Criptografia Lúdica na Educação Básica: uma abordagem sobre a Máquina Enigma

Franklin Sales de Oliveira[1], **Lucas Superti da Silva**[1], **Ulisses Brisolara Corrêa**[1]

[1]Centro de Desenvolvimento Tecnológico — Universidade Federal de Pelotas
Rua Gomes Carneiro, 01 — Pelotas — RS — Brasil

{fsoliveira,lsdsilva,ulisses}@inf.ufpel.edu.br

Abstract. *This paper highlights the educational proposal of an activity using Pringles potato chip packaging, named Pringles Can Enigma. This unplugged approach reveals significant potential to enhance computer education in Elementary School. The proposal contributes to computational thinking and basic principles of cryptography, culminating in a friendly competition where teams attempt to decrypt each other's encrypted messages. Furthermore, the proposal has the potential to transcend computer education by incorporating interdisciplinary elements such as mathematics, history, and languages.*

Resumo. *Este trabalho destaca a proposta educativa da atividade com embalagens de batata da marca Pringles, denominada Pringles Can Enigma — Enigma Lata de Pringles. Essa abordagem desplugada revela um potencial significativo para aprimorar o ensino da computação no Ensino Fundamental. A proposta contribui no pensamento computacional e princípios básicos de criptografia, culminando em uma competição amigável, na qual as equipes tentam decifrar as mensagens cifras uma das outras. Além disso, a proposta tem potencial de transcender o ensino da computação ao incorporar elementos interdisciplinares, como a matemática, história e linguagens.*

1. Descrição Geral

Conforme Wing (2006), o Pensamento Computacional (PC) não está limitado aos profissionais da área, sendo, na verdade, uma habilidade essencial para todos. Ele deveria estar presente no ensino de todas as disciplinas que envolvam o pensamento analítico de crianças. Ao abordar temas complexos, o PC desempenha um papel fundamental ao proporcionar a abstração e decomposição dos dados, utilizando raciocínio heurístico para encontrar soluções possíveis.

Segundo Bordini (2016) e colaboradores, em periódicos e ANAIS de conferências brasileiras entre 2010 e 2015, observou-se uma diversidade de aplicações na introdução de computação com interface em PC no ensino fundamental. Entre as diversas abordagens analisadas, destacaram-se: algoritmos e programação, robótica, jogos, computação desplugada, dentre outras (teatro/música e ensino híbrido).

2. Objetivos

A proposta deste resumo expandido visa divulgar uma atividade de computação desplugada, denominada Pringles Can Enigma (PCE), que possui potencial de ensinar raciocínio computacional e princípios de criptografia básica. Essa atividade, inspirada na máquina

Enigma da Segunda Guerra Mundial, ganhou popularidade em vídeos do YouTube em língua inglesa, como pode ser observado nesse vídeo[1]. Além disso, destaca-se pela simplicidade dos materiais necessários e pela oportunidade de fomentar a colaboração em equipe.

3. Habilidades Trabalhadas

A atividade Pringles Can Enigma proporciona uma abordagem interdisciplinar, que integra de maneira prática e envolvente conceitos de História, Matemática, Linguagem e a Computação. Ao introduzir os alunos à criação de uma versão simplificada da Máquina Enigma, é contextualizado a História da Segunda Guerra Mundial e a relevância da criptografia.

Simultaneamente, a leitura de instruções e discussões sobre a funcionalidade da máquina estimulam habilidades linguísticas, promovendo a melhor compreensão de textos. A atividade se enquadra na habilidade EF09CO05 — Analisar técnicas de criptografia para armazenamento e transmissão de dados da Base Nacional Comum Curricular, do 9° ano do ensino fundamental, que trata das técnicas de criptografia e o compreendimento de sua importância e uso histórico e atual.

4. Materiais Utilizados

Dois objetos cilíndricos, fita adesiva e tesouras serão necessárias para a elaboração das máquinas. Além disso será necessário imprimir duas folhas que serão coladas nos cilindros, essa impressão é relativa ao tamanho do objeto. A atividade se baseia em uma ideia inicialmente desenvolvida pela Cyber.org[2], a Pringles Can Enigma. A Cyber.org fornece apenas um PDF para "latas" de Pringles vendidas nos Estados Unidos, porém, além alto custo das "latas", as "latas" de Pringles vendidas no Brasil têm dimensões diferentes das dos Estados Unidos, impossibilitando o uso do PDF original diretamente.

