Segurança Cibernética na Base Nacional Comum Curricular – Uma proposta de abordagem de Criptografia na Educação Básica

Raquel Moreira Machado Fernandes[1,2], Claudia Lage Rebello da Motta[2] , Luiz Fernando Rust da Costa Carmo [2]

[1]Departamento de Informática Educativa – Colégio Pedro II
São Cristóvão – RJ – Brasil

[2]Programa de Pós-Graduação em Informática (PPGI) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, RJ.

raquel.fernandes@ufrj.br, claudiam@nce.ufrj.br, rust@nce.ufrj.br

Abstract. *This work presents a proposal for the development of knowledge and skills related to cryptography in the "cybersecurity" knowledge object of the "digital world" axis for teaching computing in basic education from a multiliteracy perspective using multimedia resources. The possibility of teaching about cybersecurity in a fun and meaningful way is confirmed.*

Resumo. *Neste trabalho apresentamos uma proposta para o desenvolvimento de conhecimentos e habilidades relacionadas à criptografia no objeto de conhecimento "segurança cibernética" do eixo "mundo digital" para o ensino de computação na educação básica numa perspectiva de multiletramento utilizando recursos multimidiáticos. Corroboramos a possibilidade de ensinar sobre segurança de maneira lúdica e significativa.*

1. Descrição Geral

O complemento à BNCC, organizado em três eixos, sendo eles: pensamento computacional, mundo digital e cultura digital, visa orientar uma aprendizagem para além da instrumentalização, privilegiando a criatividade, o pensamento crítico e os fundamentos que regem o desenvolvimento de artefatos tecnológicos. No contexto sócio-histórico atual, segurança digital é um tema tão importante que está presente neste complemento para todos os anos de escolaridade, desde a educação infantil até o ensino médio. Neste trabalho, apresenta-se uma proposta para o desenvolvimento de conhecimentos e habilidades relacionadas à criptografia no objeto de conhecimento "segurança cibernética" do eixo "mundo digital".

Segundo Silva (2021), "a criptografia é o estudo de métodos para ocultar o conteúdo de mensagens, tornando as informações incompreensíveis para pessoas não autorizadas. Faz parte da história da humanidade e atualmente, está presente em diversas situações senhas, compras e mensagens pela internet, cartões, aplicativos, tudo que precisa ser mantido em segredo. Portanto, está relacionada às necessidades da sociedade, atrelada ao desenvolvimento tecnológico".

2. Objetivos

Nesta proposta, os objetivos de aprendizagem são: i) Compreender o conceito de criptografia e seus fundamentos; ii) Conhecer a evolução histórica da criptografia; iii) Reconhecer os usos modernos da criptografia; iv) Experimentar, na prática, uma técnica de criptografia.

Para a experimentação prática, selecionamos a técnica conhecida como Cifra de César. Esta técnica é uma das mais antigas, tendo seu desenvolvimento sido atribuído ao general Julio Ceśar, importante figura na época da transição da República para o Império Romano. Destacamos, aqui, a possibilidade de interdisciplinaridade com as disciplinas de História e Matemática. Para além da compreensão do conceito de criptografia, este objeto de aprendizagem pode servir como estímulo à outros, como o aprendizado de funções, segundo Silva (2021). A Cifra de Ceśar também é uma das técnicas de criptografia mais fáceis, pois funciona através da substituição das letras do alfabeto e o deslocamento das letras em posições.

3. Habilidades Trabalhadas

A habilidade EF09CO05, do objeto de conhecimento "segurança cibernética", compreende "analisar técnicas de criptografia para armazenamento e transmissão de dados." No Documento "Computação – Complemento à BNCC", é uma habilidade indicada para o 9º ano do ensino fundamental. Contudo, esta proposta também abrange habilidades relacionadas à competência geral nº4, além de habilidades relacionadas às unidades temáticas de Matemática e História, pois é possível estabelecer uma relação passado/presente e refletir sobre as transformações ocorridas em função do desenvolvimento das tecnologias de comunicação e informação.

