UNIVERSIDADE FEDERAL DO CEARÁ

INSTITUTO UNIVERSIDADE VIRTUAL

PROGRAMA UNIVERSIDADE ABERTA DO BRASIL

CURSO DE LICENCIATURA EM MATEMÁTICA

FRANCISCA NEILIANE SANTOS OLIVEIRA

ENSINO DE MATRIZES APLICADO A CRIPTOGRAFIA COM USO DE FERRAMENTAS DIGITAIS

MARANGUAPE

2015

FRANCISCA NEILIANE SANTOS OLIVEIRA

ENSINO DE MATRIZES APLICADO A CRIPTOGRAFIA COM USO DE FERRAMENTAS DIGITAIS

Monografia apresentada ao Curso de Licenciatura em Matemática Semipresencial do Instituto Universidade Virtual da Universidade Federal do Ceará, como requisito parcial para a obtenção do Título de Licenciada em Matemática.

Orientador: Prof. Me. Diego de Sousa Rodrigues.

MARANGUAPE

2015

FRANCISCA NEILIANE SANTOS OLIVEIRA

ENSINO DE MATRIZES APLICADO A CRIPTOGRAFIA COM USO DE FERRAMENTAS DIGITAIS

Monografia apresentada ao Curso de Licenciatura em Matemática Semipresencial do Instituto Universidade Virtual da Universidade Federal do Ceará, como requisito parcial para a obtenção do Título de Licenciado em Matemática.

Orientador: Prof. Me. Diego de Sousa Rodrigues.

Aprovado em 11/12/2015

BANCA EXAMINADORA

_____

Prof. Me. Diego de Sousa Rodrigues (Orientador)
Universidade Federal do Ceará (UFC)

_____

Prof. Hudson de Sousa Felix
Universidade Federal do Ceará (UFC)

_____

Prof. Helton Udenes Nascimento Pontes
Universidade Federal do Ceará (UFC)

A minha família, meu alicerce, e a todos os meus professores, que no decorrer de minha trajetória estudantil foram minha inspiração.

AGRADECIMENTOS

A Deus, autor da vida, que me concedeu saúde e inspiração para o desenvolvimento deste trabalho.

A minha mãe, por ser presença e estímulo no decorrer de minha trajetória estudantil, não permitindo que nada atrapalhasse o meu tempo de estudo. A meu pai, meu grande exemplo de força e perseverança. Aos meus irmãos, pelo incentivo e disposição a sempre me ajudarem. Minha família, meu muito obrigada pelo apoio financeiro, necessário nesta trajetória e pelo amor incondicional que vocês tem a mim.

A minha grande amiga Joana, que sempre me apoiou nesta trajetória, sendo meu porto seguro nesta vida acadêmica, e a todos os meus colegas de curso que foram fundamentais nesta caminhada.

Aos amigos Braga e Marcelo e a meu irmão Jucelino que mesmo no cansaço, estiveram sempre dispostos, a guiarem o transporte até a faculdade.

Também agradeço a todos os professores do meu ensino fundamental e médio. Sendo de fundamental importância a dedicação e incentivo de todos. Ao professor Assis Bento, modelo de profissional e que sempre esteve à disposição tanto no ensino médio como na disciplina de estágio. A professora Taylana Queiroz, grande exemplo de liderança, incansável na luta pelo sucesso de seus alunos.

Agradeço ao professor Diego pela orientação, disponibilidade e paciência, em esclarecer minhas dúvidas.

Aos professores que ao longo destes quatro anos se dedicaram na orientação das disciplinas, em especial ao professor Renivaldo por seu empenho e exigência. Foram fundamentais para minha trajetória.

RESUMO

Despertar o interesse dos alunos, dando sentido ao estudo de matrizes, com a relação teoria e prática e a valorização da lógica de resolução de questões é o principal objetivo deste trabalho. O uso dos conceitos de criptografia, que aborda sua importância desde os primórdios, mostra que a matemática é crucial para vários segmentos da sociedade. Mais especificamente, o uso de matrizes aplicado à criptografia é uma estratégia que facilita a abordagem do conteúdo, tornando o estudo mais significativo. Uma fácil abordagem também requer praticidade e valorização do raciocínio lógico do estudante. O estudo de matrizes exige uma prática de cálculos, que por muitas vezes torna o conteúdo exaustivo, o que causa desgaste mental e não traz sentido ao que se pratica. Nessa busca da valorização da lógica de resolução, é proposto o uso do software winmat, que possibilita efetuar os cálculos operacionais deste conteúdo, facilitando a abordagem de matrizes aplicada a criptografia.

Palavras – chave: matrizes, relação teoria e prática, criptografia, software winmat, lógica de resolução.

ABSTRACT

The aim of this work is to arouse the interest of students, giving meaning to the study of matrices, using the theory and practice, as well as appreciation of solving problems logic. The use of cryptography concepts that addresses its importance since the beginning, shows that mathematic is crucial for various segments of society. More specifically, the use of matrix applied to the encryption is a strategy that facilitates content of approach, making the most significant study. An easy approach also requires practicality and appreciation of the logical reasoning of the student. The study requires a matrices practice of calculations, which often makes the comprehensive contents, causing mental stress and does not bring meaning to the practice. In this search the appreciation of the resolution logic, we propose the use of winmat software that enables calculations make operating this content, facilitating matrix approach applied cryptography.

Keywords: matrices, relationship between theory and practice, cryptography, winmat software, Resolution logic

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Em nosso cotidiano, seja no convívio escolar ou até mesmo familiar, já se ouviu alguém demostrando rejeição à matemática, seja por uma experiência negativa que já teve com a disciplina, ou simplesmente por já ter uma ideia pré-concebida de que a matéria é complicada. A aversão à matemática tem gerado dificuldades no processo de ensino-aprendizagem realizado na escola, tornando cada vez mais difícil o trabalho docente. O discurso que define a matemática como difícil, tornou-se algo natural, visto que é o resultado de ressignificações atribuídas ao histórico da disciplina, adicionada a visão prática do seu saber. Essas expressões estão presentes em todos os lugares a que professores e alunos estão inseridos, o que interfere diretamente no processo de ensino e aprendizagem.

