**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS**

**ESCOLA DE FORMAÇÃO DE PROFESSORES E HUMANIDADES**

**LICENCIATURA MATEMÁTICA**

**JOSÉ ABREU PEREIRA JUNIOR**

**UM BREVE ESTUDO SOBRE MATRIZES E SUA APLICAÇÃO EM CRIPTOGRAFIA**

**GOIÂNIA**

**2022**

**JOSÉ ABREU PEREIRA JUNIOR**

**UM BREVE ESTUDO SOBRE MATRIZES E SUA APLICAÇÃO EM CRIPTOGRAFIA**

Trabalho de Conclusão de Curso apresentada como requisito parcial à obtenção do título de licenciado em Matemática, da Escola de Formação de Professores e Humanidade, da Pontifícia Universidade Católica de Goiás.

Orientador: Prof. Dr. Adelino Candido Pimenta

**GOIÂNIA**

**2022**

JOSÉ ABREU PEREIRA JUNIOR

**UM BREVE ESTUDO SOBRE MATRIZES E SUA APLICAÇÃO EM CRIPTOGRAFIA**

Trabalho de Conclusão de Curso apresentado no curso de Licenciatura em Matemática da Pontifícia Universidade Católica de Goiás (PUC GO) para obtenção do grau de Licenciado em Matemática, aprovado em 14 de junho de 2022, pela banca examinadora constituída pelos seguintes professores:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Profa. Dra. Bianka Carneiro Leandro

Membro titular – PUC Goiás

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Prof. Mª. Rosimara Fachin Pelá

Membro titular – PUC Goiás

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Prof. Dr. Adelino C. Pimenta

Prof. Orientador – PUC Goiás

**AGRADECIMENTOS**

Primeiramente a Deus, que fez com que meus objetivos fossem alcançados, durante todos os meus anos de estudos.

Aos meus pais José Abreu e Aparecida, que me deram apoio, incentivo nas horas difíceis, de desânimo e cansaço. Que apesar de todas as dificuldades me fortaleceram e que para mim foi muito importante.

Agradeço ao meu orientador Adelino Pimenta por aceitar conduzir o meu trabalho de pesquisa.

A todos os meus amigos do curso de graduação que compartilharam dos inúmeros desafios que enfrentamos, sempre com o espírito colaborativo.

“Por vezes sentimos que aquilo que fazemos não é senão uma gota de água no mar. Mas o mar seria menor se lhe faltasse uma gota.”

Madre Tereza de Calcutá

**RESUMO**

Este trabalho tem como objetivo apresentar uma perspectiva diferente para as aulas de matemática principalmente para as relacionadas a matrizes. No contexto de ensino de matemática nota-se que esta não é a disciplina preferida dos alunos, questionamentos tais como “para que isso serve?”, sempre ocorrem diante de um novo conteúdo. Em seguida sanar os

questionamentos frequentes mostrando aplicações, onde são encontradas e como

podem ser vistas no nosso cotidiano.

Palavras-Chaves: matriz, aplicação, criptografia.

**ABSTRACT**

This paper aims to present a different perspective for mathematics classes, especially for those related to matrices. In the context of mathematics teaching, it is noted that this is not the students' favorite subject, and questions such as "what is this for? Then solve the frequent

frequent questioning by showing what it is used for, where it is found, and how it can be

can be applied in our daily lives.

Keywords: matrix, application, cryptography.

Sumário

[1 INTRODUÇÃO 9](#_Toc105585668)

[2 DADOS HISTÓRICOS SOBRE MATRIZES 10](#_Toc105585669)

[3 MATRIZES 10](#_Toc105585670)

[3.1 DEFINIÇÃO 10](#_Toc105585671)

[3.2 REPRESENTAÇÃO DE UMA MATRIZ 10](#_Toc105585672)

[3.3 MATRIZES ESPECIAS 11](#_Toc105585673)

[3.3.1 Matriz linha 11](#_Toc105585674)

[3.3.2 Matriz coluna 11](#_Toc105585675)

[3.3.3 Matriz quadrada 11](#_Toc105585676)

[3.3.4 Matriz nula 12](#_Toc105585677)

[3.3.5 Matriz diagonal 12](#_Toc105585678)