4. Materiais Utilizados

Para esta proposta, é possível utilizar diferentes recursos, sendo eles analógicos e/ou digitais, sendo algumas sugestões testadas: 1) Kits de encriptação com base em Silva (2021, p. 89) – Cada kit deve conter: a) 2 copos descartáveis; b) fitas de papel colorido com o alfabeto completo impresso de forma semelhante a uma fita métrica no tamanho da circunferência da borda superior do copo; c) tesoura; d) cola. 2) Aplicativos de encriptação, como o disponível em https://cifra-de-cesar-nextjs.vercel.app/. 3) Cifra de César do Super Mário – Este material foi adaptado de um material disponível sob licença *Creative Commons 4.0* em https://eduescaperoom.com/cifrado-cesar. O material possui dois discos, sendo um com o alfabeto e um com personagens e símbolos do Jogo Super Mário. A adaptação possibilitou a elaboração de um arquivo digital[1] contendo os dois discos para serem montados pelos alunos no Laboratório de Informática. Ao trabalhar no computador, é possível relembrar os atalhos do teclado para as funções de copiar e colar, possibilitar o desenvolvimento da coordenação motora através das atividades de clicar e arrastar os itens, bem como trabalhar a compreensão semiótica e a linguagem não-verbal através dos desenhos dos personagens.

1 https://bit.ly/cifra-super-mario

A Cifra de César também pode ser utilizada de forma desplugada, por meio da impressão do arquivo original ou montagem de discos giratórios utilizando papelão ou cartolina, como no exemplo de Rosseto (2018).

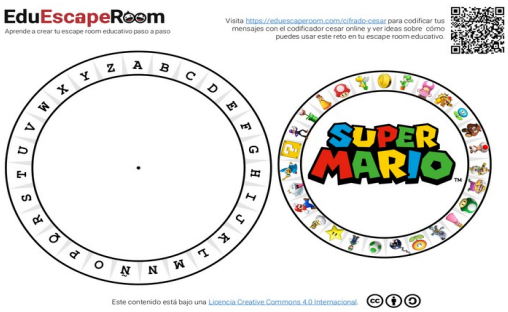

Figura 1. Cifra de César com personagens do Jogo Super Mário

Fonte: Reprodução de @Martade3a6 em https://eduescaperoom.com/cifrado-cesar

5. Metodologia

Nesta proposta, o aprendizado de criptografia pode ser distribuído da seguinte forma:

- Aula 01 – Apresentação do conceito de criptografia e experimentação analógica. Nessa aula, introduz-se o conceito e o histórico da técnica da criptografia e da Cifra de César. Algumas questões que podem ser utilizadas na discussão: Alguém já ouviu a palavra criptografia? O que é a criptografia? Para que serve a criptografia? Onde nós utilizamos criptografia? Criptografia é uma coisa difícil? A criptografia só pode ser feita através do computador? Após a discussão, divide-se os estudantes em duplas e procede-se a entrega dos kits de encriptação para que cada dupla monte seu dispositivo. Para montagem, basta que os estudantes recortem as tiras do alfabeto e colem na parte superior do copo. Para utilizar o dispositivo, basta encaixar os copos e girá-los de acordo com a posição da chave. Após a montagem dos dispositivos, cada dupla tem a missão de criptografar uma mensagem. Esta etapa pode ser realizada de forma desplugada com envelopes e papéis coloridos, ou de forma digital usando um mural do Padlet, por exemplo. Após todas as duplas concluírem, os cartões devem ser entregues a uma outra dupla para a atividade de descriptografar as mensagens. No caso do Padlet, cada dupla deve escolher a mensagem de outra dupla. Ao término da aula, os estudantes devem compartilhar as respostas para verificarem se estão corretas e contarem sobre a experiência de codificar/decodificar uma mensagem.
- Aula 02 – Consolidação do aprendizado através de jogos e Cifra de César visual. Nesta aula, reinicia-se o debate para verificar se os estudantes compreenderam conceitos importantes, como emissor, destinatário e chave. Para isto, podem ser utilizados jogos digitais, como os propostos por Silva (2018) desenvolvidos no Wordwall. Nesta aula, sugere-se a utilização do recurso *Cifra de César com personagens do Jogo Super Mário* para explorar o tema de forma lúdica e significativa para os estudantes. Utilizando o arquivo digital ou os discos

impressos, é possível fazer com que os estudantes criptografem e descriptografem mensagens utilizando símbolos. Além disso, caso seja possível utilizar computador ou celular, os estudantes podem experimentar aplicativos de encriptação para criar ou solucionar desafios propostos pelo professor.

