ÁLGEBRA LINEAR APLICADA A SISTEMAS DE SEGURANÇA: ANÁLISE DO CRIPTOSISTEMA DE HILL

Gunnar Vingren Teixeira Aparicio*
Erik Luiz Dullius Carneiro** Miguel Nunes Roso***

*Universidade Federal de Santa Maria **Universidade Federal de Santa Maria
***Universidade Federal de Santa Maria

Resumo

Este trabalho de pesquisa visa analisar a aplicação da Álgebra Linear como ferramenta fundamental na criptografia de sistemas de segurança da informação. O objetivo principal é demonstrar como conceitos de matrizes, vetores e transformações lineares são empregados no desenvolvimento de algoritmos criptográficos robustos, como o Criptosistema de Hill. A metodologia consistiu em uma revisão bibliográfica sistemática sobre a teoria de números aplicada à criptografia e as propriedades das operações matriciais, seguida pela simulação computacional de um modelo de cifragem/decifragem que utiliza a inversão e multiplicação de matrizes sobre corpos finitos. Os resultados indicam que a complexidade algorítmica e a segurança de tais sistemas estão diretamente ligadas à dimensão e à invertibilidade das matrizes-chave, sendo a Álgebra Linear essencial para garantir a confidencialidade e integridade dos dados. Conclui-se que o domínio e a aplicação correta dos princípios da Álgebra Linear são cruciais para a concepção e a avaliação da segurança de protocolos criptográficos modernos. **Palavras-chave:** Criptografia; Álgebra Linear; Sistemas de Segurança; Matrizes; Criptosistema de Hill.

Resumo

Abstract This research work aims to analyze the application of Linear Algebra as a fundamental tool in the cryptography of information security systems. The main objective is to demonstrate how concepts of matrices, vectors, and linear transformations are employed in the development of robust cryptographic algorithms, such as the

Hill Cipher. The methodology consisted of a systematic bibliographic review on number theory applied to cryptography and the properties of matrix operations, followed by a computational simulation of an encryption/decryption model that uses matrix inversion and multiplication over finite fields. The results indicate that the algorithmic complexity and security of such systems are directly linked to the dimension and invertibility of the key matrices, with Linear Algebra being essential to ensure data confidentiality and integrity. It is concluded that the mastery and correct application of Linear Algebra principles are crucial for the design and security assessment of modern cryptographic protocols. **Keywords:** Cryptography; Linear Algebra; Security Systems; Matrices; Hill Cipher.

---

1 Introdução

Em um cenário global cada vez mais **conectado**, a segurança da transmissão de dados e a **proteção da informação sensível** se tornaram requisitos cruciais. A **Criptografia**, área da ciência voltada para ocultar informações, evoluiu de técnicas rudimentares da antiguidade para sofisticadas expressões matemáticas dos séculos XX e XXI. A **Álgebra Linear**, por sua vez, provou ser uma ferramenta fundamental neste avanço.

Entre os diversos modelos criptográficos, a **Cifra de Hill**, proposta por Lester S. Hill em 1929, é notória por sua base conceitual. O método foi inovador ao ancorar-se em **conceitos de matrizes e transformações lineares**, demonstrando que operações matriciais poderiam criar sistemas de segurança robustos.

O objetivo principal deste trabalho é **analisar e demonstrar a aplicação da Álgebra Linear** como pilar teórico e prático para o funcionamento da Cifra de Hill.

A segurança do Criptosistema de Hill está intrinsecamente ligada à **invertibilidade da matriz-chave** (K). O processo de decifragem exige a aplicação da **matriz inversa** (K^{-1}) sobre corpos finitos. Uma escolha inadequada de chave (cujo determinante não seja coprimo com 26) torna a matriz não invertível e a mensagem irrecuperável.

A **implementação computacional** deste método (em linguagem Python) serve como um **teste prático** do desenvolvimento teórico. Contudo, é fundamental salientar que este projeto tem um **caráter educativo e exploratório**. A Cifra de Hill serve como um ponto de partida crucial para a

compreensão dos princípios matemáticos que fundamentam os algoritmos criptográficos modernos, mais complexos e não lineares.

2 Materiais e Métodos

A metodologia adotada para o estudo da aplicação da Álgebra Linear em criptografia e a simulação do Criptosistema de Hill seguiu duas etapas principais: **revisão bibliográfica sistemática** e **simulação computacional**.

2.1 Revisão Bibliográfica

A fase inicial consistiu na revisão sistemática de literatura sobre a **Teoria de Números** (focando em aritmética modular $\pmod{26}$) e a **Álgebra Linear** (operações matriciais e inversão de matrizes) [1, 2]. Estudos aplicados à criptografia [3, 4] forneceram o arcabouço para a aplicação.

