SEVEN
publicações acadêmicas

THE USE OF CRYPTOGRAPHY AS AN EDUCATIONAL TOOL

O USO DA CRIPTOGRAFIA COMO FERRAMENTA PEDAGÓGICA

EL USO DE LA CRIPTOGRAFÍA COMO HERRAMIENTA PEDAGÓGICA

https://doi.org/10.56238/sevened2025.038-072

Valéria C. Brum[1], Igor Godoy Borges[2]

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.

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.

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

[1] Dr. in Mathematics. 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
[2] Master's degree of Science in Mathematics. 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

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.

1 INTRODUCTION

One of the great challenges of the mathematics teacher is to make their classes attractive so that the student understands abstract concepts that can be difficult to understand without a solid foundation in critical and analytical thinking. The use of Cryptography as a pedagogical tool in teaching Linear Algebra in high school can be an innovative and attractive approach, as it manages to sharpen the interest and curiosity of students. Students have the opportunity to see practical applications of Linear Algebra in security and technology that are part of modern everyday life, in addition to developing skills in problem-solving, as many cryptographic problems require a high degree of logical reasoning and analytical ability. This work was applied with class 312 of the Coronel Pilar de Santa Maria State School.

2 GENERAL AND SPECIFIC OBJECTIVES

This work has the general objective of enabling students to understand the basic concepts of cryptography and its importance in information security and as specific objectives to introduce the concept of cryptography, including the Hill Method and demonstrate through practical examples how cryptography is used in data protection.

3 ENCRYPTION

In Greek, Cryptos means hidden secret. Encryption studies methods to encode a message so that only its legitimate recipient can interpret it.

3.1 A BIT OF CRYPTOGRAPHY HISTORY

One of the earliest records of cryptography dates back to 1900 B.C., when a scribe substituted some words in a hieroglyph in order to protect the message from some thief and prevent his access to hidden treasures. Around 50 BC, Julius Caesar used the replacement cipher to protect government communications; currently, the method is known as the Caesar Cipher. During the Middle Ages, more complex encryption systems, such as the Vigenère cipher, which uses a repeating key to perform various substitutions, began to emerge. The twentieth century, in the period of the world wars, brought significant advances with the introduction of machines such as the Enigma, used by German forces. In 1929, an American mathematician named Lester S. Hill presented one of the first examples of cryptography based on linear algebra, particularly using matrices, which represented a significant advance

in relation to the monoalphabetic and polyalphabetic substitution techniques used until then. The crypto landscape has changed dramatically with the arrival of computers. The method of encrypting and decrypting has evolved into more advanced techniques, such as DES (Data Encryption Standard) and AES (Advanced Encryption Standard).

3.2 CAESAR'S CIPHER

The Caesar cipher consists of replacing each letter of the original message with another that was 3 positions ahead in the same alphabet, as shown in Table 1

Table 1

Caesar's Cipher

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

Source: Prepared by the authors.

So the AMO MATHS message would be encoded as DPRPDWHPD-WLFD.

Caesar's cipher is a monoalphabetic substitution cipher and, although simple, became indecipherable for centuries.

3.3 CIFRA DE VIGENERE

Is a polyalphabetic substitution figure. It uses 26 different alphabets to encrypt a message as shown in figure 1.

Although the Vigenere cipher is more difficult to crack, any code that involves systematically replacing one letter with another is relatively easy to crack. This is because the average frequency with which each letter appears in a text of a given language is more or less constant. For example, the average frequency in the Portuguese language of the letter A is 14.64 percent. There are several ways to make it impossible to apply a frequency count. The simplest is Block Encryption given below.

3.4 BLOCK ENCRYPTION

This method consists of dividing a message into blocks of several letters and shuffling these blocks. For example, the message I LOVE MATH can be encoded using the following steps: step 1. Eliminate the spaces between words and complete the message with an A at the end, if you have an odd number of letters;

AMOMATEMATICAA

Step 2: divide the message into blocks of 2 letters;

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

Figure 1

Vegenere's cipher

	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

Source: Wikipedia.

Step 3: in each block swap the letters of place;

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

Step 4: fix the even blocks and swap the odd blocks, exchanging the first for the last, the third for the penultimate and so on.