- Atividade complementar – Para uma terceira aula, ou uma atividade complementar, sugere-se a leitura do livro "A Droga da Obediência", do Autor Pedro Bandeira, publicado pela Editora Moderna. No livro, um grupo de adolescentes tenta resolver alguns mistérios na escola e desenvolvem uma forma secreta para se comunicarem. Essa comunicação secreta é um tipo de criptografia e também se baseia na substituição de letras do alfabeto. Sugerimos como atividade complementar a leitura e discussão do livro, bem como a divisão dos alunos em grupos de até 5 alunos para que cada grupo crie, com base na história, uma forma de substituição para enviar mensagens secretas.

6. Avaliação

Nesta proposta, sugerimos um processo de avaliação formativa por meio do qual podem-se considerar, entre outros, os seguintes aspectos:

- Criatividade – Verificar a criatividade para elaboração das palavras / mensagens a serem codificadas. Verificar a criatividade na atividade complementar para a escolha de uma nova forma de substituição.
- Vocabulário – Verificar se o estudante demonstra expansão no vocabulário, compreendendo o significado de novas palavras como criptografia, cifra de césar, chave, entre outras.
- Coordenação Motora – Verificar se os estudantes conseguem realizar movimentos adequados para a elaboração dos discos, seja de maneira analógica ou digital, observando, por exemplo, se conseguem cortar e colar ou clicar e arrastar elementos no computador.
- Linguagem, oralidade e metacognição – Ao término da aula 01, sugerimos que os estudantes conversem e compartilhem suas experiências. Nesse momento, é possível utilizar a técnica da elaboração dirigida (Seminério, 1987) para guiar as discussões e analisar aspectos relacionados à linguagem, oralidade e metacognição.

Nesta proposta de implantação de um novo objeto de conhecimento atual e relevante no âmbito da computação na educação básica, demonstramos que é possível abordar criptografia de forma simples, lúdica e atrativa para as crianças por meio de recursos multimidiáticos, oportunizando o desenvolvimento concomitante de diferentes habilidades, trabalhando na perspectiva do multiletramento em uma experiência passível de ser reproduzida em diferentes contextos escolares, pois as atividades podem ser realizadas em salas de aula, de forma desplugada, ou em salas de Informática utilizando-se computador ou notebook. Reforçamos a importância da Segurança Cibernética e a necessidade de diálogo constante sobre essa temática, que pode e deve ser trabalhada numa perspectiva interdisciplinar.

Referências

BRASIL. Ministério da Educação. Computação - Complemento a BNCC. Brasília: MEC, 2022.

Bezerra, D. J.; Malaguitti, P.L.; Rodrigues, V.C. S. Aprendendo Criptologia de Forma Divertida. http://www.mat.ufpb.br/bienalsbm/arquivos/Oficinas/PedroMalagutti-TemasInterdisciplinares/Aprendendo_Criptologia_de_Forma_Divertida_Final.pdf

Rosseto, C. K. Criptografia como Recurso Didático: Uma Proposta Metodológica aos Professores de Matemática. Dissertação de Mestrado Profissional em Matemática. Universidade Estadual Paulista. https://docplayer.com.br/83814290-Criptografia-como-recurso-didatico-uma-proposta-metodologica-aos-professores-de-matematica.html

Seminério, F. Elaboração dirigida - um caminho para o desenvolvimento metaprocessual da Cognição humana. Rio de Janeiro / Instituto Superior de Estudos e Pesquisas Psicossociais, Cadernos do ISOP, 1987.

Silva, A. L. M. R. A criptografia como estímulo à aprendizagem matemática. Dissertação de Mestrado Profissional em Matemática. Universidade Estadual do Sudoeste da Bahia. http://www2.uesb.br/ppg/profmat/wp-content/uploads/2022/02/Dissertacao_Ana_Lourdes_Moreno_Rodrigues_Silva.pdf