O ESTUDO DA CRIPTOGRAFIA APLICADA COM ALGORITMOS: ALTERNATIVA PARA O ESTÍMULO NA APRENDIZAGEM DE MATRIZES NO ENSINO MÉDIO

Michel Ferreira Batista; Nancy Lima Costa
Universidade de Pernambuco Campus Petrolina, michelfbatista@hotmail.com.br
Universidade de Pernambuco Campus Petrolina, nancy.costa@upe.br

Introdução

A aprendizagem na educação básica, em foco nos conteúdos de Matemática, sempre foi e ainda é um desafio para muitos professores. A falta de interesse por parte dos alunos, a falta de conexão entre teoria e a pratica e a metodologia muitas vezes tradicionalista de alguns professores, propicia a insatisfação de muitos alunos, e a falta de interesse em estudar determinados conteúdos matemáticos. Com o objetivo de propor atividades acerca da criptografia e algoritmos computacionais, envolvendo uso do conteúdo de matrizes no ensino médio e na busca por reverter ou ao menos amenizar esse quadro, foram realizadas duas oficinas sendo uma de "criptografia aplicada ao ensino de matrizes" e outra de "uso de algoritmos computacionais com a criptografia". As atividades foram idealizadas e construídas na busca de dar sentido ao que é estudado em sala de aula, instigar e motivar a participação dos alunos no estudo da Matemática.

Metodologia

Compreende a realização de atividades práticas em sala de aula, com turmas do 1º ao 3º ano do Ensino Médio, que estejam estudando ou que estudaram o conteúdo de matrizes. Utilizando como temática os uso de criptografia e algoritmos computacionais buscando estabelecer ligação dos conhecimentos vivenciados em sala de aula com outras áreas profissionais, neste caso a segurança da informação. O desenvolvimento das atividades foi distribuído em quatro etapas: sondagem inicial, aplicação da oficina de criptografia e Matemática, aplicação da oficina de algoritmos computacionais e avaliação final; onde envolveu a participação de 23 alunos.

O primeiro momento foi dedicado à apresentação da proposta desse trabalho e a sondagem de conhecimentos prévios dos alunos através de questionário como método de coleta de dados, conforme Gerhardt e Silveira (2009). O questionário foi formulado com perguntas distribuídas entre abertas e fechadas (mistas), cujo foco é identificar o nível de conhecimento prévio e a opinião dos estudantes quanto às dificuldades enfrentadas no aprendizado da Matemática.

No segundo momento, foi feita uma apresentação sobre o tema "criptografia e a Matemática", com duração prevista para 2 horas/aula, com objetivo de apresentar os conceitos que envolvem a criptografia, vistos em França (2014), Litoldo (2016), Jesus (2013), Olgin (2011), e fazer uma breve revisão de conteúdos matemáticos, vistos em Boldrini *et al* (1984) e Domingues e Iezzi (2003), necessários para a realização da oficina. Posteriormente foi aplicada uma atividade proposta em grupos para cifrar e decifrar mensagens criptografadas usando a cifra de César e de Vigenére e outra usando as técnicas da cifra de Hill.

No terceiro momento com duração de 2 horas/aulas a oficina de programação foi realizada com o intuito de desenvolver fragmentos do algoritmo de criptografia de Hill. Para tal inicialmente analisou-se cada etapa, para a solução da problemática (cifrar ou decifrar), montando o algoritmo em português estruturado para resolver cada necessidade. Foi apresentada a ferramenta de

ensino e aprendizagem de algortmos“Visualg”, descrita em Leite *et al* (2013) e Rodrigues (2009), e aplicadas atividades desenvolvidas no laboratório de informática.

Por fim, aplicou-se a avaliação final para obter o feedback dos estudantes. Visando identificar o grau de satisfação quanto às atividades desempenhadas e obter suas opiniões quanto a importância em se trabalhar um tema, como o uso de criptografia e de algoritmos, para a aprendizagem de conteúdos matemáticos.

Resultados e discussão

A avaliação final externou os seguintes resultados: 70% dos participantes não sabiam que a Matemática estava presente no campo da criptografia e 30% acharam importante o uso da Matemática na segurança da informação. Observou-se também que 62% dos participantes declarou não ter apresentado dificuldades na atividade de cifra de Hill, e aqueles que tiveram, declararam ter se esquecido do conteúdo de matrizes. Sobre o estimulo, foi unânime, alguns comentaram que o assunto despertou a atenção, outros mencionaram que por se tratar de tecnologia já traz uma empolgação e até foi relatado de que alguns usariam em suas vidas.

Em seguida, 64% dos participantes declararam ter sentido dificuldades na atividade de algoritmos computacionais, dentre estes, 17% referente a problemas com a digitação, 43% referente à dificuldade com sinais e cálculos e 40% devido ao impacto inicial em trabalhar com a linguagem, algo que foi resolvido com a continuidade dos exercícios.

