Uma proposta envolvendo criptografia e o algoritmo da divisão

Ana Luiza Pecinato Gresele[1], Luis Fernando Silveira da Silva[1], Janice Teresinha Reichert[2] , Milton Kist[2]

[1]Curso de Matemática – Universidade Federal da Fronteira Sul (UFFS)
Caixa Postal 181 – 89.815-899 – Chapecó – SC – Brasil

[2]Departamento de Matemática – Universidade Federal da Fronteira Sul (UFFS)
Caixa Postal 181 – 89.815-899 – Chapecó – SC – Brasil

{analuizagresele, luisfsilveiradasilva, janice.reichert, milton.kist}@gmail.com

Abstract.

An encryption is a key mechanism used in safeguarding data and information circulating across networks. Currently, the most prevalent encryption methods involve mathematical knowledge, thus merging the two fields is highly beneficial. Considering the changes in the current laws of Basic Education, it's necessary to contemplate the inclusion of activities involving Computing that foster the skills it develops. Therefore, this present work aims to propose an activity to be implemented in Basic Education, involving the Euclidean Division Algorithm and encryption.

Resumo.

A criptografia é um mecanismo primordial utilizado na proteção de dados e informações que circulam nas redes. Os métodos mais utilizados de criptografia atualmente envolvem o conhecimento matemático e, por conta disso, unir as duas áreas é de grande valia. Considerando as mudanças nas leis vigentes da Educação Básica, é necessário pensar a respeito da inserção de atividades que envolvam Computação e que promovam as habilidades por ela desenvolvidas. Dessa forma, o presente trabalho tem como objetivo principal propor uma atividade para ser trabalhada na Educação Básica, envolvendo o Algoritmo da Divisão de Euclides e a criptografia.

1. Descrição Geral

A criptografia é muito utilizada para a segurança e armazenamento de dados no mundo tecnológico atual. Segundo Silva (2019), essa técnica surgiu com a necessidade de proteger informações militares, meio utilizado para planejar os ataques de guerra e proteger a informação do inimigo. Através da matemática, é possível encontrar diversos meios de criptografar uma mensagem, por exemplo, utilizando a decomposição em fatores primos de um número de centenas de casas decimais. Dessa forma, a criptografia vem sendo estudada pela Computação para que novos meios de proteção de dados sejam programados.

Segundo a Resolução Nº1, de 4 de outubro de 2022 (MEC, 2022), a Computação tornou-se obrigatória na Educação Básica em todo o território nacional com definição do prazo de implementação em até um ano após a homologação dessa lei, que ocorreu no dia 1 de novembro de 2022. No entanto, o que se observa é a pouca disseminação a

respeito desse assunto nas escolas e a falta de qualificação de professores para a realização deste requisito na Educação Básica.

A Base Nacional Comum Curricular (BNCC), documento que rege a Educação Básica brasileira, traz em seu corpo os três eixos que definem a Computação: Pensamento Computacional, Cultura Digital e Mundo Digital. Em particular, o Mundo Digital é definido no documento da BNCC como a habilidade que "envolve as aprendizagens relativas às formas de processar, transmitir e distribuir a informação de maneira segura [...] compreendendo a importância contemporânea de codificar, armazenar e proteger a informação" (Brasil, 2018, p. 474).

Assim, levando em consideração a obrigatoriedade das habilidades que envolvem a Computação e, sendo o Mundo Digital um dos eixos que englobam esse tema, a criptografia pode e deve entrar como um aliado no cumprimento dos documentos básicos. Dessa forma, a criação de atividades que apresentem os conceitos e que enfatizem a importância da criptografia devem ser incentivadas, já que elas desenvolvem o raciocínio lógico-matemático e são ferramentas que podem auxiliar na compreensão dos conceitos relacionados ao Mundo Digital.

2. Objetivos

Conforme apresentado anteriormente, a inserção da Computação na Educação Básica tornou-se obrigatória por lei. Ademais, pela relevância e pela falta de disseminação do assunto, este trabalho tem como objetivo principal propor uma atividade envolvendo Criptografia e o Algoritmo da Divisão de Euclides para ser trabalhada com anos finais do Ensino Fundamental, visto que esses conteúdos são necessários para o desenvolvimento do pensamento lógico-matemático do aluno.

Tal atividade abrange o desenvolvimento de algumas habilidades requeridas pelo documento "Computação - Complemento à BNCC" (Brasil, 2022) de âmbito nacional, que tem como ponto principal a implementação da Computação na Educação Básica. Ademais, a atividade proposta faz parte do eixo da Computação "Mundo Digital", onde devem ser trabalhadas as noções de proteção de dados.

3. Habilidades trabalhadas

O documento complementar à BNCC aborda algumas habilidades envolvendo a criptografia, sobretudo de segurança de dados, mas também exige o conhecimento geral de como funciona a criptografia e a importância dela.

Dessa forma, a presente atividade tem como proposta desenvolver a habilidade EF09CO05 do Complemento à BNCC, onde é destacado que os alunos devem "analisar técnicas de criptografia para armazenamento e transmissão de dados" (Brasil, 2022, p. 54). Ainda, a habilidade traz como um exemplo de sua aplicação: "apresentando o conceito de criptografia, por exemplo, usando algoritmos simples de criptografia para que os estudantes codifiquem textos e frases e troquem mensagens com os colegas" (Brasil, 2022, p. 55).

Também, a proposta trabalhará a habilidade EF07CO07, a qual exige do aluno "identificar problemas de segurança cibernética e experimentar formas de proteção"

(Brasil, 2022, p. 44). Ainda, um exemplo de como desenvolver essa habilidade é desenvolvendo “esquemas de criptografia através de um dicionário de códigos” (Brasil, 2022, p. 45).

