

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SÃO PAULO

Câmpus Presidente Epitácio

ADENDO AOS ANAIS DA MC²T 2025

Mostra Científica, Cultural e Tecnológica

ISSN 2675-9241

Inclusão de trabalho omitido na publicação original

Publicado em novembro de 2026

NOTA EDITORIAL

Adendo aos Anais da Mostra Científica, Cultural e Tecnológica (MC^2T) 2025

A Comissão Organizadora da Mostra Científica, Cultural e Tecnológica (MC^2T), do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP) — Câmpus Presidente Epitácio, informa que o trabalho intitulado *"Introdução à Criptografia via Técnicas Elementares: estudo e construção de tarefas para estudantes do Ensino Médio"*, de autoria de Livia Maria Pereira de Almeida, Fabricio Fernando Alves e Ênio Freire de Paula, aprovado e apresentado na edição de 2025 do evento, foi omitido involuntariamente da publicação original dos anais.

Com o objetivo de corrigir essa omissão e assegurar o devido registro e a divulgação da produção acadêmica vinculada à referida edição, o trabalho é disponibilizado por meio deste adendo, que complementa os anais da MC^2T 2025.

A publicação deste documento complementar visa preservar a vinculação do trabalho à edição em que foi apresentado, mantendo a integridade dos registros acadêmicos e a transparência do processo editorial.

A Comissão Organizadora lamenta a ocorrência e reafirma seu compromisso com a qualidade das publicações, a transparência editorial e a valorização dos trabalhos científicos apresentados no evento.

Presidente Epitácio, novembro de 2026

Introdução à Criptografia via Técnicas Elementares: estudo e construção de tarefas para estudantes do Ensino Médio

Livia Maria Pereira de Almeida[1], Fabricio Fernando Alves[2], Enio Freire de Paula[2]

1. Discente do Curso Técnico em Informática Integrado ao Ensino Médio – IFSP – Câmpus Presidente Epitácio;
2. Docente – IFSP – Câmpus Presidente Epitácio, Área Matemática.
E-mails: livia.pereira@aluno.ifsp.edu.br, fabricio.alves@ifsp.edu.br, eniodepaula@ifsp.edu.br.

Resumo *- Este trabalho tem por finalidade descrever as etapas já realizadas e as previstas durante a execução do projeto de iniciação científica júnior, no qual se tem realizado estudos sobre alguns métodos de Criptografia de uma perspectiva histórica, além de sua relação com conteúdos tradicionalmente abordados ao longo do Ensino Médio, tais como funções, matrizes e análise combinatória potencializando a compreensão desse conceitos, visando à elaboração de exercícios que permitam um maior engajamento dos estudantes com as aulas de Matemática e o desenvolvimento de habilidades focadas na resolução de problemas.*
Palavras-chave: *Criptografia; Funções; Matrizes.*

Introdução

Com o avanço tecnológico, a ciência criptográfica se tornou extremamente importante, popularmente servindo para proteção de dados virtuais. Mas nem sempre foi assim. Há relatos de Heródoto que, desde o século V a.C., houve a utilização da ocultação para se fazer a troca entre mensagens (SINGH, 2008, p. 20). Porém, ainda nesse período, mantém-se o sentido original do texto e com algum método para escondê-lo, atualmente esse caso é chamado de esteganografia.

Para obter mais segurança durante a troca de mensagens, a esteganografia evoluiu, constituindo-se na criptografia. Se baseando, agora, em um protocolo, um conjunto de regras que será usado na criação do seu texto cifrado, denominando esse processo de encriptação.

A criptografia se divide em duas áreas: a transposição e a substituição. A primeira pode ser definida de forma simples, no qual utiliza do embaralhamento das letras do próprio texto, logo, um anagrama. Importante ressaltar que, dependendo do caso, se seguir de forma desordenada é impossível de descriptografar.

A substituição, conhecida por cifra de substituição, usa a alteração das letras do alfabeto por outro caracteres, como: símbolos, números ou letras distintas. Para utilizá-la é necessário entender o que é o algoritmo: as regras, e a chave: personalização das regras.