2.2 Simulação Computacional

A fase prática envolveu o desenvolvimento de um **modelo de cifragem e decifragem** baseado na Cifra de Hill, utilizando a linguagem de programação Python [5].

2.2.1 Escolha da Chave

Foi selecionada uma matriz 2×2 (A) que respeitasse as regras de invertibilidade em $\pmod{26}$:

$$A = \begin{pmatrix} 5 & 4 \\ 21 & 25 \end{pmatrix}$$

O determinante de A é $\det(A) = 41$. Como $\text{mdc}(41, 26) = 1$, a matriz é invertível.

2.2.2 Processo de Cifragem e Decifragem

1. **Codificação:** A mensagem é transformada em vetores coluna numéricos (P).

2. **Cifragem:** A cifragem (C) é dada pela multiplicação da chave (A) pelo vetor de texto simples (P), seguida pela aplicação do módulo 26:

$$C = A \cdot P \pmod{26}$$

3. **Decifragem:** O vetor de texto simples (P) é recuperado pela multiplicação do vetor cifrado (C) pela matriz inversa da chave (A^{-1}):

$$P = A^{-1} \cdot C \pmod{26}$$

3 Resultados e Discussões

Os resultados obtidos na simulação e na análise teórica confirmaram o papel central da Álgebra Linear.

3.1 Matriz Inversa e Validação

O inverso modular de $\det(A) = 41$ em $\pmod{26}$ é 15. A matriz inversa A^{-1} é calculada como:

$$A^{-1} \equiv 15 \cdot \begin{pmatrix} 25 & -4 \\ -21 & 5 \end{pmatrix} \equiv \begin{pmatrix} 11 & 18 \\ 3 & 23 \end{pmatrix} \pmod{26}$$

A aplicação desta matriz inversa no texto cifrado recuperou o texto original, **validando** o funcionamento do criptosistema.

3.2 Implicações em Segurança

A discussão dos resultados aponta para as implicações da Álgebra Linear na segurança:

- **Dependência da Invertibilidade:** A segurança é totalmente dependente da **invertibilidade** da matriz-chave.
- **Vulnerabilidade Linear:** A Cifra de Hill, por ser uma transformação puramente linear, é **vulnerável** a ataques de "texto claro conhecido", o que reforça a necessidade de protocolos mais modernos que introduzam a **não linearidade**.

4 Conclusões

Este trabalho alcançou seu objetivo ao **comprovar** que as transformações lineares e matrizes são ferramentas essenciais para a construção e funcionamento de sistemas criptográficos, como o Criptosistema de Hill.

A pesquisa demonstrou que o sucesso na decifragem é condicionado à **existência e ao cálculo preciso da matriz inversa**. O estudo do Criptosistema de Hill serve como um **ponto de partida** crucial para a compreensão de métodos mais complexos que introduzem a **não linearidade**.

Portanto, a investigação de matrizes e transformações lineares é um passo vital para a **avaliação e o avanço da segurança da informação**.

Referências

BOLDRINI, José Luiz *et al.* **Álgebra Linear**. 3. ed. São Paulo: Harbra, 1986.

LEON, Steven J. **Álgebra Linear com Aplicações**. 8. ed. Rio de Janeiro: LTC, 2013.

COSTA, Leticia Correia Alexandre da. **Cifras de Hill: A utilização da Álgebra Linear em Sistemas Criptográficos**. 2022. Trabalho de Conclusão de Curso – Universidade Federal da Paraíba, Rio Tinto. Acesso em: 24 set. 2025. Disponível em: `https://repositorio.ufpb.br/jspui/handle/123456789/27681`.

QIAN, Yuling. Application of modern algebra in cryptography. **Artigo Científico**, Sino-Canada School, SUZHOU, JIANGSU Province, 215027, China, 2025. Acesso em: 25 set. 2025. Disponível em: `https://direct.ewa.pub/proceedings/tns/article/view/6757`.

APARICIO, Gunnar. **Cifra de Hill Aplicação.py**. [*S. l.: s. n.*], 2020. Código-fonte. In: linear-algebra-application-in-security-systems. GitHub. Acesso em: 16 out. 2025. Disponível em: `https://github.com/gunnaraparicio/linear-algebra-application-in-security-systems/blob/10b04a072ad8a97dd2ab378f8f35a2290a250b0e/Cifra%5C%20de%5C%20Hill%5C%20Aplica%5Cc%20c%5C~ao.py`.