

Criptaritmética: Uma Abordagem Lúdica para o Ensino de Conceitos Básicos de Criptografia na Educação Básica

Edeyson Andrade Gomes¹, Laís do Nascimento Salvador¹

¹Instituto de Computação – Universidade Federal da Bahia (UFBA)
40.170-110 – Salvador – BA – Brazil

{edeysongomes, laisns}@ufba.br

Abstract. *Cryptography is part of students' daily lives, but its teaching in Basic Education is challenging due to its mathematical abstraction. Cryptarithms emerge as a playful approach to introduce cryptographic concepts, stimulating logical reasoning and creativity. This work proposes its use in activities aligned with the BNCC, where students solve and create cryptarithmic challenges, exploring mathematical operations and symbol substitution to represent numbers, promoting engagement and autonomy in learning.*

Resumo. *A criptografia faz parte do cotidiano dos estudantes, mas seu ensino na Educação Básica é desafiador devido à sua abstração matemática. A criptaritmética surge como uma abordagem lúdica para introduzir conceitos criptográficos, estimulando o raciocínio lógico e a criatividade. Este trabalho propõe seu uso em atividades alinhadas à BNCC, onde os alunos resolvem e criam desafios criptaritméticos, explorando operações matemáticas e substituição de símbolos para representar números, promovendo engajamento e autonomia no aprendizado.*

1. Introdução

A criptografia desempenha um papel fundamental na segurança digital, protegendo dados em senhas, transações financeiras e comunicações privadas [Stallings 2005]. Apesar de sua crescente relevância, a necessidade de compreender operações matemáticas e princípios algorítmicos pode tornar o aprendizado difícil para alunos em fase de desenvolvimento do pensamento lógico-matemático.

Diante desse contexto, a **criptaritmética** surge como uma alternativa lúdica e acessível para introduzir conceitos básicos de criptografia. Por meio da substituição de números por símbolos ou letras em operações matemáticas válidas [Abbasian and Mazloom 2010, Szilagyi 2016], essa abordagem estimula o raciocínio lógico, a criatividade e a capacidade analítica dos estudantes [Widodo et al. 2019]. Além disso, ao resolver e criar seus próprios desafios, os alunos não apenas reforçam conceitos matemáticos e computacionais, mas também desenvolvem autonomia e estratégias para a resolução de problemas.

Este trabalho propõe a utilização da criptaritmética como ferramenta pedagógica para facilitar o ensino da criptografia e do pensamento computacional na Educação Básica. A proposta explora padrões numéricos, lógica matemática e decomposição de problemas, alinhando-se às diretrizes da Base Nacional Comum Curricular (BNCC)

[Brasil 2017]. Além disso, a atividade possibilita uma abordagem interdisciplinar, integrando conceitos matemáticos e computacionais de forma estimulante e contextualizada.

A metodologia incentiva os alunos a participarem ativamente do aprendizado, formulando hipóteses, testando soluções e colaborando na resolução de desafios. Dessa forma, busca-se tornar o ensino da criptografia mais acessível e envolvente, despertando o interesse dos estudantes pela computação e suas aplicações práticas no mundo real.

2. Objetivos Geral e Específicos

O objetivo geral desta proposta é introduzir conceitos básicos de criptografia por meio da criptoaritmética, utilizando desafios matemáticos como ferramenta para desenvolver habilidades de pensamento computacional e raciocínio lógico na Educação Básica.

Como objetivos específicos, pretende-se explorar os fundamentos da criptografia (como técnicas de substituição e transposição) [Stallings 2005] e suas aplicações no cotidiano e desenvolver habilidades de reconhecimento de padrões e abstração computacional, essenciais para a resolução de problemas de maneira estruturada e analítica. A proposta também visa estimular a criatividade dos estudantes, incentivando-os a elaborar seus próprios desafios criptoaritméticos, ao mesmo tempo em que fomenta a persistência e o pensamento algorítmico na busca por soluções eficientes.

3. Público-Alvo

A atividade é voltada para estudantes do Ensino Fundamental II (6º ao 9º ano) e Ensino Médio, além de professores interessados em metodologias inovadoras para o ensino de computação e matemática. A abordagem pode ser adaptada para diferentes níveis de ensino, permitindo sua aplicação tanto no ensino regular quanto em atividades extracurriculares.

4. Habilidades Exploradas

A proposta visa desenvolver competências nas áreas de Pensamento Computacional e Mundo Digital, conforme descrito na BNCC [Brasil 2017] e no Complemento de Computação na Educação Básica [SBC 2023]. O documento complementar destaca a importância do desenvolvimento do pensamento computacional, especialmente na decomposição e estruturação de problemas complexos, além da representação simbólica da informação para sua manipulação eficiente.

