b_{ij}]_{mxn}$ tal que $b_{ij} = ka_{ij}$

Exemplo: Seja $A = \begin{pmatrix} 1 & 0 & -2 \\ 4 & -1 & 0 \\ 2 & 1 & 1 \end{pmatrix}$. A matriz $3A = \begin{pmatrix} 3 & 0 & -6 \\ 12 & -3 & 0 \\ 6 & 3 & 3 \end{pmatrix}$ (7)

A multiplicação por um escalar possui as seguintes propriedades:

Sejam A e B matrizes de ordem mxn e $k_1, k_2 \in \mathbb{R}$. Então valem

$i.\ k_1(A + B) = k_1A + k_1B$

$ii.\ (k_1 + k_2)A = k_1A + k_2A$

$iii.\ k_1(k_2A) = (k_1k_2)A\text{b}$ (8)

3.5.3 Multiplicação de matrizes

Definição 7: Dadas as matrizes $A = [a_{ij}]_{mxn}$ e $B = [b_{jk}]_{nxp}$, chama-se produto de A por B a matriz $C = [c_{ik}]_{mxp}$ tal que para cada i = 1,2,..., m temos que

$$c_{ik} = a_{i1}b_{1k} + a_{i2}.b_{2k} + \ldots + a_{in}b_{nk} = \sum_{j=1}^{n} a_{ij}b_{jk} \quad (9)$$

Exemplo: Sejam as matrizes $A = \begin{pmatrix} 2 & -1 \\ 1 & 3 \end{pmatrix}$ e $B = \begin{pmatrix} 0 & 3 \\ -2 & 1 \end{pmatrix}$. (10)

Revista ARACÊ
ISSN: 2358-2472

Então a matriz $C = A.B$ é dada por $C = \begin{pmatrix} 2 & 5 \\ -6 & 6 \end{pmatrix}$ O produto entre matrizes possui as seguintes propriedades:

i. $k_1(A + B) = k_1A + k_1B$ (11)

ii. $(k_1 + k_2)A = k_1A + k_2A$ (12)

iii. $k_1(k_2A) = (k_1k_2)Ab$ (13)

O produto entre matrizes não é comutativo, ou seja, em geral $AB \neq BA$

Definição 8: Uma matriz quadrada A de ordem n é dita invertível, se existe uma matriz B de ordem n tal que $AB = BA = I_n$.

Neste caso dizemos que a matriz B é matriz inversa de A e denotamos por $B = A^{-1}$

3.6 DETERMINANTE

Definição 9: Seja A uma matriz quadrada de ordem n; $(n \leq 3)$. Chamamos de determinante de A, $detA$, o número real obtido operando com os elementos de A da seguinte forma:

1) Se A é de ordem $n = 1$, $A = [a_{11}]$ então $detA = a_{11}$ (14)

2) Se A é de ordem $n = 2$, $A = [a_{ij}]_{2x2}$ então $detA = a_{11}a_{22} - a_{12}a_{21}$ (15)

3) Se A é de ordem $n = 3$, $A = [a_{ij}]_{3x3}$ então $detA = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{21}a_{32}a_{13} - (a_{13}a_{22}a_{31} + a_{12}a_{21}a_{33} + a_{32}a_{23}a_{11})$ (16)

Exemplo: Seja $A = \begin{pmatrix} 1 & 0 & -2 \\ 4 & -1 & 0 \\ 2 & 1 & 1 \end{pmatrix}$ então $detA = 1(-1)1+4(1)(-2)-(-2(-1)2 = -13$ (17)

O determinante de uma matriz satisfaz, dentre outras, as seguintes propriedades:

i. Se todos os elementos de uma linha ou coluna de uma matriz A são nulos, então $detA =$

Revista ARACÊ
ISSN: 2358-2472

0

ii. Se trocarmos de posição duas linhas de uma matriz o determinante muda de sinal

iii. $de(AB) = detAdetB$

iv. $de(A + B) \not= detA + detB$

Teorema 1: Uma matriz quadrada A é invertível se, e somente se, $detA \neq 0$

4 ARITMÉTICA MODULAR

Definição 10: Seja m um número inteiro maior que 1. Dizemos que dois inteiros, a e b, são congruentes(ou equivalentes) módulo m e escrevemos $a \equiv b(mod\ m)$ se a e b posuirem o mesmo resto quando divididos por m. Por exemplo:

$7 \equiv 2(mod\ 5)$, pois os restos da divisão de 7 e 2 por 5 são os mesmos (iguais a 2) $15 \equiv 3(mod\ 3)$, pois os restos da divisão de 15 e 3 por 3 são os mesmos (iguais a 0).