[3.3.6 Matriz identidade 13](#_Toc105585679)

[3.3.7 Matriz transposta 13](#_Toc105585680)

[3.3.8 Matriz simétrica 13](#_Toc105585681)

[3.3.10 Igualdade de matrizes 14](#_Toc105585682)

[3.3 OPERAÇÕES COM MATRIZES 14](#_Toc105585683)

[3.3.1 Adição de Matrizes 14](#_Toc105585684)

[3.3.2 Subtração de Matrizes 15](#_Toc105585685)

[3.3.3 Multiplicação de um número real por uma matriz 15](#_Toc105585686)

[3.3.4 Multiplicação de matrizes 15](#_Toc105585687)

[3.3.5 Matriz Inversa 17](#_Toc105585688)

[4 CRIPTOGRAFIA 18](#_Toc105585689)

[5 MATRIZES E CRIPTOGRAFIA 18](#_Toc105585690)

[6 CONCLUSÃO 20](#_Toc105585691)

[REFERÊNCIAS 22](#_Toc105585692)

1 INTRODUÇÃO

Como professor de matemática, ao explicar um conteúdo para alunos, sou confrontada com indagações do tipo: “Onde vou usar este conteúdo?”. Com essas perguntas surgiu a ideia de trabalhar aplicações especificamente de matrizes em criptografia. Já que matriz é um conteúdo no qual desde o meu ensino médio me identifiquei bastante.

Sendo assim início o trabalho definindo matrizes e suas operações as quais vamos utilizar para realizar a aplicação em criptografia de mensagem, a qual vamos mais utilizar será a matriz inversa de uma determinada matriz. Assim para fazer a codificação e descodificação da mensagem.

A criptografia é uma tecnologia que mantém a privacidade das informações e é usada principalmente como meio de comunicação seguro. Assim esse trabalho foi desenvolvido para os alunos vejam além do conteúdo a importância dele na sociedade.

# 2 DADOS HISTÓRICOS SOBRE MATRIZES

Em meados do século 19, os matemáticos alemães estavam à frente de outros países em análise e geometria, com as universidades de Berlim e Göttingen liderando o caminho, e suas publicações estavam concentradas na Journal de Crelle. A álgebra, por outro lado, foi em um ponto quase um monopólio britânico, com o Trinity College Cambridge assumindo a liderança e o Cambridge Mathematics Journal o principal veículo de publicação. George Peacock (1791-1858) e Augustus De Morgan (1806-1871) eram ambos da Trinity, e havia Arthur Cayley (1821-1895), que fez grandes contribuições para a álgebra e geometria e se formou como sênior Wrangler. Cayley também foi um dos primeiros a estudar matrizes, outro exemplo do foco britânico na forma e estrutura algébrica. Este trabalho vem de um livro de memórias de 1858 sobre a teoria da transformação.

O início da teoria de matrizes se remonta a um artigo de Cayley em 1855. Diga-se de passagem, porém, que o termo matriz já fora usado, com o mesmo sentido, cinco anos antes por Sylvester. Neste artigo Cayley fez questão de salientar que, embora logicamente a ideia de matriz preceda a de determinante, historicamente ocorreu o contrário: de fato, os determinantes já eram usados há muito na resolução de sistemas lineares. Quanto às matrizes, Cayley introduziu-as para simplificar a notação de uma transformação linear. (DOMINGUES, apud IEZZI, 2004)

James Joseph Sylvester (1814-1897) também compartilhava da mesma ideia de Cayley sobre as matrizes vista a partir de transformações lineares e invariantes algébricos. Eles investigavam expressões que permaneciam invariantes quando as variáveis eram transformadas por substituições.

# 3 MATRIZES

# 3.1 DEFINIÇÃO

Matriz é uma tabela de números reais dispostos em linhas (filas horizontais) e colunas (filas verticais). Exemplos:

é uma matriz ;

é uma matriz ;

Como podemos notar nos exemplos 1 e 2 respectivamente, uma matriz pode ser representada por colchetes ou parênteses.

# 3.2 REPRESENTAÇÃO DE UMA MATRIZ

As matrizes costumam ser representadas por letras maiúsculas e seus elementos por letras minúsculas, acompanhadas de dois índices que indicam, respectivamente, a linha e a coluna ocupadas pelo elemento.

