

Ensino de Criptografia em uma Abordagem Inclusiva para Estudantes do Ensino Médio

Sylvana Karla S. L. Santos¹

¹Instituto Federal de Brasília - Campus Brasília - Brasília - DF - Brasil.

sylkarla@gmail.com

Abstract. *This is an experience report with the teaching of Cryptography, as content of the Information Security discipline, for high school students integrated in Computer Science at an institution of the Federal Network, by carrying out activities in an inclusive approach, considering new contexts for collaborative and reflective participation. The participation of students in the evaluation of the methodology adopted is highlighted, at the end of the process, to verify whether learning was achieved in a significant way.*

Resumo. *Trata-se do relato de experiência do ensino de Criptografia, como conteúdo da disciplina Segurança da Informação, para estudantes do ensino médio integrado em Informática de uma instituição da Rede Federal, por meio da realização de atividades em uma abordagem inclusiva, considerando novos contextos para a participação colaborativa e reflexiva. Ressalta-se a participação dos estudantes na avaliação da metodologia adotada, ao final do processo, para verificar se a aprendizagem foi alcançada de forma significativa.*

1. Introdução

O ensino de criptografia, em geral, está relacionado a conceitos da matemática e da lógica, ao desenvolvimento de códigos cada vez mais robustos e que são aperfeiçoados ao longo dos anos, a fim de impedir a invasão de informações secretas e sistemas computacionais.

Com o intuito de diversificar a forma usual do ensino da criptografia, de modo mais desafiador, e abordar conceitos no viés da inclusão, foram desenvolvidos roteiros didáticos que direcionam a conteúdos que fogem ao padrão daqueles mencionados nas aulas e que são comumente encontrados na literatura.

Assim, este artigo tem o objetivo de relatar a experiência de uma docente na condução da disciplina Segurança da Informação para duas turmas do terceiro ano do Ensino Médio Integrado (EMI) ao curso técnico em Informática em uma instituição da Rede Federal de Educação Profissional e Tecnológica (EPT), durante o ano letivo de 2020. Ressalta-se que, em virtude da pandemia da COVID-19, as turmas do curso tiveram suas atividades iniciadas no formato presencial, retomando as atividades no ensino remoto em agosto de 2020.

2. Criptografia

Criptografar é o mesmo que codificar. Criptografia deriva de *Kriptós* que significa oculto, escondido e *grapho* que representa escrita. A partir da criptografia é possível proteger dados contra acessos indevidos. Isso significa que podemos usar técnicas para proteger

mensagens escritas, faladas, salvas no computador ou, no contexto cibernético, assegurar que os dados que trafegam pela Internet não sejam violados [CERT.Br 2012].

De modo geral, o ensino de criptografia mantém o intrínseco relacionamento com teorias que englobam uso de chaves simétricas e assimétricas, assinatura digital, certificado digital, autenticação, entre outros conceitos técnicos [CERT.Br 2012]. É possível trabalhar os conceitos da criptografia num contexto divertido e desafiador, buscando uma aprendizagem significativa e voltada à realidade do estudante, como: uso de código de barras disponíveis em produtos comerciais, marca d'água presentes em papel moeda, cálculo dos dígitos de um CPF válido e, de forma interdisciplinar, o desafio para a decifragem do código genético.

Ao se referir a uma abordagem inclusiva, considera-se o conceito de educação inclusiva que define “o processo que ocorre em escolas de qualquer nível preparadas para propiciar um ensino de qualidade a todos os [estudantes], independentemente de seus atributos pessoais, inteligências, estilos de aprendizagem e necessidades comuns ou especiais” [Sasaki 1998 p. 8].

Neste trabalho, pondera-se com destaque à abordagem inclusiva como possibilidades de propor atividades para explorar a reflexão do estudante, motivá-lo a relacionar o contexto estudado com situações fora da sala de aula e a pensar sobre as diferenças individuais e coletivas.

3. Trabalhos relacionados

A educação inclusiva, por meio do ensino de conteúdos, tem sido abordada em trabalhos publicados neste evento [WIE] com abrangência do público da educação básica, que inclui o ensino fundamental e médio, da educação de jovens e adultos e também do ensino superior em diferentes contextos. Além do ensino, ações em projetos de extensão podem viabilizar a participação de estudantes e direcioná-los a atividades que permitam a inclusão junto à comunidade externa [Alves et al. 2019].

A explicação de conteúdos mais abstratos e de forma mais atrativa é um desafio para os docentes, ainda mais no ensino remoto com a ausência do uso de laboratórios para as atividades práticas. Como alternativa, pode-se fazer uso de softwares de simulação para exemplificar experiências, por exemplo, no contexto do ensino da física associada à robótica para estudantes do ensino médio [Lopes et al. 2018].

Considerar as necessidades específicas do público que pode participar das atividades, por vezes visto como minoritário, é um bom princípio para o planejamento adequado dos materiais, com o intuito de propor recursos para satisfazer a demanda de determinado grupo, a exemplo de crianças, jovens e adultos, que têm estilos de aprendizagens diferentes [Santos e Kondo 2019].

