UNIVERSIDADE FEDERAL DE ALAGOAS

Mestrado Profissional em Matemática em Rede Nacional

PROFMAT

RECURSO EDUCACIONAL

Cifrando Matrizes e Decifrando Segredos

Ana Carolina Gonçalves Araújo

Isnaldo Isaac Barbosa

Maceió, 2026

Instituto de Matemática

PROFMAT

Folha de aprovação

ANA CAROLINA GONÇALVES ARAÚJO

CIFRANDO MATRIZES E DECIFRANDO SEGREDOS

Produto Educacional de Mestrado apresentadoao programa de Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal de Alagoas, Campus A. C. Simões, como requisito parcial para a obtenção do título de Mestre em Matemática e aprovada em 23 de fevereiro de 2026.

Banca examinadora:

gov.br Documento assinado digitalmente
ISNALDO ISAAC BARBOSA
Data: 13/05/2026 11:19:37-0300
Verifique em https://validar.iti.gov.br

Orientador: Prof. Dr. Isnaldo Isaac Barbosa
(Universidade Federal de Alagoas)

gov.br Documento assinado digitalmente
MARCOS RANIERI DA SILVA
Data: 11/05/2026 15:14:29-0300
Verifique em https://validar.iti.gov.br

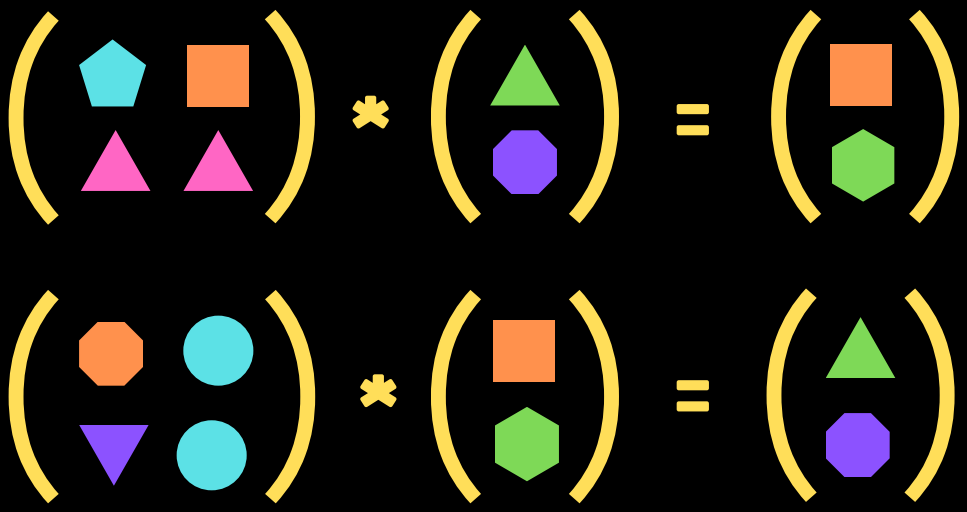
Examinador Interno: Prof. Dr. Marcos Ranieri da Silva
(Universidade Federal de Alagoas)

gov.br Documento assinado digitalmente
DANIEL NICOLAU BRANDAO
Data: 13/05/2026 10:12:24-0300
Verifique em https://validar.iti.gov.br

Examinador Externo: Prof. Dr. Daniel Nicolau Brandão
(Universidade Estadual de Alagoas)

MANUAL SOBRE A UTILIZAÇÃO DO EXCEL ALINHADO AOS FUNDAMENTOS MATEMÁTICOS DA CIFRA DE HILL PARA PROFESSORES DE MATEMÁTICA DO ENSINO MÉDIO

CIFRANDO MATRIZES E DECIFRANDO SEGREDOS



ANA CAROLINA GONÇALVES ARAÚJO
ISAAC ISNALDO BARBOSA

UNIVERSIDADE FEDERAL DE ALAGOAS

PROFMAT Mestrado Profissional em Matemática

Instituto de Matemática

MANUAL SOBRE A UTILIZAÇÃO DO EXCEL ALINHADO AOS FUNDAMENTOS MATEMÁTICOS DA CIFRA DE HILL PARA PROFESSORES DE MATEMÁTICA DO ENSINO MÉDIO

CIFRANDO MATRIZES
E DECIFRANDO SEGREDOS

ANA CAROLINA GONÇALVES ARAÚJO
ISAAC ISNALDO BARBOSA

UNIVERSIDADE FEDERAL DE ALAGOAS
PROFMAT Mestrado Profissional em Matemática
Instituto de Matemática

AO MEU PRIMEIRO
PROFESSOR DE
MATEMÁTICA, MARCELO
ARAÚJO, MEU PAI.
POR DESPERTAR EM MIM O
AMOR PELOS NÚMEROS E
ME ENSINAR O VALOR DA
PERSEVERANÇA.

CARTA AO PROFESSOR

É com grande satisfação e entusiasmo que apresento o produto educacional "Cifrando Matrizes e Decifrando Segredos", resultado de uma jornada de estudo e dedicação ao Mestrado Profissional em Matemática em Rede Nacional - PROFMAT.

O mundo está repleto de segredos matemáticos, e um dos mais fascinantes é a Criptografia. Muitas vezes, conceitos como Matrizes, Determinantes e Aritmética Modular parecem distantes da realidade, restritos aos livros didáticos. Minha maior motivação ao criar esta ferramenta e este manual foi justamente quebrar essa barreira!

Professor(a), o que você tem em mãos é mais do que uma simples planilha: é um laboratório interativo que transforma a complexidade da Cifra de Hill em uma missão de codificação e decodificação acessível e envolvente. Você verá, na prática, como o rigor da Álgebra Linear e a beleza da Matemática Pura e Aplicada se unem para proteger informações.

Este manual é seu guia nessa missão. Convido você a mergulhar, sem medo, no universo dos códigos secretos. Prepare-se para cifrar e, acima de tudo, para comprovar o poder da Matemática.

Ana Carolina

Professora de Matemática

CONTATOS

E-mail institucional: ana.goncalves@im.ufal.br

E-mail pessoal: carolinaaraujo.2573@gmail.com

Instagram: @carolinaa.aaraujo

Lattes: http://lattes.cnpq.br/3438501650845145

SUMÁRIO

Introdução

Bem-vindo ao Mundo da Cifra de Hill

"Ninguém deveria sentir orgulho por não saber matemática. O caminho para tirar essa aura impenetrável é não matar a curiosidade, é permitir que as pessoas explorem e brinquem com a matemática, especialmente desde jovens"
- Artur Avila

"Ninguém deveria sentir orgulho por não saber matemática", essa foi a reflexão feita em 2024 durante uma entrevista ao jornal Folha de São Paulo pelo pesquisador brasileiro Artur Ávila, primeiro latino-americano a ganhar a Medalha Fields.

Essa reflexão deve ecoar no coração e mente de qualquer professor(a) de matemática apaixonado(a) pelo que ensina e comprometido(a) com sua função. Em essência, o(a) educador(a) matemático(a) é um(a) matemático(a) que, transpassado seu amor ao trabalho matemático, resolveu ensinar.

> O fato é que a curiosidade existe. Eu a constato diariamente. A matemática dá medo, mas fascina ainda mais. Não é amada, mas todo mundo gostaria de amá-la. Ou pelo menos ser capaz de dar uma olhada indiscreta em seus tenebrosos mistérios. As pessoas tendem a achar que eles são inacessíveis, o que não é verdade. É perfeitamente aceitável gostar de música sem ser músico ou compartilhar uma bela refeição sem ser um grande cozinheiro. Por que, então, seria necessário ser matemático ou ter uma inteligência excepcional para entrar no mundo da matemática ou deixar a mente ser provocada pela álgebra ou pela geometria? Não é necessário entrar nos detalhes técnicos para entender as grandes ideias e se maravilhar com elas (Launay, 2019).

É com esse espírito de renovação e o objetivo de resgatar o prazer em estudar matemática que apresentamos o produto educacional "Cifrando Matrizes e Decifrando Segredos".

Ao utilizar a Cifra de Hill, este manual e a planilha interativa que o acompanha transformam a Álgebra Linear em uma atividade de espionagem, onde Matrizes, Determinantes e a Invertibilidade Modular (módulo 27) são as ferramentas essenciais para criar e desvendar códigos secretos, como também vivenciam o poder da Matemática na segurança da informação.

Parte 1 - A Cifra de Hill: História e Fundamentos

O ser humano sempre buscou formas de comunicação e, posteriormente, formas de proteger informações vitais. Da escrita hieroglífica à comunicação segura em transações bancárias, a necessidade de sigilo da informação deu origem à Criptografia, a arte e ciência de escrever em códigos. A própria palavra tem origem no grego “Kryptós”, que em português é o mesmo que “secreto”. “Para a criptografia isso seria escrever uma mensagem ou código de uma maneira na qual o receptor e remetente são os únicos capazes de decifrá-la.” (Costa, 2022).

É com o propósito de aplicar a Matemática de forma lúdica e funcional que este produto utiliza a Cifra de Hill como seu pilar pedagógico. Desenvolvida em 1929 pelo matemático americano Lester S. Hill, essa cifra é considerada um marco na história da criptografia por ter sido o primeiro sistema polialfabético a ser prático para o uso.

> No início do século XX, iniciam-se as primeiras tentativas de mecanização das técnicas criptográficas, pois os sistemas existentes, mono e polialfabéticos, estavam vulneráveis à análise de frequências. Uma das alternativas apresentadas consistia em agrupar as letras do texto normal, formando blocos com um número n de caracteres e, a cada conjunto formado, substituí-las por um conjunto n de letras cifradas. Esta técnica clássica de substituição, utilizando conceitos da Álgebra Linear e da Aritmética Modular, aprimorada por Lester S. Hill em 1929, deu origem ao que se denomina a Cifra de Hill (Jeanrenaud, 2013).

A grande inovação de Hill foi empregar a Álgebra Linear no processo de cifragem, transformando blocos de letras da mensagem em vetores e multiplicando-os por uma matriz-chave,

> “Nas cifras polialfabéticas, uma mesma letra na mensagem original pode ser substituída por letras diferentes o que dificulta o processo de decifração por análise de frequência, embora possa ser criptoanalisada por recursos de álgebra linear.” (Martíns, 2023).

Para que a decodificação seja possível, essa matriz precisa satisfazer uma condição matemática rigorosa: ser invertível dentro de um sistema de aritmética modular (no nosso caso, módulo 27). Este manual guiará o leitor passo a passo na compreensão e aplicação desses conceitos.

Parte 2 - O produto educacional: Acesso às planilha do Excel

Para prosseguir com o manual é preciso ter acesso às planilhas que serão explicadas ao decorrer dos capítulos a seguir. É possível acessá-las através dos QR Codes abaixo.

Google Drive
Pasta com as duas versões da planilha
https://acesse.one/OfEY4

Excel Online
Planilhas - ordem 2

Excel Online
Planilhas - ordem 3

Recomenda-se fazer uma cópia da planilha cujas matrizes estão na 2º ordem, para acompanhar este manual. As planilhas na 3º ordem são utilizadas de forma semelhante.

Capítulo I

A Chave

Sua Matriz Está Pronta para Criptografar?

"A educação é a chave para libertar o mundo e uma das maiores necessidades da humanidade." - Malba Tahan

Capítulo I
A Chave

Antes de começar a escrever mensagens secretas, é preciso garantir que você tem a ferramenta certa em mãos: uma matriz que funcione como uma chave confiável. Mas atenção! Nem toda matriz está apta para a missão.

Neste capítulo, vamos testar se a sua matriz quadrada de ordem 2 tem o que é necessário para entrar no mundo da criptografia com a Cifra de Hill, usando um alfabeto de 27 caracteres (de A a Z, mais o espaço). A etapa é simples, mas essencial: verificar se sua matriz é invertível no módulo 27, só assim ela poderá ser usada para codificar e decodificar mensagens secretas.