Para mostrar que $a \equiv b(mod\ m)$ não é necessário fazer a divisão de a e de b por m, como veremos na seguinte proposição.

Proposição: Tem-se que $a \equiv b(mod\ m)$ se, e somente se, $a - b$ é um multi- plo de m.

Por exemplo, $15 \equiv 3(mod\ 3)$, pois 15-3=12 é multiplo de 3.

Dado um módulo m, pode ser provado que qualquer inteiro a é congruente módulo m a exatamente um dos inteiros $0, 1, 2, \ldots, m$.

Esse conjunto é chamado de res´ıduo de a módulo m. Denotamos o conjunto de res´ıduos de a módulo m por

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m - 1\} \quad (18)$$

Teorema 2: Dado um número inteiro a e um módulo m quaisquer, seja

$$R = \text{resto de } \frac{|a|}{m} \quad (19)$$

Revista ARACÊ
ISSN: 2358-2472

Então o resíduo r de a módulo m é dado por

$$r = \begin{cases} R & \text{se } a \geq 0 \\ m - R & \text{se } a < 0 \text{ e } R \neq 0 \\ 0, & \text{se } a < 0 \text{ e } R = 0 \end{cases} \quad (20)$$

Exemplos: Encontre os resíduos módulo 26 dos seguintes números:

a) $43\ R =$ resto de $\frac{|43|}{26} = 17 \Rightarrow r = 17$. Assim $43 \equiv 17(mod\ 26)$ (21)

b) $79\ R =$ resto de $\frac{|-79|}{26} = 1 \Rightarrow r = 26 - 1 = 25$. Assim $-79 \equiv 25(mod\ 26)$ (22)

c) $26\ R =$ resto de $\frac{|-26|}{26} = 0 \Rightarrow r = 0$. Assim $-26 \equiv 0(mod\ 26)$ (23)

Definição 11**:** Seja $a \in Z_m$. Dizemos que $a^{-1} \in Z_m$ é um recíproco, ou inverso multiplicativo de a módulo m, se $aa^{-1} = a^{-1}a = 1(mod\ m)$

Teorema 3: Se a e m não tem fatores primos comuns, então a tem um único recíproco módulo m, caso contrário a não tem recíproco módulo m.

Por exemplo, o número 3 tem recíproco módulo 26, pois 3 e 26 não tem fatores primos comuns.

O recíproco é um número $x \in Z_{26}$ que satisfaz a equação modular

$$3x = 1(mod\ 26) \quad (24)$$

Iremos atribuir alguns números de 0 a 25 a fim de encontrar a solução x. Assim obtemos $x = 9$.

$$3 \cdot 9 = 27 \equiv 1(mod\ 26) \quad (25)$$

Para referência futura, fornecemos a tabela de recíprocos módulo 26 (Tabela 2)

Revista ARACÊ
ISSN: 2358-2472

Tabela 2: Resíduos módulo 26

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Fonte: Elaborada pelos autores.

Seja *A* a matriz codificadora. A fim de decifrar as Cifras de Hill, vamos estudar o conceito de matriz inversa (*mod* 26) da matriz codificadora *A*.

Definição 12: Sejam *m* um número inteiro positivo e *A* uma matriz quadrada com entrada em Z_m. Dizemos que *A* é invertível módulo *m* se existe uma matriz *B* com entradas em Z_m tal que

$$A \cdot B = B \cdot A = I(mod\ m) \qquad (26)$$

Teorema 4: Uma matriz quadrada *A* com entradas em Z_m é nvert´ıvel mó dulo *m* se, e somente se, o resíduo *detA* modulo *m* tem recíproco módulo *m*.

