PROPOSTA DE ENSINO DE CRIPTOGRAFIA PARA A DISCIPLINA DE ÁLGEBRA LINEAR

Robson Reis Amorim Junior[1], Monica Karrer[2]
[1,2] Departamento de Matemática, Centro Universitário da FEI
robbsonjunior@hotmail.com e mkarrer@fei.edu.br

Resumo: Neste artigo tem-se por objetivo apresentar um estudo qualitativo sobre o tema Criptografia, o qual representa uma importante aplicação da Álgebra Linear. Balizados na teoria dos registros semióticos de [1] e [2] e na metodologia de *Design Experiment* de [3], um experimento de ensino sobre o tema está sendo elaborado e este será aplicado a uma pequena amostra de sujeitos, com vistas a realizar as adaptações necessárias para obter um produto que possa ser aplicado futuramente na disciplina de Álgebra Linear.

1. Introdução

Neste artigo apresenta-se a descrição de um estudo em andamento, o qual tem por objetivo elaborar e aplicar um experimento de ensino sobre Criptografia, explorando conteúdos matemáticos da disciplina de Álgebra Linear.

Segundo [4], Criptologia é definida como a ciência que estuda o oculto – do grego kryptos = escondido / oculto; e logo = estudo / ciência. Criptografia, por sua vez, refere-se a um ramo da criptologia que se dedica ao desenvolvimento de métodos de manipulação alfabética e numérica que visam a transformação de uma mensagem comum em um texto cifrado, de forma que apenas o destinatário seja capaz de ter acesso à mensagem original.

A criptografia está extremamente presente em nosso cotidiano, sendo utilizada em praticamente todos os ambientes digitais, viabilizando, por exemplo, troca de mensagens instantâneas e transações bancárias por meio de dispositivos móveis.

A Álgebra Linear, disciplina presente nos currículos de todas as modalidades de Engenharia, é considerada pelos estudantes, segundo [5] e [6], como um conjunto de regras sem qualquer aplicação prática. Apesar de a Álgebra Linear ser uma disciplina com característica abstrata, ela está presente em aplicações das mais diversas áreas. A Criptografia representa uma delas, envolvendo conceitos de transformação linear, independência linear e operações matriciais.

A presente pesquisa está fundamentada na teoria dos registros de representações semióticas de [1] e [2], o qual afirma que um objeto matemático deve ser explorado em diferentes registros de representações semióticas, tais como o matricial, o algébrico e o da língua natural. Ainda, esse estudo procura se pautar nas considerações de [7], [8] e [9] a respeito dos ganhos pedagógicos obtidos ao se integrar a tecnologia no ensino de Matemática.

Desta forma, essa pesquisa, de cunho educacional, tem por objetivo elaborar e analisar um experimento de ensino sobre Criptografia, unindo a integração de recurso tecnológico com a exploração de registros de representações semióticas. Dos diversos métodos de criptografia pesquisados, selecionou-se a Cifra de Hill, uma vez que ela envolve vários conceitos de Álgebra Linear.

Pretende-se, então, criar um cenário de aprendizagem que possa ser efetivamente integrado nas aulas regulares da disciplina de Álgebra Linear.

2. Metodologia

Para a construção desse trabalho, utilizou-se a metodologia de *Design Experiment* de [3], a qual fornece elementos para a construção e condução de experimentos de ensino na área de Matemática. Essa metodologia tem caráter iterativo e é dotada de flexibilidade, sendo possível efetuar alterações durante o processo de aplicação do experimento, caso as produções dos alunos revelem tal necessidade.

Inicialmente foi realizado um estudo sobre o tema, identificando os diversos métodos criptográficos existentes. Em seguida, foram elencados os elementos matemáticos necessários para o desenvolvimento do experimento, tais como transformações lineares, operações matriciais e aritmética modular.

No presente momento, o trabalho encontra-se na fase de elaboração do experimento de ensino, o qual prevê três etapas: uma tarefa inicial de criptografia a ser realizada no ambiente papel e lápis, uma segunda tarefa utilizando um programa elaborado no Matlab exclusivamente para esse trabalho, e uma terceira relativa a um problema enigma.

Pretende-se inicialmente aplicar o experimento em pequena escala, para que seja possível avaliar, de forma minuciosa, as trajetórias dos estudantes e as necessidades de adaptações no *design,* antes de aplicá-lo em aulas regulares de Álgebra Linear.

3. O experimento de ensino

O experimento de ensino objetiva potencializar o processo de ensino-aprendizagem da Álgebra Linear por meio da criação de oportunidades de utilização do que é estudado na teoria em aplicações práticas do cotidiano. Primeiramente, o aluno será apresentado a todos os conceitos matemáticos necessários e, então, realizará o processo de criptografar uma pequena mensagem no ambiente papel e lápis por meio do método da cifra de Hill, sem o auxílio de dispositivos eletrônicos. Nesta primeira etapa, espera-se que o aluno entenda os conceitos matemáticos utilizados por Lester S. Hill na construção de seu método e perceba a necessidade do auxilio de uma ferramenta computacional para a realização do procedimento com mensagens maiores.

Nesta primeira etapa, serão explorados tratamentos e conversões entre representações dos registros algébrico, matricial e da língua natural.

Visto que o MATLAB é um software já utilizado na disciplina de Álgebra Linear da FEI, foi criado um código que criptografa e descriptografa mensagens para qualquer quantidade de letras por meio do método de Hill. Seguem exemplos de execução do código no MATLAB. No primeiro caso, foi inserida a mensagem "criptoanálise", e no segundo, foi inserida a mensagem "A matemática é a rainha das ciências".