Você descobrirá como calcular o determinante, aplicar o módulo 27, e verificar se a matriz passa no teste de segurança. Pense nisso como o "scan de segurança" antes de liberar acesso ao cofre da informação.

PREPARE SUA MATRIZ, SIGA OS PASSOS E DESCUBRA:
ELA É SEGURA O BASTANTE PARA PROTEGER SEGREDOS?

1.1 Conhecendo a Primeira Planilha: Matriz-chave

Este módulo da planilha tem como propósito auxiliar os alunos a compreenderem como verificar se uma matriz de ordem 2 pode ser utilizada na Cifra de Hill, utilizando o alfabeto com 27 caracteres. Observe na imagem abaixo a interface criada com esse propósito, você pode ter acesso a ela através do link já disponibilizado na Parte 2 da introdução desse manual.

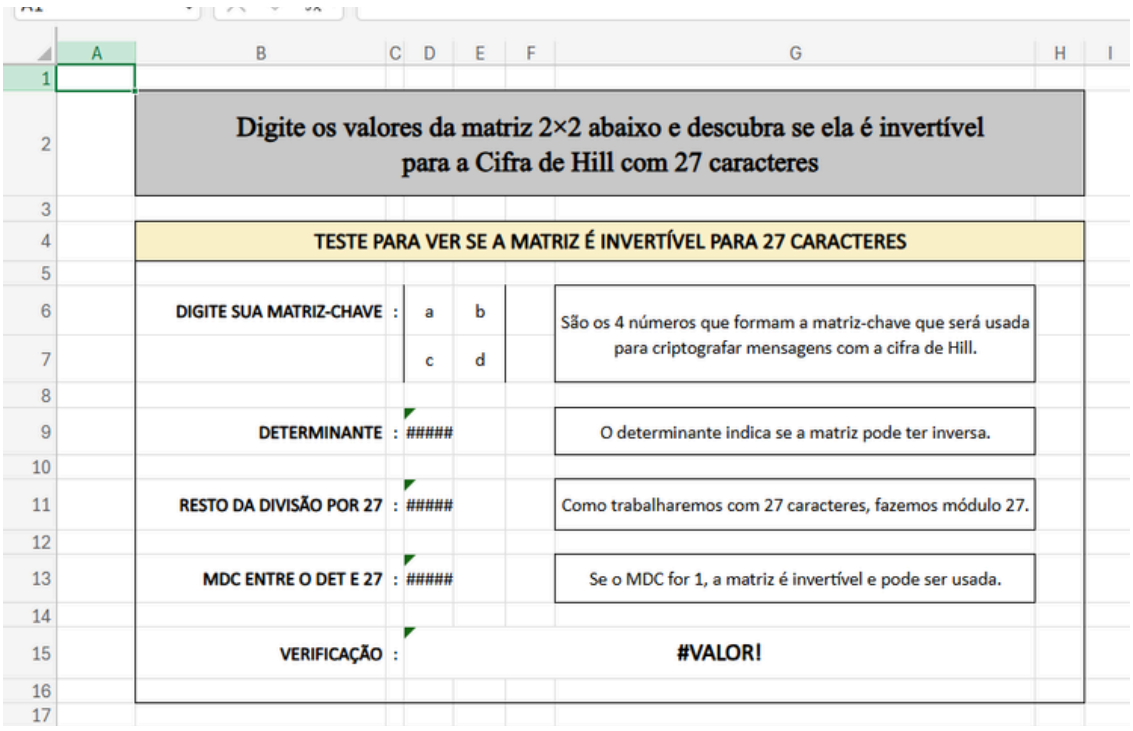


Imagem 1.1. interface da planilha “Matriz-chave”.

Nesta planilha, apenas as células D6, D7, E6 e E7 são editáveis. Essas células representam as entradas da matriz quadrada de ordem 2 que será utilizada como matriz de codificação na próxima etapa. Inicialmente, essas células contêm letras como marcadores de posição. O usuário deve substituí-las exclusivamente por valores numéricos.

Para garantir a integridade dos dados, as demais células da planilha estão protegidas contra edição. Além disso, a tabela está automatizada, para representar bem a validação ou não da utilização da matriz escrita.

Veja a seguir o que ocorre ao substituirmos D6 por 7, D7 por 7, E6 por 5 e E7 por 2.

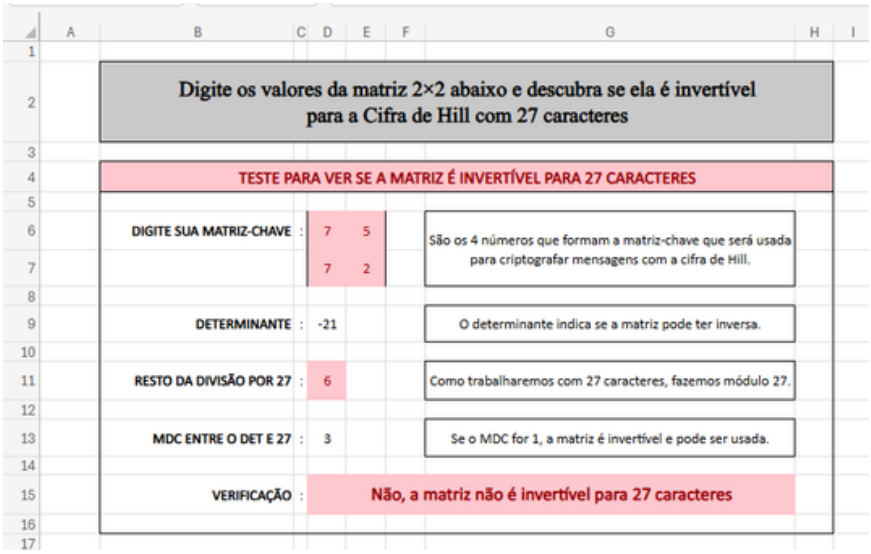


Imagem 1.2. Matriz não invertível módulo 27.

Automaticamente, a planilha calcula o determinante da matriz na célula D11, através de fórmula “=D6E7-E6D7”, isto é, fazendo a diferença entre os produtos da diagonal principal e da diagonal secundária. Neste exemplo, o determinante ficou “-21”.

Ocorre que, para poder ser utilizada como matriz-chave no processo da Cifra de Hill com 27 caracteres, é necessário que o seu determinante, em módulo 27, seja primo com 27, ou seja, que o máximo divisor comum (MDC) entre os dois seja igual a 1.

Por isso, na célula D11 foi implementada a fórmula “=MOD(D9;27)”, que gera o resto da divisão do determinante, anteriormente calculado, por 27. Neste caso, gerando o resultado “6”, o professor pode instruir os alunos a fazerem essa verificação ao somar 27 quantas vezes forem necessárias ao determinante, até encontrar um valor inteiro positivo, como no exemplo -21+27=6.

Em seguida, na célula D13, através da fórmula “=MDC(D11;27)” é calculado o MDC entre 6 e 27, que deu “3”. Como esse MDC é diferente de 1, a matriz é dita não invertível módulo 27 e a planilha

troca as cores para vermelho e informa a seguinte mensagem: “Não, a matriz não é invertível para 27 caracteres”

Para poder prosseguir basta fazer alterações nas entradas da matriz até que a planilha alerte uma que seja viável ao processo. Uma opção é, por exemplo, Trocar o valor da célula D6 para 3, veja abaixo.

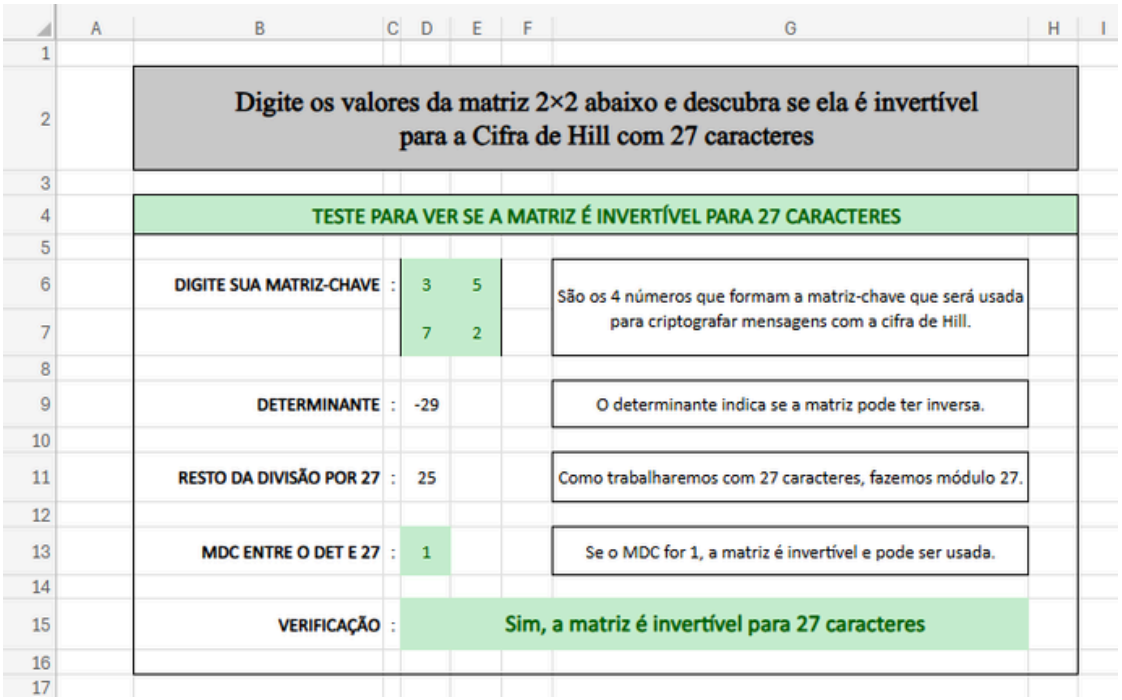


Imagem 1.3. Matriz invertível módulo 27.

Como o determinante, neste caso, deu 1, a planilha troca as cores para verde e informa a seguinte mensagem: “Sim, a matriz é invertível para 27 caracteres”. O que significa que o usuário pode utilizar essa matriz para criptografar mensagens na próxima planilha.

A fim de garantir a segurança dos próximos capítulos continuaremos a utilizar a matriz-chave da Imagem 1.3.

Capítulo II

Hora de Codificar

Transformando Palavras em Códigos Secretos

"Tudo é número" - Pitágoras

Agora que sua matriz de codificação está pronta e segura, é hora de colocar a criptografia em ação. Nesta etapa, cada letra da sua mensagem será convertida em um código matemático único, seguindo as regras definidas pela sua matriz. É como trocar o idioma comum por uma língua secreta, compreendida apenas por quem possui a chave correta para decifrá-la.

Ao longo deste capítulo, você vai aprender a inserir sua mensagem na planilha de criptografia, acompanhar a transformação passo a passo e entender como a matemática garante que seu texto original se torne praticamente indecifrável para curiosos.

AFINAL, AQUI, CADA PALAVRA CONTA
E CADA NÚMERO GUARDA UM SEGREDO

2.1 Conhecendo a Segunda Planilha: Codificação

Esta segunda planilha pretende ser um auxílio completo para a codificação de mensagens de até 16 caracteres, desde a primeira transformação da mensagem em números pré-definidos até as multiplicações de matrizes e construção da mensagem já codificada.