Note que *detA* módulo *m* terá recíproco módulo *m* se, e somete se, este resíduo e *m* não tiverem fatores primos em comum.

Como os únicos fatores primos de 26 são 2 e 13, temos que *detA*(*mod* 26) terá recíproco (mod 26) se não for divisível por 2 ou 13.

Podemos obter a inversa módulo *m* de uma matriz

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ por}$$

$$A^{-1} = (detA)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} (mod\ m) \qquad (28)$$

Exemplo: Encontre a inversa de *A* módulo 26 se $A = \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}$ (29)

Solução: $detA = 15 - 12 = 3 \Rightarrow (detA)^{-1} = 3^{-1} = 9(mod\ 26)$ conforme Tabela 1.

$$\text{Assim } A^{-1} = 9 \begin{pmatrix} 3 & -6 \\ -2 & 5 \end{pmatrix} = \begin{pmatrix} 27 & -54 \\ -18 & 45 \end{pmatrix} \qquad (30)$$

Revista ARACÊ
ISSN: 2358-2472

Cálculo dos resíduos módulo 26:

$$\begin{aligned} R &= \text{resto de } \frac{|27|}{26} = 1 \Rightarrow r = 1 \\ R &= \text{resto de } \frac{|-54|}{26} = 2 \Rightarrow r = 26 - 2 = 24 \\ R &= \text{resto de } \frac{|-18|}{26} = 18 \Rightarrow r = 28 - 18 = 8 \\ R &= \text{resto de } \frac{|19|}{26} = 19 \Rightarrow r = 19 \end{aligned} \quad (31)$$

Então

$$A^{-1} = \begin{pmatrix} 1 & 24 \\ 8 & 19 \end{pmatrix} (mod\ 26) \quad (32)$$

Conferindo:

$$AA^{-1} = \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 24 \\ 8 & 19 \end{pmatrix} = \begin{pmatrix} 53 & 234 \\ 26 & 105 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (mod\ 26) \quad (33)$$

Em posse desses conceitos matemáticos, podemos agora estudar o método de criptografia denominado Cifras de Hill

4.1 CIFRAS DE HILL

A partir daqui vamos supor que cada letra do texto comum ou texto cifrado tenha um correspondente numérico que especifica sua posição no alfabeto padrão, com exceção da letra Z cujo correspondente numérico será o número 0, conforme Tabela 3

Tabela 3: Cifra de Hill

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	0

Fonte: Elaborada pelos autores.

Revista ARACÊ
ISSN: 2358-2472

Exemplo 1: Use a Cifra de Hill para codificar e descodificar a mensagem ALUNO utilizando a matriz codificadora *A* com entradas em Z_{26}

$$A = \begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix} \quad (34)$$

4.2 PROCESSO DE CODIFICAÇÃO:

Passo 1) Separar a palavra em pares de letras. Caso o número de letras seja ímpar, repita a última letra:

AL - UN - OO

Passo 2) Use a Tabela 3 para obter o equivalente numérico e obtenha os vetores cifrados:

1 12 - 21 14 - 15 15

$$p_1 = \begin{pmatrix} 1 \\ 12 \end{pmatrix} \quad p_2 = \begin{pmatrix} 21 \\ 14 \end{pmatrix} \quad p_3 = \begin{pmatrix} 15 \\ 15 \end{pmatrix} \quad (35)$$

Passo 3) fazer o produto da matriz codificadora A pelos vetores cifrados, ou seja, determinar Ap1, Ap2, Ap3.

