CONTEXTUALIZAÇÃO EM ÁLGEBRA LINEAR UM EXPERIMENTO DE ENSINO SOBRE CRIPTOGRAFIA NO MATLAB

Robson R. A. Júnior – robbsonjunior@hotmail.com
Centro Universitário FEI, Curso de Engenharia Mecânica
Avenida Humberto de Alencar Castelo Branco, 3972-B
09850-901 – São Bernardo do Campo – São Paulo

Monica Karrer – mkarrer@fei.edu.br
Centro Universitário FEI, Departamento de Matemática
Avenida Humberto de Alencar Castelo Branco, 3972-B
09850-901 – São Bernardo do Campo – São Paulo

Resumo: *Neste artigo tem-se o objetivo de apresentar a Álgebra Linear contextualizada por meio de um experimento de ensino sobre o conteúdo de Criptografia. Visando desenvolver principalmente as competências de compreensão de fenômenos reais por meio de modelos computacionais, de aprendizagem autônoma e de comunicação eficiente e, fundamentados no Modelo da Matemática em Contexto de Camarena e na teoria dos Registros de Representações Semióticas de Duval, foi elaborado e aplicado um experimento de ensino nos ambientes papel e lápis e Matlab, o qual procurou tratar do tema Criptografia relacionando-o com os conteúdos matemáticos de transformação linear, independência linear, matrizes, congruência módulo m e inversa modular de uma matriz. Os resultados evidenciaram que os sujeitos mostraram habilidade em relacionar a Álgebra Linear com uma abordagem real e contextualizada, demostrando autonomia na resolução das situações propostas tanto no ambiente Matlab como no papel e lápis, estabelecendo de forma eficiente a comunicação em diferentes registros semióticos.*

Palavras-chave: *Criptografia. Álgebra linear. Contextualização. Recurso computacional. Representações semióticas.*

1 INTRODUÇÃO

Com esse artigo, tem-se o objetivo de apresentar uma situação real da Álgebra Linear, referente ao conteúdo de Criptografia. A Álgebra Linear é uma disciplina presente nos currículos de Engenharia e, segundo Hannah et al. (2011) e Isik (2014), os estudantes a enxergam como um conjunto de regras sem qualquer aplicação prática. Apesar do caráter abstrato dessa disciplina, ela está presente em aplicações das mais diversas áreas e, no presente trabalho, selecionou-se uma delas, referente à Criptografia, que envolve, da Álgebra Linear, conceitos de transformação linear, independência linear e operações matriciais.

As novas diretrizes curriculares dos cursos de Engenharia indicam a necessidade de se trabalhar um currículo com base em competências. As disciplinas básicas de Matemática, se estruturadas de acordo com essas indicações, podem contribuir para o alcance de importantes competências, tais como a compreensão de fenômenos por meio de modelos matemáticos, a

comunicação nas mais diversas formas, a autonomia e a habilidade de trabalho em equipe, dentre outras.

Por exemplo, ao trabalhar a matemática em situações contextualizadas e com uso de software matemático algébrico, gráfico ou de simulação, favorece-se a compreensão de fenômenos. Ao utilizar diferentes representações semióticas, tais como a gráfica, a algébrica, a da língua natural e a matricial, pode-se contribuir para obter avanços na comunicação. Por fim, um ensino de matemática focado no uso de metodologias ativas, permite que o estudante desenvolva autonomia e consiga administrar diferentes pontos de vista, favorecendo o trabalho em equipe.

Em concordância com as indicações das diretrizes curriculares dos cursos de Engenharia, tem-se o modelo proposto por Camarena (2018), denominado Modelo da Matemática em Contexto, o qual representa um referencial elaborado especificamente para o ensino de Matemática na Engenharia. Para essa pesquisadora, é necessário preparar o estudante para que ele consiga utilizar sua bagagem de conhecimentos, habilidades, atitudes e valores quando do ingresso no mercado profissional. Nesse sentido, o engenheiro necessita de uma sólida formação em Matemática, mas em Matemática no contexto da Engenharia, ou seja, em uma formação preocupada em desenvolver competências profissionais de sua área.