Essas dificuldades de aprendizagem que a maioria dos alunos apresenta principalmente na disciplina de matemática tem sido objeto de pesquisa de vários estudiosos. Eles apontam que uma das principais causas para esse déficit de aprendizagem é o ensino tradicionalista que não torna significativo o que se aprende. A maioria dos professores usam as definições e exercícios dos livros didáticos como principal metodologia de ensino, onde na maioria das vezes não é considerado a natureza dos conteúdos. Para alguns autores como Sanches (2002) e D' Ambrósio (1999) é preciso saber manipular a natureza dos conteúdos para obter uma aprendizagem mais significativa de matemática. Sanches (2002, p.1) afirma que:

> *"A aprendizagem deve capacitar o indivíduo a se relacionar de maneira consciente com o meio social e instrumental, permitindo o seu desenvolvimento intelectual, tornando-o capaz de fazer escolhas. Para tanto, é necessário se considerar: a natureza do conhecimento e do processo de ensino-aprendizagem; o conhecimento significativo de conceitos e princípios; os procedimentos e estratégias necessárias para a solução de problemas; a representação do conhecimento; a experiência passada; o desenvolvimento de competências e habilidades; a influência do ambiente, das atitudes, da tecnologia; a relação da Matemática com outras áreas do conhecimento humano e a construção histórica do conhecimento, dentre outras."*

No que se refere ao processo de ensino-aprendizagem de matrizes pode-se deduzir que a metodologia usada neste processo resume-se a utilização de regras que na maioria dos casos não possui nenhuma relação com a realidade dos alunos, ou seja, o ensino de matrizes não é relacionado a nenhuma aplicabilidade do mesmo. Para Sanches (2002, p.6) o ensino de matrizes se dá em "total descompasso com os avanços tecnológicos e com os estudos já realizados pela Psicologia Educacional". No estudo de matrizes é desprezado o fato de que essa área da álgebra está presente na vida cotidiana dos alunos, por exemplo, em jogos.

Enfim, é um assunto que tem relevância na vida dos alunos desde o ensino fundamental, porém só é exigido no ensino médio. Neste é abordado de forma inquestionável e sem considerar que as matrizes podem ser usadas no estudo de outros conceitos.

As matrizes estão presentes em diversas áreas da ciência como economia, engenharia, e também podem ser aplicadas em criptografia. O presente trabalho apresenta uma alternativa metodológica do ensino de matrizes que considera os aspectos históricos, as aplicações do conteúdo, e as tecnologias que são favoráveis ao ensino. No que concerne aos aspectos históricos e a aplicabilidade do assunto, é proposta a utilização da criptografia. A necessidade de enviar e receber mensagens secretas são usadas desde a época do antigo Egito, passando pelas guerras até os tempos atuais, onde são mais utilizadas em transações eletrônicas. Existem várias técnicas para codificar e decodificar mensagens. Dentre estas a técnica que utiliza a álgebra linear será usada no estudo de matrizes, como forma de estimular o interesse do aluno em aprender.

Considerando também que a álgebra matricial exige cálculos que em determinada parte do conteúdo tornam-se cansativos para os alunos. E ainda visando que essa exaustão pode ser uma das causas para o desinteresse dos estudantes, é proposto também a utilização do software winmat. Este programa permite a manipulação de matrizes, e possibilita aos professores e estudantes valorizarem a lógica do conteúdos sem se deterem apenas a prática de cálculos.

A busca pela aprendizagem significativa de matrizes torna-se o principal objetivo deste trabalho. As definições e sugestões apresentadas enfatizam que o aprendizado passa por um processo de descobertas, que não pode ser algo pronto e que é simplesmente repassado para os alunos. No proceder do desenvolvimento ficará explicito que o conhecimento só se tornará aprendizagem quando construído.

2 DEFINIÇÃO DE MATRIZES

Por definição, dados dois números m e n naturais e não nulos, chama-se matriz m por n (indica-se m x n) toda tabela M composta por números reais distribuídos em m linhas e n colunas. Geralmente os elementos de uma matriz são dispostos entre parênteses ou entre colchetes como exemplo a seguinte matriz:

$$A = \begin{bmatrix} 1 & 3 & 0 \\ -5 & 5 & 8 \end{bmatrix}_{2\,x\,3}$$ Matriz A de ordem dois por três.

No modelo de uma matriz qualquer, cada elemento é apontado por a_{ij}, sendo os índices i e j indicadores da posição do elemento na matriz. O índice i indica a linha e o índice j indica a coluna. Sendo que as linhas são numeradas de cima para baixo $(1 \leq i \leq m)$ e as colunas da esquerda para a direita $(1 \leq j \leq n)$. Portanto uma matriz m x n é representada por:

$$M = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{bmatrix}_{m\,x\,n}$$

2.1 Tipo de matrizes

Por apresentarem características específicas, há matrizes que recebem denominações especiais:

a) Matriz linha tem ordem 1 x n, ou seja, possui uma única linha.

$D = [3 \quad 4 \quad 5]_{1\,x\,3}$ Matriz linha de ordem um por três;

b) Matriz coluna, tem ordem m x 1, ou seja, possui uma única coluna.

$$E = \begin{bmatrix} 5 \\ 8 \\ 10 \end{bmatrix}_{3\,x\,1}$$ Matriz coluna de ordem três por um;

c) Matriz nula tem todos os elementos iguais à zero

$F = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ Matriz nula de ordem três por quatro;

d) Matriz quadrada é a matriz que possui o número de linhas iguais ao número de colunas. Nesse caso diz-se que a matriz é quadrada de ordem n.

$C = \begin{bmatrix} 5 & 10 \\ -11 & 3 \end{bmatrix}_{2\,x\,2}$ Matriz quadrada de ordem 2.

Dada uma matriz $D = [a_{ij}]$ quadrada de ordem n.

$$D = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{bmatrix}$$

Diz-se que a diagonal principal é o conjunto dos elementos que têm dois índices iguais, ou seja, $\{a_{ij} | i = j\} = \{a_{11}, a_{22}, a_{33}, a_{44}, \dots, a_{nn}\}$. E chama-se de diagonal secundária o conjunto dos elementos que possuem a soma dos índices igual a n+1, ou seja, $\{a_{ij} | i + j = n + 1\} = \{a_{1n}, a_{2,n-1}, a_{3,n-2}, a_{4,n-3}, \dots, a_{n1}\}$.

Exemplo

$G = \begin{bmatrix} 1 & 5 & 3 & 7 \\ -3 & 4 & -1 & -5 \\ -2 & -6 & 0 & -4 \\ 6 & 8 & 9 & 2 \end{bmatrix}$ é uma matriz quadrada de ordem 4.

Sua diagonal principal é {1, 4, 0, 2} e sua diagonal secundária é {7, -1, -6, 6};

e) Matriz identidade (I_n)

A matriz identidade é uma matriz quadrada onde cada elemento da diagonal principal tem valor 1 e os demais elementos tem valor zero.

Obs.: Na notação I_n, n representa a ordem da matriz identidade.

$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ Matriz identidade de terceira ordem.

2.2 Matriz Transposta

Dada uma matriz H de ordem m x n, diz-se que a matriz transposta de H, que é indicada por H^t, é a matriz de ordem n x m, sendo as suas linhas ordenadamente iguais às colunas da matriz H. Como exemplo:

a) $Se\ H = \begin{bmatrix} 1 & 3 \\ 6 & 8 \end{bmatrix}$, então $H^t = \begin{bmatrix} 1 & 6 \\ 3 & 8 \end{bmatrix}$;

b) Se $J = \begin{bmatrix} 2 & 3 & 8 \\ -6 & 5 & 4 \end{bmatrix}$, então $J^t = \begin{bmatrix} 2 & -6 \\ 3 & 5 \\ 8 & 4 \end{bmatrix}$.

