CRIPTOGRAFIA COM UTILIZAÇÃO DE CIFRA DE HILL E CIFRA AFIM

Edson Marques Costa
Instituto Federal do Triângulo Mineiro
edsonmarques@iftm.edu.br

Natalia Gonçalves Caetano
Instituto Federal do Triângulo Mineiro
nataliagcmat@gmail.com

RESUMO

Este trabalho consiste no estudo de dois métodos criptográficos de substituição *Cifra de Hill* e *Cifra Afim*, que servirão de auxilio ao estudo da matemática, incentivando atividades que estão relacionadas com a Teoria dos Números, envolvendo Números Inteiros, Divisibilidade, Números Primos e Congruência com os Números Inteiros mostrando suas aplicabilidades. Trabalharemos estes métodos voltados para $\mathbb{Z}_{26}$ que será análogo para $\mathbb{Z}_n$.

ABSTRACT

This work is a study of two cryptographic methods of Hill Cipher and Cipher afim substitution, which will serve as aid to the study of mathematics, encouraging activities that are related to the Theory of Numbers, involving whole numbers, divisibility, prime numbers and congruence with whole numbers showing their applicability. These methods will be worked facing $\mathbb{Z}_{26}$ that will be analogue to $\mathbb{Z}_n$.

Palavras-chave: Criptografia, Teoria dos Números, Aritmética das Classes Residuais.

1 INTRODUÇÃO

Um dos problemas da Teoria dos Números que os estudantes de engenharia e matemática têm dificuldades é de tentar fazer ligações com teorias vistas em sala aplicando as mesmas no cotidiano. Estas dificuldades podem ser minimizadas quando se transforma conceitos teóricos em práticos mostrando suas aplicabilidades, um exemplo disto é a codificação e decodificação de mensagens. Abordaremos a Cifra de Hill e Cifra Afim aplicadas a Teoria dos Números mostrando como as mesmas podem auxiliar neste entendimento.

Para os conceitos introdutórios das cifras Afim e de Hill, o inverso multiplicativo é de suma importância para tal atividade. Nos Inteiros apenas 1 e -1 têm inverso multiplicativo, mas em $\mathbb{Z}_n$ é diferente. Suponha que a seja um inteiro tal que $(a, n) = 1$. Logo existem inteiros α e β tais que $\alpha a + \beta n = 1$ e daí

$$\overline{1} = \overline{\alpha a + \beta n} = \overline{\alpha a} + \overline{\beta n} = \overline{\alpha}\ \overline{a}.$$

Proposição 1.1: *Se $(a, n) = 1$, então $\overline{a}$ possui inverso multiplicativo em $\mathbb{Z}_n$.*

Dessa maneira, em $\mathbb{Z}_{26}$, o inverso de $\overline{23}$ é $\overline{17}$ já que

$$\begin{aligned} 1 &= 3-2 \\ &= 3-(23-7.3) \\ &= 8.3-23 \\ &= 8.(26-23)-23 \\ &= 8.26-9.23 \end{aligned}$$

pelo algorítmo de euclides para cálculo do maior divisor, tomando classes de congruência. Assim, podemos afirmar que,

$$\begin{aligned} \overline{1} &= \overline{8.26-9.23} \\ &= \overline{8.26}+\overline{(-9.23)} \\ &= \overline{8}.\overline{26}+\overline{(-9)}\overline{23} \\ &= \overline{0}+\overline{(-9)}\overline{23} \\ &= \overline{17}.\overline{23} \end{aligned}$$

Para referência futura, temos a tabela com os inversos multiplicativos módulo 26.

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

TABELA 1: Inversos multiplicativos módulo 26

2 CIFRA DE HILL

Esta cifra inventada pelo americano Lester Hill, em 1929, contribuiu em larga escala para tornar a criptografia mais algébrica. Ela consiste em, inicialmente, tomar uma matriz quadradra invertível $n \times n$ módulo 26 da forma

$$M = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

em que cada entrada a_{ij} é um número inteiro em $\mathbb{Z}_{26}$. Essa é a matriz chave do processo.