Sempre que um número inteiro for maior que 25 ele será substituído pelo resíduo r.

$$Ap_1 = \begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} 1 \\ 12 \end{pmatrix} = \begin{pmatrix} 14 \\ 63 \end{pmatrix} = \begin{pmatrix} 14 \\ 11 \end{pmatrix} \ (mod\ 26)$$

$$Ap_2 = \begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} 21 \\ 14 \end{pmatrix} = \begin{pmatrix} 56 \\ 133 \end{pmatrix} = \begin{pmatrix} 4 \\ 3 \end{pmatrix} \ (mod\ 26)$$

$$Ap_3 = \begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} 15 \\ 15 \end{pmatrix} = \begin{pmatrix} 45 \\ 120 \end{pmatrix} = \begin{pmatrix} 19 \\ 16 \end{pmatrix} \ (mod\ 26) \quad (36)$$

Revista ARACÊ
ISSN: 2358-2472

Usando a Tabela 3 obtemos a mensagem cifrada:

NKDCSP

Agora vamos para o processo de descodificação da mensagem codificada recebida NKDCSP.

4.3 PROCESSO DE DESCODIFICAÇÃO:

Passo 1) Separar a mensagem cifrada recebida em pares de letras:

NK - DC - SP

Passo 2) Use a Tabela 3 para obter o equivalente numérico e obtenha os vetores cifrados: 14 11 - 4 3 - 19 16

$$v_1 = \begin{pmatrix} 14 \\ 11 \end{pmatrix} \quad v_2 = \begin{pmatrix} 4 \\ 3 \end{pmatrix} \quad v_3 = \begin{pmatrix} 19 \\ 16 \end{pmatrix} \tag{37}$$

Passo 3) Encontre a matriz inversa módulo 26 de A

$$A^{-1} = (detA)^{-1} \begin{pmatrix} 5 & -1 \\ -3 & 2 \end{pmatrix} (mod\ 26) = 7^{-1} \begin{pmatrix} 5 & -1 \\ -3 & 2 \end{pmatrix} (mod\ 26), \tag{38}$$

onde $7^{-1} = 15$ é o inverso módulo 26 de 7 dado na tabela 1.

Então

$$A^{-1} = 15 \begin{pmatrix} 5 & -1 \\ -3 & 2 \end{pmatrix} = \begin{pmatrix} 75 & -15 \\ -45 & 30 \end{pmatrix} = \begin{pmatrix} 23 & 11 \\ 7 & 4 \end{pmatrix} (mod\ 26) \tag{39}$$

Passo 4) Multiplicar a matriz A^{-1} pelos vetores cifrados v_1, v_2 e v_3

Revista ARACÊ
ISSN: 2358-2472

$$A^{-1}v_1 = \begin{pmatrix} 23 & 11 \\ 7 & 4 \end{pmatrix}\begin{pmatrix} 14 \\ 11 \end{pmatrix} = \begin{pmatrix} 443 \\ 142 \end{pmatrix} = \begin{pmatrix} 1 \\ 12 \end{pmatrix} (mod\ 26)$$

$$A^{-1}v_2 = \begin{pmatrix} 23 & 11 \\ 7 & 4 \end{pmatrix}\begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 125 \\ 40 \end{pmatrix} = \begin{pmatrix} 21 \\ 14 \end{pmatrix} (mod\ 26)$$

$$A^{-1}v_3 \begin{pmatrix} 23 & 11 \\ 7 & 4 \end{pmatrix}\begin{pmatrix} 19 \\ 16 \end{pmatrix} = \begin{pmatrix} 613 \\ 197 \end{pmatrix} = \begin{pmatrix} 15 \\ 15 \end{pmatrix} (mod\ 26) \quad (40)$$

Pela Tabela 3 , os equivalentes alfabéticos destes vetores são:

AL UN OO

Que nos fornecem a mensagem ALUNO

5 SEQUÊNCIA DIDÁTICA E APLICAÇÃO

5.1 AULA 1: INTRODUÇÃO AO CONCEITO DE CRIPTOGRAFIA.

Nesta aula foi dado uma introdução ao conceito de criptografia, contexto hist´orico e sua importância na segurançaa de informações. Foi exibido um exemplo da criptografia utilizando Cifra de César, relacionando as letras do alfabeto com números de 1 a 26. Além disso foi introduzida a Cifra de Hill, demonstrando sua aplicação prática.