2.3 Igualdade de Matrizes

Duas matrizes $A = [a_{ij}]_{m\,x\,n}$ e $B = [b_{ij}]_{m\,x\,n}$, de mesma ordem serão iguais (A=B) se, e somente se, os seus elementos de mesma posição forem iguais. Portanto, para duas matrizes serem iguais devem ser do mesmo tipo e apresentar todos os elementos com índices iguais.

Exemplo

$$A = \begin{bmatrix} 0{,}5 & 4 & 1 \\ -3 & 8 & 0 \end{bmatrix}_{2\,x\,3} \text{ e } B = \begin{bmatrix} \frac{1}{2} & 4 & 6^0 \\ -\frac{6}{2} & 2^3 & 0 \end{bmatrix}_{2\,x\,3}$$

Nota-se que as matrizes A e B são da mesma ordem , 2 x 3, e todos os elementos de mesma posição são iguais. Portanto, A=B.

2.4 Operações com matrizes

2.4.1 Adição de matrizes

A soma de duas matrizes $A = [a_{ij}]_{m\,x\,n}$ e $B = [b_{ij}]_{m\,x\,n}$ é a matriz $C = [c_{ij}]_{m\,x\,n}$, que é obtida com a adição dos elementos de mesma posição das matrizes A e B. Ou seja, $c_{ij} = a_{ij} + b_{ij}$.

Exemplo

Dadas as matrizes:

$$A = \begin{bmatrix} 2 & 3 \\ 1 & -5 \end{bmatrix} \text{ e } B = \begin{bmatrix} 6 & 8 \\ 9 & 4 \end{bmatrix}, \text{ a soma será}$$

$$A + B = \begin{bmatrix} 2+6 & 3+8 \\ 1+9 & -5+4 \end{bmatrix} \Rightarrow C = \begin{bmatrix} 8 & 11 \\ 10 & -1 \end{bmatrix}.$$

Considerando matrizes de mesma ordem, são válidas as seguintes propriedades:

a) é comutativa: A + B = B + A;

b) é associativa: A + (B + C) = (A + B) + C;

c) todo elemento tem simétrico: A + (-A) = 0;

d) tem elemento neutro: A + 0 = A.

2.4.2 Subtração de matrizes

A diferença de duas matrizes $A = [a_{ij}]_{m\,x\,n}$ e $B = [b_{ij}]_{m\,x\,n}$ é a matriz $C = [c_{ij}]_{m\,x\,n}$ obtida pela adição da matriz A com a oposta da matriz B. Destaca-se que a matriz oposta de B (que é a matriz B') é tal que B + B'=0. Ou seja, A – B = A + (- B).

Exemplo

Dadas as matrizes, $A = \begin{bmatrix} 7 & 6 & 2 \\ 1 & 5 & 4 \end{bmatrix}$ e $B = \begin{bmatrix} 5 & 2 & -2 \\ 3 & 4 & 1 \end{bmatrix}$, a diferença será:

$$A - B = \begin{bmatrix} 7 & 6 & 2 \\ 1 & 5 & 4 \end{bmatrix} + \begin{bmatrix} -5 & -2 & 2 \\ -3 & -4 & -1 \end{bmatrix} \Rightarrow C = \begin{bmatrix} 2 & 4 & 4 \\ -2 & 1 & 3 \end{bmatrix}$$

2.4.3 Produto de um número real por uma matriz

O produto de um número real k por uma matriz $A = [a_{ij}]_{m\,x\,n}$ é obtido pela multiplicação de cada elemento da matriz A por esse número real k.

Exemplo

$$5 \cdot \begin{bmatrix} 2 & 4 & 8 & 5 \\ 1 & 6 & -2 & 0 \\ 3 & -4 & -3 & 7 \end{bmatrix} = \begin{bmatrix} 10 & 20 & 40 & 25 \\ 5 & 30 & -10 & 0 \\ 15 & -20 & -15 & 35 \end{bmatrix}$$

O produto de um número por uma matriz admite as seguintes propriedades:

a) a . {b . A} = {ab} . A;

b) a . {A + B} = a . A + a . B;

c) {a + b} . A = a . A + b . A;

d) 1 . A = A.

2.4.4 Multiplicação de matrizes

Dadas duas matrizes $A = [a_{ij}]_{m \text{ x } n}$ e $B = [b_{jk}]_{p \text{ x } n}$, o produto A . B é a matriz $C = [c_{ik}]_{m \text{ x } n}$, sendo cada elemento c_{ik} obtido através da soma dos produtos dos elementos da i-ésima linha de A pelos elementos correspondentes da k-ésima coluna de B. A multiplicação de duas matrizes, A e B, só é possível quando o número de colunas da matriz A for igual ao número de linhas da matriz B, tendo a matriz $C = A \,.\, B$ o mesmo número de linhas de A e o mesmo número de colunas de B.

Exemplo

Dadas as matrizes $A = \begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}_{2 \text{ x } 2}$ e $B = \begin{bmatrix} -2 & 4 \\ 5 & 1 \end{bmatrix}_{2 \text{ x } 2}$, o produto de A por B será a matriz $C = \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix}_{2 \text{ x } 2}$. Calculando separadamente cada elemento.

$C_{11} = [1.(-2)] + (3.5) = -2 + 15 = 13$
$C_{12} = (1.4) + (3.1) = 4 + 3 = 7$
$C_{21} = [2.(-2)] + (5.5) = -4 + 25 = 21$
$C_{22} = (2.4) + (5.1) = 8 + 5 = 13$
Portanto $C = \begin{bmatrix} 13 & 7 \\ 21 & 13 \end{bmatrix}_{2 \text{ x } 2}$.

A multiplicação de matrizes admite as seguintes propriedades:

a) é associativa: (A . B) . C = A . (B . C);

b) é distributiva à direita: (A + B) . C = AC + BC;

c) é distributiva à esquerda: C . (A + B) = CA + CB;

d) Quaisquer que sejam o número k e as matrizes A e B, vale que

(kA)B = A(kB) = k(AB).

Vale ressaltar que a propriedade comutativa não é válida no produto de matrizes

2.5 Matriz inversa

Considerando A uma matriz quadrada de ordem n. Diz-se que A^{-1} é a matriz inversa de A se, e somente se, $A \cdot A^{-1} = I_n$ e $A^{-1} \cdot A = I_n$, sendo I_n a matriz identidade de mesma ordem da matriz A.

Para encontrar a inversa de uma matriz quadrada de ordem n, deve-se obter n^2 incógnitas, resolver n sistemas de n equações a n incógnitas cada um.

Exemplo: Dada uma matriz $A = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$, determinar a inversa A^{-1}.

Sendo $A^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Por definição $A.A^{-1} = I_n$, logo:

$\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, efetuando a multiplicação: $\begin{bmatrix} 2a + c & 2b + d \\ 3a + 2c & 3b + 2d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Com a igualdade são obtidos dois sistemas: $\begin{cases} 2a + c = 1 \\ 3a + 2c = 0 \end{cases}$ e $\begin{cases} 2b + d = 0 \\ 3b + 2d = 1 \end{cases}$

Resolvendo os sistemas encontra-se os valores a = 2, b = -1, c = -3 e d = 2, logo a matriz inversa da matriz A é $A^{-1} = \begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix}$.