Para a utilização da Cifra de Hill é necessário alguns resultados que serão de suma importância para o seu desenvolvimento.

Proposição 2.1: *Um número $[a] \in \mathbb{Z}_m$ é invertível se, e somente se, a e m não têm fatores primos comuns, isto é, $mdc(a,m) = 1$*

Demonstração

Suponha que $[a]$ seja invertível, então existe $[b] \in \mathbb{Z}_m$ tal que $[1] = [a] \cdot [b] = [a \cdot b]$. Logo, $ab \equiv 1 \mod m$. Consequentemente, $mdc(a,m) = 1$.
Reciprocamente, se $mdc(a,m) = 1$, existem naturais b e t tais que $ab - mt = 1$ logo, $[1 + mt] = [ab]$. Assim,

$$[1] = [1] + [mt] = [1 + mt] = [a \cdot b] = [a] \cdot [b].$$

Portanto, $[a]$ é invertível.

■

Teorema 2.1: *Uma matriz 2×2 com entradas em $\mathbb{Z}_m$ é invertível módulo m se, e somente se, o resíduo de $det(A)$ módulo m tem um inverso multiplicativo módulo m.*

Demonstração

Seja $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_m)$ e $det(A) = D = ad - bc \in \mathbb{Z}_m$. Suponhamos que a matriz A possua uma inversa multiplicativa módulo m, isto é, existe uma matriz quadrada A^{-1}, com entrada em A, tal que,

$$AA^{-1} = A^{-1}A = I$$

Tomando determinantes, obtemos que,

$$det(A)det(A^{-1}) = det(AA^{-1}) = det(I) = 1 \mod m.$$

Consequentemente $det(A^{-1})$ é o inverso multiplicativo módulo m de $det(A)$.
Reciprocamente, suponhamos que $mdc(m, D) = 1$. Então, $\exists D^{-1} \in \mathbb{Z}_m$ tal que $DD^{-1} = 1 \mod m$. É fácil verificar que

$$A^{-1} = \begin{pmatrix} D^{-1}a & -D^{-1}b \\ -D^{-1}c & D^{-1}d \end{pmatrix}$$

é a matriz inversa de A.

Combinando a Proposição 1 e o Teorema 1, obtemos o seguinte corolário:

Corolário 2.1: *Uma matriz quadrada A com entradas em $\mathbb{Z}_m$ é invertível módulo m se, e somente se, m e o resíduo de $det(A)$ módulo m não tem fatores primos comuns.*

Dessa maneira, dada uma matriz $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, podemos obter a inversa de $M \pmod{26}$ com $det(M) = ad - bc$ não divisivel por 2 ou 13, pela expressão:

$$M^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

onde $(ad - bc)^{-1}$ é o inverso multiplicativo de $det(M)$.

Para criptografar uma mensagem utilizando a cifra de Hill, deve-se primeiramente quebrar a mensagem em partes contendo **n** caracteres, sendo **n** a ordem da matriz dada. Seja X o texto a ser criptografado e

$$x_1x_2x_3...x_n$$

cada letra do bloco partido em **n** caracteres. Para cada letra do alfabeto, atribui-se um valor pré-estabelecido.

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

TABELA 2: Atribuição dos valores

Após a troca das letras pelos seus devidos valores, efetua-se o produto matricial

$$\begin{pmatrix} y_{11} \\ y_{21} \\ \vdots \\ y_{n1} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & ... & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} x_{11} \\ x_{21} \\ \vdots \\ x_{n1} \end{pmatrix}$$

onde as operações são efetuadas módulo 26, para obter-se o bloco criptografado

$$y_1y_2y_3...y_n$$

Se o último bloco de letras do texto original não possuir exatamente **n** letras, ele deve ser completado com letras que não alterem o sentido original da frase. Após esse processo, troca-se os valores $y_1y_2y_3...y_n$ que nesse momento estão em formato numérico, por suas respectivas letras. Utilizando-se esse método até se esgotarem os blocos, o texto estará codificado.