5.2 AULA 2: REVISÃO DE CONCEITOS BÁSICOS DE MATRIZES E OPERAÇÕES MATRICIAIS

Nesta aula foi realizado uma revisão dos conceitos de matrizes incluindo:

- Definição de matriz
- Tipos especiais de matrizes tais como: Matriz quadrada, matriz identidade, matriz nula, matriz triangular
- Igualdade de matrizes
- Adição de matrizes
- Produto de matrizes por um escalar

A aula foi concluída com exercícios de fixação para reforçar a compreensão dos alunos.

Revista ARACÊ
ISSN: 2358-2472

5.3 AULA 3. REVISÃO DO CONCEITO DE PRODUTO DE MATRIZES

Nesta etapa foi abordado o produto de matrizes, condições para a existência do produto. Foram discutidas as propriedades do produto de matrizes, como a não comutatividade e a associatividade. A aula foi concluída com exercícios de fixação para consolidar seu entendimento.

5.4 AULA 4. REVISÃO DO CONCEITO DE MATRIZ INVERSA

Nesta aula foi apresentada a definição de matriz invertível e um método para calcular a matriz inversa de uma matriz A, denotada por A^{-1}. Ao final da aula foi dada uma matriz A invertível para os alunos determinarem sua inversa A^{-1}.

5.5 AULA 5. REVISÃO DO CONCEITO DE DETERMINANTE E ASSOCIATIVIDADE NA MULTIPLICAÇÃO DE MATRIZES

Nesta aula foi apresentada uma introdução aos conceitos de determinante de ordem 2 e ordem 3, com o objetivo de utilizar um método prático para deter- minar a matriz inversa. Além disso foi revisado a propriedade associativa na multiplicação de matrizes para entender porque a criptografia de Hill funciona.

5.6 AULA 6. APRESENTAÇÃO DA ARITMÉTICA MODULAR

Nesta etapa foi introduzido o conceito de aritmética modular fundamental para a criptografia. Os alunos aprenderam a realizar operações aritméticas dentro de um módulo específico, o que é essencial para a codificação e decodificação de mensagens. Foi dado como exercício para os alunos, com o auxílio do professor, fazerem a codificação e descodificação da palavra ALUNO, dada no Exemplo 1, deste artigo.

5.7 AULA 7. ATIVIDADE EM GRUPO

Foi elaborada a seguinte atividade: Usar a Cifra de Hill para codificar e descodificar a mensagem SAUDE utilizando a matriz codificadora A com entradas em $\mathbb{Z}_{26}$

$$A = \begin{pmatrix} 2 & 5 \\ 1 & 4 \end{pmatrix} \qquad (41)$$

Revista ARACÊ
ISSN: 2358-2472

5.8 PROCESSO DE CODIFICAÇÃO:

Passo 1) Separar a palavra em pares de letras. Caso o número de letras seja ímpar, repita a última letra:

SA - UD - EE

Passo 2) Use a Tabela 2 para obter o equivalente numérico e obtenha os vetores cifrados:

19 1 - 21 4 - 5 5

$$p_1 = \begin{pmatrix} 19 \\ 1 \end{pmatrix} \quad p_2 = \begin{pmatrix} 21 \\ 4 \end{pmatrix} \quad p_3 = \begin{pmatrix} 5 \\ 5 \end{pmatrix} \tag{42}$$

Passo 3) fazer o produto da matriz codificadora *A* pelos vetores cifrados, ou seja, determinar Ap_1, Ap_2, Ap_3.

Sempre que um número inteiro for maior que 25 ele será substituído pelo resíduo *r*.

$$\begin{pmatrix} 2 & 5 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 19 \\ 1 \end{pmatrix} = \begin{pmatrix} 43 \\ 23 \end{pmatrix} = \begin{pmatrix} 17 \\ 23 \end{pmatrix} \ (mod\ 26)$$

$$\begin{pmatrix} 2 & 5 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 21 \\ 4 \end{pmatrix} = \begin{pmatrix} 62 \\ 37 \end{pmatrix} = \begin{pmatrix} 10 \\ 11 \end{pmatrix} \ (mod\ 26)$$

$$\begin{pmatrix} 2 & 5 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 5 \\ 5 \end{pmatrix} = \begin{pmatrix} 35 \\ 25 \end{pmatrix} = \begin{pmatrix} 9 \\ 25 \end{pmatrix} \ (mod\ 26) \tag{43}$$