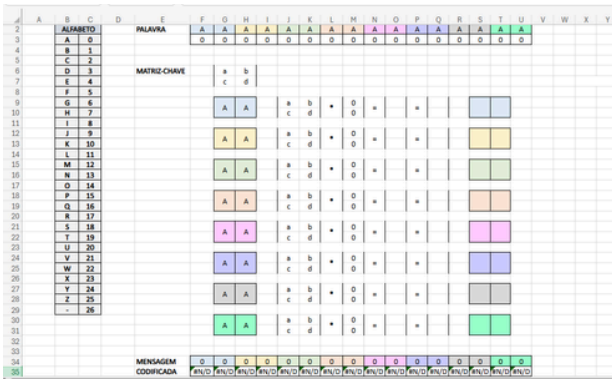


Imagem 2.1. Interface da planilha “Codificação”.

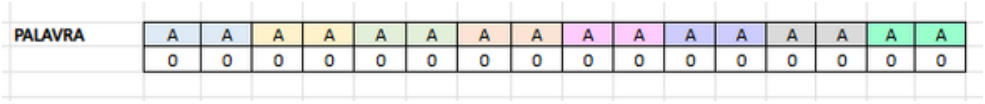
No lado esquerdo da tela da Imagem 2.1 há o alfabeto a ser utilizado em todo o processo. Ele foi composto por 27 caracteres, sendo estas as 26 letras do alfabeto brasileiro mais o caractere "-", que funciona como um espaço entre palavras e também para completar frases com número ímpar de caracteres. A Imagem 2.2 a seguir mostra melhor essa disposição.

ALFABETO	
A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25
-	26

Imagem 2.2. Alfabeto com 27 caracteres.

De A a Z foram distribuídos os números de 0 a 25, de acordo com a ordem do próprio alfabeto brasileiro, sendo A=0 e Z=25, já para o "-" foi atribuído o valor 26.

No canto superior da planilha há os espaços para escrita da mensagem a ser codificada (Ver Imagem 2.1). As células devem ser preenchidas apenas com as informações contidas na tabela da Imagem 2.2 e a planilha fará a conversão dos sinais informados para os respectivos números, automaticamente.



PALAVRA	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Imagem 2.3. Local de inserção da mensagem inicial.

Abaixo dessa área encontra-se o local de inserção da matriz-chave já verificada na primeira planilha. Inicialmente, a matriz apresenta as entradas "a", "b", "c" e "d", que devem ser substituídas pelos números da matriz que ser quer utilizar (ver Imagem 2.4).

MATRIZ-CHAVE		a	b
		c	d

Imagem 2.4. Local de inserção da matriz-chave.

No centro da planilha está localizado o ambiente em que ocorrerá toda a transformação, já com comandos pré-definidos e que iremos conhecer nas próximas seções deste capítulo. Mas, por hora, observe esse ambiente na Imagem 2.5.

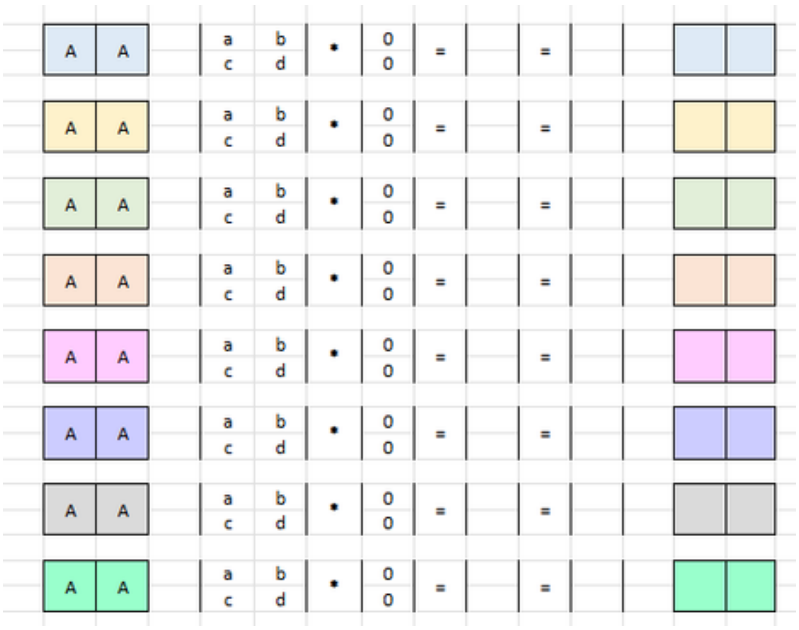


Imagem 2.5. Ambiente de transformação da mensagem.

Note que, desde o ambiente de inserção da mensagem, a mesma encontra-se separada por 8 cores, cada par de letra está representado por uma cor diferente. Isso ocorre devido à escolha de fazer a transformação da mensagem com uma matriz-chave de ordem dois, pois, assim, a mensagem precisa ser codificada a cada par de letras.

No ambiente de transformação da mensagem (Imagem 2.5) é possível ver de forma mais clara essa separação, pois a planilha aponta, ao lado esquerdo, cada dupla de caracteres e, ao lado direito, irá gerar a nova dupla de caracteres que irá substituir as iniciais.

Todo o processo ocorre por meio de multiplicações de matrizes e também da "redução" dos resultados ao módulo 27. Essas funções irão ocorrer na parte central do espaço e como mencionado anteriormente, serão executadas por meio de alguns comandos já programados.

Por fim, a planilha conta com uma parte inferior que "monta" a mensagem codificada ao final do processo.

2.2 Escolhendo a mensagem

Volte sua atenção novamente ao canto superior dessa planilha. Você, como usuário dela, pode digitar letra por letra da mensagem ou, simplesmente, selecionar a letra desejada no cursor que aparece ao clicar em cada célula. Perceba que, sem perda de originalidade da mensagem, ela só pode ser composta por letras maiúsculas.

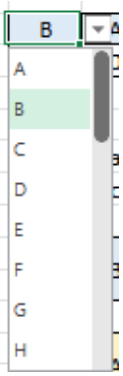


Imagem 2.5. Cursor de seleção de letra.

A mensagem não precisa ter necessariamente todos os 16 caracteres, mas é importante que ela tenha um número par de símbolos; caso não tenha, deve-se acrescentar o ícone "-" ao final, para ajustar ao modelo.

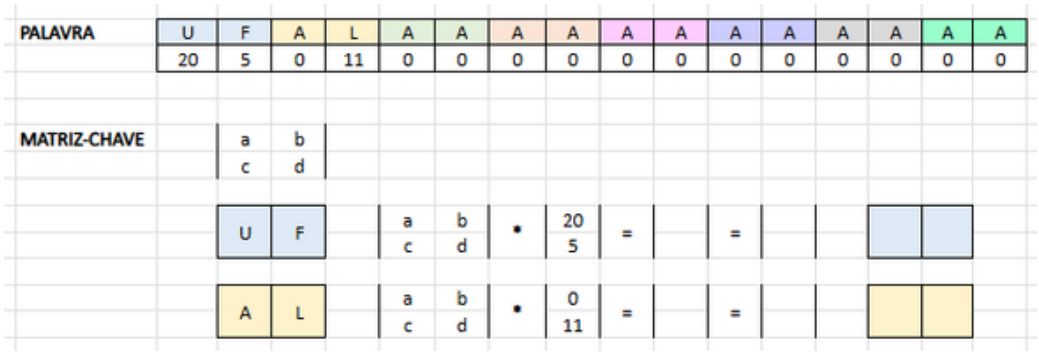


Imagem 2.6. Iserção da palavra "UFAL".

Na Imagem 2.6 tem-se a adição da mensagem “UFAL” à planilha. Essa mensagem contém 4 letras, isto é, um número par de letras, tornando possível a separação delas em dois pares no ambiente de transformação da mensagem, os pares “UF” e “AL”. Perceba também que a planilha faz essa separação de forma automática.

Em contrapartida, a mensagem “PROFMAT” tem 7 letras, por ser um número ímpar, a última letra não teria um par, por isso acrescentamos o espaço (representado por “-”) e optamos por usar a mensagem “PROFMAT-”. Veja a Imagem 2.7.

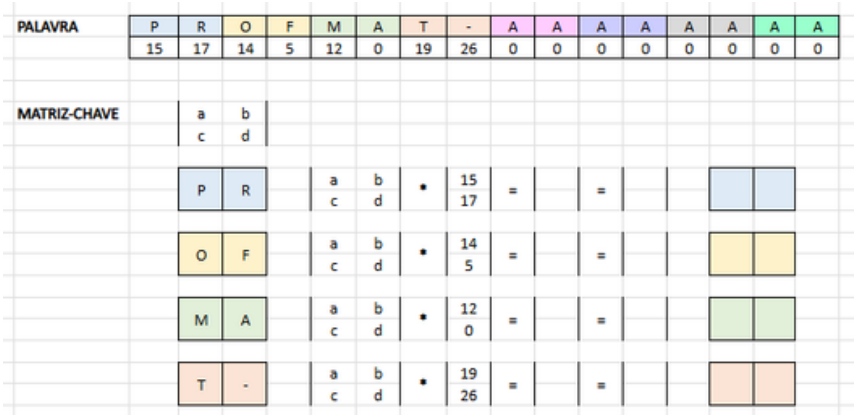


Imagem 2.7. Iserção da palavra “PROFMAT-”.

É perceptível que, ao inserir ambas as mensagens, a planilha faz a conversão automática das letras para os respectivos números. Essa função está ativada a partir da utilização da fórmula “PROCV”, e não pode ser alterada pelos usuários, já que a planilha está restrita para que os usuários só possam modificar uma quantidade limitada de células.

A fim de exemplificar a codificação de uma mensagem de 16 letras, utilizaremos a frase “UFAL-PROFMAT-IM-” a partir de agora.

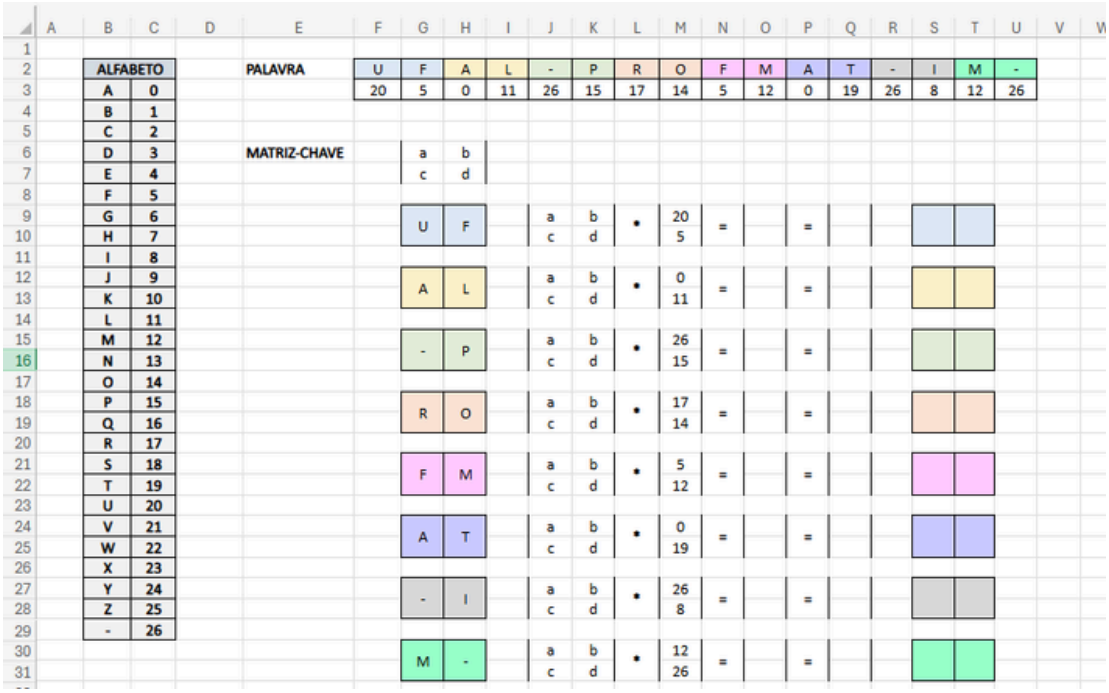


Imagem 2.8. Mensagem “UFAL-PROFMAT-IM-”

Ao dispor da frase completa, a planilha faz a conversão para os números e já converte as duplas de símbolos para uma matriz coluna de seus números. Como, por exemplo, “UF” que nas células M9 e M10 tem sua representação matricial.

