APLICAÇÃO DA ÁLGEBRA LINEAR EM CIFRAS DE HILL: UMA PERSPECTIVA PRÁTICA

Augusto Junior[1]

RESUMO

Este artigo explora a aplicação prática da álgebra linear nas Cifras de Hill, um método criptográfico que utiliza operações matriciais para cifragem e decifragem. Destacamos a interseção entre princípios da álgebra linear e a eficácia das Cifras de Hill, fornecendo uma visão introdutória e prática. Analisamos a estrutura do algoritmo e sua implementação em situações do mundo real, destacando a relevância dessa abordagem matemática na segurança criptográfica. Este estudo contribui para a compreensão teórica e prática da criptografia baseada em álgebra linear, enfatizando a importância desses métodos em cenários contemporâneos de segurança da informação.

Palavras-chave: criptografia. álgebra linear. segurança.

1 INTRODUÇÃO

A criptografia, desde seus primórdios, tem sido um campo essencial na proteção da comunicação sensível e confidencial. À medida que a tecnologia avança, os métodos criptográficos evoluem para lidar com ameaças cada vez mais sofisticadas. Dentro desse cenário, a álgebra linear emerge como uma ferramenta poderosa na concepção e análise de sistemas criptográficos robustos. Este artigo visa explorar a aplicação prática da álgebra linear em um contexto específico: as Cifras de Hill.

As Cifras de Hill, introduzidas por Lester S. Hill em 1929, representam uma classe fascinante de algoritmos criptográficos que se baseiam em conceitos fundamentais da álgebra linear. Ao contrário de muitos métodos criptográficos tradicionais, as Cifras de Hill operam sobre blocos de texto, aproveitando-se de operações matriciais para realizar a cifragem e a decifragem. Essa abordagem não apenas adiciona uma camada adicional de complexidade à segurança do sistema, mas também oferece uma perspectiva prática que pode ser explorada para aplicações diversas.

Nesta análise, examinaremos de perto a estrutura e o funcionamento das Cifras de Hill, destacando como os princípios da álgebra linear se entrelaçam de maneira intrínseca com a eficácia desse método criptográfico. Além disso, iremos explorar casos de uso prático das Cifras de Hill, demonstrando como esses algoritmos podem ser implementados em

[1]Graduando em sistemas de informação pela UFOPA

situações do mundo real, proporcionando segurança e confidencialidade em diferentes contextos.

À medida que mergulhamos nesta exploração da aplicação prática da álgebra linear nas Cifras de Hill, esperamos fornecer uma visão clara e abrangente de como esses conceitos matemáticos podem ser traduzidos em soluções criptográficas tangíveis. Este estudo não apenas contribuirá para a compreensão teórica desses métodos, mas também lançará luz sobre a importância de considerações práticas na implementação de sistemas de segurança criptográfica baseados em álgebra linear.

2 EXPLORAÇÃO DE CONCEITOS DE ALGEBRA LINEAR NAS CIFRAS DE HILL

Antes de avançarmos nos estudos sobre a Cifra de Hill, é essencial explorar os fundamentos da álgebra linear que serão aplicados. Neste contexto, serão empregados conceitos como matrizes, matrizes inversas, determinantes e operações modulares, fornecendo a base teórica necessária para a compreensão do método criptográfico em questão.

2.1 Matrizes

Nas Cifras de Hill, as mensagens são representadas por matrizes. Cada matriz é composta por blocos de texto, e a cifragem ocorre por meio de multiplicação matricial. Entender como as matrizes representam dados é crucial para a implementação e análise dessa cifra.

2.2 Determinantes

A existência da matriz inversa, vital para o processo de decifragem, está intrinsecamente ligada aos determinantes. Se o determinante de uma matriz não for zero, a matriz é invertível. Portanto, o estudo dos determinantes é essencial para avaliar a viabilidade de aplicação da Cifra de Hill em determinados contextos.

2.3 Operações Modulares

As operações modulares são incorporadas às Cifras de Hill para assegurar que os cálculos permaneçam dentro de um conjunto finito. Isso é crucial para a segurança e eficácia da cifragem. Ao entender como as operações modulares são aplicadas em conjunto com matrizes, garantimos a integridade e a confidencialidade dos dados cifrados.

3 A CIFRA DE HILL

3.1 Criptografando

Primeiro, precisamos criar uma associação entre os caracteres utilizados e números inteiros. Nesse caso, os caracteres serão as 26 letras do alfabeto:

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	26

Para o propósito deste exercício, usaremos a letra Z como um caractere coringa.

Após montar a associação, precisamos definir uma matriz quadrada qualquer que será a chave criptográfica usada no procedimento. Por questões de praticidade, será usada uma matriz quadrada 2×2:

$$A_{2\times 2} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

Definindo $a_{11} = 2, a_{12} = 1, a_{21} = -1$ e $a_{22} = 4$, teremos:

$$A = \begin{bmatrix} 2 & 1 \\ -1 & 4 \end{bmatrix}$$

Neste exemplo, será criptografada a palavra UFOPA. Para isso, serão atribuídos números inteiros correspondentes às letras da palavra, conforme na tabela de correspondência:

U	F	O	P	A
21	6	15	16	1

Após isso, encontraremos o produto entre a matriz A e o vetor formado pelos números correspondentes da palavra UFOPA:

$$\begin{bmatrix} 2 & 1 \\ -1 & 4 \end{bmatrix} \cdot \begin{bmatrix} 21 \\ 6 \end{bmatrix} = \begin{bmatrix} 2 \cdot 21 + 1 \cdot 6 \\ (-1) \cdot 21 + 4 \cdot 6 \end{bmatrix} = \begin{bmatrix} 48 \\ 3 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ -1 & 4 \end{bmatrix} \cdot \begin{bmatrix} 15 \\ 16 \end{bmatrix} = \begin{bmatrix} 2 \cdot 15 + 1 \cdot 16 \\ (-1) \cdot 15 + 4 \cdot 16 \end{bmatrix} = \begin{bmatrix} 46 \\ 49 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ -1 & 4 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 26 \end{bmatrix} = \begin{bmatrix} 2 \cdot 1 + 1 \cdot 26 \\ (-1) \cdot 1 + 4 \cdot 26 \end{bmatrix} = \begin{bmatrix} 28 \\ 103 \end{bmatrix}$$