Diferentes estratégias, como jogos, competição, computação plugada e desplugada, possibilitam o envolvimento de estudantes no processo de aprendizado, promovem a curiosidade e convidam à participação [Rodrigues et al 2019]. Além disso, trabalhar a construção de conteúdos técnicos aplicados em grupo, ainda que de forma remota, incentiva a organização do tempo, a divisão de tarefas e a responsabilidade, que são habilidades que merecem ser, cada vez mais, exploradas e incentivadas [Araújo e Santos 2021].

4. Metodologia

No ensino de Criptografia, percebe-se que comumente são referenciados princípios e técnicas de codificação de mensagens recorrentes na literatura. A organização das atividades, aqui propostas, buscaram oferecer dinâmicas mais interessantes, que fogem ao padrão do uso da Cifra de César ou de algoritmos já conhecidos.

4.1 Participantes

As atividades planejadas foram apresentadas para duas turmas de estudantes do terceiro ano do curso EMI em Informática de uma instituição da Rede Federal EPT durante o ano de 2020, totalizando 48 participantes com idade entre 16 e 18 anos, dos quais 15 são do gênero feminino, ou seja, a menos de um terço do grupo [Santos 2021]. Com relação às necessidades específicas dos estudantes, um deles, do gênero masculino, possui deficiência intelectual.

4.2 Materiais

O conteúdo técnico dos materiais teve base nas produções didáticas disponibilizadas no Repositório Educacional Online do Ministério da Educação - ProEdu <www.proedu.rnp.br>, que é um Acervo de Recursos Educacionais para EPT. Em complemento, foram indicados aos estudantes a consulta a artigos, notícias e vídeos disponibilizados a partir da curadoria da docente da disciplina.

As atividades da disciplina Segurança da Informação foram configuradas e disponibilizadas no Ambiente Virtual de Aprendizagem (AVA) da instituição, que é o Moodle, com acesso restrito aos estudantes das turmas. A sala virtual foi organizada de forma integrada, ou seja, em um espaço formatado em blocos, os quais, ao serem clicados, direcionam aos conteúdos da respectiva disciplina do curso.

4.3 Atividades

Cada atividade foi aberta no AVA com prazo para ser cumprida em um período semanal ou quinzenal. Para possibilitar uma experiência diferenciada, todas as atividades indicaram códigos pouco conhecidos, ou seja, fora do modelo usualmente disposto nos livros didáticos ou mesmo na web. A seguir, será descrito o relato da experiência.

5. Relato da experiência

Ao longo do ano letivo, foram elaboradas três atividades sobre o tema Criptografia. Neste relato, será enfatizada a descrição de uma das atividades que é composta por três questões. Cada código foi, inicialmente, apresentado aos estudantes para, em seguida, propor sua aplicação na atividade.

O roteiro didático, elaborado para a atividade, objetivou um diálogo com os estudantes, convidando-os a conhecer os conceitos básicos de Criptografia e a participar da atividade. O recurso Fórum de discussão do Moodle foi configurado de forma que os estudantes deveriam registrar primeiro sua participação para, só depois, visualizar as contribuições dos demais colegas. A participação de cada estudante correspondeu ao registro da frequência nos dias da aula.

A primeira questão trazia como desafio a decodificação de uma mensagem escrita em Braille. A ferramenta Matbraille¹ foi sugerida para ser usada, uma vez que possibilita a conversão do texto para a escrita em Braille. Sugeriu-se, ainda, que fossem identificados produtos (alimentícios, farmacêuticos, etc.) que trazem a escrita em Braille e qual a utilidade dessa informação. A mensagem da figura 1 é: “mantenha sistemas de detecção de invasores presenciais e digitais sempre atualizados”.

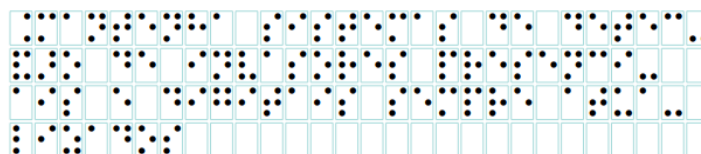


Figura 1. Mensagem em Braille. Fonte: Matbraille.

A segunda questão propôs criptografar a mensagem anteriormente escrita em Braille e utilizar o Código Morse. Indicou-se a ferramenta gratuita disponibilizada pela página invertexto.com², que permite a entrada de um texto escrito e a saída em código Morse, no formato escrito ou sonoro, e vice-versa, com a entrada em código Morse para a escrita. A figura 2 ilustra a respectiva mensagem codificada.