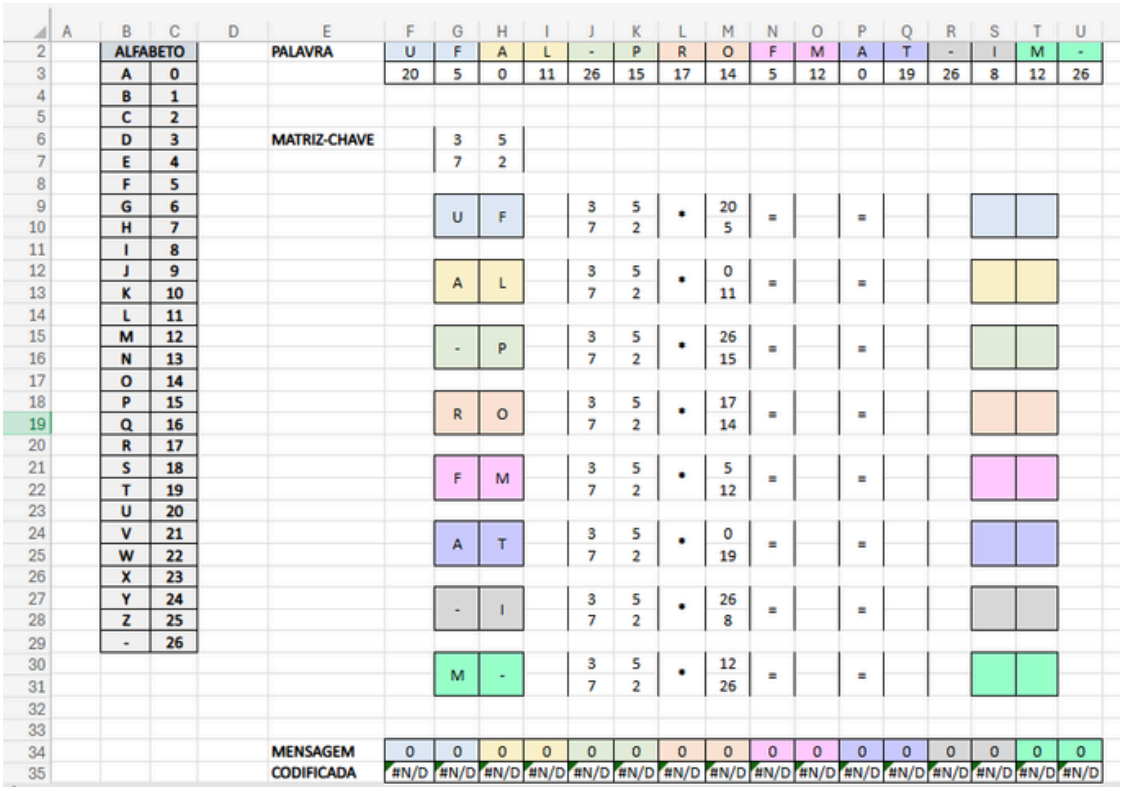
2.3 Codificando a mensagem

Na etapa atual o primeiro passo é atribuir a matriz-chave já verificada. A planilha irá substituir no mesmo instante todas as matrizes no ambiente de transformação da mensagem.

A exemplo, na imagem 2.8, adotamos a matriz-chave já verificada no capítulo I deste manual, cujas entradas são 3, 5, 7 e 2.

É importante sempre lembrar de verificar antes, pois, embora qualquer matriz de ordem 2 possa ser colocada nessa etapa, matrizes

que não são invertíveis módulo 27 serão incapazes de servir para recuperar a mensagem codificada.



ALFABETO	
A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25
-	26

PALAVRA	U	F	A	L	-	P	R	O	F	M	A	T	-	I	M	-
	20	5	0	11	26	15	17	14	5	12	0	19	26	8	12	26
MATRIZ-CHAVE		3	5													
		7	2													
	U	F			3	5	•	20	=		=					
					7	2		5								
	A	L			3	5	•	0	=		=					
					7	2		11								
	-	P			3	5	•	26	=		=					
					7	2		15								
	R	O			3	5	•	17	=		=					
					7	2		14								
	F	M			3	5	•	5	=		=					
					7	2		12								
	A	T			3	5	•	0	=		=					
					7	2		19								
	-	I			3	5	•	26	=		=					
					7	2		8								
	M	-			3	5	•	12	=		=					
					7	2		26								
MENSAGEM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CODIFICADA	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D	#N/D

Imagem 2.9. Matriz-chave substituida

A ideia da planilha é justamente reduzir processos demasiadamente extensos para permitir o foco no processo e em como utilizar a ferramenta de forma adequada.

Assim, ao colocar a matriz-chave, a planilha já irá efetuar todo o processo de codificação, como é possível observar na Imagem 2.10 abaixo. Nessa mesma imagem, note que é fundamental que o professor atue como mediador nessa parte, para que os alunos direcionem a atenção para o processo ao qual o Excel codificou a mensagem.

ALFABETO	
A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25
-	26

MATRIZ-CHAVE

3	5
7	2

PALAVRA	U	F	A	L	-	P	R	O	F	M	A	T	-	I	M	-
	20	5	0	11	26	15	17	14	5	12	0	19	26	8	12	26

U	F		3	5	•	20	=	85	=	4		E	P
			7	2		5		150		15			
A	L		3	5	•	0	=	55	=	1		B	W
			7	2		11		22		22			
-	P		3	5	•	26	=	153	=	18		S	X
			7	2		15		212		23			
R	O		3	5	•	17	=	121	=	13		N	M
			7	2		14		147		12			
F	M		3	5	•	5	=	75	=	21		V	F
			7	2		12		59		5			
A	T		3	5	•	0	=	95	=	14		O	L
			7	2		19		38		11			
-	I		3	5	•	26	=	118	=	10		K	J
			7	2		8		198		9			
M	-		3	5	•	12	=	166	=	4		E	B
			7	2		26		136		1			

MENSAGEM CODIFICADA	E	P	B	W	S	X	N	M	V	F	O	L	K	J	E	B
	4	15	1	22	18	23	13	12	21	5	14	11	10	9	4	1

Imagem 2.10. Mensagem Codificada.

Dessa forma, a mensagem original “UFAL-PROFMAT-IM-” virou a mensagem codificada “EPBWSXNMVFOLKJEB”.

MENSAGEM CODIFICADA	E	P	B	W	S	X	N	M	V	F	O	L	K	J	E	B
	4	15	1	22	18	23	13	12	21	5	14	11	10	9	4	1

Imagem 2.11. Mensagem final codificada.

Agora que sua mensagem foi transformada em um enigma matemático, é hora de guardá-la com segurança. Nos próximos capítulos, vamos revelar o caminho inverso: como decodificar cada número e recuperar o texto original, letra por letra. A missão está apenas começando.

Capítulo III

Quebrando o Código

Montando a Chave para Desvendar Mensagens

"A única forma de aprender Matemática é fazendo Matemática" - Paul Halmoss

Capítulo III
Quebrando o código

Depois de aprender a transformar palavras em códigos secretos, chegou a hora de dar o próximo passo: desvendar as mensagens codificadas. Para isso, precisamos encontrar uma ferramenta especial, a matriz de decodificação.

Neste capítulo, você vai aprender a "quebrar o código" seguindo um método passo a passo. Usaremos nossa terceira planilha interativa para calcular o determinante, identificar o inverso multiplicativo e construir a matriz que permite transformar códigos aparentemente indecifráveis em palavras compreensíveis. Prepare-se como um detetive que junta pistas para solucionar um mistério.

REUNA NÚMEROS, FÓRMULAS E CONCEITOS MATEMÁTICOS
MONTE A CHAVE QUE REVELA SEGREDOS

3.1 Conhecendo a Terceira Planilha: Matriz de decodificação

A terceira planilha, intitulada "Matriz de decodificação" serve para encontrar a matriz de decodificação com base na matriz-chave que foi usada para codificar a mensagem anteriormente,

Ela conduz o processo de forma simples e organizada, dividindo-o em três etapas: na Parte 1, você insere os números da matriz-chave e obtém automaticamente o determinante e seu valor módulo 27; na Parte 2, identifica-se o inverso multiplicativo do determinante, fundamental para o cálculo da inversa; e na Parte 3, a planilha combina a matriz adjunta com esse inverso para gerar a matriz de decodificação, que permitirá reverter o código e recuperar a mensagem original. Observe na Imagem 3.1.

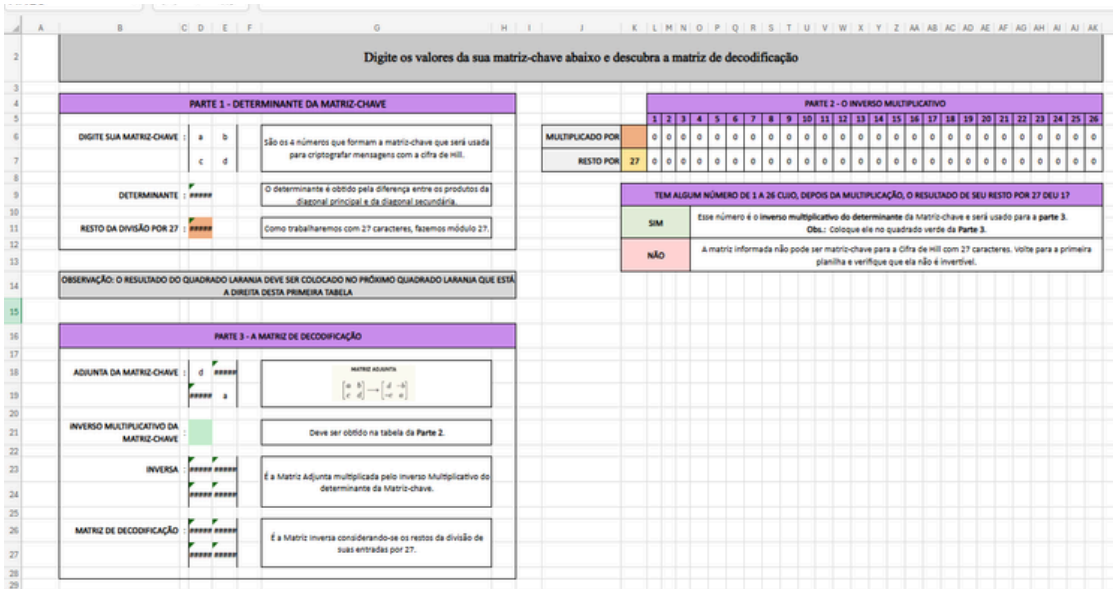


Imagem 3.1. Interface da planilha “Matriz de Decodificação”.

A tabela da parte superior esquerda é a primeira a ser utilizada. Nela, basta digitar a matriz-chave de codificação nas células D6, D7, E6 e E7.

De forma similar a da primeira planilha (Ver no Capítulo I), ao informar as entradas da matriz-chave, a interface está programada para calcular, automaticamente, o determinante dessa matriz e aplicar o módulo 27 a esse determinante, o segundo de forma a procurar pelo “Resto da divisão por 27”. Na Imagem 3.2 encontra-se a aplicação dessa etapa para a matriz de referência que está sendo utilizada desde o primeiro capítulo deste manual.