4. Materiais utilizados

Para a realização da atividade serão necessários os seguintes materiais: folha de ofício, lápis, borracha e impressão das tabelas de exemplo.

5. Metodologia

Para que a atividade a ser realizada cumpra com os objetivos expostos anteriormente e desenvolva as habilidades propostas, é necessário que o momento seja realizado com a turma dividida em grupos de 5 alunos cada (por afinidade). Após a formação dos grupos, o professor deve iniciar a atividade com uma motivação, instigando os alunos a respeito do assunto criptografia através de perguntas, como “Vocês sabem como os soldados de guerra se comunicavam sobre os próximos ataques sem que o inimigo soubesse?”, “Vocês sabem o que é criptografia?”. Além disso, comentar sobre a sua história e a sua importância. Além disso, o professor deve retomar o conteúdo do Algoritmo da Divisão de Euclides (Domingues, 2009), explicando cada elemento da divisão.

Tabela 1. Tabela com os números de cada letra do alfabeto

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

Nesse momento, o professor deve desenvolver com os alunos a atividade instigando-os e dialogando a respeito do que eles sugerem realizar em cada coluna da tabela. Os passos para a codificação são: após codificar a palavra através do algarismo posicional de cada letra do alfabeto, os alunos devem somar uma chave secreta “X” com o valor posicional da letra. Em seguida, devem calcular através do Algoritmo de Euclides o resto da divisão pelo divisor 26. Logo, a mensagem codificada será o resto da divisão de cada letra somada à chave secreta por 26. Por fim, basta substituir a letra correspondente ao número encontrado na coluna de restos.

Para a decodificação da palavra, os alunos necessitam da chave secreta “X”. O primeiro passo é calcular a subtração do valor da mensagem codificada e da chave. Caso esse resultado seja negativo, é preciso somar 26 para ajustá-lo para um algarismo positivo. O próximo passo é substituir pela letra correspondente ao algarismo encontrado na coluna “Mensagem decodificada”. Nas tabelas 4 e 5 é possível observar a codificação e decodificação da palavra “Matemática”.

Tabela 2. Exemplo de codificação da palavra “Matemática”

Codificação					
Letra	Nº	Nº somado a chave	Algoritmo da	Codificação	Mensagem

	correspondente	L=11	divisão	(restos)	Criptografada
M	13	13+11 = 24	24=0*26+24	24	X
A	1	1+11 = 12	12=0*26+12	12	L
T	20	20+11 = 31	31=1*26+5	5	E
E	5	5+11 = 16	16=0*26+16	16	P
M	13	13+11 = 24	24=0*26+24	24	X
Á	1	1+11 = 12	12=0*26+12	12	L
T	20	20+11 = 31	31=1*26+5	5	E
I	9	9+11 = 20	20=0*26+20	20	T
C	3	3+11 = 14	14=0*26+14	14	N
A	1	1+11 = 12	12=0*26+12	12	L

Tabela 3. Exemplo de decodificação da palavra “Matemática”

Decodificação						
Mensagem Criptografada	Nº correspondente	Nº subtraído da chave L=11	Resultado	Ajuste nºs negativos	Mensagem decodificada	Mensagem original
X	24	24-11 = 13	13		13	M
L	12	12-11 = 1	1		1	A
E	5	5-11 = -6	-6	-6+26 = 20	20	T
P	16	16-11 = 5	5		5	E
X	24	24-11 = 13	13		13	M
L	12	12-11 = 1	1		1	Á
E	5	5-11 = -6	-6	-6+26 = 20	20	T
T	20	20-11 = 9	9		9	I
N	14	14-11 = 3	3		3	C
L	12	12-11 = 1	1		1	A

Apropriando-se do exemplo de aplicação da atividade exposto no documento de Complemento à BNCC, a presente proposta tem como principal metodologia a interação e troca entre alunos. Ou seja, depois dos passos já apresentados, a proposta é que os alunos codifiquem mensagens e troquem entre si, possibilitando o pleno entendimento a respeito da criptografia, além de desenvolver o raciocínio matemático, proporcionando aos alunos a habilidade do trabalho em equipe e de comunicação.

6. Avaliação

Considera-se a avaliação como um processo contínuo, dessa forma, os alunos serão avaliados pela participação e engajamento durante o desenvolvimento da atividade, como por exemplo, foco na realização, compartilhamento de resultados, trabalho em equipe e dúvidas possíveis. Além disso, será solicitado aos alunos que codifiquem mensagens e troquem entre si, possibilitando o pleno entendimento a respeito da criptografia, essa atividade será entregue ao professor.

Referências

Brasil. Ministério da Educação, (2018) “Base Nacional Comum Curricular”. Brasília. Disponível em: http://basenacionalcomum.mec.gov.br/. Acesso 29 de janeiro de 2024.

Brasil. Ministério da Educação, (2022) “Complemento à Base Nacional Comum Curricular”, Disponível em: http://portal.mec.gov.br/docman/fevereiro-2022-pdf/236791-anexo-ao-parecer-cneceb-n-2-2022-bncc-computacao/file. Acesso 29 de janeiro de 2024.

Domingues, H. Fundamentos da Aritmética. Florianópolis: Ed. da UFSC, 2009.

Ministério da Educação (MEC). (2022) “Normas sobre Computação na Educação Básica – Complemento à BNCC”. Resolução nº1, de 4 de outubro de 2022. Brasília.

Silva, W. W. M. (2019) “A Evolução da criptografia e suas técnicas ao longo da história”. Disponível em: https://repositorio.ifgoiano.edu.br/bitstream/prefix/795/1/tcc_Willian_Wallace_de_Matteus_Silva.pdf. Acesso 29 de janeiro de 2024.