No eixo do **Pensamento Computacional**, a atividade aborda a habilidade **EF69CO04**, que envolve a decomposição de problemas, permitindo que os alunos dividam desafios complexos em partes menores para facilitar sua solução. Esse processo estimula o raciocínio estruturado, essencial para a construção de estratégias lógicas e matemáticas na resolução de criptogramas. Além disso, trabalha-se a habilidade **EF69CO03**, que enfatiza a importância da descrição precisa de soluções, levando os estudantes a formularem respostas claras e detalhadas ao explorar a estrutura dos algoritmos criptográficos.

No eixo do **Mundo Digital**, a proposta desenvolve a habilidade **EF09CO06**, que trata da codificação da informação, permitindo aos alunos compreenderem a representação simbólica de números e letras na resolução de desafios criptoaritméticos.

Esse conhecimento é essencial para entender os princípios fundamentais da criptografia e sua aplicação na segurança digital, tornando os estudantes mais conscientes sobre a relevância da proteção de dados e do uso responsável da tecnologia.

Dessa forma, a atividade não apenas fomenta habilidades técnicas, mas também estimula o pensamento analítico, a abstração e a capacidade dos alunos de interpretar e resolver problemas de maneira lógica e estruturada, preparando-os para desafios computacionais e matemáticos dentro e fora do ambiente escolar.

5. Recursos, Materiais e Metodologia

Para a realização da atividade, serão utilizados materiais simples e acessíveis, como papel, lápis, borrachas e cartões com desafios impressos. Esses elementos servirão de suporte para a dinâmica proposta, permitindo a manipulação dos problemas de forma tangível e facilitando a participação ativa dos alunos.

A atividade será estruturada em etapas bem definidas para garantir que os objetivos estabelecidos sejam alcançados e que as habilidades propostas sejam desenvolvidas de maneira eficaz. Inicialmente, a turma será dividida em pequenos grupos, incentivando a colaboração e o aprendizado coletivo. O professor iniciará com um momento de motivação, despertando a curiosidade dos alunos por meio de perguntas instigantes, como: "Como protegemos nossas informações na internet?" ou "Vocês já usaram alguma senha ou código secreto para se comunicar com alguém?". Além disso, exemplos práticos serão apresentados, como a necessidade de criptografia em mensagens de aplicativos, a proteção de senhas bancárias e até mesmo cifras utilizadas em jogos e brincadeiras infantis, como a cifra de César. Essa abordagem inicial permitirá aos alunos perceberem a relevância do tema e conectá-lo ao seu cotidiano.

Em seguida, será apresentada uma introdução teórica sobre criptografia, destacando sua relevância para a segurança digital no cotidiano. O professor abordará a relação entre a força de uma senha, seu tamanho e a complexidade dos caracteres utilizados, demonstrando exemplos de senhas fracas e fortes e simulando o tempo necessário para que cada uma seja quebrada por força bruta. Na sequência, serão introduzidos os conceitos fundamentais da criptografia, incluindo a substituição de caracteres, exemplificada por métodos históricos como a cifra de César e o código de Vigenère. Para reforçar a compreensão, os alunos serão desafiados a decodificar mensagens cifradas por deslocamento de letras e a identificar padrões em textos criptografados. Além disso, exemplos resolvidos passo a passo serão apresentados, permitindo que os estudantes compreendam a lógica da codificação e desenvolvam estratégias para solucionar desafios de maneira estruturada.

Após essa introdução, os alunos, já organizados em grupos, receberão os desafios criptoaritméticos impressos. A resolução dos problemas será realizada de forma colaborativa, com a mediação do professor para auxiliar na estratégia de decomposição dos desafios. Cada grupo deverá analisar as relações matemáticas envolvidas e propor soluções estruturadas, reforçando, assim, a importância do pensamento computacional e da lógica matemática.

5.1. Exemplo de Problema Resolvido Passo a Passo

No distante **Reino dos Espelhos Mágicos**, existia um oráculo matemático que só revelava segredos para aqueles que conseguiam decifrar seus números encantados. O grande **Mes-**

tre dos Cálculos deixou a seguinte mensagem para quem quisesse desvendar o mistério:

”Encontre o número mágico! Multiplique-o por 4 e verá o reflexo perfeito. Esse número abrirá o portal para a verdade.”

No centro do reino, havia uma porta secreta trancada com um código de cinco dígitos. A única pista disponível era a seguinte operação:

$$\begin{array}{r} \text{A B C D E} \\ \times 4 \\ \hline \text{E D C B A} \end{array}$$

A lenda dizia que apenas quem conseguisse encontrar os valores corretos de ABCDE poderia digitar a senha no portal e atravessar para a Câmara do Conhecimento Infinito.

Desafio: Resolva a multiplicação e descubra o número secreto ABCDE. Será que você consegue desvendar este enigma e descobrir os números distintos que correspondem às letras A, B, C, D e E ?

