Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 8, n. 1, 2021.

Trabalho apresentado no XL CNMAC, Evento Virtual - Co-organizado pela Universidade do Mato Grosso do Sul (UFMS).

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Uso da Função Quadrática em Criptografia

Willa da S. Medeiros[1]
EEEFM Antônio Gomes, PB
Maria Joseane F. G. Macêdo[2]
Paulo César Linhares da Silva[3]
Centro de Ciências Exatas e Naturais, UFERSA, Mossoró, RN

No Brasil, vivemos a grande contradição ao integrar o grupo de elite mundial em pesquisa matemática em nível superior, enquanto que no nível básico somos um dos países com pior desempenho. No sentido de melhorar essa perspectiva, a prática de desenvolver o ensino por meio da contextualização e interdisciplinaridade vem se tornando cada vez mais frequente. Segundo [1], citado por [3], a contextualização ocorre quando o aluno é levado a estudar um conteúdo por meio de uma situação-problema, sendo essa situação próxima à realidade do aluno e inserida num cenário que seja capaz de atribuir significado e sentido ao objeto de estudo.

A criptografia é a ciência que estuda os métodos para tornar o conteúdo de uma mensagem incompreensível para todos aqueles que não têm permissão de lê-la, de modo que somente o destinatário legítimo possa obter a mensagem verdadeira. Não é novidade que a matemática é essencial para a criptografia, constituindo sua base conceitual de segurança. Desse modo, essa pesquisa objetiva investigar a relação entre matemática básica e criptografia, através das funções polinomiais de grau 2 (função quadrática), e como essa relação pode render ferramentas para a melhoria do ensino e aprendizagem de matemática no Ensino Médio. Este estudo fundamenta-se em obras como [2], entre outros.

Nosso propósito é descrever um método de criptografia com base na função quadrática. O método em questão possui como espaço de texto comum o alfabeto $\{1, 2, 3, 4, \ldots, 26\}$ e é uma cifra de blocos com comprimento 1, isto é, codifica letra por letra. Seu espaço de texto cifrado é um subconjunto (finito) de $\mathbb{N}$. Assim, a mensagem codificada passa a ser representada por uma sequência de números separados por um traço. Será apresentado um guia de desenvolvimento e aplicação do método, onde numa primeira etapa a mensagem é pré-codificada através da Tabela 1. Em seguida, utiliza-se uma função quadrática para codificá-la. Na segunda etapa será explicado o processo de decodificação, isto é, como retomar a mensagem original através da mensagem cifrada. Para uma simplificada ilustração do processo, vejamos o exemplo a seguir.

Tabela 1: Tabela de Pré-codificação.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

[1] willamedeiros@hotmail.com
[2] joseane@ufersa.edu.br
[3] linhares@ufersa.edu.br

Exemplo 1. *Vamos codificar a mensagem* ***A VIDA É UM SOPRO*** *utilizando a função quadrática* $f(x) = 2x^2+x+1$. *A mensagem é pré-codificada através da Tabela 1, obtendo* $1-22-9-4-1-5-21-13-19-15-16-18-15$. *A tabela a seguir resume o processo, onde a mensagem será representada pela sequência de blocos* $4-991-172-37-4-56-904-352-742-466-529-667-466$.

Tabela 2: Codificando a mensagem.

Bloco (x)	1	22	9	4	5	21
B. codificado $f(x)$	f(1)=4	f(22)=991	f(9)=172	f(4)=37	f(5)=56	f(21)=904
Bloco (x)	13	19	15	16	18	
B. codificado $f(x)$	f(13)=352	f(19)=742	f(15)=466	f(16)=529	f(18)=667	

Vale salientar que o código depende da função quadrática escolhida. Para recuperar a mensagem original utiliza-se uma função de decodificação, neste caso a inversa de f. Fazendo a restrição necessária ao domínio de f no Exemplo 1, temos $f^{-1} : [7/8, +\infty) \to \mathbb{R}$ dada por $f^{-1}(x) = \frac{-1+\sqrt{1-8(1-x)}}{4}$.

Neste contexto do uso da função quadrática na criptografia, o aluno estudará tópicos como radiciação, potenciação, domínio e imagem de função, bijetividade, função inversa, entre outros, de maneira dinâmica e instigadora, contrapondo as aulas tradicionais. Esperamos que tal estudo motive o professor, e sirva de suporte, na busca da contextualização e interdisciplinaridade, refletindo em melhorias para o ensino de matemática, uma vez que fora acrescido significado e sentido ao objeto de estudo. Ademais, pretende-se ampliar a visão do professor para utilizar tais exercícios de criptografia para o caso de outras funções e aplicações.

Agradecimentos

Este trabalho é parte do estudo desenvolvido durante o mestrado no PROFMAT/UFERSA. Os autores agradecem o apoio da UFERSA na execução deste trabalho.

Referências

[1] Brosseau, G. *Fondement et méthodes de la didactique des Mathématiques*. In J. Brun (Ed), Didactique des Mathématiques, Lausanne: Delachaux et Niestlê, pages 45 - 144, 1996.

[2] Buchmann, J. A. *Introdução à Criptografia, 1a. edição*. Berkeley, São Paulo, 2002.

[3] Pinheiro, F. M. D. L. Contextualização do saber: formação inicial dos professores de 1º e 2º ciclo do Ensino Básico, 159f, Dissertação de Mestrado, Universidade de Lisboa, 2012.