Cifra de Hill: um breve estudo da Criptografia através da Álgebra Linear

Thalita Alves Veron[1] **& Saradia Sturza Della Flora**[2]

Universidade Federal de Santa Maria - RS

[1]thalitaalvesveron@gmail.com

[2]saradia.flora@ufsm.br

Introdução

Desde a antiguidade, destaca-se a necessidade de obter segurança na transmissão de informações. O estudo da codificação e decodificação de mensagens secretas é denominado Criptografia. As cifras são os códigos usados para transformar um texto comum em texto cifrado. O processo de converter um texto comum em cifrado é chamado codificar, e o processo inverso é chamado decodificar. Neste trabalho, vamos estudar a cifra de Hill, elaborada por Lester S. Hill, em meados de 1929.

Embasamento Teórico

Iremos assumir que cada letra de texto comum e de texto cifrado, excluindo o Z, está associado a um valor numérico, de acordo com a sua posição no alfabeto, conforme a Tabela 1. Além disso, vamos atribuir ao Z o valor 0.

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
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	0

Tabela 1: Equivalentes Numéricos

Para codificar uma mensagem utilizando a cifra de Hill, transformamos pares sucessivos de texto comum em texto cifrado, de acordo com o seguinte procedimento.

Passo 1. Escolher uma matriz $\boldsymbol{A}$ de ordem $\mathbf{2\times 2}$ com entradas em $\mathbb{Z}_{26}$ para efetuar a codificação (matriz codificadora).

Passo 2. Agrupar as letras sucessivas do texto comum em pares, e substituir cada letra de texto comum por seu valor numérico.

Passo 3. Converter cada par de letras de texto comum, $\boldsymbol{p_1}$ $\boldsymbol{p_2}$ em um vetor coluna

$$\boldsymbol{p} = \begin{pmatrix} \boldsymbol{p_1} \\ \boldsymbol{p_2} \end{pmatrix}$$

obtendo $\boldsymbol{Ap}$. Dizemos que $\boldsymbol{p}$ é o vetor comum e $\boldsymbol{Ap}$ o correspondente vetor cifrado.

Passo 4. Converter cada vetor cifrado em seu equivalente alfabético.

Desde que 26 não é primo, $\mathbb{Z}_{26}$ não é corpo. A tabela a seguir, mostra os elementos inversíveis e seus respectivos inversos multiplicativos. Por uma questão de simplicidade, vamos omitir as barras ao escrever uma classe módulo 26.

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

Tabela 2: Inversos Multiplicativos módulo 26

Para decifrar as cifras de Hill, vamos usar a inversa (mod 26) da matriz $\boldsymbol{A}$. Uma matriz com entradas em $\mathbb{Z}_{26}$ é inversível módulo 26 se somente se o resíduo do $\det(\boldsymbol{A})$ módulo 26, não é divisível por 2 ou 13. Também utilizaremos o seguinte resultado que pode ser encontrado em [1].

Teorema: Sejam $\boldsymbol{p_1}, \ldots, \boldsymbol{p_n}$ vetores comuns linearmente independentes e $\boldsymbol{c_1}, \ldots, \boldsymbol{c_n}$ os correspondentes vetores cifrados de uma cifra de Hill de ordem $\boldsymbol{n}$. Se $\boldsymbol{P}$ for a matriz $\boldsymbol{n \times n}$ de vetores linha $\boldsymbol{{p_1}^T, \ldots, {p_n}^T}$, e $\boldsymbol{C}$ a matriz $\boldsymbol{n \times n}$ de vetores linha $\boldsymbol{{c_1}^T, \ldots, {c_n}^T}$ então, a sequência de operações elementares com as linhas que reduz $\boldsymbol{C}$ a $\boldsymbol{I}$ transforma $\boldsymbol{P}$ em $(\boldsymbol{A^{-1}})^T$.

Problema

Vamos utilizar a matriz codificadora $\boldsymbol{A} = \begin{pmatrix} \mathbf{1} & \mathbf{2} \\ \mathbf{1} & \mathbf{3} \end{pmatrix}$ para obter a cifra de Hill da mensagem

ÁLGEBRA LINEAR

Agrupando o texto em pares de letras, encontraremos os respectivos valores numéricos, de acordo com a Tabela 1.

AL	GE	BR	AL	IN	EA	RR
1 12	7 5	2 18	1 12	9 14	5 1	18 18

Para efetuar a codificação é necessário realizar a multiplicação entre a matriz $\boldsymbol{A}$ e os valores numéricos de cada par de letras de texto comum e observar os seus equivalentes alfabéticos:

$$\begin{pmatrix} \mathbf{1} & \mathbf{2} \\ \mathbf{1} & \mathbf{3} \end{pmatrix} \begin{pmatrix} \mathbf{1} \\ \mathbf{12} \end{pmatrix} = \begin{pmatrix} \mathbf{25} \\ \mathbf{11} \end{pmatrix}, \quad \begin{pmatrix} \mathbf{1} & \mathbf{2} \\ \mathbf{1} & \mathbf{3} \end{pmatrix} \begin{pmatrix} \mathbf{7} \\ \mathbf{5} \end{pmatrix} = \begin{pmatrix} \mathbf{17} \\ \mathbf{22} \end{pmatrix},$$