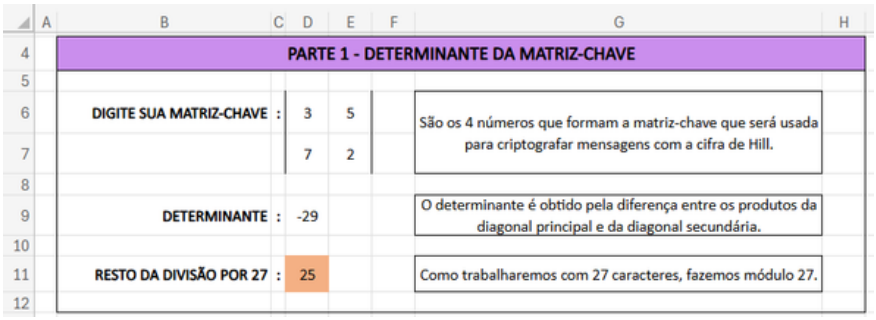


Imagem 3.2. Parte 1 - Determinante da Matriz-chave.

Diante dessa aplicação, a tabela gera o produto final na casa D11, que, nesse caso em específico, foi o número 25. O resultado dessa célula, já destacado no tom laranja, representa o resto da divisão por 27 do determinante da matriz-chave e deve ser utilizado como ponto de partida na próxima tabela da planilha.

A segunda tabela também contém uma célula na cor laranja, a K6. O resultado final da Tabela 1 deve ser posto nessa casa e, após essa alteração, a tabela irá verificar imediatamente qual dos números de 0 a 26 é inverso multiplicativo desse valor, isto é, qual deles gera resultado igual a 1 em módulo 27 quando multiplicado pelo valor especificado.

	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK
4			PARTE 2 - O INVERSO MULTIPLICATIVO																									
5			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
6	MULTIPLICADO POR	25	25	50	75	100	125	150	175	200	225	250	275	300	325	350	375	400	425	450	475	500	525	550	575	600	625	650
7	RESTO POR	27	25	23	21	19	17	15	13	11	9	7	5	3	1	26	24	22	20	18	16	14	12	10	8	6	4	2

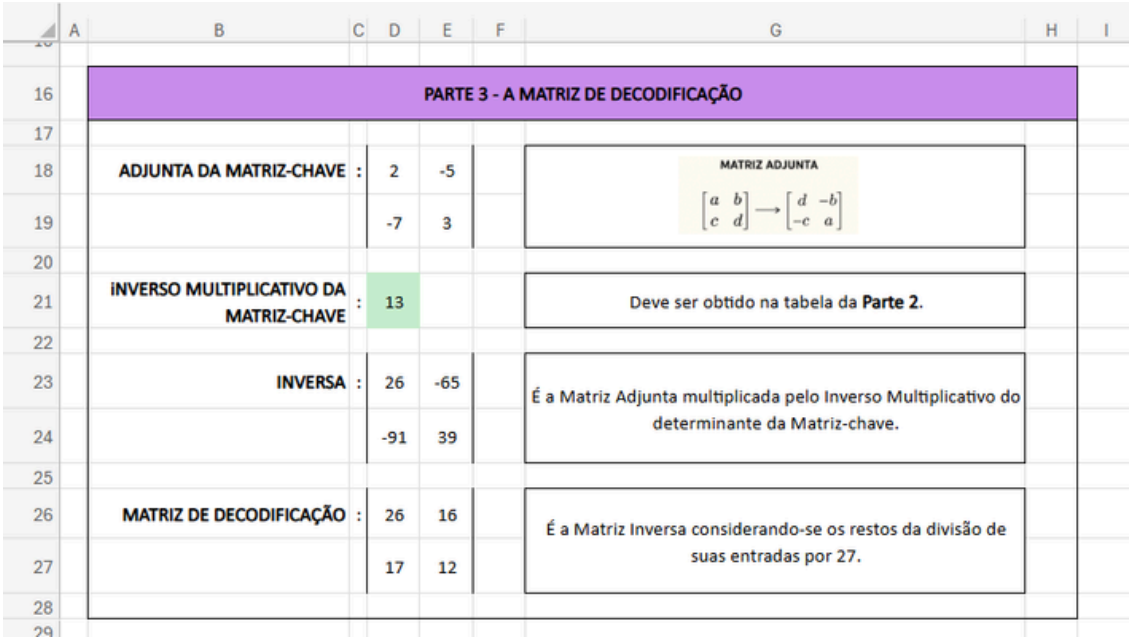
Imagem 3.3. Parte 2 - O inverso multiplicativo.

Na Imagem 3.3 está apontado, em verde, o inverso multiplicativo para o 25, o inverso é o número 13. Ocorre que, para cada número haverá um inverso multiplicativo diferente e a tabela aponta de modo automático esse número, através da coloração verde.

Nessa parte o cuidado foi o de transformar um conceito muito específico do trabalho com a aritmética modular em algo visual para que um estudante de Ensino Médio possa compreender o processo. Então, mediante o auxílio do professor, o aluno irá fazer a verificação de todas as multiplicações nessa tabela, verificando cada caso e que só há um número, dentre as opções disponíveis, que seja inverso multiplicativo para a matriz-chave informada.

Na próxima tabela, a da Parte 3 da planilha, há uma célula nesse mesmo tom esverdeado. Nela, deve-se pôr o inverso multiplicativo encontrado na Tabela 2, que será usado para enfim gerar a matriz de decodificação.

Além disso, a Parte 3 conta também com a adjunta da matriz-chave que, unida ao inverso multiplicativo, gerará, como resultado final, a inversa da matriz-chave, a tão esperada matriz de decodificação. Esse processo está disponível na Imagem 3.4 a seguir.



PARTE 3 - A MATRIZ DE DECODIFICAÇÃO				
ADJUNTA DA MATRIZ-CHAVE :	2	-5	MATRIZ ADJUNTA $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \rightarrow \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$	
	-7	3		
INVERSO MULTIPLICATIVO DA MATRIZ-CHAVE :	13		Deve ser obtido na tabela da **Parte 2**.	
INVERSA :	26	-65	É a Matriz Adjunta multiplicada pelo Inverso Multiplicativo do determinante da Matriz-chave.	
	-91	39		
MATRIZ DE DECODIFICAÇÃO :	26	16	É a Matriz Inversa considerando-se os restos da divisão de suas entradas por 27.	
	17	12		

Imagem 3.3. Parte 3 - A matriz de decodificação.

A tabela apresenta rapidamente a adjunta da matriz-chave, pois ela já pega como referência as entradas da matriz posta pelo estudante na Tabela 1, então ele consegue acompanhar esse processo de forma conjunta, porém, para um auxílio maior, ao lado direito da adjunta há uma explicação sobre a mesma.

Ademais, ao colocar o valos do inverso multiplicativo, a tabela faz

a multiplicação pela adjunta e já expressa também essa matriz pelo módulo 27, como a “matriz de decodificação”, que nada mais é do que a inversa módulo 27 da matriz-chave.

3.2 Conhecendo a Planilha Extra: Decodificação

Essa planilha não ganhou um capítulo só para si porque ela é, essencialmente, a planilha dois, a de codificação. Sua estrutura é igual a da anterior, mudando apenas “matriz-chave” para “matriz de decodificação” e “mensagem codificada” para “mensagem decodificada.

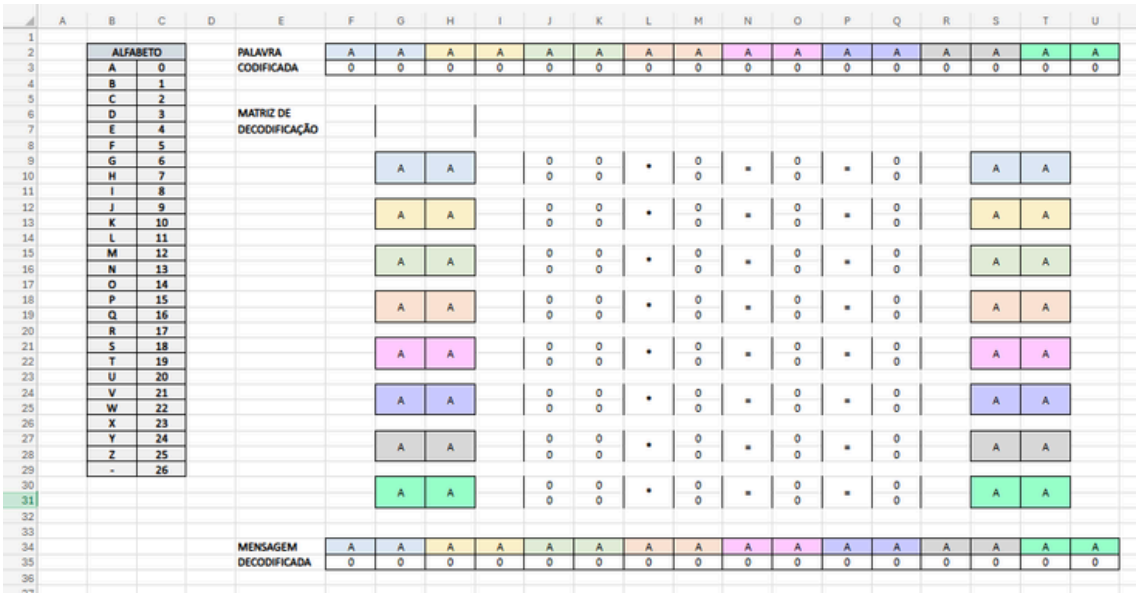
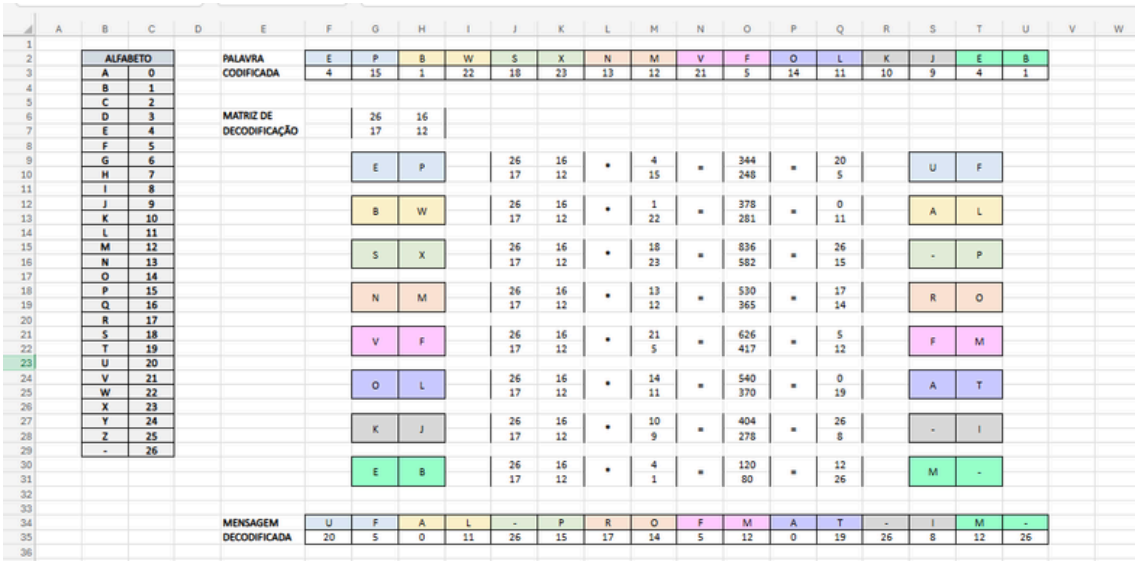


Imagem 3.4. Planilha extra: ambiente de decodificação de mensagem.