Para favorecer o alcance da competência de comunicação nas mais diversas formas, utilizou-se a teoria dos registros de representações semióticas de Duval (2011). Para ele, o acesso a um objeto matemático requer, necessariamente, do uso de representações semióticas, tais como a algébrica, a gráfica, a da língua natural, a matricial, dentre outras, uma vez que a Matemática é abstrata. Segundo Duval (2011), uma transformação entre representações pode ser um tratamento ou uma conversão. Se a transformação ocorrer no interior de um mesmo registro semiótico, tem-se um tratamento. Caso contrário, tem-se uma conversão, a qual, na visão do autor, assume um papel crucial como atividade cognitiva, por requerer do estudante a habilidade de coordenar representações de diferentes registros semióticos, auxiliando-o na competência de se comunicar nas mais diferentes formas.

O experimento aqui apresentado foi desenvolvido em dois ambientes, no papel e lápis e no Matlab. Segundo Baki (2015) e Drijvers (2015), integrar ferramentas computacionais no ensino traz ganhos pedagógicos, uma vez que, ao sistematizar os cálculos, pode-se focar no conceito, elaborando conjecturas e identificando padrões.

Diante do exposto, com o presente trabalho, teve-se o objetivo de investigar que aspectos pedagógicos poderiam ser evidenciados diante de um experimento de ensino sobre uma importante aplicação da Álgebra Linear, elaborado de modo a integrar um recurso computacional e diferentes registros de representações semióticas.

A metodologia adotada para a elaboração e condução do experimento foi a de *Design Experiment* de Cobb et al. (2003), a qual representa um modelo para a construção de experimentos de ensino na área de Matemática, com vistas a propor inovações.

Das diversas formas de manifestação previstas nesta metodologia, optou-se pelo modelo em pequena escala, para que fosse possível avaliar, de forma minuciosa, as trajetórias dos estudantes e as necessidades de adaptações no *design* antes de aplicá-lo em salas regulares.

Participaram do estudo preliminar dois alunos do oitavo semestre de uma instituição confessional de ensino, que já dominavam o software Matlab e que já haviam estudado a disciplina de Álgebra Linear por um foco exclusivamente algébrico, sem inclusão de problemas contextualizados. O experimento foi desenvolvido no laboratório de informática, uma vez que o software Matlab já era um recurso presente na instituição.

2 DESCRIÇÃO DO EXPERIMENTO E DOS RESULTADOS

O experimento foi desenvolvido em quatro etapas. Antes da aplicação das atividades, foi realizada uma revisão dos conceitos de Álgebra Linear relativos à transformação linear, independência linear e operações matriciais. Ainda, foi apresentada uma breve contextualização histórica da criptografia, dos diversos métodos criptográficos, tais como a cifra por substituição mono e polialfabética, a cifra de Hill, a máquina enigma, a criptografia assimétrica e RSA, porém com um maior detalhamento ao método de Hill, dado que ele envolve vários conceitos de Álgebra Linear. Ainda, para a compreensão do método, foram apresentados os tópicos de congruência módulo m e de inversa modular de uma matriz, uma vez que os alunos não haviam tido contato com esses conteúdos.

2.1 Descrição da primeira etapa

A primeira etapa teve por objetivo apresentar uma atividade prática no ambiente papel e lápis, elaborada com base em Castro (2012), para que os alunos percebessem como Lester S. Hill se utilizou de conceitos de Álgebra Linear para construir o método de criptografia mais eficiente da época. Ainda, essa atividade representou a base matemática necessária para os alunos programarem no Matlab, o que foi posteriormente requerido na Atividade 3. Nesta fase, os alunos efetuaram conversões entre representações dos registros matricial e da língua natural. A atividade é apresentada no Quadro 1.

Quadro 1 – Primeira atividade

Considerando o operador linear $L: \mathbb{R}^2 \to \mathbb{R}^2$ dado por $L(X) = CX$, na qual C é a matriz chave e X é a matriz coluna dos representantes numéricos de cada par de letras, obtenha a cifra da palavra "CRIPTOANÁLISE" através do método da cifra de Hill.

Dados: Matriz chave $C = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$

Tabela 1 - Conversão Alfabética Numérica

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

Fonte: Acervo próprio

Para resolver essa situação, a dupla foi orientada a agrupar as letras da mensagem em pares e a obter seus respectivos representantes numéricos por meio da tabela de conversão dada.

