CÓDIGOS EM BLOCOS: A MATEMÁTICA DAS MATRIZES NA CRIPTOGRAFIA DA CIFRA DE HILL

Carolyne Oliveira Mendes – IFPI, Campus Floriano

Elane Pereira Nunes – IFPI, Campus Floriano

Mariellen Simões de Carvalho Miranda – IFPI, Campus Floriano

Victor Hugo Fonsêca Moura – IFPI, Campus Floriano

Marcelo Teixeira Carneiro – IFPI, Campus Floriano

André Luiz Ferreira de Carvalho Melo – IFPI, Campus Floriano

Gildon Cesar de Oliveira – IFPI, Campus Floriano

RESUMO

No cenário contemporâneo, marcado pelo constante fluxo de informações no meio digital, torna-se fundamental garantir a segurança e a privacidade dos dados. Diante dessa necessidade, a criptografia se consolida como uma ferramenta indispensável na proteção de informações, fundamentando-se em princípios matemáticos aplicados. Nesse contexto, destaca-se a utilização das matrizes como elemento essencial nos processos de codificação e decodificação de mensagens, uma vez que os algoritmos criptográficos têm como principal finalidade assegurar a confidencialidade dos dados, tornando-os inacessíveis a indivíduos não autorizados (Terada, 2008). É importante salientar que as matrizes são estruturas numéricas dispostas em tabelas retangulares, formadas por linhas e colunas, onde cada elemento é identificado por sua linha (numerada de cima para baixo) e coluna (numerada da esquerda para a direita), no qual possibilita a execução de operações matemáticas básicas, cruciais para o avanço de processos como a criptografia, que se baseiam diretamente nos princípios da Álgebra Linear (Nicholson, 2015). Dessa forma, este estudo tem como objetivo geral apresentar a relevância da Álgebra Linear nos processos de codificação e decodificação de mensagens por meio da Cifra de Hill, ressaltando sua aplicabilidade no campo da segurança digital. De acordo com Costa (2022), a Cifra de Hill, desenvolvida por Lester S. Hill em 1929, é classificada como uma cifra de substituição em blocos, sendo baseada em conceitos da Álgebra Linear, como transformações lineares e congruências. Além disso, Da Cunha (2016) enfatiza que esse método criptográfico utiliza uma matriz quadrada associada a uma tabela numérica que representa as letras do alfabeto, permitindo que pares de letras sejam convertidos em vetores, a partir disso, ao multiplicar esses vetores pela matriz escolhida, obtém-se o texto cifrado. Ademais, para a efetiva aplicação da Cifra de Hill, torna-se indispensável o domínio de operações fundamentais da Álgebra Linear, como o cálculo do determinante, a obtenção da matriz inversa e a utilização de congruências modulares. Tais procedimentos são essenciais para garantir tanto a codificação quanto a decodificação correta das mensagens. A elaboração deste material utilizou uma metodologia qualitativa e exploratória, baseada em estudo bibliográfico acerca dos princípios da álgebra linear e sua utilização na criptografia. Empregaram-se referências teóricas que discutem tanto as bases das matrizes quanto seu uso prático na segurança da informação. Dessa maneira, conclui-se que as matrizes desempenham um papel crucial na criptografia, auxiliando na salvaguarda de dados e na criação de sistemas de segurança eficazes. Ademais, essa

metodologia potencializa o ensino de matrizes, tornando-o mais contextualizado e pertinente, ao destacar a presença da matemática em contextos tecnológicos e do dia a dia, fomentando um aprendizado mais relevante e alinhado às necessidades do universo digital.

PALAVRAS-CHAVE: Criptografia; Matrizes; Cifra de Hill.

REFERÊNCIAS

COSTA, Letícia Correia Alexandre da. Cifras de Hill: a utilização da álgebra linear em sistemas criptográficos. 2022. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/27681. Acesso em: 14 de jun. 2025.

DA CUNHA, Rhuan Gonzaga et al. Criptografia de dados utilizando matrizes. **RE3C-Revista Eletrônica Científica de Ciência da Computação**, v. 11, n. 1, 2016. Disponível em: https://revistas.unifenas.br/index.php/re3c/article/view/100. Acesso em: 15 de jun. 2025.

NICHOLSON, W. Keith. Álgebra Linear - 2. Ed. AMGH Editora, 2015. Disponível em: https:/books.google.com.br/books?hl=pt-BR&lr=&id=P2mfCAAAQBAJ&oi=fnd&pg=PP1&dq=defini%C3%A7%C3%A3o+de+matriz. Acesso em: 15 de jun. 2025.

TERADA, Routo. Segurança de dados: criptografia em rede de computador. Editora Blucher, 2008. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=lIe6DwAAQBAJ&oi=fnd&pg=PA15&dq=CRIPTOGRAFIA&ots=wJmYPUglQI&sig=oVAoLuzbk1BEmI3BMymXB5L8d2E#v=onepage&q=CRIPTOGRAFIA&f=false. Acesso em: 14 de jun. 2025.