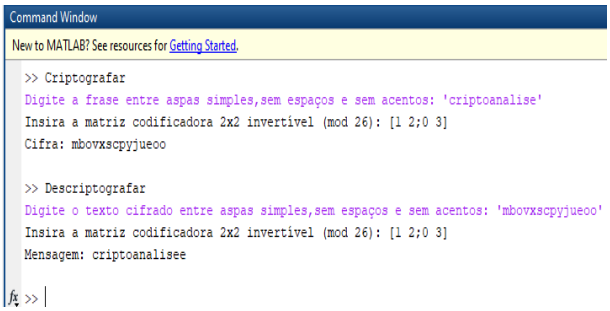

Figura 1 – Cifra de Hill no MATLAB – Exemplo 1

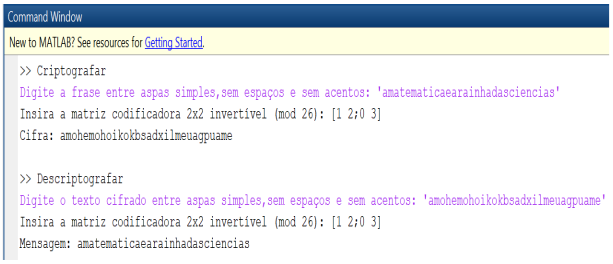

Figura 2 – Cifra de Hill no MATLAB – Exemplo 2

Na segunda etapa, o aluno realizará o procedimento de criptografar e descriptografar uma mensagem no software MATLAB, porém, sem o auxílio do código criado. Dado que a tarefa será aplicada para estudantes do curso de Engenharia, para tal fim foi elaborado um roteiro com todos os comandos do MATLAB necessários para a realização da atividade. Visto que o aluno já possui os conceitos matemáticos necessários, o objetivo da segunda etapa é a familiarização com o software MATLAB, o qual é amplamente utilizado nos cursos de Engenharia. Nesta fase, serão explorados tratamentos e conversões entre representações dos registros simbólico especializado (código) e da língua natural.

Na terceira etapa, será aplicado um problema desafio, o qual ainda está em fase de elaboração.

4. Conclusões e Etapas Futuras

Até o presente momento, foram realizadas as etapas de delimitação do objeto matemático, estudo da fundamentação teórica, análise da revisão de literatura e construção prévia do experimento. Nessa fase foram detectados diversos métodos criptográficos, sendo selecionado, para a elaboração do experimento de ensino, o método que utiliza vários conceitos de Álgebra Linear. A revisão de literatura apontou a necessidade de propostas de ensino que tenham a preocupação de integrar a teoria da Álgebra Linear com aplicações práticas, uma vez que os estudantes enxergam essa disciplina como uma área exclusivamente abstrata. Ainda, um trabalho de exploração de diferentes registros semióticos se mostrou viável, para que essa disciplina não se limite a um conjunto de procedimentos algébricos.

Como continuidade do estudo, estão previstas as fases de finalização da construção do experimento e sua aplicação a uma amostra de estudantes de Engenharia que já cursaram a disciplina de Álgebra Linear. Em seguida, serão realizadas a análise dos dados e as conclusões do estudo.

5. Referências

[1] DUVAL, R. A cognitive analysis of problems of comprehension in a learning of mathematics. Educational Studies in Mathematics, Springer, v. 61, p. 103-131, 2006.

[2] DUVAL, R. Ver e ensinar a matemática de outra forma: entrar no modo matemático de pensar: os registros de representações semióticas. São Paulo: PROEM, v. 1, 2011.

[3] COBB, P.; CONFREY,J.; DISESSA, A.; LEHRER,R.; SCHAUBLE, L. Design experiments in education research. Educational Researcher, v.32, n.1, p. 9-13, 2003.

[4] ROCHA, Eugênio C. Rosa. Fundamentos matemáticos aplicado a alguns métodos de criptografia. Florianópolis, SC: UFSC, 2008.

[5] HANNAH, J. ; STEWART, S. THOMAS, M. Teaching Linear Algebra: one lecturer's engagement with students. Mathematics: traditions and new practices. AAMT & MERGA, 2011.

[6] ISIK, A. et al. Linear Algebra from students' perspectives. Middle eastern & African Journal of Educational Research, 2014. p. 29 – 40.

[7] DRIJVERS, P. Digital Technology in Mathematics Education: why it works (or doesn't). In: SUNG JE CHO (ed.). Selected Regular Lectures from the 12th International Congress on Mathematical Education. Switzerland: Springer International Publishing, 2015. p. 135-151.

[8] BAKI, A. Integration of Technology into Mathematics Teaching: past, presente and future. In: SUNG JE CHO (ed.). Selected Regular Lectures from the 12th International Congress on Mathematical Education. Switzerland: Springer International Publishing, 2015. p. 17-26. BOLDRINI, J.L et al. Álgebra Linear. Harbra, 1986.

[9] BORBA, M.; PENTEADO, M.G. Informática e Educação Matemática. São Paulo: Autêntica, 2010.

Agradecimentos

Ao Centro Universitário da FEI pelo incentivo recebido para a elaboração desse trabalho.

[1] Aluno de IC do Centro Universitário FEI. Projeto com vigência de 03/17 a 03/18.