5.1.1. Passo 1: Descobrindo os Primeiros Dígitos

$$\begin{array}{r} \text{A B C D E} \\ \times 4 \\ \hline \text{E D C B A} \end{array}$$

O primeiro dígito A tem que ser um número válido. Como estamos lidando com um número de cinco dígitos, A não pode ser 0.

Observando a equação formada na primeira coluna: $4 \times A = E$, nota-se que E tem apenas um dígito (ou seja, $E \leq 9$). Então, A só pode ser **1** ou **2**, pois $4 \times 1 = 4$ e $4 \times 2 = 8$.

Agora, olhamos para o dígito A do resultado da multiplicação (última linha). Ele deve ser o último dígito do resultado da multiplicação de $E \times 4$. Mas, não há múltiplo de 4 que termine em 1, então A não pode ser 1. Logo, $A = 2$.

Sabendo que $E = 4 \times A$, o valor de E é $4 \times 2 = 8$.

5.1.2. Passo 2: Determinando o Dígito C

Agora temos a equação parcialmente preenchida:

$$\begin{array}{r} \text{2 B C D 8} \\ \times 4 \\ \hline \text{8 D C B 2} \end{array}$$

Observe que o dígito C ocupa a terceira posição tanto no número original quanto no resultado da multiplicação. Dessa forma, a relação matemática que rege essa posição pode ser expressa como $(4 \times C) + x = C$, onde x representa o valor transportado (o “vai algo”) proveniente da multiplicação de $4 \times D$.

Assim, C deve ser um número que, ao ser multiplicado por 4 e somado a x , mantém inalterado o seu último dígito.

Testando valores possíveis para C :

- $4 \times 6 = 24 \Rightarrow 24 + 2 = 26$ (C pode ser 6 se $x = 2$).
- $4 \times 9 = 36 \Rightarrow 36 + 3 = 39$ (C pode ser 9 se $x = 3$).

Portanto, C pode ser 6 ou 9. Agora, testamos os dois casos possíveis.

5.1.3. Caso 1: $C = 6$

Se $C = 6$, a equação fica:

$$\begin{array}{r} 2\ B\ 6\ D\ 8 \\ \times 4 \\ \hline 8\ D\ 6\ B\ 2 \end{array}$$

Agora, analise a segunda coluna, onde temos: $4 \times B + 2 = D$.

Observe que D tem de ser menor que 9, pois não há "vai um" nesta operação (o 2 da primeira coluna não recebe "vai um").

Neste caso, B só pode ser 1, resultando em D ser 6 ($4 \times 1 + 2$). Porém, como o valor 6 já foi usado para C , essa opção não funciona. Logo, $C \neq 6$.

5.1.4. Caso 2: $C = 9$

Agora, testamos $C = 9$. A equação fica:

$$\begin{array}{r} 2\ B\ 9\ D\ 8 \\ \times 4 \\ \hline 8\ D\ 9\ B\ 2 \end{array}$$

Agora, analisamos a segunda coluna, onde temos: $4 \times B + 3 = D$.

Reusando o raciocínio do passo anterior, sabendo que $D \leq 9$, temos que $D = 6$ ($4 \times 1 + 2$).

Conclusão: $A = 2$, $B = 1$, $C = 9$, $D = 7$, $E = 8$

6. Avaliação

A avaliação será processual e baseada no engajamento dos alunos durante a atividade, considerando aspectos como participação ativa, colaboração em grupo, organização do raciocínio e resolução dos desafios propostos. Além disso, os estudantes serão incentivados a criar seus próprios desafios criptoaritméticos e compartilhá-los com os colegas, promovendo a troca de conhecimento e a validação das estratégias utilizadas. Para complementar o processo avaliativo, cada grupo deverá apresentar a solução de um desafio, explicando os passos seguidos e justificando suas escolhas, permitindo ao professor verificar a compreensão dos conceitos trabalhados e o desenvolvimento do pensamento computacional e lógico.

Referências

- Abbasian, R. and Mazloom, M. (2010). Solving cryptarithmic problems using parallel genetic algorithm. volume 1, pages 308 – 312.
- Brasil, M. d. E. S. d. E. B. (2017). Base nacional comum curricular. Acesso em: 12 feb. 2025.
- SBC, S. B. d. C. (2023). Computação na educação básica – complemento à base nacional comum curricular. Acesso em: 7 jul. 2023.
- Stallings, W. (2005). *Cryptography and network security*. Pearson, Upper Saddle River, NJ, 4 edition.
- Szilagyi, M. N. (2016). Cryptarithmetics: A primer. https://www.parabola.unsw.edu.au/sites/default/files/2024-03/vol52_no3_3.pdf. [Accessed 12-02-2025].
- Widodo, S., Najati, U., and Rahayu, P. (2019). A study of cryptarithmic problem-solving in elementary school. *Journal of Physics: Conference Series*, 1318:012120.