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

What does the AAMOTAMET message give us above

There is an encryption method called Hill Cipher that is based on matrix transformations. This method was invented by the American mathematician Lester S. Hill in 1929. A message encoded with an *nxn* matrix is called *a Hill cipher.*

To study this method, let's first review some mathematical concepts, such as matrices, invertible matrices, and modular arithmetic.

3.5 MATHEMATICAL FOUNDATION

3.5.1 Matrix

Definition 1: The matrix *m* by *n* with entries in the real numbers is called every table *A* formed by real numbers distributed in *m* rows and *n* columns. We use the following notation A_{mxn}

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

Definition 2: An array whose number of rows is equal to the number of columns is called a Square Array.

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

Definition 3: A square matrix where $a_{ij} = 0 \text{ para } i \neq j$ it is called a Diagonal Matrix

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

Definition 4: A square matrix of order nxn where$a_{ij} = 0 \text{ para } i \neq j$ and $a_{ij} = 1 \text{ para } i = j$ is termed Matrix Identity denoted by I_n

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

3.5.2 Operations with dies

3.5.2.1 Addition

Definition 5: Given Two Matrices $A = [a_{ij}]_{mxn}$ and $B = [b_{ij}]_{mxn}$ It Is Called Sum $A + B$ a matriz $C = [c_{ij}]_{mxn}$, onde $c_{ij} = a_{ij} + b_{ij}$

Example: Let the matrices

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

Then the matrix *C* = A + B is given by *C* = $\begin{pmatrix} 2 & 2 \\ -1 & 4 \end{pmatrix}$ (6)

3.5.2.1 Multiplication by a scalar:

Definition 6: Let $A = [a_{ij}]_{mxn} \text{ e } K \in \mathbb{R}.$ us define the product kA as the matrix $B = [b_{ij}]_{mxn} \text{ tal que } b_{ij} = ka_{ij}$

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

Multiplication by a scalar has the following properties:

Let A *and* B *arrays of order* Then $mxn \text{ e } k_1, k_2 \in \mathbb{R}.$ be valid

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

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

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

3.5.3 Multiplication of matrices

Definition 7: Given the matrices $A = [a_{ij}]_{mxn} \text{ e } B = [b_{jk}]_{nxp}$, the product of *A* by *B is called* the matrix *C* = $[c_{ik}]_{mxp}$ such that for every i = 1.2,..., *m* we have to

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

Example: Let the matrices A = $\begin{pmatrix} 2 & -1 \\ 1 & 3 \end{pmatrix}$ e $B = \begin{pmatrix} 0 & 3 \\ -2 & 1 \end{pmatrix}$. (10)

So the matrix $C = A.B$ is given by $C = \begin{pmatrix} 2 & 5 \\ -6 & 6 \end{pmatrix}$ The product between matrices has the following properties:

i. $k1(A + B) = k1A + k1B$ (11)

ii. $(k1 + k2)A = k1A + k2A$ (12)

iii. $k1(k2A) = (k1k2)Ab$ (13)

The product between matrices is not commutative, i.e., in general $AB \neq BA$

Definition 8: A square matrix A of order n is called invertible, if there exists a matrix B of order n such that $AB = BA = In$.

In this case we say that the matrix B is the inverse matrix of A and we denote it by $B = A-1$

3.6 DETERMINANT

Definition 9: Let A be a square matrix of order n; ($n \leq 3$). We call the determinant of A, $detA$, the real number obtained by operating with the elements of A as follows:

1) If A é of order $n = 1$, $A = [a11]$ then $detA = a11$ (14)

2) If A é of order $n = 2$, $A = [aij]_{2x2}$ then $detA = a11a22 - a12a21$ (15)

3) If A é of order $n = 3$, $A = [aij]_{3x3}$ then $detA = a11a22a33 + a12a23a31$ +a21a32a13 − ($a13a22a31 + a12a21a33 + a32a23a11$) (16)

Example: Let $A = \begin{pmatrix} 1 & 0 & -2 \\ 4 & -1 & 0 \\ 2 & 1 & 1 \end{pmatrix}$ then $detA = 1(-1)1+4(1)(-2)-(-2(-1)2 = -13$ (17)