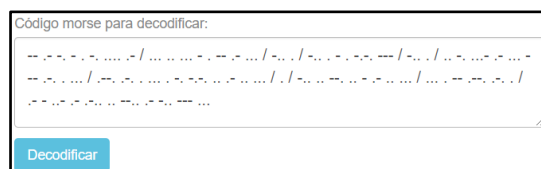


Figura 2. Mensagem em Código Morse. Fonte: Invertexto.com

A terceira e última questão da atividade buscou explorar habilidades mais visuais e orientar a realização de uma pesquisa para conhecer e criar uma palavra ou frase utilizando a comunicação com flâmulas ou bandeiras e registrar no fórum. A participação nesta questão gerou poucas contribuições para a discussão, com o registro de apenas dois estudantes que conseguiram associar essa codificação àquela usada em atividades de grupos escoteiros, além do contexto marítimo comumente associado.

A partir das orientações e da escolha dos estudantes, foi lançado o desafio de criar uma mensagem e disponibilizar no fórum para estimular a capacidade de decodificação dos colegas. Houve a participação de 42 estudantes (87,5%), dentre os quais a totalidade das 15 meninas. Para cada postagem, a professora da turma deu o *feedback* com uma mensagem decifrando o código apresentado, caso um colega não o tenha feito antes. A maioria dos participantes optou pela mensagem em Braille (71,5%) e oito escolheram o Código Morse (19%). Os demais estudantes não elaboraram a mensagem codificada (9,5%) em um dos códigos propostos.

6. Conclusão

A partir de um roteiro didático é possível apresentar o conteúdo a ser trabalhado e convidar o estudante a realizar uma atividade prática, ampliando a experiência para o contexto da educação inclusiva. Ao tratar da criptografia com códigos que abordam técnicas de acesso à informação para pessoas cegas (Braille e Morse) e pessoas surdas

¹ <https://www.atractor.pt/mat/matbr/matbraille.html>

² <https://www.invertexto.com/codigo-morse>

(Bandeiras), a experiência buscou fornecer alternativas que promovessem a reflexão acerca do conteúdo que estava sendo estudado.

A participação dos estudantes na atividade foi considerada positiva, indo além da obrigatoriedade para o registro da frequência semanal, visto que alguns participaram mais de uma vez do fórum e puderam interagir com os colegas para descobrir as mensagens enviadas em diferentes códigos. Apenas um dos participantes afirmou que não gostou da atividade, pois achou “meio complicada”, mas não respondeu ao ser questionado sobre possíveis sugestões de melhoria. Os demais afirmaram que gostaram.

Como forma de avaliar a estratégia adotada, os estudantes foram questionados, ao final do bimestre, sobre a metodologia adotada na disciplina. Um deles mencionou que não sabia que a escrita em Braille se assemelhava à codificação e que a atividade contribuiu com novos conhecimentos, corroborando com a abordagem inclusiva.

Por fim, evidenciou-se que não há muitos trabalhos publicados no WIE que relacionem a educação inclusiva no ensino de conteúdos técnicos, o que se torna um tema atrativo para outras investigações.

Referências

- Alves, M. R. F., Farias, R. S., Oliveira, K. R. S., Medeiros Junior, V., Sousa, W. P., Filgueira, J. D. B. (2019) Análise do Projeto de Extensão de Inclusão Digital e Informática Educativa no Ensino Fundamental da Rede Pública. In: *Workshop de Informática na Escola*, 25., p. 1214-1218. DOI: <https://doi.org/10.5753/cbie.wie.2019.1214>.
- Araújo, V. A., Santos, S. K. S. L. (2021) "Integração no processo de ensino e aprendizagem: relato de experiência na formação técnica". In: *Educação Profissional e Tecnológica: inclusão, pesquisa, ensino e ação* (2021) Orgs.: Silva, Q. P., Santos, S. K. S. L., Cap. 5, p. 60-73.
- CERT.Br. (2012) “Cartilha de Segurança para Internet”. São Paulo: Comitê Gestor da Internet no Brasil. CGI.Br. 142p. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf> Acesso em: 22 jul. 2021.
- Lopes, A. R. S., Cruz, E., Siebra, C. (2018) Uma Análise com Foco Quantitativo sobre o Uso da Robótica Educacional no Ensino da Física. In: *Workshop de Informática na Escola*, 24., p. 99-108. DOI: <https://doi.org/10.5753/cbie.wie.2018.99>
- Rodrigues, G., Braga, R., Amorim, T. (2019) Criptografia e Segurança Web: um relato de experiência do ensino de conceitos computacionais para crianças. In: *Workshop de Informática na Escola*, 25., p. 1099-1103. DOI: <https://doi.org/10.5753/cbie.wie.2019.1099>.
- Santos, S. K., Kondo, C. (2019) Stop motion como estratégia de ensino e aprendizagem para crianças, jovens e adultos. In: *Workshop de Informática na Escola*, 25, p. 1044-1048. DOI: <https://doi.org/10.5753/cbie.wie.2019.1044>
- Santos, S. K. S. L. (2021) Análise da Participação de Meninas e Mulheres no Ensino Médio em Informática do Instituto Federal de Brasília. In: *Women In Information Technology* (WIT), 15. p. 270-274. DOI: <https://doi.org/10.5753/wit.2021.15864>
- Sasaki, R. K. (1998) “Inclusão: o paradigma da próxima década”. Mensagem, Brasília, 34(83), 29p.