Em seguida, calcularemos o resto da divisão dos elementos encontrados por 26, que é o total de caracteres:

$$\begin{bmatrix} 48 \\ 3 \end{bmatrix} \mod (26) = \begin{bmatrix} 22 \\ 3 \end{bmatrix}$$

$$\begin{bmatrix} 46 \\ 49 \end{bmatrix} \mod (26) = \begin{bmatrix} 20 \\ 23 \end{bmatrix}$$

$$\begin{bmatrix} 28 \\ 103 \end{bmatrix} \mod (26) = \begin{bmatrix} 2 \\ 25 \end{bmatrix}$$

3.2 Descriptografando

Para descriptografar os dados obtidos, será usada a matriz inversa de A e seu determinante:

$$A = \begin{bmatrix} 2 & 1 \\ -1 & 4 \end{bmatrix} \implies A^{-1} = \begin{bmatrix} 4 & -1 \\ 1 & 2 \end{bmatrix}$$

$$det(A^{-1}) = \begin{vmatrix} 4 & -1 \\ 1 & 2 \end{vmatrix} = (4 \cdot 2) - ((-1) \cdot 1) = 8 - (-1) = 9$$

Em seguida, encontraremos o inverso modular do determinante da matriz inversa A^{-1}, ou seja:

$$det(A^{-1}) \cdot I \mod (26) = 1$$
$$9 \cdot I \mod (26) = 1 \implies I = 3$$

A chave de descriptografia será o resto da divisão por 26 do produto entre o inverso modular I e a matriz inversa A^{-1}:

$$I \cdot A^{-1} \mod (26) \implies 3 \cdot \begin{bmatrix} 4 & -1 \\ 1 & 2 \end{bmatrix} \mod (26)$$

$$\begin{bmatrix} 12 & -3 \\ 3 & 6 \end{bmatrix} \mod (26)$$

$$\begin{bmatrix} 12 & 23 \\ 3 & 6 \end{bmatrix}$$

Para encontrar a mensagem descriptografada, faremos o produto entre a chave de descriptografia e os dados criptografados:

$$\begin{bmatrix} 12 & 23 \\ 3 & 6 \end{bmatrix} \cdot \begin{bmatrix} 22 \\ 3 \end{bmatrix} = \begin{bmatrix} 12 \cdot 22 + 23 \cdot 3 \\ 3 \cdot 22 + 6 \cdot 3 \end{bmatrix} = \begin{bmatrix} 333 \\ 84 \end{bmatrix}$$

$$\begin{bmatrix} 12 & 23 \\ 3 & 6 \end{bmatrix} \cdot \begin{bmatrix} 20 \\ 23 \end{bmatrix} = \begin{bmatrix} 12 \cdot 20 + 23 \cdot 23 \\ 3 \cdot 20 + 6 \cdot 23 \end{bmatrix} = \begin{bmatrix} 769 \\ 198 \end{bmatrix}$$

$$\begin{bmatrix} 12 & 23 \\ 3 & 6 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 25 \end{bmatrix} = \begin{bmatrix} 12 \cdot 2 + 23 \cdot 25 \\ 3 \cdot 2 + 6 \cdot 25 \end{bmatrix} = \begin{bmatrix} 599 \\ 156 \end{bmatrix}$$

Por fim, os dados descriptografados, serão encontrados através do resto da divisão dos termos encontrados por 26:

$$\begin{bmatrix} 333 \\ 84 \end{bmatrix} \mod (26) = \begin{bmatrix} 21 \\ 6 \end{bmatrix}$$

$$\begin{bmatrix} 769 \\ 198 \end{bmatrix} \mod (26) = \begin{bmatrix} 15 \\ 16 \end{bmatrix}$$

$$\begin{bmatrix} 599 \\ 156 \end{bmatrix} \mod (26) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Portanto, a mensagem descriptografada será :

21	6	15	16	1
U	F	O	P	A

4 CONSIDERAÇÕES FINAIS

As cifras de Hill, baseadas na multiplicação matricial, destacam-se como uma aplicação prática e eficaz da álgebra linear. A capacidade de manipular blocos de texto por meio de operações matriciais não apenas adiciona uma camada adicional de complexidade à criptografia, mas também abre portas para soluções criptográficas versáteis em diversas áreas.

Este estudo reforça a importância de entender não apenas os fundamentos teóricos, mas também a aplicação prática da álgebra linear na criptografia. A análise das cifras de Hill não se limita a uma abordagem puramente matemática; ela se estende à implementação em cenários do mundo real, onde a segurança da informação é uma prioridade constante.

REFERÊNCIAS

BOLDRINI, José Luiz et al. **Álgebra Linear**. 3. ed. revista e atualizada. UNICAMP, 1980.

SOUZA, Maycon Pereira. **CIFRA DE HILL**. nstituto Federal de Goiás – Campus Uruaçu. Disponível em: <http://cts.luziania.ifg.edu.br/CTS1/article/download/100/pdf_30>

SILVA. Sógenes G. P. da. CRIPTOGRAFIA. Disponível em: <http://pt.slideshare.net/sogenes/criptografia-1805777>. Acesso em: 02 Jan. 2015.