The determinant of a matrix satisfies, among others, the following properties:

i. If all elements of a row or column of an array A are null, then $detA = 0$
ii. If we swap two lines of a matrix, the determinant changes sign
iii. $de(AB) = detAdetB$
iv. $de(A + B) \neq detA + detB$

Theorem 1: A square matrix A is invertible if, and only if, $detA \neq 0$

4 MODULAR ARITHMETIC

Definition 10: Let a single integer be greater than 1. We say that two integers, a and b, are congruent (or equivalent) modules m and write $the \equiv b(mod\ m)$ if a and b have the same remainder when divided by m. For example:

7 ≡ 2 (*mod* 5), because the remnants of the division of 7 and 2 by 5 are the same (equal to 2) 15 ≡ 3 (*mod* 3), since the remnants of the division of 15 and 3 by 3 are the same (equal to 0).

To show that $the \equiv b(mod\ m)$ it is not necessary to make the division of a and b by m, as we shall see in the following proposition.

Proposition: It is held that $the \equiv b(mod\ m)$ if, and only if, $a - b$ is a multiple of m.

For example, 15 ≡ 3(*mod* 3), because 15-3=12 is a multiple of 3.

Given a modulo m, it can be proved that any integer a is congruent modulus m to exactly one of the integers 0, 1, 2, . . . , m.

This set is called the residual of *the* module. We denote the set of waste from a module *to*

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

Theorem 2: Given an integer number a and any *module*, let

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

Then the residue *r* of the modulus *m* é dado por

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

Examples: Find the residuals module 26 of the following numbers:

a) 43 $R = \text{remainder of } \frac{|43|}{26} = 17 \Rightarrow r = 17$. Thus $43 \equiv 17 (mod\ 26)$ (21)

b) 79 $R = \text{remainder of } \frac{|-79|}{26} = 1 \Rightarrow r = 26 - 1 = 25$. Thus $-79 \equiv 25 (mod\ 26)$ (22)

c) 26 $R = \text{remainder of } \frac{|-26|}{26} = 0 \Rightarrow r = 0$. Thus $-26 \equiv 0 (mod\ 26)$ (23)

Definition 11: Be $a \in Zm$. We say that $a^{-1} \in Zm$ é seu módulo inverso ou módulo recíproco módulo *m*, if $aa^{-1} = a^{-1}a = 1 (mod\ m)$

Theorem 3: If *a* and *m* have no common prime factors, then *a* has a single reciprocal modulus *m*, otherwise *a* has no reciprocal modulus *m*.

For example, the number 3 has reciprocal modulus 26, because 3 and 26 have no common prime factors.

The reciprocal is a number $x \in Z26$ that satisfies the modular equation

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

We will assign some numbers from 0 to 25 in order to find solution *x*. Thus we obtain $x = 9$.

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

For future reference, we have provided the reciprocal table module 26 (Table 2)

Table 2

Waste module 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

Source: Prepared by the authors.

Let *A* be the coding matrix. In order to decipher Hill Ciphers, let's study the concept of inverse matrix (*mod* 26) of the encoding matrix *A*.

Definition 12: Let *m* be a positive integer and *A* a square matrix with input in Zm. We say that *A* is invertible modulo *m* if there exists a matrix *B* with inputs in Zm such that

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

Theorem 4: A square matrix *A* with inputs in Zm´evert´ıvel modulo *m* if, and only if, the residue *deA* modulo *m* has reciprocal modulo *m*.

Note that *this* modulo *m* will have reciprocal modulo *m* if, and only if, this residue and *m* do not have prime factors in common.

As the only prime factors of 26 are 2 and 13, we have *to deA*(*mod* 26) will have reciprocal (mod 26) if it is not divisible by 2 or 13.

We can get the inverse modulo *m* of a matrix

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

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

Example: Find the inverse of *A* modulo 26 if *A* = $\begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}$ (29)

Solution: *detA* = 15 − 12 = 3 ⇒ (*detA*)$^{-1}$ = 3−1 = 9(*mod* 26) as shown in Table 1.