Ela serve de apoio para a verificação da decodificação da mensagem, sem excluir o progresso feito na Planilha 2, tendo em vista sua separação da mesma. Observe na Imagem 3.5, nela utilizamos a men-

sagem codificada no Capítulo 2 e a matriz de decodificação encontrada na Seção 3.1 deste capítulo.



ALFABETO	
A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25
-	26

PALAVRA CODIFICADA	E	P	B	W	S	X	N	M	V	F	O	L	K	J	E	B
	4	15	1	22	18	23	13	12	21	5	14	11	10	9	4	1

MATRIZ DE DECODIFICAÇÃO

26	16
17	12

MENSAGEM DECODIFICADA	U	F	A	L	-	P	R	O	F	M	A	T	-	I	M	-
	20	5	0	11	26	15	17	14	5	12	0	19	26	8	12	26

Imagem 3.4. Mensagem decodificada.

Assim, fica fácil verificar que conseguimos retomar a mensagem original e compreender todo o processo por trás disso.

Capítulo IV

O Impasse do Módulo 27

Quando a Cifra Trava

"A Matemática não mente. Mente quem faz mau uso dela."
- Albert Einstein

Depois de aprender a transformar palavras em códigos secretos, chegou a hora de discutirmos o que ocorre quando usamos uma matriz que não é invertível módulo 27. Será que o processo de codificação e decodificação permanece possível? Neste capítulo, investigaremos esse impasse matemático e compreenderemos por que a invertibilidade não é apenas um detalhe técnico, mas o elemento que garante a segurança e a recuperação fiel das mensagens.

NEM TODO CÓDIGO ENCONTRA O CAMINHO DE VOLTA
A INVERTIBILIDADE É A CHAVE

4.1 Codificando sem Inversão

Voltemos a observar a matriz da Imagem 1.2 (abaixo, na Imagem 4.1), matriz essa que não é invertível para o módulo 27.

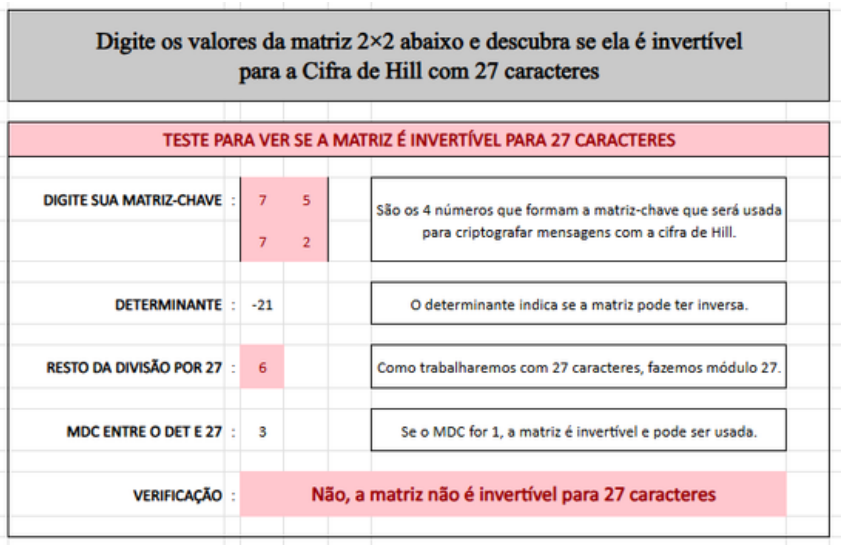
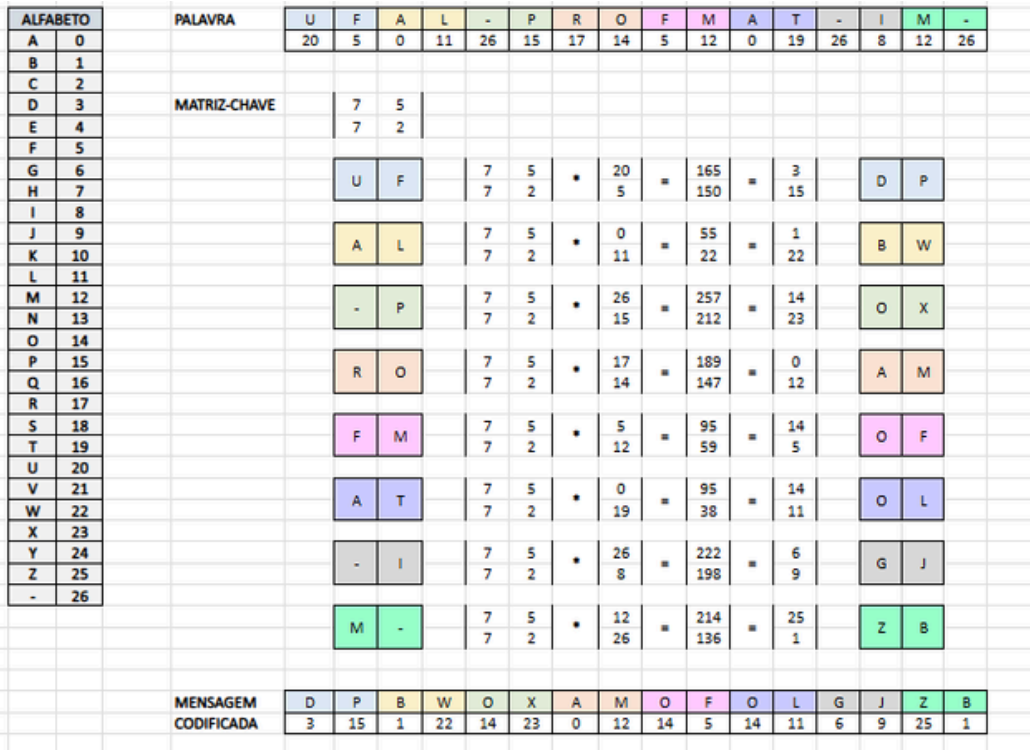


Imagem 4.1. Matriz não invertível em módulo 27.

Por curiosidade, um aluno, mesmo com a instrução da primeira planilha, pode querer continuar a utilizar essa matriz. O próximo

passo desse estudante será codificar uma mensagem na segunda planilha. Aqui utilizaremos da mesma mensagem já codificada nos capítulos anteriores, mas, dessa vez, utilizaremos da matriz não invertível para codificá-la, vejamos o que ocorre no ambiente de codificação da mensagem, sob essas circunstâncias, na Imagem 4.2.



ALFABETO	
A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25
-	26

PALAVRA	U	F	A	L	-	P	R	O	F	M	A	T	-	I	M	-
	20	5	0	11	26	15	17	14	5	12	0	19	26	8	12	26

MATRIZ-CHAVE

7	5
7	2

U	F	7 7	5 2	•	20 5	=	165 150	=	3 15					D	P	
A	L	7 7	5 2	•	0 11	=	55 22	=	1 22					B	W	
-	P	7 7	5 2	•	26 15	=	257 212	=	14 23					O	X	
R	O	7 7	5 2	•	17 14	=	189 147	=	0 12					A	M	
F	M	7 7	5 2	•	5 12	=	95 59	=	14 5					O	F	
A	T	7 7	5 2	•	0 19	=	95 38	=	14 11					O	L	
-	I	7 7	5 2	•	26 8	=	222 198	=	6 9					G	J	
M	-	7 7	5 2	•	12 26	=	214 136	=	25 1					Z	B	

MENSAGEM CODIFICADA	D	P	B	W	O	X	A	M	O	F	O	L	G	J	Z	B
	3	15	1	22	14	23	0	12	14	5	14	11	6	9	25	1

Imagem 4.2. Codificação da mensagem com a nova matriz.

A mensagem foi aparentemente codificada, de fato, a mensagem “UFAL-PROFMAT-IM-” tornou-se “DPBWOXAMOFOLGJZB”. Dessa forma, o estudante pode até achar que deu certo e que “quebrou” o código, afinal, a mensagem foi transformada em outra que é irreconhecível, entretanto, agora ele terá que verificar qual a matriz que pode ser usada para recuperar a mensagem, sigamos então para a terceira planilha na Imagem 4.3.

PARTE 1 - DETERMINANTE DA MATRIZ-CHAVE			
DIGITE SUA MATRIZ-CHAVE :	7	5	São os 4 números que formam a matriz-chave que será usada para criptografar mensagens com a cifra de Hill.
	7	2	
DETERMINANTE :	-21		O determinante é obtido pela diferença entre os produtos da diagonal principal e da diagonal secundária.
RESTO DA DIVISÃO POR 27 :	6		Como trabalharemos com 27 caracteres, fazemos módulo 27.

OBSERVAÇÃO: O RESULTADO DO QUADRADO LARANJA DEVE SER COLOCADO NO PRÓXIMO QUADRADO LARANJA QUE ESTÁ A DIREITA DESTA PRIMEIRA TABELA

Imagem 4.3. Parte 1, inserindo a matriz na planilha

Como visto no Capítulo 3 deste manual, essa primeira parte da planilha serve para obter o determinante da matriz de codificação para prosseguir com a obtenção da matriz de decodificação, acompanhemos, na Imagem 4.4, essa transformação na parte 2, aplicando o valor "6" da célula destacada em laranja na próxima parte, também em uma célula destacada na mesma cor.

		PARTE 2 - O INVERSO MULTIPLICATIVO																								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
MULTIPLICADO POR	6	6	12	18	24	30	36	42	48	54	60	66	72	78	84	90	96	102	108	114	120	126	132	138	144	150	156
RESTO POR	27	6	12	18	24	3	9	15	21	0	6	12	18	24	3	9	15	21	0	6	12	18	24	3	9	15	21

TEM ALGUM NÚMERO DE 1 A 26 CUJO, DEPOIS DA MULTIPLICAÇÃO, O RESULTADO DE SEU RESTO POR 27 DEU 1?	
SIM	Esse número é o **inverso multiplicativo do determinante** da Matriz-chave e será usado para a **parte 3**. **Obs.:** Coloque ele no quadrado verde da **Parte 3**.
NÃO	A matriz informada não pode ser matriz-chave para a Cifra de Hill com 27 caracteres. Volte para a primeira planilha e verifique que ela não é invertível.

Imagem 4.4. Parte 2, tentando encontrar o inverso multiplicativo.

É aqui que o processo apresenta sua falha, ocorre que não há nenhum número que, ao ser multiplicado por 6 e, em seguida, ao ser dividido por 27 dará resto 1. Assim, a matriz não tem inverso multiplicativo e, dessa forma, também não há como encontrar uma matriz de decodificação, tendo em vista que essa matriz tem que ser resultante da multiplicação do inverso multiplicativo pela adjunta da matriz inicial.

No próximo capítulo, exploraremos como esses conceitos podem ser levados à sala de aula e como situações específicas — como o uso da matriz identidade — podem se transformar em oportunidades de reflexão e aprendizagem sobre o papel das matrizes na criptografia.

Capítulo V

Desdobramentos Pedagógicos

Decifre-me Se For Capaz

"Forasteiro — respondeu o Homem que Calculava —, não censuro a curiosidade que te levou a perturbar a marcha de meus cálculos e a serenidade dos meus pensamentos."

- Malba Tahan em "O Homem que Calculava"

Capítulo V
Desdobramentos Pedagógicos

Nos capítulos anteriores, apresentamos as bases matemáticas da Cifra de Hill e exploramos, passo a passo, as planilhas desenvolvidas no Excel para automatizar processos como codificação, decodificação e análise de matrizes no módulo 27. Esses materiais foram construídos para tornar os procedimentos mais acessíveis, organizados e visualmente claros, permitindo que o professor compreenda a lógica por trás de cada etapa.