(C R) (I P) (T O) (A N) (A L) (I S) (E E)
(3 18) (9 16) (20 15) (1 14) (1 12) (9 19) (5 5)

Em seguida, cada par de representantes numéricos foi colocado na forma de matriz coluna, obtendo:

$$M_1 = \begin{bmatrix} 3 \\ 18 \end{bmatrix} \quad M_2 = \begin{bmatrix} 9 \\ 16 \end{bmatrix} \quad M_3 = \begin{bmatrix} 20 \\ 15 \end{bmatrix} \quad M_4 = \begin{bmatrix} 1 \\ 14 \end{bmatrix} \quad M_5 = \begin{bmatrix} 1 \\ 12 \end{bmatrix} \quad M_6 = \begin{bmatrix} 9 \\ 19 \end{bmatrix} \quad M_7 = \begin{bmatrix} 5 \\ 5 \end{bmatrix}$$

Foram realizadas as multiplicações da matriz chave C por cada matriz coluna M_n obtida e em seguida aplicou-se o resíduo módulo 26.

$$C * M_n \ (mod\ 26) \ \forall\ 1 \leq n \leq 7$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} * \begin{bmatrix} 3 \\ 18 \end{bmatrix} = \begin{bmatrix} 39 \\ 54 \end{bmatrix} = \begin{bmatrix} 13 \\ 2 \end{bmatrix} (mod\ 26) \qquad \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} * \begin{bmatrix} 9 \\ 16 \end{bmatrix} = \begin{bmatrix} 41 \\ 48 \end{bmatrix} = \begin{bmatrix} 15 \\ 22 \end{bmatrix} (mod\ 26)$$

$$\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix} * \begin{bmatrix}20\\15\end{bmatrix} = \begin{bmatrix}50\\45\end{bmatrix} = \begin{bmatrix}24\\19\end{bmatrix} (mod\ 26) \qquad \begin{bmatrix}1 & 2\\0 & 3\end{bmatrix} * \begin{bmatrix}1\\14\end{bmatrix} = \begin{bmatrix}29\\42\end{bmatrix} = \begin{bmatrix}3\\16\end{bmatrix} (mod\ 26)$$

$$\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix} * \begin{bmatrix}1\\12\end{bmatrix} = \begin{bmatrix}25\\36\end{bmatrix} = \begin{bmatrix}25\\10\end{bmatrix} (mod\ 26) \qquad \begin{bmatrix}1 & 2\\0 & 3\end{bmatrix} * \begin{bmatrix}9\\19\end{bmatrix} = \begin{bmatrix}47\\57\end{bmatrix} = \begin{bmatrix}21\\5\end{bmatrix} (mod\ 26)$$

$$\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix} * \begin{bmatrix}5\\5\end{bmatrix} = \begin{bmatrix}15\\15\end{bmatrix} = \begin{bmatrix}15\\15\end{bmatrix} (mod\ 26)$$

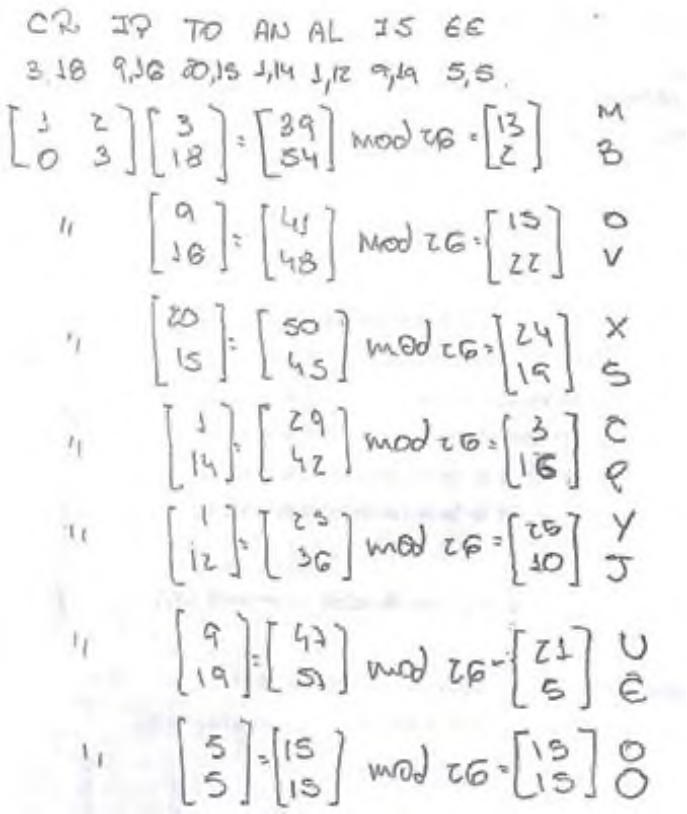
Por fim, as matrizes obtidas foram transpostas e colocadas em sequência. Utilizou-se a tabela de conversão alfabética numérica para obter a mensagem cifrada:

[13 2]	[15 22]	[24 19]	[3 16]	[25 10]	[21 5]	[15 15]
(M B)	(O V)	(X S)	(C P)	(Y J)	(U E)	(O O)

O resultado encontrado foi: **MBOVXSCPYJUEOO**

Nesta etapa os alunos não apresentaram dificuldades e mostraram habilidade em efetuar as conversões entre representações do registro numérico e da língua natural. Parte da produção da dupla é apresentada na Figura 1.

Figura 1. Resolução dos alunos - Primeira Atividade



Fonte: Acervo próprio

Os participantes questionaram se seria possível agrupar as letras em trios ao invés de pares. O professor pesquisador respondeu que sim, alertando que, para isso, a matriz chave utilizada deveria ser 3x3 ao invés de 2x2, o que tornaria o procedimento consideravelmente mais trabalhoso.

2.2 Descrição da segunda etapa

Nesta segunda etapa, o objetivo consistiu em apresentar um código para a Cifra de Hill no Matlab, a fim de mostrar ao aluno a possiblidade do uso de um recurso computacional para vencer a complexidade do processo de descriptografia e para reduzir o trabalho manual inerente ao tratamento criptográfico de mensagens maiores.

Desta forma, foi criado, exclusivamente para este experimento de ensino, um código no Matlab capaz de criptografar e descriptografar mensagens com qualquer quantidade de letras por meio do método da cifra de Hill. O programa também verifica se a matriz criptográfica inserida é compatível com a cifra de Hill, ou seja, se é invertível mod 26.

Os alunos utilizaram primeiramente o programa para verificar a criptografia construída na etapa anterior, conforme apresentado na Figura 2.

Figura 2 – Resolução da Atividade 2 – Primeira Criptografia

```
Command Window
>> Criptografar
Digite a frase entre aspas simples,sem espaços e sem acentos: 'criptoanalise'
Insira a matriz codificadora 2x2 invertível (mod 26): [1 2;0 3]
Cifra: mbovxscpyjueoo

fx >>
```

Fonte: Acervo próprio

Em seguida, executaram o programa para descriptografar a cifra obtida, conforme apresentado na Figura 3.

Figura 3 – Resolução da Atividade 2 – Primeira Descriptografia

```
>> Descriptografar
Digite o texto cifrado entre aspas simples,sem espaços e sem acentos: 'mbovxscpyjueoo'
Insira a matriz codificadora 2x2 invertível (mod 26): [1 2;0 3]
Mensagem: criptoanalisee

fx >>
```

Fonte: Acervo próprio

Os participantes foram solicitados a utilizar o programa para uma mensagem qualquer com maior quantidade de letras. Inicialmente, por terem usado uma matriz chave incompatível (não invertível modulo 26), o programa apresentou a mensagem da Figura 4.

Figura 4 - Resolução da Atividade 2 – Mensagem de erro

```
>> Criptografar
Digite a frase entre aspas simples,sem espaços e sem acentos: 'microondasfoiaprimeiracoisaqueeupensei'
Insira a matriz codificadora 2x2 invertível (mod 26): [3 7;5 2]

determinante =

   -29

Para ser invertível mod 26, o valor do determinante da matriz precisa ser co-primo de 26.
Portanto, os valores de determinante aceitáveis são: 1; 3; 5; 7; 9; 11; 15; 17; 19; 21; 23 e 25
```

Fonte: Acervo próprio

De acordo com as instruções do próprio programa, a dupla partiu para a escolha de uma matriz chave compatível e executou o processo novamente, obtendo o resultado presente na Figura 5.