3 CRIPTOGRAFIA

Se analisarmos o histórico das várias ciências e tecnologias existentes, todas terão como justificativa de criação a necessidade do homem. Na criptografia não é diferente. Desde a época do antigo Egito, o homem sentiu a necessidade de guardar mensagens secretas, que eram consideradas importantes, e apenas as pessoas destinadas poderiam decodificar a mensagem. A palavra criptografia vem do grego *kryptos* que significa escondido, oculto e *grapho* que quer dizer grafia, escrita. Para (Menezes, 2003 p.14) a criptografia é uma ciência que "consiste de um conjunto de métodos que permitem codificar um texto, tornando-o ininteligível, de modo que apenas seu destinatário legítimo consiga decodifica-lo".

No decorrer da história, o homem criou vários métodos de criptografia, que durante muito tempo consistia apenas em codificar mensagens. As primeiras técnicas utilizavam métodos bem simples, que não exigiam muito conhecimento da área matemática. Pode-se citar como exemplo a substituição de letras por símbolos. Seguindo este mesmo modelo para criptografar mensagens, porém com mais segurança, e acompanhando a evolução das habilidades do homem, que neste momento se davam pelo surgimento da escrita, os Gregos detinham um sistema de numeração cifrado, que eles nomearam de sistema de numeração Jônico ou Alfabético. Sua principal característica é que esse sistema é decimal, e relaciona os 27 caracteres as 24 letras do alfabeto grego, acrescentando mais três outras que não são usadas. Sendo este, portanto, um sistema que utiliza tabelas de substituições para decifrar a mensagem codificada. Atualmente este método é conhecido por sistema de numeração cifrada, e tem como finalidade a interpretação de texto.

Com o passar do tempo, surgia à necessidade de tornar mais seguras as mensagens secretas. Com isso cada vez em que o método utilizado era descoberto, era preciso criar novas técnicas com artifícios mais aprimorados matematicamente. Para Coutinho (2009, p. 1):

> *"Ao se mandar uma mensagem criptografada, quando a mesma for recebida, existe duas alternativas de leitura: ela poderá ser decodificada ou decifrada. Quando se fala em decodificar uma mensagem, se parte do princípio que o receptor da mensagem já conhece o procedimento usado para codificação da mensagem e o usa para retirar o código, podendo desta forma obter a mensagem através da decodificação. Já a palavra decifrada é utilizada quando o receptor da mensagem codificada não é o usuário legítimo a quem ela foi enviada, sendo necessário desvendar qual foi o procedimento utilizado para codificação para somente depois utilizá-lo na decodificação."*

Nos dias atuais, o procedimento para criptografar mensagens, além de um código, também utiliza chaves ou senhas. Estas devem ser sigilosas e fundamentais para o processo de

decodificação. Para Alecrim (2005) as chaves utilizadas na criptografia, que podem ser nomeadas por chaves criptográficas são classificadas em chaves simétricas e chaves assimétricas. Cada uma com suas características próprias. A chave simétrica é dita como chave comum, pois quem envia a mensagem e quem recebe, pode usar a mesma chave tanto para codificar a mensagem, quanto para decodifica-la. As chaves assimétricas, que também são denominadas de chave pública, utiliza, no processo de criptografar, duas chaves: uma pública para codificar a mensagem e uma chave secreta para decodificar as informações enviadas com sigilo.

Com a necessidade de avanço no processo de criptografar informações secretas, surgiu também a criptoanálise. Coutinho (2009, p.1) diz que "A criptografia tem uma irmã gêmea na arte de decifrar códigos secretos, ou criptoanálise". Com essa definição, deve-se atentar para o seguinte. Mesmo que ambas tenham a mesma finalidade, a criptoanálise é mais especificamente direcionada a encontrar algoritmos para decifrar as mensagens codificadas.

Decifrar códigos para decodificar mensagens, tornou-se muito comum, isso graças ao estudo de técnicas usadas anteriormente. Com isso, até os tempos atuais, vários códigos foram criados e devidamente testados. Isso, pois a técnica de criptografia para o envio de mensagens foi crucial para o sucesso dos vencedores de guerra, e até hoje tem um papel muito importante para garantir a segurança na troca de informações sigilosas.

Essa evolução atualmente se dá ainda mais com o avanço das tecnologias e do conhecimento matemático. São vários os métodos de criptografia utilizados no decorrer da história, para as mais diversas finalidades. Por exemplo, pode-se citar o método de César, que é caracterizado por substituir cada letra da palavra por sua sucessora. Dessa forma utilizando o alfabeto, teríamos associações de acordo com a Tabela 1:

Tabela 1 - Correspondência do Método de César

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
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	A

Fonte: Imagem da autora

A aplicação na prática, por exemplo, com a palavra AMOR, se daria da seguinte forma: A codificação da palavra criptografada seria BNPS. Para decodificar, basta substituir cada letra da palavra por sua antecessora. Assim como na época em que foi utilizado é perceptível que esse método é bem simples, e portanto decifrado facilmente. Enfim, há uma infinidade de estratégias e metodologias distintas para criptografar mensagens. A maioria

utilizam conceitos matemáticos, que dificultam uma possível descoberta da estratégia utilizada.

3.1 A criptografia aplicada ao ensino de matrizes

Partindo do princípio da aplicabilidade de conceitos matemáticos na codificação e decodificação de mensagens, será descrito um método em que os conceitos utilizados para o processo de criptografia são matrizes. Neste caso o conceito de criptografia, torna-se uma alternativa metodológica, de tornar o estudo da álgebra linear mais significativo, contribuindo diretamente no processo ensino aprendizagem.

O método que utiliza esses conceitos é conhecido por método das transformações lineares. Este método, utiliza conceitos de multiplicação de matrizes e também o cálculo da matriz inversa. Neste caso estas compõe as chaves de codificação e decodificação. Inicialmente associa-se cada letra do alfabeto a um número, como mostra a tabela 2.