Considerando essas dificuldades criamos PDFs para "latas" de Pringles brasileiras e "latas" de Ruffles, além de 25 tamanhos diferentes para objetos com diâmetros entre 3 cm e 9 cm. Uma ferramenta imprimível para medição de cilindros foi criada para facilitar a identificação do PDF certo. Também foi criada uma ferramenta para testar as tiras dos 25 PDFs sem precisar imprimir todos eles. Estes PDFs e ferramentas foram colocados em um repositório no GitHub[3] junto com instruções.

5. Metodologia

Duas equipes são formadas, ambas com a mesma lista de tarefas a serem desempenhadas: realizar o recorte preciso e montagem das suas respectivas enigmas; escolher três palavras para serem criptografadas e, em seguida, criptografar as palavras utilizando suas Enigmas. Ambas as equipes registram as configurações iniciais dos rotores no início do processo, além de anotar as letras que surgem durante a criptografia, formando uma mensagem cifrada. Essa mensagem será crucial como guia durante a etapa subsequente de descriptografia. Dessa forma, os grupos compartilham igualmente as responsabilidades em um processo colaborativo.

[1] veja: `https://www.youtube.com/watch?v=8CsYBKnYNmk` Acesso em: 14 fev 2024.
[2] `https://cyber.org/find-curricula/pringles-can-enigma`
[3] `https://github.com/CommandPromptGamer/Enigma`

Na etapa subsequente, as equipes vão escrever no quadro suas três respectivas configurações de rotores e letras que surgiram no processo. Adicionalmente, a título de escolha, pode-se fazer a escolha em optar por dinamizar ainda mais a atividade ao colocar como regra que os alunos não compartilhem imediatamente suas três de configurações de rotores, mas que forneçam dicas que levem o outro grupo a encontrar estas informações. Essas pistas devem estar relacionadas ao conteúdo das aulas anteriores, incentivando assim a aplicação prática dos conhecimentos adquiridos. Essa abordagem promove a colaboração e o engajamento, enquanto estimula a reflexão sobre os conceitos previamente aprendidos.

Exemplo retirado do documento para impressão da Cyber.org, a configuração de rotores "**A-(A-A-A)-A**", resulta nas letras criptografadas — "**IVWYQDV**", no pdf chamada de mensagem cifrada. Logo em seguida, as equipes terão um momento para decriptar as letras ou mensagens cifradas uma das outras. No exemplo dado a palavra decriptada é "**DECODED**". A equipe que conseguir decifrar as três mensagens cifras primeiro será declarada vencedora da competição.

5.1. Recorte da Impressão e Colagem na Lata

Após a impressão do PDF adequado, para iniciar o recorte é necessário que cada tira de papel ou rotor seja recortada ao longo do contorno cinza em cada uma. Em seguida, as tiras são enroladas em volta da lata ou objeto cilíndrico, seguindo a mesma ordem em que foram impressas na folha. Para garantir a estabilidade e integridade da estrutura, abas nas extremidades de cada tira são fixadas com fita adesiva transparente. É importante certificar-se que cada um dos anéis de papel, representando os rotores, possam girar livremente para assegurar o funcionamento adequado do dispositivo. As tiras relativas à entrada e ao refletor devem ser coladas à lata para ficarem fixas, estas tiras devem ficar na mesma posição de forma que as letras estejam alinhadas.

5.2. Criptografia da palavra "ACE"

Os passos a seguir são referentes ao funcionamento da criptografia da palavra em inglês "ACE", abordada no manual da Cyber. Inicialmente, posicionamos os rotores 1, 2 e 3 alinhados em todas as letras, esta configuração inicial é chamada de "**A-(A-A-A)-A**" (Figura 1), que é a base para o processo e pode ser escolhidas outras configurações com a finalidade de dificultar a descriptografia. Nos próximos passos a configuração dos rotores mudarão.