Exemplo: Uma matriz **A** do tipo m x n é representada por:

ou, abreviadamente, , onde e representam, respectivamente, a linha e a coluna que o elemento ocupa,

.

Por exemplo, na matriz anterior, é o elemento da segunda linha com o da terceira coluna.

Exemplo: Seja a matriz , onde :

Genericamente, temos:

Utilizando a regra de formação dos elementos dessa matriz, temos:

Assim, .

# 3.3 MATRIZES ESPECIAS

# 3.3.1 Matriz linha

É toda matriz do tipo , isto é, com uma única linha.

Exemplo: .

# 3.3.2 Matriz coluna

É toda matriz do tipo , isto é, com uma única coluna.

Exemplo:

# 3.3.3 Matriz quadrada

É toda matriz do tipo , isto é, com o mesmo número de linhas e colunas. Neste caso, dizemos que a matriz é de ordem .

Exemplo:

Matriz de ordem

Matriz de ordem

Seja uma matriz quadrada de ordem .

Obs.:

1. Diagonal principal de uma matriz quadrada é o conjunto de elementos dessa matriz, tais que .
2. Diagonal secundária de uma matriz quadrada é o conjunto de elementos dessa matriz, tais que .

Exemplo:

Descrição da matriz:

- O subscrito indica a ordem da matriz;

- A diagonal principal é a diagonal formada pelos elementos e ;

- A diagonal secundária é a diagonal formada pelos elementos e ;

- é elemento da diagonal principal, pois ;

- é elemento da diagonal secundária, pois .

# 3.3.4 Matriz nula

É toda matriz em que todos os elementos são nulos.

Notação:

Exemplo:

# 3.3.5 Matriz diagonal

É toda matriz quadrada onde só os elementos da diagonal principal são diferentes de zero.

Exemplo:

.

# 3.3.6 Matriz identidade

É toda matriz quadrada onde todos os elementos que não estão na diagonal principal são nulos e os da diagonal principal são iguais a .

Notação: onde indica a ordem da matriz identidade.

Exemplo:

ou:

# 3.3.7 Matriz transposta

Chamamos de matriz transposta de uma matriz a matriz que é obtida a partir de , trocando-se ordenadamente suas linhas por colunas ou suas colunas por linhas.

Notação: .

Exemplo:

Se então

Desse modo, se a matriz é do tipo , é do tipo . Note que a primeira linha de corresponde à primeira coluna de e a segunda linha de corresponde à segunda coluna de .

# 3.3.8 Matriz simétrica

Uma matriz quadrada de ordem n é simétrica quando .

Observação: Se , dizemos que a matriz é anti-simétrica.

Exemplo:

Se

Então é simétrica.

**3.3.9 Matriz oposta**

Chamamos de matriz oposta de uma matriz a matriz que é obtida a partir de A, trocando-se o sinal de todas os seus elementos.

Notação:

Exemplo:

Se então

# 3.3.10 Igualdade de matrizes

Duas matrizes, e , do mesmo tipo , são iguais se, todos os elementos que ocupam a mesma posição são idênticos.

Notação: .

Exemplo:

Se e , então e

Simbolicamente: para todo .

# 3.3 OPERAÇÕES COM MATRIZES

# 3.3.1 Adição de Matrizes

Dadas as matrizes e , chamamos de soma das matrizes e a matriz , tal que , para todo e todo .

Notação:

existe se, e somente se, e são do mesmo tipo .

Propriedades: e são matrizes do mesmo tipo , valem as seguintes propriedades:

1. Associativa:
2. Comutativa:
3. Elemento Neutro:

onde é a matriz nula .

1. Elemento Oposto:

Exemplo:

# 3.3.2 Subtração de Matrizes

Dadas as matrizes e , chamamos de diferença entre as matrizes e a soma de com a matriz oposta de .

Notação:

existe se, e somente se, e são do mesmo tipo .

Exemplo:

# 3.3.3 Multiplicação de um número real por uma matriz

Dados um número real e uma matriz do tipo , o produto de por é uma matriz do tipo , obtida pela multiplicação de cada elemento de por .