Após essa aproximação, o estudo de métodos de interpretações utilizando a matemática foi aprofundado. Seguindo a seguinte ordem: funções, aritmética modular e matrizes. As definições de cada conteúdo abordado estão a seguir.

Em primeira análise, foram abordadas as funções injetoras, sobrejetoras e bijetoras. No nosso caso, a mais importante é a função bijetora. A definição, conforme Iezzi (2004, p.222-223), se dá pela seguinte forma: uma função é bijetora quando é, simultaneamente, sobrejetora e injetora, isto é: a todo x presente no domínio, há um elemento y correspondente em seu contradomínio, e, cada elemento dos dois conjuntos são diferentes ou, de forma equivalente, são iguais.

Em segundo lugar, foi estudado a aritmética modular, no qual se estuda a congruência, "Congruência trata-se de um conteúdo aritmético que trabalha com restos da divisão euclidiana por um número fixado inicialmente." (FREIRE, 2020, p.30). Com essa afirmação, obtemos a operação (1).

$$a \equiv b \mod(x) \quad (1)$$

Na forma oral: "a é congruente de b módulo de x", se dando por verdade através da equação (2) e (3).

$$\frac{a}{x} \text{ e } \frac{b}{x} \text{ possuírem os mesmos restos} \quad (2)$$

$$\frac{(a-b)}{x} = y \in \mathbb{Z} \quad (3)$$

Para finalizar, foram abordados estudos sobre matrizes. "tabelas, compostas de certa quantidade de linhas (fileiras horizontais) e de colunas (fileiras verticais), são chamadas na matemática de matrizes." (SOUZA, 2016, p. 46). Uma matriz pode ser representada por meio de uma letra maiúscula do alfabeto latino. Partindo disso, é possível realizar, sob certas condições, operações entre ou com matrizes, tais como a adição, a subtração, a multiplicação por um número real e a multiplicação entre matrizes.

As matrizes inversas utilizam dessas operações, e é determinada pela equação (4).

$$A_n \times B_n = I_n \text{ e } B_n \times A_n = I_n \quad (4)$$

Ou seja, uma matriz A admite inversa, se existir uma matriz B, tal que a multiplicação entre essas matrizes resulta na matriz identidade.

Metodologia

A metodologia aplicada a este projeto baseou-se em sua maior parte na pesquisa bibliográfica de dissertações, livros didáticos e artigos científicos. Para fixar os conteúdos mais práticos, como funções e matrizes, utilizamos exercícios envolvendo esses conteúdos.

Durante o momento de estudo, foi apresentado por um dos professores responsáveis, uma tarefa que visava buscar questões em olimpíadas. Essa atividade possui o objetivo de analisar como a criptografia é abordada em ambientes escolares, a fim de compreender as estratégias de ensino utilizadas, além de servir como banco para a oficina a ser realizada entre as atividades da Semana Nacional de Ciência e Tecnologia (SNCT) no IFSP/PEP.

Para a busca das questões a respeito da temática criptografia, consultamos os arquivos das seguintes competições científicas: Olimpíada Brasileira de Raciocínio Lógico (OBRL), Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) e Canguru de Matemática Brasil, entre os anos de 2015 - 2024.

Resultados esperados

Dessa forma, usamos as definições matemáticas apresentadas, para estabelecer uma relação dos temas com a criptografia. Utilizando da definição das funções bijetoras, pode-se associá-las de modo que: o domínio é o texto original, e, ao passar nas

operações da função, paralelo a chave, é obtido o texto cifrado, o contradomínio.

O conteúdo de matrizes pode ser aplicado à criptografia através de matrizes inversas ou em conjunto com aritmética modular. Como ações principais para se cifrar, é preciso transformar o alfabeto em números e, no texto a ser cifrado, deve-se dividir em grupos com duas letras cada, que serão substituídas pelos números feitos anteriormente. Criando, assim, uma matriz $A_{2\times n}$. Segue o exemplo desse processo inicial nas figuras 1 e 2.

Figura 1. Exemplo prático

C	I	F	R	A	R	E	U	M	A	A	R	T	E
2	8	5	17	0	17	4	20	12	0	0	17	19	4

Fonte: (SANTOS, 2013, p.46)

A figura 1 apresenta a frase "CIFRAR É UMA ARTE", dividida em blocos de dois caracteres, assumindo um número para cada letra. Resultando na matriz presente na figura 2.