Tabela 2 - Correspondência entre letras e números

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	26

Fonte: Imagem da autora

Com as letras devidamente associadas aos números, pode ser sugerida uma frase, onde as letras que formam as palavras serão substituídas pelos respectivos números, para gerarem o código. Como exemplo será aplicado o método para codificar a frase “APRENDER MATRIZ”. Associando as letras aos números obtém-se:

A	P	R	E	N	D	E	R	M	A	T	R	I	Z
1	16	18	5	14	4	5	18	13	1	20	18	9	26

Portanto foi gerado um código para a frase, porém este é decifrado facilmente. Para dificultar a descoberta da mensagem, este método propõe o uso de chaves para codificação e decodificação. Para isso, é proposto que com os valores dos números associados às letras, se construa a matriz original organizando de tal forma que tenha uma matriz com duas linhas para facilitar os cálculos. Chamaremos de M a matriz original.

$$M = \begin{bmatrix} 1 & 16 & 18 & 5 & 14 & 4 & 5 \\ 18 & 13 & 1 & 20 & 18 & 9 & 26 \end{bmatrix}$$

Para codificação adote uma matriz que admita inversa. Portanto, a chave para codificação é a matriz original (A) que atenda as condições dadas anteriormente, e para decodificação, a chave assimétrica é a matriz inversa (A^{-1}). Seguindo os critérios já estabelecidos, pode-se adotar uma matriz com 2 linhas e 2 colunas, destacando mais uma vez, que esse critério do formato das matrizes é sugerido pra facilitar os cálculos. Tem-se a seguinte matriz:

$$A = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}$$

Para a codificação da frase faz-se a multiplicação da matriz A pela matriz M, nomeando o resultado de C.

$$\mathrm{C} = \begin{bmatrix} 20 & 45 & 37 & 30 & 46 & 17 & 36 \\ 39 & 74 & 56 & 55 & 78 & 30 & 67 \end{bmatrix}$$

Portanto, a mensagem a ser enviada, é o código:

20 45 37 30 46 17 36 39 74 56 55 78 30 67

Para decodificar a mensagem, o destinatário irá usar a chave assimétrica, que neste método de criptografia é a matriz inversa de A. Neste processo basta multiplicar a matriz codificada (matriz C) pela matriz inversa de A, sendo a matriz inversa, a matriz D.

$$D = \begin{bmatrix} 2 & -1 \\ -3 & 2 \end{bmatrix}$$

Da multiplicação de D por C, encontra-se a matriz original:

$$D * C = \begin{bmatrix} 1 & 16 & 18 & 5 & 14 & 4 & 5 \\ 18 & 13 & 1 & 20 & 18 & 9 & 26 \end{bmatrix}$$

E, portanto essa matriz fornece à mensagem.

4 SOFTWARE WINMAT

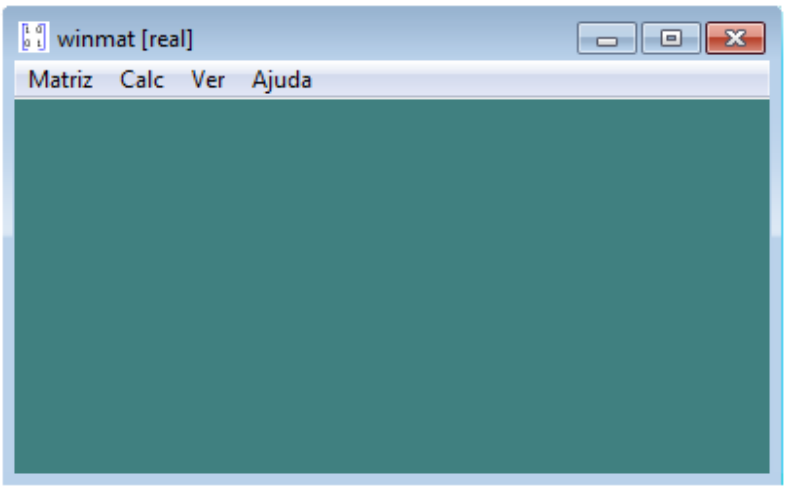
Winmat é um software de domínio público criado por Richard Parris, do departamento de matemática da Academia Phillips Exeter. Está disponível no site http://math.exeter.edu/rparris/winmat.html. Tem por objetivo efetuar cálculo com matrizes, que vai desde a sua lei de formação, soma e multiplicação, inversa de uma matriz, determinante e solução de sistemas. As vantagens do uso desse software, além da gratuidade, é o fácil manuseio. Sua praticidade para inserir comandos ao programa facilita o uso e aplicabilidade dessa ferramenta no processo ensino aprendizagem, já que não são necessárias muitas habilidades no uso do computador.

No estudo de matrizes, a prática de exercícios com cálculos longos e repetitivos torna o conteúdo exaustivo, o que interfere diretamente no interesse dos alunos em aprender. O software winmat é uma ferramenta que irá estimular no aluno o desenvolvimento da lógica das resoluções das questões, já que o mesmo não irá se preocupar em fazer grandes cálculos. O winmat vai possibilitar ao aluno manipular as matrizes de diferentes formas, com isso o professor terá a possibilidade de ensinar matrizes com suas aplicações, dando mais sentido ao que está sendo abordado.

4.1 Conhecendo o software

Ao abrir o programa winmat, aparecerá a seguinte tela, com a barra de menu inicial.

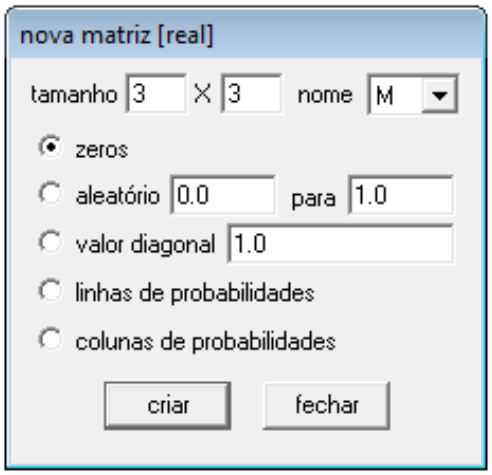
Figura 1 - Tela Inicial do Winmat



Fonte: Imagem da autora

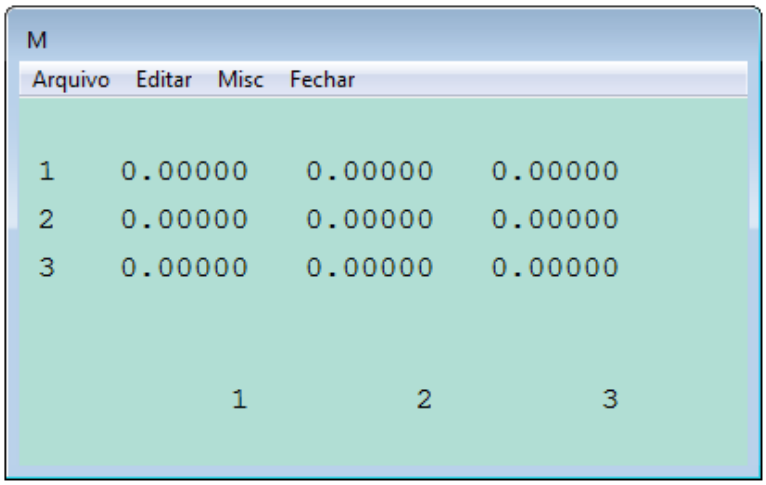
Para inserir uma matriz, acione na barra de menu do winmat, “matriz” e em seguida “nova”. Ao ativar esses comandos, aparecerá uma nova janela que possibilita escolher a dimensão, o nome e o tipo da matriz. Ao clicar no botão “criar”, aparecerá a matriz. Para uma matriz particular, pode-se escolher qualquer tipo de matriz e trocar os elementos da matriz que foi criada. Para alterar os valores dos elementos da matriz basta clicar no botão esquerdo do mouse e depois acionar a tecla Enter do teclado.