Notação:

Cada elemento de é tal que

Propriedades: Sendo e matrizes do mesmo tipo e e números reais quaisquer, valem as seguintes propriedades:

1. Associativa:
2. Distributiva de um número real em relação a adição de matrizes:
3. Distributiva de uma matriz em relação a soma de dois números reais:
4. Elemento Neutro: , para , ou seja:

Exemplo:

# 3.3.4 Multiplicação de matrizes

O produto de uma matriz por outra **não** pode ser determinado através do produto dos seus respectivos elementos. A multiplicação de matrizes **não** é análoga à multiplicação de números reais.

Dada uma matriz do tipo e uma matriz do tipo , o produto da matriz pela matriz é a matriz do tipo tal que o elemento é calculado multiplicando-se ordenamente os elementos da linha , da matriz , pelos elementos da coluna , da matriz , e somando-se os produtos obtidos.

Para dizer que a matriz é o produto de por , vamos indica-la por .

OBS: Elementos correspondentes de matrizes do mesmo tipo , são os elementos que ocupam a mesma posição nas duas matrizes.

Exemplo:

Sejam e . Os elementos e são elementos correspondentes.

Decorrência da definição:

A matriz produto existe apenas se o número de colunas da primeira matriz é igual ao número de linhas da segunda matriz .

Assim: e

Note que a matriz produto terá o número de linhas do primeiro fator e o número de colunas do segundo fator.

Exemplos:

1. Se
2. Se
3. Se

Propriedades: Verificadas as condições de existência, para a multiplicação de matrizes são válidas as seguintes propriedades:

1. Associativa:
2. Distributiva em relação à adição:
3. Elemento Neutro:

onde é a matriz identidade de ordem .

Atenção: **Não valem** as seguintes propriedades:

1. Comutativa, pois, em geral, .
2. Sendo uma matriz nula, não implica, necessariamente, que ou .

Exemplo:

Sendo e , vamos determinar e e comparar os resultados

Solução:

Assim:

Comparando os resultados, observamos que , ou seja, a propriedade comutativa para multiplicação de matrizes **não** vale.

# 3.4 Matriz Inversa

Dada uma matriz , quadrada, de ordem , se existir uma matriz , de mesma ordem, tal que , então é matriz inversa de .(Em outras palavras: Se , isto implica que é a matriz inversa de , e é indicada por ).

Notação:

Exemplo:

Sendo , vamos determinar a matriz inversa de , se existir.

Solução:

Existindo, a matriz inversa é de mesma ordem de .

Passo: Impomos a condição de que e determinamos :

A partir da igualdade de matrizes, resolvemos o sistema acima pelo método da adição e chegamos à:

Assim temos:

Passo: Verificamos se :

Portanto temos uma matriz , tal que:

Logo, é inversa de e pode ser representada por:

# 4 CRIPTOGRAFIA

Desde a época do Antigo Egito, era necessário guardar mensagens secretas, onde somente algumas pessoas podiam decifrar. A criptografia vem do Grego, *Kryptósque*, significa secreto *egrápheinque* significa escrever um código ou mensagem de modo que somente quem envia e quem recebe a mensagem original são capazes de interpretá-la. A criptografia é uma técnica de manter sigilo sobre informações e principalmente como meio de segurança para comunicações em: caixas eletrônicos, home banking, cartões de crédito, mensagens telefônicas e páginas da internet, onde são utilizadas senhas.

# 5 MATRIZES E CRIPTOGRAFIA

Uma forma de se usar matrizes na criptografia é envolver matrizes inversas. Sejam e , sendo que é a matriz inversa de .

Segue um exemplo abaixo de matrizes onde a matriz irá codificar a mensagem e o destinatário usará a matriz para descodificar

A matriz é apropriada, pois seus elementos são números inteiros, assim como os da matriz . O remetente vai usar a matriz para codificar a mensagem, e o destinatário vai usar a matriz para decodificá-la. O objetivo deste método é que a mensagem seja codificada utilizando pares de caracteres, de modo que tabelas de frequência de letras e outras alternativas não ajudem em nada a um decodificador não-amigável.