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

Calculation of residuals module 26:

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

So

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

Checking out:

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

In possession of these mathematical concepts, we can now study the cryptography method called Hill Ciphers

4.1 HILL CIPHERS

From here on, let's assume that each letter of the common text or ciphertext has a numerical correspondent that specifies its position in the standard alphabet, with the exception of the letter Z, whose numerical correspondent will be the number 0, as shown in Table 3

Table 3

Hill's Cipher

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

Source: Prepared by the authors.

Example 1: Use the Hill Cipher to encode and decode the STUDENT message using the encoder matrix *A* with inputs in Z26

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

4.2 CODING PROCESS

Step 1) Separate the word into pairs of letters. If the number of letters is odd, repeat the last letter:

$$\text{AL - UN - OO}$$

Step 2) Use Table 3 to get the numerical equivalent and get the cipher vectors:

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

Step 3) make the product of the encoding matrix A by the ciphered vectors, that is, determine Ap1, Ap2, Ap3.

Whenever an integer is greater than 25, it will be replaced by the residue r.

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

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

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

Using Table 3 we get the ciphered message:

NKDCSP

Now let's move on to the process of decoding the incoming NKDCSP encoded message.

4.3 DECODING PROCESS:

Step 1) Separate the received encrypted message into pairs of letters:

NK - DC - SP

Step 2) Use Table 3 to get the numerical equivalent and get the figured vectors: 14 11 - 4 3 - 19 16

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

Step 3) Find A Inverse Matrix Modulo 26

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

where 7−1 = 15 is the inverse modulo 26 of 7 given in table 1.

So

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

Step 4) Multiply the matrix *A−1* by the ciphered vectors *v1, v2,* and *v3*

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

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

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

Table 3 shows the alphabetical equivalents of these vectors

AL UN OO

That provide us with the message STUDENT

5 DIDACTIC SEQUENCE AND APPLICATION

5.1 LESSON 1: INTRODUCTION TO THE CONCEPT OF CRYPTOGRAPHY

In this class, an introduction was given to the concept of cryptography, historical context and its importance in information security. An example of cryptography using Caesar's Cipher, relating the letters of the alphabet to numbers from 1 to 26, was shown. In addition, the Hill Cipher was introduced, demonstrating its practical application.

5.2 LESSON 2: REVIEW OF BASIC CONCEPTS OF MATRICES AND MATRIX OPERATIONS

In this class, a review of the concepts of matrices was carried out, including:

- Matrix Definition
- Special types of arrays such as: Square array, identity array, null array, triangular array
- Equality of matrices
- Adding matrices
- Product of matrices by a scalar

The lesson concluded with fixation exercises to strengthen the students' understanding.

5.3 LESSON 3. REVIEW OF THE PRODUCT CONCEPT OF DIES

In this stage, the product of matrices, conditions for the existence of the product, was addressed. The properties of the product of matrices, such as non-commutativity and associativity, were discussed. The class concluded with fixation exercises to consolidate your understanding.

5.4 LESSON 4. REVISION OF THE CONCEPT OF INVERSE MATRIX

In this lesson, the definition of an invertible matrix and a method to calculate the inverse matrix of a matrix A, denoted by A^{-1}, were presented. At the end of the class, an invertible *matrix A* was given to the students to determine its inverse A^{-1}.

5.5 LESSON 5. REVIEW OF THE CONCEPT OF DETERMINANT AND ASSOCIATIVITY IN MATRIX MULTIPLICATION

In this class, an introduction to the concepts of order determinant 2 and order 3 was presented, with the objective of using a practical method to determine the inverse matrix. In addition, the associative property in matrix multiplication was reviewed to understand why Hill cryptography works.

5.6 LESSON 6. INTRODUCING MODULAR ARITHMETIC

In this stage, the concept of modular arithmetic, fundamental for cryptography, was introduced. Students learned how to perform arithmetic operations within a specific module,

which is essential for encoding and decoding messages. It was given as an exercise for the students, with the help of the teacher, to encode and decode the word STUDENT, given in Example 1 of this article.