Assim como na atividade da oficina de criptografia, todos se sentiram estimulados com o software, devido a praticidade de criptografar, outros disseram que uso de computador é atrativo, e perde menos tempo para resolver um problema. Já sobre qual atividade foi mais interessante, com 56% foi escolhida a atividade com uso de algoritmos no VisualG. Isso mostra que ambas as atividades despertaram o interesse em sua realização.

A avaliação quanto a aceitação das atividades mostraram que, 81% aprovaram a primeira oficina e 85% aprovaram a segunda oficina. E quanto as opiniões e impressões sobre as atividades, 71% dos estudantes comentaram sobre o tempo insuficiente para a realização das mesmas, 37% despertou o desejo de que essas atividades se estendam pelas escolas públicas e 55% elogiaram quanto ao trabalho e conteúdos apresentados.

Em síntese, observou-se dificuldades encontradas pelos estudantes na oficina de “criptografia aplicada no estudo de matrizes”, mais relacionadas com cálculos matemáticos, como para calcular determinantes e o produto de matrizes. Durante a revisão de conteúdos matemáticos, alguns participantes alegaram ter aprendido de fato assuntos como números primos, m.m.c. e matrizes, naquela apresentação. É relevante pontuar que assuntos até então desconhecidos por muitos estudantes como, aritmética modular, congruência e inversos modulares, foram compreendidos de forma rápida, a partir de aplicações no cotidiano, como foi o caso da criptografia.

As dificuldades observadas com o emprego de uma ferramenta computacional para a elaboração de algoritmos ocorreram como era de se esperar. Algumas estavam relacionadas com erro de sintaxe durante a compilação dos programas e a atenção quanto a digitação das palavras reservadas ao vocabulário do software.

O êxito e desempenho dos estudantes em realizar alguns exercícios propostos, merece destaque; já que esse foi o primeiro contato deles com essa

ferramenta. Ademias, muitos se sentiram motivados com as atividades propostas e demonstram interesse em continuar estudando os conteúdos matemáticos e a linguagem computacional.

Conclusões

Conforme objetivos propostos, concluimos que houve êxito na execução da proposta. É notável que a realização das oficinas, mostram que esse trabalho vai mais além do que a proposta pretendida, pois além de trabalhar com sistemas lineares, matrizes, determinantes; é possível envolver outros conteúdos, como por exemplo: funções afim, funções quadráticas, logaritmos, entre outros.

Fica evidente, a necessidade de incentivar os professores e alunos a criarem estruturas que possibilitem o desenvolvimento de atividades como a apresentada que tragam a Matemática para dentro da sala de aula de forma indireta, com temáticas, longe dos métodos tradicionais; rompendo com os medos e aversões à própria Matemática, tornando a mais amigável e lúdica, possibilitando o gosto pelos estudos, aumentando a motivação dos estudantes em frequentar as salas de aula.

Palavras-Chave: Criptografia; Matemática; Algoritmos; Matrizes; Segurança da informação.

Referências

BOLDRINI, J.L. *et al*. **Álgebra Linear**. São Paulo, Harper & Row do Brasil, 1984. 411p.

DOMINGUES, H.H. IEZZI; Gelson et al. **Álgebra linear e aplicações**. São Paulo, Atual, 2003.

FRANÇA, W. B.de A.. A utilização da criptografia para uma aprendizagem contextualizada e significativa. 2014. 63f. **Dissertação** (Mestrado Profissional em Matemática) – Universidade de Brasília, Instituto de Ciências Exatas. Brasília.

GERHARDT ,T. E.; SILVEIRA, D. T.. **Métodos de pesquisa**, 2009. 120f.
Universidade Aberta do Brasil – UAB/UFRGS. Porto Alegre: Editora da UFRGS.

JESUS, A. L. N. Criptografia na educação básica: utilização da criptografia como elemento motivador para o ensino aprendizagem de matrizes. 2013. 70f. **Dissertação** (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal do Vale do São Francisco. Juazeiro-BA.

LITOLDO, B. F.. As potencialidades de atividades pedagógicas envolvendo problemas criptográficos na exploração das ideias associadas à função afim. 2016. 198f**. Dissertação** (Mestrado Educação Matemática) – Universidade Estadual Paulista. Rio Claro – SP.

OLGIN, Clarissa de Assis. Currículo no Ensino Médio: Uma Experiência com o Tema Criptografia. 2011. 136f. **Dissertação** (Mestrado em Ensino de Ciências e Matemática.) – Universidade Luterana do Brasil. Canoas – SP.

RODRIGUES, A. **Manual do Visualg**. 2009. 20f. IFCE Campus Iguato. Disponível em: <http://www.slideshare.net/jkolive/apostila-de-visualg> Acessado em: 10/02/2017.