Chegado este ponto, é hora de deslocar o olhar: das ferramentas para a sala de aula. Neste capítulo, discutiremos como utilizar essas planilhas de forma pedagógica, criando oportunidades de investigação, experimentação e construção de sentido por parte dos estudantes. A criptografia aparece aqui não apenas como contexto motivador, mas como recurso metodológico capaz de integrar tecnologia, raciocínio matemático e resolução de problemas.

Com isso, buscamos mostrar que a matemática pode ser vivida, manipulada e descoberta — e não apenas aplicada mecanicamente.

QUANDO A FERRAMENTA SE TORNA PONTE
A MATEMÁTICA ENCONTRA O ESTUDANTE

5.1 Decifre-me se for capaz

Desafiar a lógica e a interpretação é o ponto de partida deste enigma. Nele, decifrar é mais do que resolver, é compreender os caminhos ocultos do raciocínio matemático daquele que decifrou a mensagem em primeiro lugar. A provocação lógica assemelha-se a um caça palavras, diferenciado apanas pelo fatos de que, primeiramente, as palavras dispostas no jogo estão codificadas e, posteriormente, pelo fato de que toda a tabela representa uma única mensagem completa. Observe um modelo desse desafio na Imagem 5.1.

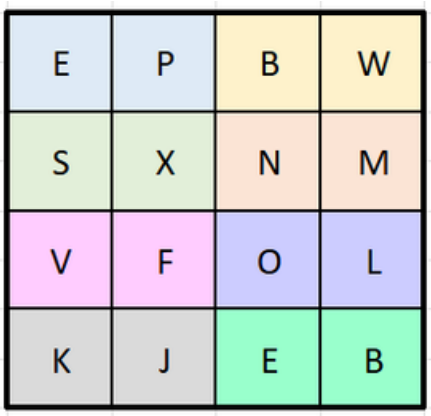


Imagem 5.1. Caça-palavras criptografado com uma matriz-chave de ordem 2.

O caça-palavras codificado tem como objetivo levar os estudantes a entender, para o além de somente aplicar as planilhas. Isto é, além de compreender sua utilização, usá-la como artificio para a construção do conhecimento e como auxílio para a solução do problema que o envolve: encontrar a matriz de codificação de uma mensagem para poder decodificá-la por completo.

Na Imagem 5.1, encontra-se o caça-palavras criptografado com a mesma mensagem utilizada nos capítulos anteriores, a modelo de exemplificação. Como a mensagem foi criptografada com uma matriz-chave de ordem 2, é necessário saber ao menos 2 blocos, de 2 caracteres cada, da mensagem original. Assim, imagine que, neste exemplo, apenas sabemos que, em alguma linha do tabuleiro, encontra-se criptografada a palavra “UFAL” e que todas as linhas juntas formam uma mensagem legitima, isto é, uma mensagem compreensível na lingua portuguesa.

Alguns conhecimentos prévios sobre as condições de codificação da mensagem precisam fazer parte da consciência comum dos desafiados, para que haja a possibilidade de resolução, são elas:

1. A mensagem foi codificada pela utilização da Cifra de Hill;
2. O alfabeto utilizado contém 27 caracteres, sendo os 26 primeiros as letras do alfabeto latino e o 27º o caractere Hífen (-);
3. A matriz chave utilizada é de ordem 2;
4. As entradas da matriz chave são números naturais menores ou iguais a 10;
5. Cada parte da mensagem está disponibilizada em uma linha da tabela;
6. Cada linha deve ser lida da esquerda para a direita.

Assim, vamos começar a solucionar esse quebra-cabeça lógico. Consideremos primeiramente a matriz M abaixo como a nossa matriz-chave de ordem 2 genérica, isto é, a matriz que não conhecemos suas entradas, mas que foi utilizada para codificar a mensagem original. O objetivo aqui é justamente encontrar esses valores para só então conseguir decodificar as mensagens.

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

Por se tratar de uma mensagem já conhecida por nós, sabemos que “UFAL” está escondida na primeira linha do tabuleiro, no entanto, vamos adotar a solução considerando as duas primeiras linhas como possibilidades, para observar o que ocorre quando consideramos que a palavra está escondida em uma linha em que ela não está.

O fato é que, considerando o nosso conjunto alfabético como o descrito no item 2 dos conhecimentos prévios, para qualquer uma das linhas a palavra UFAL dividida nos blocos “UF” e “AL” só tem uma possibilidade de matrizes relacionadas, que está descrita abaixo.

$$\mathrm{UF} \rightarrow \begin{bmatrix} 20 \\ 5 \end{bmatrix} \text{ e } \mathrm{AL} \rightarrow \begin{bmatrix} 0 \\ 11 \end{bmatrix}$$

A primeira linha da tabela é a mensagem “EPBW”, neste caso, consideramos que “UF” virou “EP” e “AL” virou “BW”. Veja abaixo como fica isto consideranto a nossa matriz M.

$$\mathrm{UF} \rightarrow \mathrm{EP} \text{ e } \mathrm{AL} \rightarrow \mathrm{BW}$$

Isto é,

$$\mathrm{EP} \rightarrow \begin{bmatrix} 4 \\ 15 \end{bmatrix} \text{ e } \mathrm{BW} \rightarrow \begin{bmatrix} 1 \\ 22 \end{bmatrix}$$

ou ainda,

$$\mathrm{M} \cdot \mathrm{UF} \equiv \mathrm{EP} \mod 27 \text{ e } \mathrm{M} \cdot \mathrm{AL} \equiv \mathrm{BW} \mod 27$$

Traduzindo isto para o formato matricial:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 20 \\ 5 \end{bmatrix} \equiv \begin{bmatrix} 4 \\ 15 \end{bmatrix} \mod 27 \text{ e } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 11 \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 22 \end{bmatrix} \mod 27$$

$$\Longrightarrow \begin{bmatrix} 20a + 5b \\ 20c + 5d \end{bmatrix} \equiv \begin{bmatrix} 4 \\ 15 \end{bmatrix} \mod 27 \text{ e } \begin{bmatrix} 11b \\ 11d \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 22 \end{bmatrix} \mod 27$$

Em sistemas isto fica:

$$\textbf{(i)}\begin{cases} 20a + 5b \equiv 4 \mod 27 \\ 11b \equiv 1 \mod 27 \end{cases} \text{ e } \textbf{(ii)}\begin{cases} 20c + 5d \equiv 15 \mod 27 \\ 11d \equiv 22 \mod 27 \end{cases}$$

Agora resta apenas resolver os sistemas, lembrando sempre que a congruência em módulo 27 nada mais é do que o resto da divisão por 27. Nesta parte usaremos a tabela 5, que será explicada a medida em que for utilizada. Nesta etapa pode-se utilizar os métodos de solução de sistemas convencionais, no entanto, neste exemplo não será necessário, pois cada sistema apresenta uma de suas duas equivalências com apenas uma incógnita. Começemos então pelo sistema (i), na equivalência mais simples desta.

$$11b \equiv 1 \mod 27$$

Quer se encontrar o número b ao qual, ao multiplicá-lo por 11 e dividí-lo por 27 seu resto será de 1. Para isso irmos utilizar a planilha exposta na Imagem 5.2 abaixo,

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
COEFICIENTE DA ICÓGNITA		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DIVISÃO POR	27	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
QUOCIENTE DA DIVISÃO POR	27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
RESTO DA DIVISÃO POR	27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Recurso de apoio para resolver congruências modulares no módulo 27

Observação: Coloque, na célula C6 (amarela), o coeficiente da icógnita.

Imagem 5.2. Apoio ao “Decifre-me se for capaz”.

Esta planilha serve para testar todos os valores prováveis para a incógnica b na equivalência pontada. Para tanto, colocaremos o coeficiente 11 na célula C6 (em amarelo) e iremos verificar em qual caso o resto da divisão por 27 dá 1, como queremos.

Recurso de apoio para resolver equações modulares no módulo 27																										
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
COEFICIENTE DA ICÓGNITA	11	11	22	33	44	55	66	77	88	99	110	121	132	143	154	165	176	187	198	209	220	231	242	253	264	275	286	297
DIVISÃO POR	27	0,41	0,81	1,22	1,63	2,04	2,44	2,85	3,26	3,67	4,07	4,48	4,89	5,30	5,70	6,11	6,52	6,93	7,33	7,74	8,15	8,56	8,96	9,37	9,78	10,19	10,59	11,00
QUOCIENTE DA DIVISÃO POR	27	0	0	1	1	2	2	2	3	3	4	4	4	5	5	6	6	6	7	7	8	8	8	9	9	10	10	11
RESTO DA DIVISÃO POR	27	11	22	6	17	1	12	23	7	18	2	13	24	8	19	3	14	25	9	20	4	15	26	10	21	5	16	0
Observação: Coloque, na célula C6 (amarela), o coeficiente da incógnita.																												

Imagem 5.3. Apoio para coeficiente igual a 11.

Observando a Imagem 5.3 é possível notar que o resto só dará um na célula H9, que ocorre na multiplicação de 11 pelo valor 5, logo, b tem valor 5. Substituindo isto na primeira congruência do sistema (i), obteremos:

$$\begin{aligned} & 20a + 5b \equiv 4 \mod 27 \\ \Longrightarrow\ & 20a + 5 \cdot 5 \equiv 4 \mod 27 \\ \Longrightarrow\ & 20a + 25 \equiv 4 \mod 27 \\ \Longrightarrow\ & 20a \equiv -21 \mod 27 \end{aligned}$$

Como na planilha de apoio no Excel os restos são positivos, basta orientar que sempre que a equivalência resultar em um número negativo como resto some-se quantos 27 forem necessários até encontrar o primeiro inteiro positivo. Neste caso, basta somar 27 apenas uma vez, resultanto em:

$$20a \equiv 6 \mod 27$$

Com o auxilio da planilha, colocando 20 na célula C6 e procurando, na linha 9, o resto igual a 6, obteremos que tem valor igual a 3 (Ver Imagem 5.4).

Recurso de apoio para resolver equações modulares no módulo 27																										
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
COEFICIENTE DA ICÓGNITA	20	20	40	60	80	100	120	140	160	180	200	220	240	260	280	300	320	340	360	380	400	420	440	460	480	500	520	540
DIVISÃO POR	27	0,74	1,48	2,22	2,96	3,70	4,44	5,19	5,93	6,67	7,41	8,15	8,89	9,63	10,37	11,11	11,85	12,59	13,33	14,07	14,81	15,56	16,30	17,04	17,78	18,52	19,26	20,00
QUOCIENTE DA DIVISÃO POR	27	0	1	2	2	3	4	5	5	6	7	8	8	9	10	11	11	12	13	14	14	15	16	17	17	18	19	20
RESTO DA DIVISÃO POR	27	20	13	6	26	19	12	5	25	18	11	4	24	17	10	3	23	16	9	2	22	15	8	1	21	14	7	0
Observação: Coloque, na célula C6 (amarela), o coeficiente da incógnita.																												

Imagem 5.4. Apoio para coeficiente igual a 20.

Resolveremos o sistema (ii) de forma semelhante, começando pela equivalência mais simples.

$$11d \equiv 22 \mod 27$$

Verificando na Imagem 5.3, o valor de d será 2, pois 11 vezes 2 dá 22 e o resto de 22 na divisão por 27 é ele próprio. Substituindo isso na primeira congruência de (ii), obteremos:

$$\begin{aligned} & 20c + 5d \equiv 15 \mod 27 \\ \Longrightarrow\ & 20c + 5 \cdot 2 \equiv 15 \mod 27 \\ \Longrightarrow\ & 20c + 10 \equiv 15 \mod 27 \\ \Longrightarrow\ & 20c \equiv 5 \mod 27 \end{aligned}$$

E, com o auxílio da Imagem 5.4, c tem valor igual a 7, resultando na matriz M igual a:

$$M = \begin{bmatrix} 3 & 5 \\ 7 & 2 \end{bmatrix}$$

Utilizando as planilhas de matriz de decodificação e a de decifrar a mensagem, obtemos, utilizando o mesmo processo dos capítulos anteriores, a mensagem “UFAL-IM-PROFMAT” que, de fato, é a mensagem que estamos utilizando. Mas ainda vamos verificar esse mesmo processo para a segunda linha do caça-palavras.