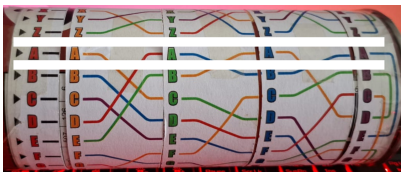
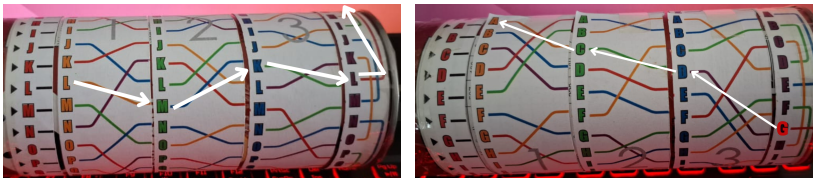


Figura 1. Figura 1 — Uma Enigma configurada em "A-(A-A-A)-A"

O passo subsequente envolve a identificação da letra de entrada, no caso, A, no rotor inicial. Acompanhe seu percurso pelos rotores 1, 2 e 3, culminando no refletor. Durante esse trajeto, observamos um caminho específico que transforma a letra A em L. Prossiga seguindo o caminho de A até o rotor 2, onde a letra C é alcançada. Daí,



Figuras 2 e 3. Passos para decriptar a primeira letra, A

siga para o rotor 3, atingindo a letra D. Continue então até o refletor, chegando à letra G. Subsequentemente, trace o caminho de G ainda no refletor, resultando na letra L. O percurso inverso, retroceda até o rotor 1, e ao alcançá-lo, a letra de saída deverá ser L. Este resultado indica que L é a letra criptografada correspondente à letra A nesse processo de codificação.

Após obter uma letra de saída, no caso a L, gire o rotor 3 uma letra para cima, configurando-os como "**A-(A-A-B)-A**". Para codificar nossa próxima letra, localize a letra C no rotor de entrada. Trace-o através dos rotores 1, 2 e 3, através do refletor e de volta 3, 2 e 1. A letra de saída deve ser B, indicando que B é a letra criptografada de A.

Novamente, gire o rotor 3 uma letra para cima, a configuração agora é "**A-(A-A-C)-A**". Vamos criptografar a letra E da palavra "**ACE**" seguido o mesmo caminho, a letra correspondente deverá ser V. Desse modo, a palavra "**ACE**" é integralmente criptografada como "**LBC**" na Pringles Can Enigma.

5.3. Descriptografia da palavra "ACE"

Para descrever o processo de descriptografia da palavra cifrada com os rotores na posição "**A-(A-A-A)-A**", é fundamental inicializar os rotores nessa mesma configuração. Considerando que a primeira letra da palavra criptografia é L, segue-se o caminho do rotor de entrada de L através do rotor 1 até M no rotor 2, depois para K no rotor 3 e através de L até o refletor.

Em seguida, trace o caminho da letra L no refletor, resultando em G. Depois para D no rotor 3, depois para C no rotor 2 e, finalmente, para letra A no rotor 1, que é alinhado com A em nosso rotor de entrada. Portanto, a primeira letra descriptografada é a letra A.

Essa sequência de passos exemplifica a importância de inicializar o processo com os rotores na posição correta para obter os resultados precisos. Ao prosseguir com os passos seguintes, é crucial lembrar de girar o rotor três uma letra para cima após cada letra descriptografada. Esse padrão é mantido para cada caractere, assegurando que a descriptografia ocorra de maneira precisa e dinâmica.

6. Avaliação

A atividade naturalmente mede a capacidade dos alunos de compreender o funcionamento de um simulador da máquina de criptografia Enigma. Afinal, a criptografia e descriptografia das palavras somente são possíveis quando se compreende seu funcionamento. Desse modo, é possível avaliar a compreensão e entendimento dos alunos observando as dificuldades e facilidades durante a realização da atividade. Além disso, elementos objetivos, como resultado da competição entre os grupos e a vantagem no placar, também podem ser avaliados.

Referências

WING, Jeannette M. Computational thinking. Communications of the ACM, v. 49, n. 3, p. 33-35, 2006.

BORDINI, A. et al. Computação na Educação Básica no Brasil: o Estado da Arte. Revista de Informática Teórica e Aplicada, [S. l.], v. 23, n. 2, p. 210–238, 2016. DOI: 10.22456/2175-2745.64431. Disponível em: https://seer.ufrgs.br/index.php/rita/article/view/RITA-VOL23-NR2-210. Acesso em: 14 fev. 2024.