Figura 5 – Resolução da Atividade 2 – Segunda Criptografia

```
>> Criptografar
Digite a frase entre aspas simples,sem espaços e sem acentos: 'microondasfoiaprimeiracoisaqueeupensei'
Insira a matriz codificadora 2x2 invertível (mod 26): [1 2;0 3]
Cifra: eambssvlmejskczbimwatcgsueiyeoukzozewa
```

Fonte: Acervo próprio

Em seguida, a dupla executou o programa para descriptografar a cifra obtida encontrando a mensagem original, conforme apresentado na Figura 6.

Figura 6 – Resolução da Atividade 2 – Segunda Descriptografia

```
>> Descriptografar
Digite o texto cifrado entre aspas simples,sem espaços e sem acentos: 'eambssvlmejskczbimwatcgsueiyeoukzozewa'
Insira a matriz codificadora 2x2 invertível (mod 26): [1 2;0 3]
Mensagem: microondasfoiaprimeiracoisaqueeupensei
```

Fonte: Acervo próprio

Com isso, os participantes puderam constatar a importância de se utilizar um recurso computacional para facilitar a realização dos cálculos envolvidos na atividade de criptografia e a necessidade de levar em consideração as condições matemáticas para esse fim.

2.3 Descrição da terceira etapa

Considerando que os alunos desenvolveram uma atividade no ambiente papel e lápis com o detalhamento do método de Hill e que tiveram contato como usuários com um programa no Matlab que sistematizava as atividades de criptografar e descriptografar, na terceira etapa teve-se o objetivo de solicitar ao aluno a construção de um programa no Matlab partindo de conceitos de Álgebra Linear, de forma a criptografar e descriptografar qualquer mensagem.

Isso foi possível pelo fato de os alunos já possuírem os conceitos matemáticos necessários e o domínio do Matlab, software amplamente utilizando nos cursos de engenharia da instituição.

2.4 Descrição da quarta etapa

Essa etapa consistiu em apresentar um problema enigma para que o aluno utilizasse os conceitos e recursos apresentados, a fim de solucionar uma situação envolvendo criptografia. O enigma é apresentado no Quadro 2.

Quadro 2 – Apresentação do Problema Enigma

A polícia está investigando um grupo de assaltantes e vem interceptando as mensagens enviadas pelos integrantes do grupo. Sabe-se que as mensagens interceptadas estão criptografadas através do modelo da cifra de Hill, porém, a chave criptográfica utilizada é alterada em cada mensagem dificultando o processo de criptoanálise. Através de um informante, a polícia descobriu que a última mensagem obtida poderia conter informações importantes sobre o próximo assalto que o grupo estaria planejando, portanto, contratou um especialista em criptografia para ajudar a quebrar o código e tentar interceptar os assaltantes. O informante revelou, também, que cada integrante do grupo possuía um codinome e que os integrantes costumavam iniciar a mensagem com esse codinome para sua identificação. Devido à origem da mensagem em questão, a polícia constatou que ela havia sido enviada pelo integrante conhecido como "alfa". Dada a mensagem interceptada e a tabela de conversão alfabética numérica, obtenha a mensagem original.

KJICECWIXIUPVBKJEAONYPIO

Tabela 2 - Tabela de Conversão Alfabética Numérica

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

Fonte: Acervo próprio

Os alunos poderiam resolver o enigma por dois caminhos. No primeiro, eles partiriam da palavra conhecida e da respectiva cifra.