Para decodificar a mensagem, é necessário encontrar a matriz inversa da chave M. Uma matriz quadrada A com elementos em $\mathbb{Z}_{26}$ é invertível em $\mathbb{Z}_{26}$ se existir outra matriz B com elementos em $\mathbb{Z}_{26}$ tal que $AB = I$ onde I é a matriz identidade de ordem n em $\mathbb{Z}_{26}$.

Essa necessidade se dá pelo fato de que

$$\begin{pmatrix} y_{11} \\ y_{21} \\ \vdots \\ y_{n1} \end{pmatrix} = M. \begin{pmatrix} x_{11} \\ x_{21} \\ \vdots \\ x_{n1} \end{pmatrix}$$

$$M^{-1} \begin{pmatrix} y_{11} \\ y_{21} \\ \vdots \\ y_{n1} \end{pmatrix} = M^{-1}M. \begin{pmatrix} x_{11} \\ x_{21} \\ \vdots \\ x_{n1} \end{pmatrix} = \begin{pmatrix} x_{11} \\ x_{21} \\ \vdots \\ x_{n1} \end{pmatrix}$$

assim,

$$\begin{pmatrix} x_{11} \\ x_{21} \\ \vdots \\ x_{n1} \end{pmatrix} = M^{-1} \begin{pmatrix} y_{11} \\ y_{21} \\ \vdots \\ y_{n1} \end{pmatrix},$$

onde $y_1y_2y_3...y_n$ corresponde ao texto codificado inicialmente e $x_1x_2x_3...x_n$ corresponde ao texto original.

3 EXEMPLO DA APLICAÇÃO DA CIFRA DE HILL

Seja uma matriz M da forma

$$M = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

Supondo querer-se criptografar a palavra **amor**. Fazendo a substituição letra a letra pelos seus respectivos valores, tem-se que **amor = (0, 12, 14, 17)**. Vamos utilizar a técnica de Hill para fazer a codificação. Utilizando M como chave e efetuando as operações módulo 26 tem-se.

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 0 \\ 12 \end{pmatrix}$$

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 96 \\ 84 \end{pmatrix} = \begin{pmatrix} 18 \\ 6 \end{pmatrix} = \begin{pmatrix} s \\ g \end{pmatrix}$$

$$\begin{pmatrix} y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix}$$

$$\begin{pmatrix} y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 290 \\ 161 \end{pmatrix} = \begin{pmatrix} 4 \\ 5 \end{pmatrix} = \begin{pmatrix} e \\ f \end{pmatrix}$$

A mensagem cifrada é então **sgef**.

Para decodificar a mensagem é necessário encontrar a inversa da matriz

$$M = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

em $\mathbb{Z}_{26}$, que é dada por

$$M^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}.$$

já que

$$M^{-1} = (11.7 - 8.3)^{-1} \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} = (53)^{-1} \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}.$$

Seja a mensagem codificada **sgef**. Temos que **sgef = (18, 6, 4, 5)** dessa forma, para encontrar os valores originais de $x_1x_2x_3...x_n$ tem-se que

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \begin{pmatrix} 18 \\ 6 \end{pmatrix}$$

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 234 \\ 480 \end{pmatrix} = \begin{pmatrix} 0 \\ 12 \end{pmatrix} = \begin{pmatrix} a \\ m \end{pmatrix},$$

assim como,

$$\begin{pmatrix} x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \begin{pmatrix} 4 \\ 5 \end{pmatrix}$$

$$\begin{pmatrix} x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 118 \\ 147 \end{pmatrix} = \begin{pmatrix} 14 \\ 17 \end{pmatrix} = \begin{pmatrix} o \\ r \end{pmatrix},$$

O que fornece a decodificação da mensagem **sgef** para a mensagem original **amor**.