$$\begin{pmatrix} \mathbf{1} & \mathbf{2} \\ \mathbf{1} & \mathbf{3} \end{pmatrix} \begin{pmatrix} \mathbf{2} \\ \mathbf{18} \end{pmatrix} = \begin{pmatrix} \mathbf{12} \\ \mathbf{4} \end{pmatrix}, \quad \begin{pmatrix} \mathbf{1} & \mathbf{2} \\ \mathbf{1} & \mathbf{3} \end{pmatrix} \begin{pmatrix} \mathbf{9} \\ \mathbf{14} \end{pmatrix} = \begin{pmatrix} \mathbf{11} \\ \mathbf{25} \end{pmatrix},$$

$$\begin{pmatrix} \mathbf{1} & \mathbf{2} \\ \mathbf{1} & \mathbf{3} \end{pmatrix} \begin{pmatrix} \mathbf{5} \\ \mathbf{1} \end{pmatrix} = \begin{pmatrix} \mathbf{7} \\ \mathbf{8} \end{pmatrix}, \quad \begin{pmatrix} \mathbf{1} & \mathbf{2} \\ \mathbf{1} & \mathbf{3} \end{pmatrix} \begin{pmatrix} \mathbf{18} \\ \mathbf{18} \end{pmatrix} = \begin{pmatrix} \mathbf{2} \\ \mathbf{20} \end{pmatrix},$$

resultando no texto cifrado:

YKQVLDYKKYGHBT

Agora, vamos decodificar o texto cifrado, sabendo que o texto comum inicia-se com ALGE. Primeiramente, é necessário agrupar a parte inicial do texto comum e do texto cifrado em pares de letras:

AL	GE	YK	QV
1 12	7 5	25 11	17 22

Os vetores comuns e os correspondentes cifrados são:

$$\boldsymbol{p_1} = \begin{pmatrix} \mathbf{1} \\ \mathbf{12} \end{pmatrix} \leftrightarrow \mathrm{c}_1 = \begin{pmatrix} \mathbf{25} \\ \mathbf{11} \end{pmatrix}, \quad \boldsymbol{p_2} = \begin{pmatrix} \mathbf{7} \\ \mathbf{5} \end{pmatrix} \leftrightarrow \mathrm{c}_2 = \begin{pmatrix} \mathbf{17} \\ \mathbf{22} \end{pmatrix}.$$

Assim, obtemos as matrizes:

$$\boldsymbol{P} = \begin{pmatrix} \mathbf{1} & \mathbf{12} \\ \mathbf{7} & \mathbf{5} \end{pmatrix}, \quad \boldsymbol{C} = \begin{pmatrix} \mathbf{25} & \mathbf{11} \\ \mathbf{17} & \mathbf{22} \end{pmatrix}.$$

Escalonando a matriz $[\boldsymbol{C}|\boldsymbol{P}]$, resulta em

$$\left(\begin{array}{cc|cc} \mathbf{1} & \mathbf{0} & \mathbf{3} & \mathbf{25} \\ \mathbf{0} & \mathbf{1} & \mathbf{24} & \mathbf{1} \end{array}\right).$$

Portanto, a matriz decodificadora é $\boldsymbol{A^{-1}} = \begin{pmatrix} \mathbf{3} & \mathbf{24} \\ \mathbf{25} & \mathbf{1} \end{pmatrix}$.

Para decifrar a mensagem, agrupamos o texto cifrado em pares de letras, determinando os respectivos equivalentes numéricos, de acordo com a Tabela 1. Na sequência, efetuamos a multiplicação entre a matriz decodificadora e os vetores $\boldsymbol{c_1}, \ldots, \boldsymbol{c_7}$, com o intuito de recuperar os vetores $\boldsymbol{p_1}, \ldots, \boldsymbol{p_7}$, como segue o exemplo abaixo:

$$\begin{pmatrix} \mathbf{3} & \mathbf{24} \\ \mathbf{25} & \mathbf{1} \end{pmatrix} \begin{pmatrix} \mathbf{25} \\ \mathbf{11} \end{pmatrix} = \begin{pmatrix} \mathbf{1} \\ \mathbf{12} \end{pmatrix}.$$

Dando continuidade às multiplicações, e de acordo com a Tabela 1, obtemos o texto original:

AL GE BR AL IN EA RR

Conclusão

A cifra de Hill foi extremamente revolucionária, visto que, foi a primeira cifra de substituição poligráfica, que introduziu ideias de proteção de dados por meio de matrizes. Com o passar dos anos e com o advento das novas tecnologias, algoritmos mais poderosos surgiram e tornaram a respectiva cifra obsoleta, em razão das suas vulnerabilidades. Todavia, é inquestionável o legado deixado pela cifra de Hill.

Trabalho apoiado pelo programa PET-MEC/FNDE

Referências

[1] ANTON, Howard; RORRES, Chris. **Álgebra Linear com Aplicações**. 10. ed. Porto Alegre: Bookman, 2012.

[2] MILIES, César Polcino; COELHO, Sônia Pitta **Números: Uma Introdução à Matemática.** 3. ed. Editora da Universidade de São Paulo. São Paulo, 2013.