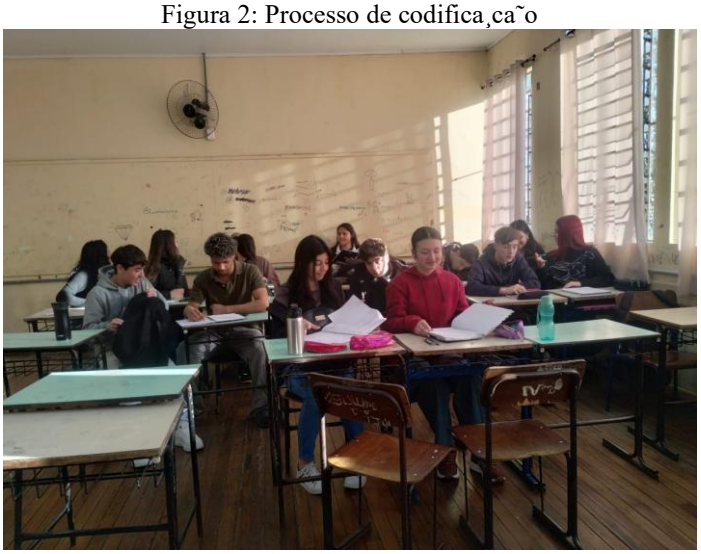
Usando a Tabela 3 obtemos a mensagem cifrada:

QWJKIY

Revista ARACÊ
ISSN: 2358-2472

Agora vamos para o processo de descodificação da mensagem codificada recebida QWJKIY.

Figura 2: Processo de codifica¸ca˜o



Fonte: Elaborada pelos autores.

5.9 PROCESSO DE DESCODIFICAÇÃO

Passo 1) Separar a mensagem cifrada recebida em pares de letras:

QW - JK – IY

Passo 2) Use a Tabela 2 para obter o equivalente numérico e obtenha os vetores cifrados:
17 23 - 10 11 - 9 25

$$v_1 = \begin{pmatrix} 17 \\ 23 \end{pmatrix} \quad v_2 = \begin{pmatrix} 10 \\ 11 \end{pmatrix} \quad v_3 = \begin{pmatrix} 9 \\ 25 \end{pmatrix} \tag{45}$$

Passo 3) Encontre a matriz inversa módulo 26 de A

$$A^{-1} = (detA)^{-1} \begin{pmatrix} 4 & -5 \\ -1 & 2 \end{pmatrix} (mod\ 26) = 3^{-1} \begin{pmatrix} 4 & -5 \\ -1 & 2 \end{pmatrix} (mod\ 26), \tag{46}$$

Revista ARACÊ
ISSN: 2358-2472

onde $3^{-1} = 9$ é o inverso módulo 26 de 3 dado na tabela

Então

$$A^{-1} = 9 \begin{pmatrix} 4 & -5 \\ -1 & 2 \end{pmatrix} \ (mod\ 26) = \begin{pmatrix} 10 & 7 \\ 17 & 18 \end{pmatrix} \ (mod\ 26) \tag{47}$$

Passo 4) Multiplicar a matriz A^{-1} pelos vetores cifrados v_1, v_2 e v_3

$$\begin{pmatrix} 10 & 7 \\ 17 & 18 \end{pmatrix} \begin{pmatrix} 17 \\ 23 \end{pmatrix} = \begin{pmatrix} 331 \\ 703 \end{pmatrix} = \begin{pmatrix} 19 \\ 1 \end{pmatrix} (mod\ 26)$$

$$\begin{pmatrix} 10 & 7 \\ 17 & 18 \end{pmatrix} \begin{pmatrix} 10 \\ 11 \end{pmatrix} = \begin{pmatrix} 177 \\ 368 \end{pmatrix} = \begin{pmatrix} 21 \\ 4 \end{pmatrix} (mod\ 26)$$