4 CIFRA AFIM

Assim como a Cifra de Hill, a Cifra Afim consiste em fazer uma substituição das letras do alfabeto por números inteiros entre 0 e 25, seguindo a tabela 2 e depois tomar a seguinte função de criptografar.

$$y_i = c(x_i) \equiv (ax_i + b) \mod 26,$$

Onde **a** e **b** são números em $\mathbb{Z}_{26}$, x_i é a i-ésima letra do alfabeto original, y_i é a i-ésima letra do texto cifrado e $c(x_i)$ corresponde à codificação da letra x_i.

É importante observar que a função acima deve ser injetiva em $\mathbb{Z}_{26}$, pois caso contrário, para duas ou mais letras do alfabeto original ter-se-ia que as elas corresponderiam a uma mesma letra quando cifrada.

Verificando um exemplo para a função $y_i \equiv (13x_i + 3) \mod 26$.

- Para a letra A temos que $x_i = 0$ logo:

  $y_i \equiv (13.0 + 3) \mod 26 \rightarrow y_i \equiv 3 \mod 26 \rightarrow y_i = D$

- Para a letra B temos que $x_i = 1$ logo:
  $y_i \equiv (13.1 + 3) \mod 26 \rightarrow y_i \equiv 16 \mod 26 \rightarrow y_i = Q$
- Para a letra C temos que $x_i = 2$ logo:
  $y_i \equiv (13.2 + 3) \mod 26 \rightarrow y_i \equiv 29 \mod 26 \rightarrow y_i \equiv 3 \mod 26 \rightarrow y_i = D$

$$\vdots$$

Observe-se que essa função não é injetiva, logo não serve para criptografar uma mensagem, pois leva os números pares 0, 2, 4, ... em $\mathbb{Z}_{26}$ no 3 que corresponde a D e os números ímpares em $\mathbb{Z}_{26}$ no 16 que corresponde a Q assim, o texto cifrado só teria duas letras o D e o Q.

Para que a função $y_i = ax_i + b$ seja injetiva em $\mathbb{Z}_{26}$ devemos ter que a e 26 sejam primos entre si. Quando isso ocorre, tem-se que a função

$$y_i = c(x_i) \equiv (ax_i + b) \mod 26,$$

serve para codificar o texto original, e a função

$$x_i = d(y_i) \equiv a^{-1}(y_i - b) \mod 26$$

serve para decodificar o texto cifrado, já que

$$y_i \equiv (ax_i + b) \mod 26, y_i - b \equiv ax_i \mod 26, a^{-1}(y_i - b) \equiv x_i \mod 26, x_i = d(y_i) \equiv a^{-1}(y_i - b) \mod 26$$

em que a^{-1} indica o inverso módulo 26 de a.

5 EXEMPLO DE APLICAÇÃO DA CIFRA AFIM

Considerando-se o codificador:

$$y_i = c(x_i) \equiv (7x_i + 1) \mod 26.$$

Temos que 7 e 26 são primos entre si dessa forma, a função é injetiva módulo 26.

- Para a letra A temos que $x_i = 0$ logo:
  $y_i \equiv (7.0 + 1) \mod 26 \rightarrow y_i \equiv 1 \mod 26 \rightarrow y_i = B$
- Para a letra B temos que $x_i = 1$ logo:
  $y_i \equiv (7.1 + 1) \mod 26 \rightarrow y_i \equiv 8 \mod 26 \rightarrow y_i = I$
- Para a letra C temos que $x_i = 2$ logo:
  $y_i \equiv (7.2 + 1) \mod 26 \rightarrow y_i \equiv 15 \mod 26 \rightarrow y_i = P$

$$\vdots$$

A tabela 3 fornece as devidas codificações das letras bem como sua correspondencia em $\mathbb{Z}_{26}$ isso faz com que a letra A seja representada pela letra B quando codificada, a letra B pela letra I, a letra C pela letra P e assim sucessivamente.