Figura 2 - Janela para inserir uma nova matriz



Fonte: Imagem da autora

Figura 3 - Tela de uma matriz com tamanho 3x3



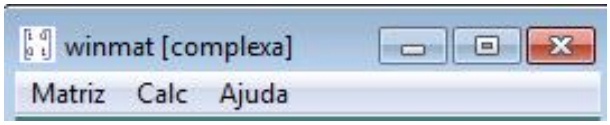
Fonte: Imagem da autora

Observa-se que aparece escrito “nova matriz [real]” na parte superior da janela nova matriz. Esse termo indica que a matriz que irá ser criada possui elementos reais. O programa possibilita ainda criar matrizes com elementos inteiros e complexos. Para alterar a forma dos elementos, basta na barra de menu clicar “matriz”, e em seguida acionar “modo”.

De forma geral os comandos são bem visíveis e nomeados de acordo com a nomenclatura usada em sala de aula, o que facilita muito aplica-lo nas aulas. Segue agora todos os comandos possíveis do winmat na barra de menu que aparece na tela inicial do winmat e também na barra de menu da matriz.

4.1.1 Comandos da barra de menu do winmat:

Figura 4 - Barra de Menu



Fonte: Imagem da autora

Menu matriz

Nova: permite criar uma matriz;

Abrir: possibilita abrir uma matriz que já está salva;

Colar: esse comando permite colar uma tabela de números reais, que está inserida em um texto fora do software. Cada campo numérico é interpretado como uma entrada da matriz;

Modo: escolher o tipo de elementos da matriz, que pode ser real, inteiro ou complexo;

Rotação 2D: matriz de rotação em duas dimensões, ou seja, rotação do plano;

Rotação 3D: rotação em três dimensões, ou seja, matriz de rotação do espaço;

Refletir/ Projetar: Matriz para projeção e reflexão;

Fórmula: permite escolher o tipo de matriz e inserir a lei de formação;

Copiar coluna: permite criar uma nova matriz que é formada por uma coluna de uma matriz já definida;

Fundo branco: a cor de fundo da matriz branco;

Ajuda: permite ao usuário tirar dúvidas sobre os itens do menu inicial;

Sair: para sair do programa.

Menu cal

Uma matriz: permite obter informações sobre a matriz (posto, traço, determinante, polinômio característicos com suas raízes);

Calcular: este comando é o mais utilizado pois permite efetuar operações com matrizes (soma, produto, inversa, transposta);

Resolver: para encontrar a solução de um sistema de equações lineares que estão na forma matricial MX = B, sendo B uma matriz coluna;

Prog Linear: permite maximizar ou minimizar funções lineares definidas em regiões convexas descritas por desigualdades lineares.

Forma Escalonada: abre uma caixa de diálogo que possibilita levar uma matriz "passo a passo" à forma escalonada por linhas.

Operações linhas/ colunas: realiza operações elementares sobre linhas e colunas;

Ver: ao acionar fechar na janela de uma matriz, a janela desaparece. Para ver a matriz novamente, basta clicar em ver e em seguida, a letra que nomeia a matriz;

Destaca-se que os comandos possíveis neste menu, em sua maioria, só aparecem quando o tipo dos elementos matriz selecionado é o tipo real.

4.1.2 Comandos da barra de menu da janela da matriz criada

Arquivo: permite salvar a matriz como matriz (salvar ou salvar como), como texto (texto externo) ou .text (TeXto matriz);

Editar:

Desfazer: desfaz as últimas operações;

Dimensões: permite mudar as dimensões da matriz;

Formato: define o formato da matriz, onde "espessura do campo" define o espaço de cada elemento e "num decimais" define o número de casas decimais após a vírgula;

Resolver: resolve linhas ou colunas;

Inserir: insere linhas ou colunas;

Trocar: troca linhas ou colunas;

Col por col autoavanço: permite entrar com os elementos por colunas. Neste caso clicando com o botão direito do mouse. Caso contrário, a entrada dos elementos da matriz será feita por linhas.

Misc:

Fonte: permite escolher o tipo de fonte;

Hifen do menos: possibilita aumentar o sinal de menos;

Cor do bordo: Permite alterar a cor dos índices do bordo;

Notas: permite digitar notas suplementares sobre uma matriz.

Fechar: permite fazer desaparecer a janela da matriz;

Através desses comandos o software permite efetuar operações com matrizes, cálculo da inversa, dentre outras. A seguir será mostrada qual sequência de comandos deve ser acionada para manipular as matrizes, tendo como foco o estudo de matrizes no ensino médio.

4.2 Adição e subtração de matrizes no Winmat

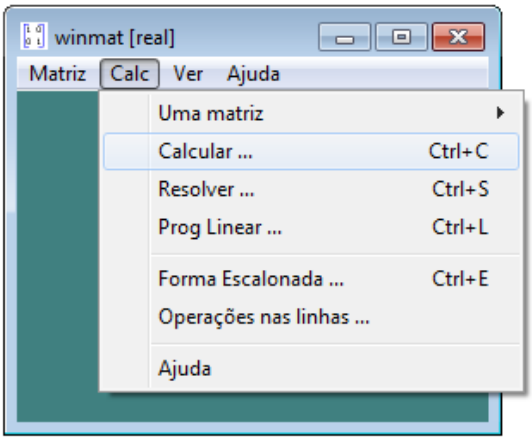
Com as matrizes A e B, para efetuar a soma (A + B) ou subtração (A – B), as matrizes dadas devem possuir o mesmo formato. Por exemplo, uma matriz $A_{2\ x\ 2}$, só pode ser somada ou calculada a diferença com outra matriz $B_{2\ x\ 2}$.

Para efetuar essas operações no winmat, inicialmente é preciso criar as matrizes. Para isso no menu superior esquerdo aciona o comando "matriz", e em seguida clica em "nova". Após criar as matrizes, faz-se necessário calcular as operações de soma e subtração. Destaca-se que o resultado das operações soma e diferença é uma nova matriz no mesmo formato das matrizes inseridas. Para fazer os cálculos, basta clicar no menu "calc", e na sequência clicar em "calcular". Aparecerá uma janela para digitar a operação desejada, por exemplo, A + B ou A – B. Nesta mesma janela a matriz resultante da soma é nomeada, e em seguida basta clica em "criar", para que seja calculada a operação. Como exemplo, dadas as matrizes A e B:

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}; B = \begin{bmatrix} -3 & 5 \\ 4 & 2 \end{bmatrix}$$

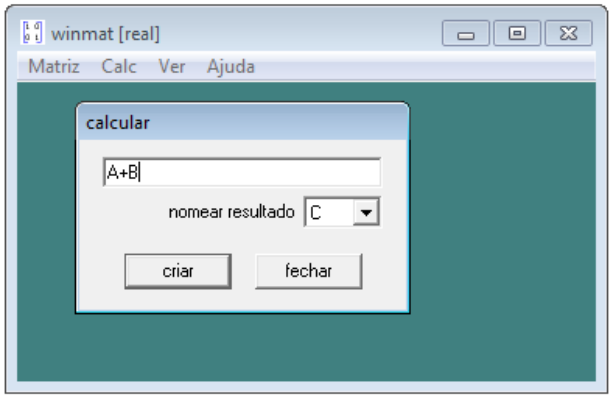
Após inserir essas duas matrizes no winmat, basta clicar em calc e calcular, e logo em seguida na janela que se abre, inserir o comando A + B (adição), ou A – B (subtração).