Palavra conhecida		Respectiva cifra	
(AL)	(FA)	(KJ)	(IC)
(1 12)	(6 1)	(11 10)	(9 3)

de modo que os vetores comuns e seus respectivos vetores cifrados são

$$p_1 = \begin{bmatrix} 1 \\ 12 \end{bmatrix} \quad c_1 = \begin{bmatrix} 11 \\ 10 \end{bmatrix} \qquad p_2 = \begin{bmatrix} 6 \\ 1 \end{bmatrix} \quad c_2 = \begin{bmatrix} 9 \\ 3 \end{bmatrix}$$

A partir deles seriam construídas as seguintes matrizes

$$C = \begin{bmatrix} {c_1}^t \\ {c_2}^t \end{bmatrix} = \begin{bmatrix} 11 & 10 \\ 9 & 3 \end{bmatrix} \text{ e } P = \begin{bmatrix} {p_1}^t \\ {p_2}^t \end{bmatrix} = \begin{bmatrix} 1 & 12 \\ 6 & 1 \end{bmatrix}$$

Em seguida, aplicando operações sobre linhas em $\begin{bmatrix} 11 & 10 \\ 9 & 3 \end{bmatrix}\begin{bmatrix} 1 & 12 \\ 6 & 1 \end{bmatrix}$, a matriz C seria reduzida à identidade, obtendo $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 25 & 9 \end{bmatrix}$. Como a matriz C foi reduzida à identidade, ao transpor a matriz P obtemos a inversa da matriz codificadora, dada por $\begin{bmatrix} 1 & 25 \\ 0 & 9 \end{bmatrix}$.

Ao multiplicar esta matriz por cada par de representantes numéricos da mensagem cifrada, seriam obtidos os representantes numéricos da mensagem original:

$$\begin{bmatrix} 1 & 25 \\ 0 & 9 \end{bmatrix} * \begin{bmatrix} 11 \\ 10 \end{bmatrix} = \begin{bmatrix} 1 \\ 12 \end{bmatrix} mod\ 26 \begin{bmatrix} A \\ L \end{bmatrix} \qquad \begin{bmatrix} 1 & 25 \\ 0 & 9 \end{bmatrix} * \begin{bmatrix} 9 \\ 3 \end{bmatrix} = \begin{bmatrix} 6 \\ 1 \end{bmatrix} mod\ 26 \begin{bmatrix} F \\ A \end{bmatrix}$$

$$\begin{bmatrix} 1 & 25 \\ 0 & 9 \end{bmatrix} * \begin{bmatrix} 5 \\ 3 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix} mod\ 26 \begin{bmatrix} B \\ A \end{bmatrix} \qquad \begin{bmatrix} 1 & 25 \\ 0 & 9 \end{bmatrix} * \begin{bmatrix} 23 \\ 9 \end{bmatrix} = \begin{bmatrix} 14 \\ 3 \end{bmatrix} mod\ 26 \begin{bmatrix} N \\ C \end{bmatrix}$$

$$\begin{bmatrix} 1 & 25 \\ 0 & 9 \end{bmatrix} * \begin{bmatrix} 24 \\ 9 \end{bmatrix} = \begin{bmatrix} 15 \\ 3 \end{bmatrix} mod\ 26 \begin{bmatrix} O \\ C \end{bmatrix} \qquad \begin{bmatrix} 1 & 25 \\ 0 & 9 \end{bmatrix} * \begin{bmatrix} 21 \\ 16 \end{bmatrix} = \begin{bmatrix} 5 \\ 14 \end{bmatrix} mod\ 26 \begin{bmatrix} E \\ N \end{bmatrix}$$

$$\begin{bmatrix}1 & 25\\0 & 9\end{bmatrix} * \begin{bmatrix}22\\2\end{bmatrix} = \begin{bmatrix}20\\18\end{bmatrix} mod\ 26 \begin{bmatrix}T\\R\end{bmatrix} \qquad \begin{bmatrix}1 & 25\\0 & 9\end{bmatrix} * \begin{bmatrix}11\\10\end{bmatrix} = \begin{bmatrix}1\\12\end{bmatrix} mod\ 26 \begin{bmatrix}A\\L\end{bmatrix}$$

$$\begin{bmatrix}1 & 25\\0 & 9\end{bmatrix} * \begin{bmatrix}5\\1\end{bmatrix} = \begin{bmatrix}4\\9\end{bmatrix} mod\ 26 \begin{bmatrix}D\\I\end{bmatrix} \qquad \begin{bmatrix}1 & 25\\0 & 9\end{bmatrix} * \begin{bmatrix}15\\14\end{bmatrix} = \begin{bmatrix}1\\22\end{bmatrix} mod\ 26 \begin{bmatrix}A\\V\end{bmatrix}$$