Dada uma mensagem para ser codificada, o primeiro passo será convertê-la da forma alfabética para a forma numérica. Para isso usamos a seguinte correspondência entre letras e números:

Foto em preto e branco

Descrição gerada automaticamente

Tanto o remetente quanto o destinatário devem estar cientes desta tabela. Qualquer outra numeração dos 29 símbolos tipográficos também seria possível, mas o remetente e o destinatário teriam que combiná-la previamente. Para maior clareza usamos o símbolo # para indicar inexistência de letras (espaços entre palavras etc.).

Exemplo 1:

Vamos codificar a seguinte frase: “A EDUCAÇÃO NÃO TEM PREÇO. SUA FALTA TEM CUSTO.”

A#EDUCACAO#NAO#TEM#PRECO.#SUA#FALTA#TEM#CUSTO.

1 29 5 4 21 3 1 3 1 15 29 14 1 15 29 20 5 13 29 16 18 5 3 15 27 29 19 21 1 29 6 1 12 20 1 29 20 5 13 29 3 21 19 20 15 27

Vamos colocar a sequência de números dispostos em uma matriz de duas linhas. Se o número de elementos da matriz for ímpar, deve-se acrescentar um caractere vazio.

Para codificar a mensagem, multiplicamos a matriz por , tal que :

Ou seja

Os elementos de constituem a mensagem codificada, e utilizaremos virgulas entre esses elementos para maior clareza:

6, 102, 42, 41, 82, 30, 4, 38, 9, 46, 99, 62, 32, 65, 92, 73, 44, 42, 108, 97, 68, 69, 42, 5, 73, 37, 61, 27, 3, 35, 8, 31, 70, 48, 31, 50, 63, 53, 39, 29, 79, 71, 52, 51, 37.

Quando esta mensagem codificada chegar ao destinatário este deve utilizar a matriz decodificadora para reverter os passos acima, pois

Portanto, se o decodificador usar a mensagem codificada para construir uma matriz com duas linhas e depois multiplicar esta matriz a esquerda por , irá obter a matriz do remetente.

Vejamos:

Note que o produto é de fato a matriz do remetente. O passo final de decodificação é:

1 29 5 4 21 3 1 3 1 15 29 14 1 15 29 20 5 13 29 16 18 5 3 15 27 29 19 21 1 29 6 1 12 20 1 29 20 5 13 29 3 21 19 20 15 27

A#EDUCACAO#NAO#TEM#PRECO.#SUA#FALTA#TEM#CUSTO.

Em resumo, o remetente multiplica a mensagem original (na forma de uma matriz numérica ) por para obter a mensagem codificada. O receptor multiplica a mensagem codificada (na forma de matriz ) por para reconstruir a mensagem original. Como e são matrizes inversas, a multiplicação do receptor por cancela a multiplicação do emissor por .

O processo pode ser rapidamente automatizado por um computador (aumentando assim sua segurança), mas pode ser feito usando apenas lápis e papel se necessário (realçando sua utilidade). Tudo o que precisa ser mantido em segredo são as matrizes do codificador e do decodificador.

# 6 CONCLUSÃO

Conforme relatado neste trabalho, aplicamos matrizes que podem interessar aos alunos e tornar as aulas de matemática mais envolventes, e porque não nos desviamos das regras, tratamos toda a teoria com rigor. Os alunos de hoje estão cercados de tecnologia e é difícil competindo com tão poucas armas, então leve isso em consideração para demonstrar atratividade que prende a atenção do aluno. Outra consideração importante é que podemos aplicar essa estrutura as aulas vão para outros conteúdos, não apenas para a matriz, que exige apenas que o professor estude um pouco mais, e um pouco mais de detalhes sobre sua classe. Por fim, notamos que as aulas expositivas, elas podem ser aumentadas com uma pequena quantidade de recursos.

# REFERÊNCIAS

IEZZI, G.; HAZZAN, S. **Fundamentos de matemática elementar**, vol 4: sequências,

matrizes, determinantes, sistemas. – 7. Ed – São Paulo: Atual, 2004

EVES, H. **Introdução à história da matemática**, tradução: Hygino H. Domingues, Campinas, SP: Editora da UNICAMP, 2004

DANTE, Luiz R. **Matemática: contexto e aplicações**, vol único, São Paulo: Editora

Ática, 2007

MENEZES, S. **Mensagens Secretas com Matrizes-Criptografia**. Rio De Janeiro. 2013.