Figura 5 - Comando para calcular operações com matrizes



Fonte: Imagem da autora

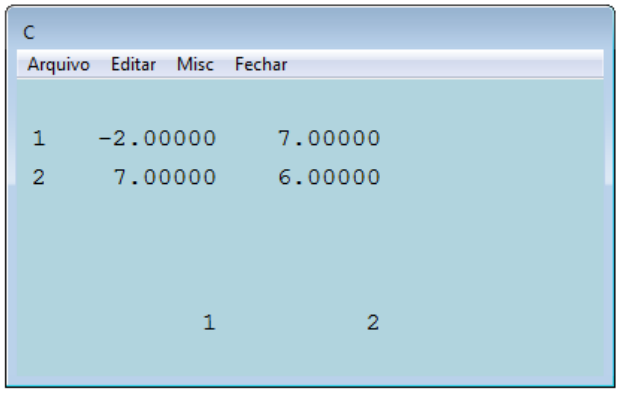
Figura 6 – comando para efetuar a soma de duas matrizes A e B



Fonte: Imagem da autora

Nesta mesma janela em que o comando da operação é inserido, o usuário pode nomear a nova matriz. Neste caso a matriz será nomeada por C. Pra finalizar basta clicar no botão criar, e a matriz C, que é a soma da matriz A com a matriz B, aparecerá em outra janela.

Figura 7 - Matriz C resultante da soma de duas outras matrizes

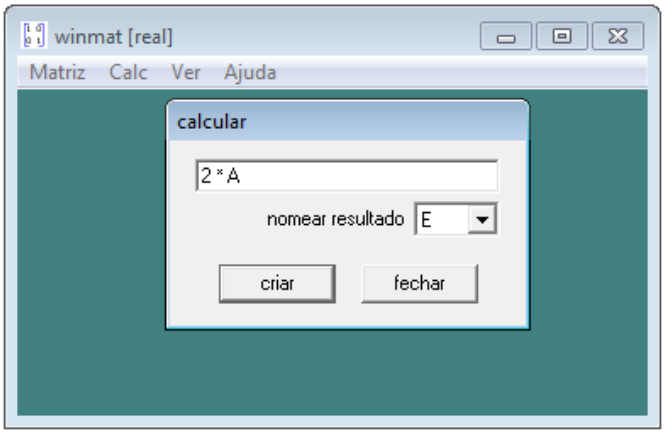


Fonte: Imagem da autora

4.3 Multiplicação de um número real por uma matriz

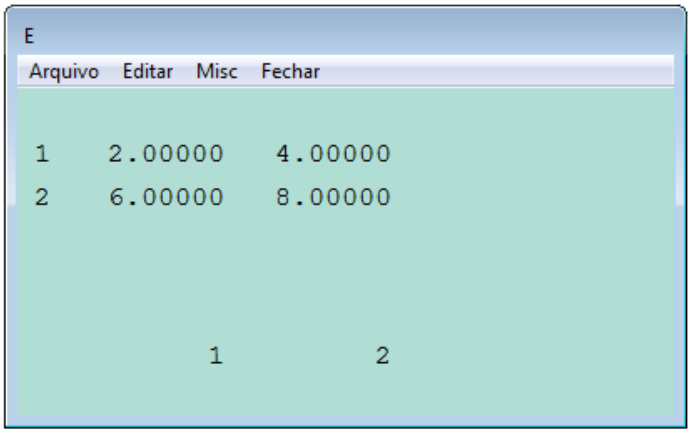
Como todas as operações a serem efetuadas, inicialmente é necessário criar a matriz. Em seguida aciona o menu “calc” e em sequência “calcular”. Digita a operação, que neste caso é um número real multiplicado pela matriz. O sinal de multiplicação reconhecido pelo programa é o asterisco (*). Por exemplo a multiplicação do número real 2 pela matriz A do exemplo anterior, é inserida no winmat como 2*A ou simplesmente por 2A.

Figura 8 - comando para efetuar o produto de um número natural por uma matriz A



Fonte: Imagem da autora

Figura 9 - Matriz E resultante do produto de um número natural por uma matriz



Fonte: Imagem da autora

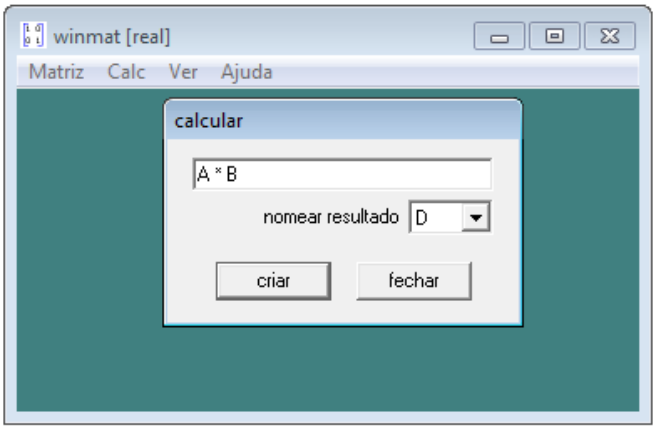
4.4 Multiplicação de matrizes

Na multiplicação de matrizes, dadas as matrizes $A_{m,n}$ e $B_{p,q}$, a condição de existência da matriz C = A x B, é que p seja igual a n (p = n), ou seja o número de linhas de B

deve ser igual ao número de colunas de A. A matriz C que é o resultado da multiplicação é no formato $C_{m,q}$, que possui o número de linhas de A e o número de colunas de B. Assim como nas outras operações, para fazer a multiplicação de matrizes, basta clicar em "calc" e em seguida "calcular". Na janela que abriu digita o comando de multiplicação, por exemplo, A*B, nomeia a matriz resultante e clica em criar.

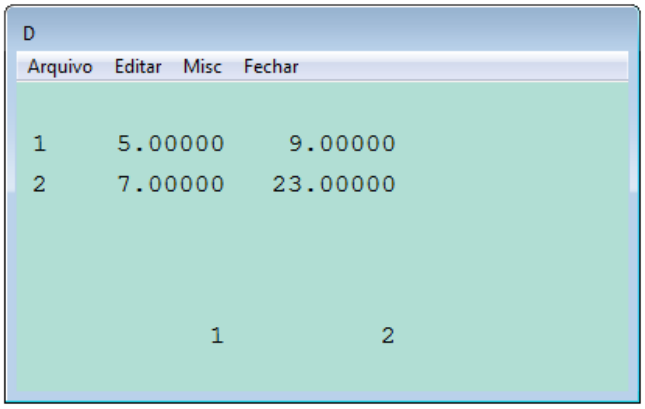
Utilizando as matrizes A e B, e seguindo os passos descritos acima. No winmat, ao abrir a janela, basta digitar o comando da operação multiplicação que é A * B, e clicar em criar, que matriz produto (nomeada por D) será gerada.