$$\begin{bmatrix}1 & 25\\0 & 9\end{bmatrix} * \begin{bmatrix}25\\16\end{bmatrix} = \begin{bmatrix}9\\14\end{bmatrix} mod\ 26 \begin{bmatrix}I\\N\end{bmatrix} \qquad \begin{bmatrix}1 & 25\\0 & 9\end{bmatrix} * \begin{bmatrix}9\\15\end{bmatrix} = \begin{bmatrix}20\\5\end{bmatrix} mod\ 26 \begin{bmatrix}T\\E\end{bmatrix}$$

Desta forma, o enigma seria solucionado, obtendo:

ALFABANCOCENTRALDIAVINTE
ALFA BANCO CENTRAL DIA VINTE

Um segundo modo de resolver o problema seria por meio da determinação da matriz codificadora utilizada para realizar a criptografia, ou seja, a inversa mod 26 da matriz $\begin{bmatrix}1 & 25\\0 & 9\end{bmatrix}$ Isso poderia ser feito com o auxílio do Matlab. Primeiramente, atribui-se a matriz a uma variável no matlab, dada por $chave = [1\ 25; 0\ 9]$. Calcula-se o determinante da matriz obtendo $\det(chave) = 9$. Por meio dos dados presentes na Tabela 1, obtém-se o seu recíproco inverso módulo 26.

Tabela 1 - Recíprocos mod 26

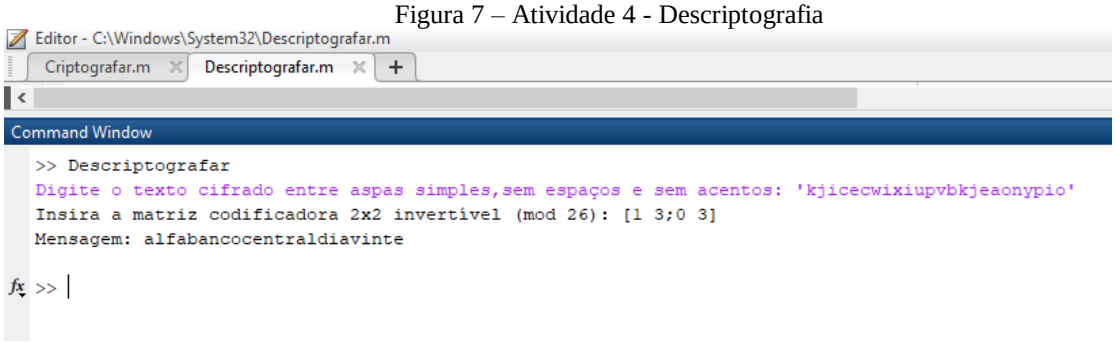
a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Fonte: Acervo próprio

$$9^{-1} = 3\ mod\ 26$$

Atribui-se o valor encontrado em uma variável no Matlab, dado por $inverso = 3$ e calcula-se a matriz adjunta, dada por $adj = (inv(chave') * \det(chave))' = \begin{bmatrix}9 & -25\\0 & 1\end{bmatrix}$. Efetua-se o produto e atribui-se o valor encontrado na variável chave, obtendo $chave = inverso * adj = \begin{bmatrix}27 & -75\\0 & 3\end{bmatrix}$. Aplica-se o módulo 26, por meio de $chave = mod(chave, 26) = \begin{bmatrix}1 & 3\\0 & 3\end{bmatrix}$ e descobre-se que a matriz utilizada para criptografar a mensagem foi $\begin{bmatrix}1 & 3\\0 & 3\end{bmatrix}$. A partir daí, pode-se executar o programa do Matlab para descriptografar a mensagem obtendo o resultado presente na Figura 7.

Figura 7 – Atividade 4 - Descriptografia



Fonte: Acervo próprio

Nessa atividade os alunos pensaram apenas na primeira forma de execução e apresentaram dificuldades na obtenção da matriz inversa mod 26 através das operações sobre linhas. O pesquisador teve que intervir discutindo com a dupla sobre esse fato e, com essa intervenção, os estudantes conseguiram efetuar a atividade desafio.

