Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 11, n. 1, 2025.

Trabalho apresentado no XLIII CNMAC, Centro de Convenções do Armação Resort - Porto de Galinhas - PE, 2024

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Uma Abordagem da Criptografia com Tecnologia para o Aprimoramento da Aprendizagem de Funções Polinomiais

Douglas V. A. Rodrigues[1], Junior C. B. da Silva[2], Anna L. O. Soares[3]
UFMT, Cuiabá, MT

Muitas vezes profissionais da área da educação em matemática deparam-se em determinar quais estratégias pedagógicas necessitam ser mantidas ou renovadas na intensão de proporcionar práticas educativas eficientes e eficazes que sejam incentivadoras no aprendizado de matemática. Este trabalho tem como objetivo apresentar uma abordagem para o aprimoramento do conhecimento sobre funções matemáticas, utilizando a criptografia como ferramenta pedagógica e a linguagem de programação Python para automatizar o processo.

A proposta está direcionada a estudantes do ensino médio e é baseada na BNCC e no Pensamento Computacional, explorando a codificação e decodificação de mensagens utilizando funções afim e quadrática, demonstrando a aplicação prática desses conceitos matemáticos e desenvolvendo habilidades de resolução de problemas.

A metodologia proposta se baseia na construção de um sistema de criptografia simplificado, em que os coeficientes das funções polinomiais atuam como chaves criptográficas (Figura 1). A mensagem a ser codificada é inicialmente convertida em uma sequência numérica, utilizando uma tabela de associação entre caracteres e números (Figura 2). Em seguida, cada número da sequência é transformado pela função polinomial, gerando a mensagem codificada. Para decodificar a mensagem, o processo inverso é realizado, utilizando a função inversa ou resolvendo uma equação [1], [2].

Definiremos a chave criptográfica como uma sequência de $n+2$ termos, para todo $n \geq 1$, de tal forma que os primeiros $n+1$ números representam os coeficientes da função polinomial de grau n, e o último dígito m representa a quantidade de caracteres de cada letra a ser decodificada. A Figura 2 apresenta a função injetiva que associa cada $p(x_i)$ a um caractere, em que $x_i, a_i \in \mathbb{Z}$ e $i \in \mathbb{N}$.

Chave	Função
$(a_1,\ a_0,\ m)$	$p(x) = a_1x + a_0$
$(a_2,\ a_1,\ a_0,\ m)$	$p(x) = a_2x^2 + a_1x + a_0$
$(a_3,\ a_2,\ a_1,\ a_0,\ m)$	$p(x) = a_3x^3 + a_2x^2 + a_1x + a_0$
$\vdots$	$\vdots$
$(a_n,\ a_{n-1},\ ...,\ a_1,\ a_0,\ m)$	$p(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$

Figura 1: Relação entre a chave e a função polinomial. Fonte: Pontes et al. (2022).

[1]douglasvar22@gmail.com
[2]serabicont_cesarjr@hotmail.com
[3]anna.soares@ufmt.br

$p(x)$	Caractere	$p(x)$	Caractere
$p(x_1)$	A	$p(x_{10})$	J
$p(x_2)$	B	$p(x_{11})$	K
$p(x_3)$	C	$p(x_{12})$	L
$p(x_4)$	D	$p(x_{13})$	M
$p(x_5)$	E	$p(x_{14})$	N
$p(x_6)$	F	$p(x_{15})$	O
$p(x_7)$	G	$p(x_{16})$	P
$p(x_8)$	H	$\vdots$	$\vdots$
$p(x_9)$	I	$p(x_r)$	

Figura 2: Correspondência entre a função e a letra do alfabeto. Fonte: dos autores.

Para realização do processo criptográfico por funções polinomiais é necessário que o aluno tenha conhecimento prévio de função afim e/ou quadrádica, desta forma, o aluno poderá desenvolver e aprimorar os conhecimentos matemáticos que envolvem domínio e imagem de função, conceito de injetividade e sobrejetividade, resolução de sistemas lineares, função inversa, raízes de polinômios, entre outros, colocando em prática o processo de codificar e decodificar mensagens por funções polinomiais. Cabe ressaltar que o objetivo desta atividade é o aprimoramento do conhecimento matemático através da metologia do processo criptográfico, realizado com lápis e papel.

A automação do processo criptográfico inicia somente quando o aluno tem a destreza do processo criptográfico por funções polinomiais, para isso, desenvolvemos códigos no Python que codifica e decodifica mensagens, em que o aluno escolhe a chave criptográfica (função polinomial), tendo como objetivo proporcionar uma ferramenta que permita a investigação e compreensão que o processo criptográfico não funciona para todas as funções polinomais. Além disso, detalhamos cada etapa do algoritmo fazendo a relação entre o código da linguagem e os conteúdos matemáticos, facilitando a apresentação da linguagem de programação Python aos estudantes e descrevemos passo a passo o código para realizar o processo criptográfico automatizado, desta forma, os alunos poderão realizar os procedimentos da criptografia feitos a mão para a linguagem de programação Python.

Resumindo, estabelecemos a metodologia de aprendizagem do processo criptografico em três partes, sendo a primeira o processo do aprendizado feito com papel e lápis, simplesmente para entender o processo criptográfico por funções polinomiais. A segunda parte é mostrar aos alunos os códigos prontos em Python, em que eles devem escolher a função polinomial que servirá como chave criptográfica, além da mensagem a ser codificada/decodificada. Finalmente, a terceira parte é ensinar os códigos do Python que serão necessários para realizar o processo de automoção da criptografia. Desta forma, este trabalho prentende auxiliar nas estratégias pedagógicas do processo de ensino aprendizagem de matemática no ensino básico promovendo uma reflexão sobre a importância da matemática.

Referências

[1] V. M. C. Fiarresga. “Criptografia e matemática”. Dissertação de mestrado. Universidade de Lisboa (Portugal), 2010.

[2] E. A. S. Pontes et al. “Criptografia em Funções Polinomiais: Um Processo de Ensino e Aprendizagem de Matemática na Educação Básica”. Em: **The Journal of Engineering and Exact Sciences** 8.6 (2022).