Figura 10 - comando para efetuar o produto de uma matriz A por uma matriz B



Fonte: Imagem da autora

Figura 11 - Matriz D resultante do produto de duas matrizes

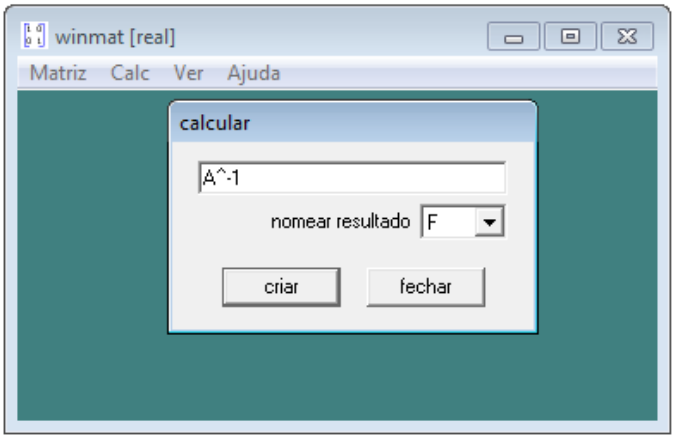


Fonte: Imagem da autora

4.5 Cálculo da inversa de uma matriz

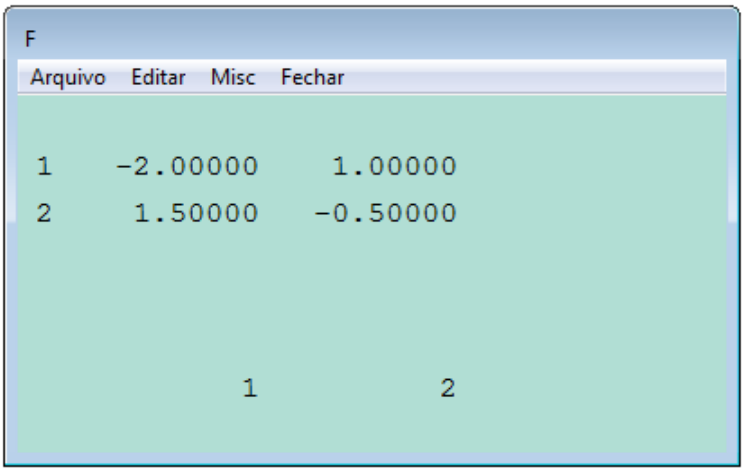
A inversa de uma matriz é a matriz elevada à potência -1, portanto a inversa de uma matriz A é A^{-1}. Neste caso o comando a ser inserido na janela calcular do winmat é A^-1. Ainda utilizando a matriz A, encontramos como sua inversa a seguinte matriz nomeada por F:

Figura 12 - Comando para calcular a inversa de uma matriz



Fonte: Imagem da autora

Figura 13 - matriz F inversa da matriz A



Fonte: Imagem da autora

5 CONCLUSÃO

Este trabalho teve por motivação a busca pela aprendizagem significativa de matrizes, que nesse estudo foi entendida como a aplicação do conteúdo e a valorização da lógica de resolução de questões, sem se deter a prática exaustiva de cálculos. Ao propor o ensino de matrizes aplicado a criptografia, além de estimular o aluno com a ligação direta do conteúdo a algo real, o coloca frente a fatos importantes que aconteceram no decorrer da história. Como consequência desta aplicação, vem à importância da matemática, mais especificamente de matrizes para que grandes desafios com relevância mundial tenham obtido sucesso. Portanto, colocar o que se estuda em uma realidade prática e histórica facilita o aprendizado da matéria, além de contribuir no desenvolvimento pessoal do aluno.

Como consequência do estudo de todo conteúdo em matemática, vem à necessidade de exercitar o que inicialmente é apenas teórico. Neste caso, colocar em prática a manipulação de matrizes com o cálculo de suas operações. Essa prática proposta com uso de recursos digitais não deve excluir esta etapa do estudo, mas sim possibilitar esse exercício de forma ainda mais ampla. Sabe-se que exercitar operações com matrizes na forma escrita, não torna possível um aprofundamento maior no assunto abordado, visto que é necessário mais tempo do que o planejamento permite. O uso do winmat irá possibilitar a prática do estudo de matrizes de forma mais intensa, sem deixar que essa prática seja exaustiva para o aluno. Portanto, a aplicação da criptografia e o uso do winmat no estudo de matrizes, torna-se uma estratégia de ensino com grandes chances de sucesso, visto que promovem aprendizagem com significado.

REFERÊNCIAS

Criptografia com Álgebra Linear. Disponível em: <https://danieldonda.wordpress.com/2011/04/08/criptografia-com-lgebra-linear-matrizesparte-1/>. Acesso em: 03 nov. 2015.

Criptografia e Álgebra. Disponível em: <http://www.mat.ufmg.br/~marques/CRIPTOGRAFIA.pdf >. Acesso em: 04 out. 2015.

Coutinho, S. C. *Números Inteiros e Criptografia RSA.* 2. Ed. Rio de Janeiro: Instituto Nacional de Matemática Pura e Aplicada-IMPA. 2009.

Estudando Matrizes e Determinantes utilizando o Software Winmat. Disponível em: <http://www.edumat.com.br/wp-content/uploads/2008/11/apostilawinmat-202006.pdf>. Acesso em: 02 out. 2015.

MESSIAS, M. A. V. F. ; SÁ, P. F ; FONSECA, R. V . Um Estudo diagnóstico sobre as dificuldades em matrizes. In: IX ENEM, 2007, Belo Horizonte. Encontro nacional de educação matemática. Belo Horizonte: Dantas Projetos digitais, 2007. p. 3-180.

O uso da criptografia no ensino de Matemática. Disponível em: < http://www.gente.eti.br/lematec/CDS/XIIICIAEM/artigos/1817.pdf >. Acesso em 10 out. 2015.

SANCHES, Maria Helena Figueiredo. *Efeitos de uma estratégia diferenciada de ensino do conceito de matrizes.* 2002. 142 f. Dissertação (Mestrado em Educação), Universidade Estadual de Campinas, Faculdade de Educação, Campinas, 2002. Disponível em: <http://www.bibliotecadigital.unicamp.br/document/?code=vtls000253634>. Acesso em: 03 out. 2015.

SILVA, Claudio Xavier; BARRETO FILHO, Benigno. *Matemática aula por Aula*. 2. ed. São Paulo: Ftd, 2005.

IEZZI, Gelson; HAZZAN, Samuel. *Fundamentos de Matemática Elementar.* 2. ed. São Paulo: Atual Editora, v.4, 1977.

Winmat (em português). Disponível em: <http://wwwp.fc.unesp.br/~mauri/Down/Winmatpr.pdf>. Acesso em: 16 out. 2015.