A segunda forma de resolução foi apresentada e discutida com os alunos ao final da atividade e eles reconheceram que essa outra possibilidade seria menos trabalhosa. Para a realização desta atividade, os alunos efetuaram conversões entre representações dos registros semióticos algébrico, numérico, matricial e especializado da área computacional.

3 CONSIDERAÇÕES FINAIS

Com esse trabalho, pôde-se destacar diferentes aspectos pedagógicos referentes à aplicação do experimento de ensino. Primeiramente, os alunos puderam ter contato com a Álgebra Linear, que normalmente é considerada puramente abstrata, em uma situação contextualizada sobre Criptografia, tema muito presente nos dias atuais. Tal fato favoreceu o desenvolvimento da competência de compreensão de fenômenos reais por meio de modelos matemáticos. Ao terem um contato inicial com uma situação de criptografia no ambiente papel e lápis, puderam construir os conhecimentos matemáticos necessários para a compreensão do método de Hill e, ao programarem no Matlab, puderam estabelecer um ambiente favorável para trabalhar com situações mais complexas. Tratar as atividades nesses dois ambientes permitiu explorar representações de diferentes registros semióticos, bem como seus tratamentos e conversões, favorecendo o desenvolvimento da competência de comunicação em diferentes formatos. Por fim, ao lidar com o problema enigma, os alunos tiveram que desenvolver estratégias de resolução, favorecendo o desenvolvimento da competência de autonomia. Diante disso, entende-se que o presente trabalho pode representar um cenário de ensino compatível com as indicações das novas diretrizes curriculares dos cursos de Engenharia.

Agradecimentos

Agradecemos o apoio recebido pelo Centro Universitário FEI para a realização desta pesquisa.

REFERÊNCIAS

BAKI, Adnan. Integration of Technology into Mathematics Teaching: past, present 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.

CAMARENA, Patricia Gallardo. Formación por competencias en las ciencias básicas de la ingeniería. **Revista Brasileira de Ensino em Ciência e Tecnologia**, Ponta Grossa, v. 11, n. 2, p. 84-110, 2018.

CASTRO, Elisangela Regina Diocesano de**. Álgebra Linear e Teoria dos Números na Criptografia**. Campo Mourão, PR: UTFPR, 2012.

COBB, Paul; CONFREY, Jere; DISESSA, Andrea; LEHRER, Richard; SCHAUBLE, Leona. Design experiments in education research. **Educational Researcher**, Flórida: SAGE Journals, n.1, p. 9-13, 2003.

DRIJVERS, Paul. 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.

DUVAL, Raymond. **Ver e ensinar a Matemática de outra forma** - entrar no modo matemático de pensar: os registros de representações semióticas. São Paulo: PROEM, 2011.

HANNAH, John. ; STEWART, Sepideh. THOMAS, Michael. **Teaching Linear Algebra: one lecturer's engagement with students**. Mathematics: traditions and new practices. AAMT & MERGA, 2011.

ISIK, Ahmet. et al. Linear Algebra from students' perspectives. **Middle eastern & African Journal of Educational Research**, 2014. p. 29 - 40.

CONTEXTUALIZATION IN LINEAR ALGEBRA
A TEACHING EXPERIMENT ABOUT CRYPTOGRAPHY IN MATLAB

Abstract: *This article aims to present a Linear Algebra contextualized problem through a teaching experiment on the content of cryptography. Aiming to develop mainly the competencies of understanding real phenomena through computational models, autonomous learning and efficient communication, based on the context mathematical model of Camarena and on the Duval's theory about semiotic representations registers, a teaching experiment was elaborated in the paper and pencil and Matlab environments, which sought to deal with the theme cryptography relating it to the mathematical contents of linear transformation, linear independence, matrices, module m congruence and inverse modular matrix. The results showed that the students presented ability to relate the Linear Algebra with a real and contextualized approach, demonstrating autonomy in resolution of the situations proposed both in the Matlab and in the paper and pencil environments, establishing communication in different semiotic registers.*

Key-words: *Cryptography. Linear Algebra. Contextualization. Computational resources. Semiotic representations.*