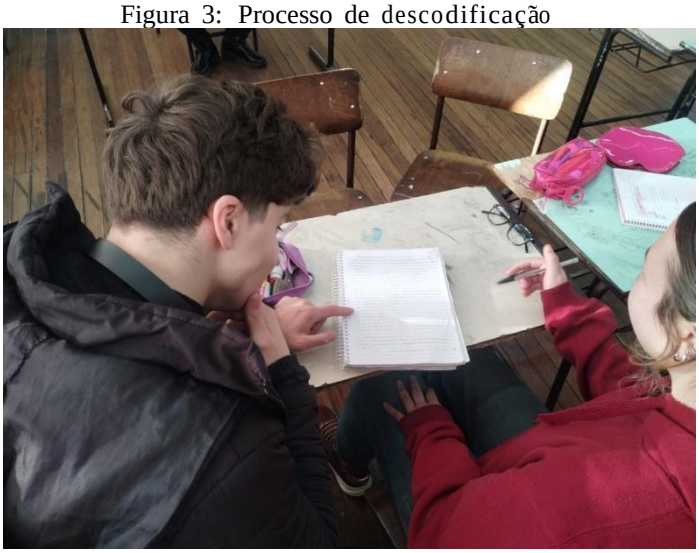
$$\begin{pmatrix} 10 & 7 \\ 17 & 18 \end{pmatrix} \begin{pmatrix} 9 \\ 25 \end{pmatrix} = \begin{pmatrix} 365 \\ 603 \end{pmatrix} = \begin{pmatrix} 5 \\ 5 \end{pmatrix} (mod\ 26) \tag{48}$$

Pela Tabela 3 , os equivalentes alfabéticos destes vetores são

SA UD EE

Que nos fornecem a mensagem SAUDE

Figura 3: Processo de descodificação



Fonte: Elaborada pelos autores.

Revista ARACÊ
ISSN: 2358-2472

6 RELATÓRIO DA EXPERIÊNCIA

A experiência realizada com a turma 312 do Colégio Estadual Coronel Pilar, composta por 15 alunos, revelou resultados diversificados em relação ao interesse e compreensão do assunto abordado. A seguir são apresentados os principais pontos observados:

Alunos com facilidade: 5 alunos demostraram grande facilidade no entendimento do assunto, mesmo no primeiro contato, mostrando uma boa base nos conceitos de matrizes

Alunos com interesse, mas com dificuldades de entendimento: 3 alunos demonstraram um interesse significativo no assunto, mas apresentaram algumas dificuldades iniciais, que foram sanadas com uma explicação mais personalizada e individual do professor

Alunos com dificuldades significativas: Infelizmente o restante dos alunos apresentou dificuldades consideráveis na compreensão do assunto, revelando lacunas significativas na aprendizagem dos conceitos de matrizes. Isso sugere a necessidade de uma maior revisão e reforço desses conceitos para garantir uma melhor compreensão da criptografia e suas aplicações.

7 CONCLUSÃO

A introdução aos alunos ao mundo da criptografia não só despertou um notável interesse mas também destacou o valor prático e teórico dos conceitos matemáticos tornando o processo de aprendizagem mais dinâmico e significativo. Embora alguns alunos tenham enfrentado uma maior dificuldade, através de uma abordagem personalizada do professor a grande maioria dos alunos alcançaram um nível satisfatório de compreensão e aproveitamento dos conteúdos abordados.

Revista ARACÊ
ISSN: 2358-2472

REFERÊNCIAS

ANTON, H; RORRES, C. Álgebra Linear com aplicações. 8. ed. Porto Alegre, Bookman, 2001

IEZZI, G; HAZZAN, S. Fundamentos da Matemática Elementar 8 ed. São Paulo, Atual, 2004 . vol. 4. 7 ed.

SEVERINO, C. Criptografia. Rio de Janeiro, IMPA, 2016 SANTOS, J; Teoria dos Números. Rio de Janeiro, IMPA, 2001