Por exemplo, a mensagem:

"Mais vale a lágrima da derrota, do que a vergonha de não ter lutado."

fica assim codificada:

Letra Original	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
x_i	00	01	02	03	04	05	06	07	08	09	10	11	12
y_i	01	08	15	22	03	10	17	24	05	12	19	00	07
Letra Cifrada	B	I	P	W	D	K	R	Y	F	M	T	A	H
Letra Original	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
x_i	13	14	15	16	17	18	19	20	21	22	23	24	25
y_i	14	21	02	09	16	23	04	11	18	25	06	13	20
Letra Cifrada	O	V	C	J	Q	X	E	L	S	Z	G	N	U

TABELA 3: Decodificação das letras

"HBFX SBAD B ABRQFHB WB WDQQVEB, WV JLD B SDQRVOYB WD OBV EDQ ALEBWV."

Para decifrar a mensagem já codificada, inicialmente deve-se encontrar o inverso de 7 módulo 26 que é 15 já que, $15 \cdot 7 \equiv 1 \mod 26$. A função que serve como decodificador da mensagem é dada por:

$$x_i = d(y_i) \equiv a^{-1}(y_i - b) \mod 26,$$

logo,

$$x_i = d(y_i) \equiv 15(y_i - 1) \mod 26,$$

que equivale à:

$$x_i = d(y_i) \equiv (15y_i + 11) \mod 26$$

ou seja, quando o texto está codificado, a letra P correspondente a $y_i = 15$ representa

$$\begin{gathered} x_i = d(15) \equiv (15.15 + 11) \mod 26 \\ x_i = d(15) \equiv (236) \mod 26 \\ x_i = d(15) \equiv 2 \mod 26 \end{gathered}$$

logo, P corresponde a $x_i = 2$ que equivale a C quando codificado. Fazendo esse processo para todas as letras do alfabeto codificadas do texto, temos que a mensagem estará decodificada.

6 CONCLUSÃO

Neste trabalho propusemos dois métodos cifrários de codificação e decodificação de mensagens com a utilização dos conceitos de Teoria dos Números. Os métodos de cifragem, são excelentes aplicações dos conceitos de congruência podendo desta maneira mostrar aplicabilidades das matérias vistas em sala em situações que possam vir a ser necessárias.

Mostrar a importância de como a criatividade acompanha o desenvolvimento da matemática, dando suporte para evoluções tecnológicas atuais, pode fazer com que o aluno aumente sua capacidade de interligar os conteúdos vistos em sala com outras aplicações, conseguindo identificar situações possíveis de utilizar tais conhecimentos.

Os livros [1] e [2] são excelentes para o estudo de conceitos envolvendo Teoria dos Números já [3], [4], [5] e principalmente [6] são excelentes livros para um bom entendimento dos processos criptográficos.

REFERÊNCIAS

[1] J. P. O. SANTOS, *Introdução à Teoria dos Números*. Rio de Janeiro: IMPA, 3 ed., 2000.

[2] C. M. MARQUES, *Introdução à Teoria de Anéis*. Departamento de Matemática-UFMG, Belo Horizonte, 1995.

[3] N. KOBLITZ, *A Course in Number Theory and Cryptography*. Springer-Verlag, 2 ed., 1987.

[4] A. C. FALEIROS, *Criptografia*. Centro de Matemática, Computação e Cognição Universidade Federal do ABC, Santo André, São Paulo, 2010.

[5] P. J. ALMEIDA, *Criptografia e Segurança*. Departamento de Matemática de Aveiro, Portugal: Engebook, 2012.

[6] V. M. C. FIARRESGA, "Criptografia e matemática," Master's thesis, Universidade de Lisboa, Faculdade de Ciências, 2010.