A segunda linha da tabela é a mensagem “SXNM”, neste caso, consideramos que “UF” virou “SX” e “AL” virou “NM”. Veja abaixo como fica isto considerando a nossa matriz M.

$$\mathrm{UF} \rightarrow \mathrm{SX} \text{ e } \mathrm{AL} \rightarrow \mathrm{NM}$$

Isto é,

$$\mathrm{SX} \rightarrow \begin{bmatrix} 18 \\ 23 \end{bmatrix} \text{ e } \mathrm{NM} \rightarrow \begin{bmatrix} 13 \\ 12 \end{bmatrix}$$

ou ainda,

$$\mathrm{M} \cdot \mathrm{UF} \equiv \mathrm{SX} \mod 27 \text{ e } \mathrm{M} \cdot \mathrm{AL} \equiv \mathrm{MN} \mod 27$$

Traduzindo isto para o formato matricial:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 20 \\ 5 \end{bmatrix} \equiv \begin{bmatrix} 18 \\ 23 \end{bmatrix} \mod 27 \text{ e } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 11 \end{bmatrix} \equiv \begin{bmatrix} 13 \\ 12 \end{bmatrix} \mod 27$$

$$\Longrightarrow \begin{bmatrix} 20a + 5b \\ 20c + 5d \end{bmatrix} \equiv \begin{bmatrix} 18 \\ 23 \end{bmatrix} \mod 27 \text{ e } \begin{bmatrix} 11b \\ 11d \end{bmatrix} \equiv \begin{bmatrix} 13 \\ 12 \end{bmatrix} \mod 27$$

Em sistemas isto fica:

$$(*) \begin{cases} 20a + 5b \equiv 18 \mod 27 \\ 11b \equiv 13 \mod 27 \end{cases} \text{ e } (**) \begin{cases} 20c + 5d \equiv 23 \mod 27 \\ 11d \equiv 12 \mod 27 \end{cases}$$

Começando a resolver pela equivalência mais simples de (*) e comparando com a Imagem 5.3, b, neste caso, tem valor igual a 11 , fazendo a devida substituição na outra equivalência teremos:

$$\begin{aligned} & 20a + 5b \equiv 18 \mod 27 \\ \Longrightarrow\ & 20a + 5 \cdot 11 \equiv 18 \mod 27 \\ \Longrightarrow\ & 20a + 55 \equiv 18 \mod 27 \\ \Longrightarrow\ & 20a \equiv -37 \mod 27 \end{aligned}$$

Somando 27 duas vezes, teremos:

$$20a \equiv 17 \mod 27$$

Dessa forma, pela Imagem 5.4, o valor de a é 13.

Agora, solucionando (**) da mesma forma, obteremos os valores 1 r 6 para as entradas c e d, respectivamente. Gerando a Matriz-chave de codificação abaixo.

$$M = \begin{bmatrix} 13 & 11 \\ 1 & 6 \end{bmatrix}$$

Com esta matriz, voltemos a utilizar as planilhas deste produto. Primeiramente, utilizaremos a planilha de Matriz de decodificação para achar a inversa de M, acompanhe esse processo nas Imagens 5.5, 5.6 e 5.7 abaixo, que seguem o exposto no Capítulo 3 deste manual.

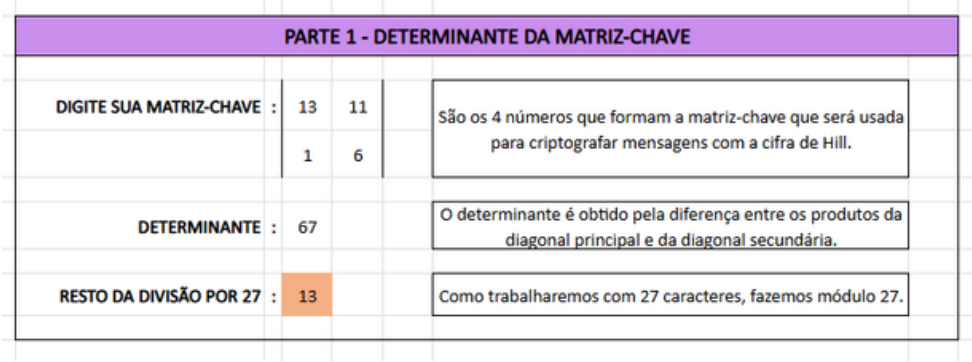


Imagem 5.5. Parte I do processo.

		PARTE 2 - O INVERSO MULTIPLICATIVO																							
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
MULTIPLICADO POR	13	13	26	39	52	65	78	91	104	117	130	143	156	169	182	195	208	221	234	247	260	273	286	299	312	325	338
RESTO POR	27	13	26	12	25	11	24	10	23	9	22	8	21	7	20	6	19	5	18	4	17	3	16	2	15	1	14

TEM ALGUM NÚMERO DE 1 A 26 CUJO, DEPOIS DA MULTIPLICAÇÃO, O RESULTADO DE SEU RESTO POR 27 DEU 1?	
SIM	Esse número é o **inverso multiplicativo do determinante** da Matriz-chave e será usado para a **parte 3**. **Obs.:** Coloque ele no quadrado verde da **Parte 3**.
NÃO	A matriz informada não pode ser matriz-chave para a Cifra de Hill com 27 caracteres. Volte para a primeira planilha e verifique que ela não é invertível.

Imagem 5.6. Parte II do processo.

PARTE 3 - A MATRIZ DE DECODIFICAÇÃO			
ADJUNTA DA MATRIZ-CHAVE :	6	-11	MATRIZ ADJUNTA $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \longrightarrow \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$
	-1	13	
iNVERSO MULTIPLICATIVO DA MATRIZ-CHAVE :	25		Deve ser obtido na tabela da **Parte 2**.
INVERSA :	150	-275	É a Matriz Adjunta multiplicada pelo Inverso Multiplicativo do determinante da Matriz-chave.
	-25	325	
MATRIZ DE DECODIFICAÇÃO :	15	22	É a Matriz Inversa considerando-se os restos da divisão de suas entradas por 27.
	2	1	

Imagem 5.7. Parte III do processo.

Assim, com o auxílio dessa matriz de decodificação e com a planilha de decodificação aplidada à mensagem do caça-palavras obteremos a tradução exposta na Imagem 5.8 a seguir.

MENSAGEM	M	X	N	Y	U	F	A	L	U	U	U	M	Y	C	B	J
DECODIFICADA	12	23	13	24	20	5	0	11	20	20	20	12	24	2	1	9

Imagem 5.8. Decodificação.

De fato, a palavra “UFAL” aparece nos blocos 3 e 4 da mensagem, no entanto, a decodificação não traduz-se em uma mensagem entendível e, portanto, essa não é uma solução para o caça-palavras criptografado.

5.2 Desafio: ès capaz?

DECIFRE-ME SE FOR CAPAZ
É CLARO QUE VOCÊ NÃO IRIA FICAR DE FORA DA BRINCADEIRA

Vamos ao exercício para ver se você pegou o jeito do quebra-cabeça, lembre-se: é importante achar uma mensagem que faça sentido. Observe o caça-palavras na Imagem 5.9 abaixo.

R	T	C	U
-	E	N	V
G	C	P	N
R	T	Z	W

Imagem 5.9. O seu desafio.

Aqui são válidas as mesmas considerações anteriores:

1. A mensagem foi codificada pela utilização da Cifra de Hill;
2. O alfabeto utilizado contém 27 caracteres, sendo os 26 primeiros as letras do alfabeto latino e o 27º o caractere Hífen (-);
3. A matriz chave utilizada é de ordem 2;
4. As entradas da matriz chave são números naturais menores ou iguais a 10;
5. Cada parte da mensagem está disponibilizada em uma linha da tabela;
6. Cada linha deve ser lida da esquerda para a direita.

Dessa vez, porém está escondido "-O-S", de forma que o bloco "-O" é o último de alguma linha e o bloco "-S" é o primeiro da linha seguinte.

Então Professor-leitor, tente inicialmente resolver o desafio proposto, vivenciando a experiência de decodificação antes de levá-la para a sala de aula. Essa etapa é importante para compreender as possíveis dificuldades dos estudantes e para explorar adaptações, como a criação de novos caça-palavras criptografados, ajustando o nível de complexidade conforme o contexto da turma.

5.3 Para além do "Decifre-me se for capaz"

Estamos chegando ao final deste manual, mas não ao fim das possibilidades de trabalho com a Cifra de Hill em sala de aula. Este capítulo teve como objetivo oferecer subsídio para que você, professor, explore a criptografia como uma ferramenta pedagógica capaz de articular conceitos matemáticos, investigação e resolução de problemas.

O desafio “Decifre-me se for capaz” representa apenas um ponto de partida. Ao vivenciar a experiência de decodificação, você é convidado a refletir sobre o potencial dessa abordagem e a adaptá-la às especificidades de suas turmas, seja por meio da criação de novos caça-palavras criptografados, da alteração das mensagens ou da escolha de diferentes matrizes-chave.

Espera-se, assim, que este material sirva como inspiração para práticas pedagógicas que promovam a participação ativa dos estudantes, valorizem o raciocínio lógico e favoreçam a construção significativa do conhecimento matemático, reconhecendo a criptografia como um campo fértil para a integração entre teoria, prática e criatividade.

Neste manual, além da versão para matriz-chave de ordem 2, deixei também acesso para as mesmas planilhas na versão da matriz-chave de ordem 3. Mas, por fim, quero deixar o convite para que, junto aos seus alunos, você possa também adaptar essas planilhas para outros objetivos, seja envolver matrizes de ordem maiores ou, até mesmo, utilizar alfabetos com uma variedade maior de caractéres.

Queremos que a Matemática deixe de ser apenas um conjunto de procedimentos e passa a ser um espaço de experimentação, diálogo e construção coletiva de sentidos. Vamos juntos nessa?

REFERÊNCIAS

- ARAÚJO, Ana Carolina Gonçalves. A Cifra de Hill sob o olhar das planilhas eletrônicas: o estudo de matrizes aplicado à criptografia por meio do Excel. 2026. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal de Alagoas. Maceió, 2026.

- INSTITUTO DE MATEMÁTICA PURA E APLICADA – IMPA. Retrospectiva 2024: 10 anos da medalha Fields de Artur Avila. IMPA – Instituto de Matemática Pura e Aplicada, 03 jan. 2025. Disponível em: https://impa.br/notices/retrospectiva-2024-10-anos-da-medalha-fields-de-artur-avila/. Acesso em: Dez/2025

- JEANRENAUD, Maria de Lourdes R. de A. A cifra de Hill. Temas e Conexões, ano I, n. 1, 2º semestre, 2013.

- LAUNAY, Mickaël. A fascinante história da matemática: da pré-história aos dias de hoje. Tradução de Clóvis Marques. Revisão da tradução de Anna Maria Sotero. 1. ed. Rio de Janeiro: Bertrand Brasil, 2019.

- MARTÍNS, Wellington de Sousa. Aplicação da álgebra moderna nos fundamentos da criptografia: cifras de César e cifras de Hill. 2016. Trabalho de Conclusão de Curso (Licenciatura em Matemática) – Universidade Federal do Tocantins, Campus Universitário de Araguaína, Araguaína, 2016.