5.7 LESSON 7. GROUP ACTIVITY

The following activity was elaborated: Use the Hill Cipher to encode and decode the HEALTH message using the encoding matrix *A* with entries in $\mathbb{Z}_{26}$

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

5.8 ENCODING PROCESS:

Step 1) Separate the word into pairs of letters. If the number of letters is odd, repeat the last letter:

SA - UD - EE

Step 2) Use Table 2 to get the numerical equivalent and get the cipher vectors:

19 1 - 21 4 - 5 5

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

Step 3) make the product of the encoding matrix *A* by the ciphered vectors, that is, determine *Ap1, Ap2, Ap3*.

Whenever an integer is greater than 25, it will be replaced by the residue *r*.

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

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

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

Using Table 3 we get the ciphered message:

QWJKIY

Now let's move on to the process of decoding the incoming QWJKIY encoded message.

Figure 2

Coding process

Source: Prepared by the authors.

5.9 DECODING PROCESS

Step 1) Separate the received encrypted message into pairs of letters:

QW - JK – IY

Step 2) Use Table 2 to get the numerical equivalent and get the cipher vectors:

17 23 - 10 11 - 9 25

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

Step 3) Find A Inverse Matrix Modulo 26

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

where 3−1 = 9 is the inverse modulo 26 of 3 given in the table

So

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

Step 4) Multiply the matrix *A−1* by the ciphered vectors *v1, v2,* and *v3*

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

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

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

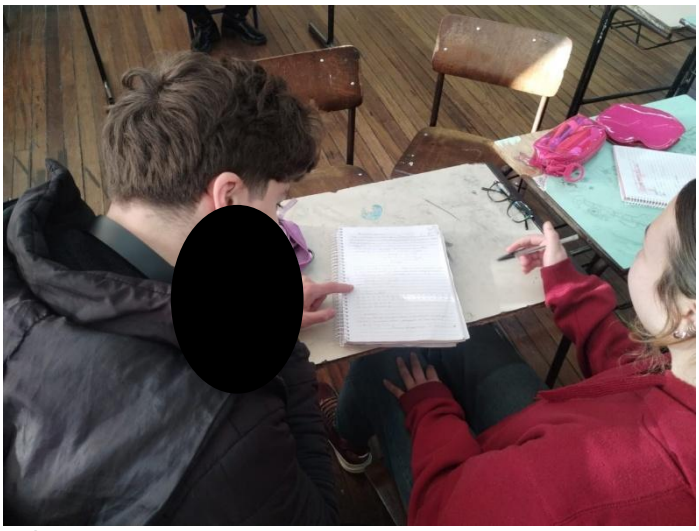
Table 3 shows the alpha equivalents of these vectors

SA UD EE

Who provide us with the message HEALTH

Figure 3

Decoding process



Source: Prepared by the authors.

6 EXPERIENCE REPORT

The experience carried out with class 312 of the Coronel Pilar State School, composed of 15 students, revealed diversified results in relation to the interest and understanding of the subject addressed. The main points observed are presented below:

Students with ease: 5 students showed great ease in understanding the subject, even in the first contact, showing a good foundation in the concepts of matrices

Students with interest, but with difficulties in understanding: 3 students showed significant interest in the subject, but presented some initial difficulties, which were solved with a more personalized and individual explanation from the teacher

Students with significant difficulties: Unfortunately, the rest of the students presented considerable difficulties in understanding the subject, revealing significant gaps in the learning of matrix concepts. This suggests the need for further revision and reinforcement of these concepts to ensure a better understanding of cryptography and its applications.

7 CONCLUSION

The introduction to students to the world of cryptography not only sparked remarkable interest but also highlighted the practical and theoretical value of mathematical concepts, making the learning process more dynamic and meaningful. Although some students faced greater difficulty, through a personalized approach of the teacher, the vast majority of students achieved a satisfactory level of understanding and use of the contents covered.

REFERENCES

Anton, H., & Rorres, C. (2001). Álgebra linear com aplicações (8ª ed.). Bookman.

Coutinho, S. C. (2016). Criptografia. IMPA.

Iezzi, G., & Hazzan, S. (2004). Fundamentos da matemática elementar: Vol. 4. (8ª ed.). Atual.

Santos, J. P. O. (2001). Teoria dos números. IMPA.