Figura 2. Matriz elaborada a partir da Figura 1.

$$\begin{bmatrix} 2 & 5 & 0 & 4 & 12 & 0 & 19 \\ 8 & 17 & 17 & 20 & 0 & 17 & 4 \end{bmatrix}$$

Fonte: Elaborada pelos autores.

Em casos que utilizam matrizes inversas, a chave será uma matriz obrigatoriamente invertível. Cifrando, é necessário efetuar a multiplicação da matriz $A_{2\times n}$ pela a matriz da chave, no qual a resultante será a que apresenta o texto codificado. A fim de decodificar, é preciso inverter a chave e multiplicar pelo texto cifrado.

Contudo, de acordo com Santos (2013, p.45-46) a Cifra de Hill utiliza as matrizes e a aritmética modular. Primeiramente, é feito as mesmas ações citadas anteriormente. Para cifrar, efetua-se a multiplicação entre a matriz do texto com a matriz chave. Por fim, usa-se como divisor o total de letras, ou símbolos, do seu alfabeto. O resto dessas divisões será a nova matriz, com os números sendo o índice da mensagem cifrada, bastando trocar pelas letras pertencentes a ele.

Conclusões

Concluindo, o projeto tem o objetivo de desenvolver os saberes sobre a criptografia da bolsista. Partindo do momento histórico à associação com conteúdos matemáticos vistos no Ensino Médio. Além da compreensão conceitual, esse estudo facilitou a elaboração de questões envolvendo o tema, utilizando, também, a procura nas olimpíadas desejadas. Os resultados dessa atividade não atingiram as expectativas, pois, a maioria, se concentrou em apenas uma competição, a OBRL nos níveis iniciais de escolaridade.

Inferimos que a ausência em níveis posteriores (Anos Finais da Educação Básica e Ensino Médio) são decorrentes do grande repertório de conteúdos matemáticos já presentes na Base Nacional Comum Curricular (BNCC). Esse fato é corroborado por esse documento não possuir, de forma explícita, habilidades que descrevem a temática da criptografia.

Agradecimentos

Os autores agradecem ao Programa Institucional de Bolsas de Iniciação Científica e Tecnológica (PIBIFSP) e ao IFSP, campus Presidente Epitácio pela infraestrutura e suporte disponibilizados.

Referências

FREIRE, Tércio Rodrigues. **Criptografia RSA no Ensino Médio**: um recurso de motivação e aprendizagem. Orientadora : Hellena Christina Fernandes Apolinário. Dissertação (Mestrado Profissional) - Universidade Federal do Tocantins. Mestrado Profissional em Matemática. Palmas, TO, 2020.

IEZZI, G.; MURAKAMI, C. **Fundamentos de Matemática Elementar** - conjuntos e funções. Volume 1. 8ª edição. São Paulo, Atual Editora, 2004.

SANTOS, J. L. **A Arte de Cifrar, Criptografar, Esconder e Salvaguardar como Fontes Motivadoras para Atividades de Matemática Básica**. Orientador: Vinícius Moreira Mello, 2013. Dissertação (mestrado) - Universidade Federal da Bahia, Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, Salvador, 2013.

SILVA, A.L.M.R.; PEROVANO, A.P. SILVA, F.S. **A Criptografia como motivação para a aprendizagem matemátic**a. REMAT: Revista Eletrônica da Matemática, Bento Gonçalves, RS, Brasil, v. 9, n. 1, p. e2002, 2023. DOI: 10.35819/remat2023v9i1id5890. Disponível em: https://periodicos.ifrs.edu.br/index.php/REMAT/article/view/5890. Acesso em: 11 jun. 2025.

SINGH, S. **O Livro dos Códigos**: a Ciência do Sigilo - do antigo egito à criptografia quântica. 7ª edição. Rio de Janeiro, Record, 2008.

SOUZA, Joamir; GARCIA, Jacqueline. Matrizes e determinantes. *In*: SOUZA, Joamir; GARCIA, Jacqueline. **#Contato** Matemática 2º ano. 1. ed. São Paulo: FTD, 2016. p. 44-73.