

## O CONHECIMENTO DE MATRIZES E O ENVIO DE MENSAGENS CODIFICADAS

Igor Sthaynny Costa do Nascimento<sup>(1)</sup>; Elizieb Luiz Liberato Pereira<sup>(2)</sup>; Mônica Paula de Sousa<sup>(3)</sup>;

1 *Universidade Federal do Semi-Árido*, igorsthaynny@gmail.com

2 *Universidade Federal do Semi-Árido*, elizieb@outlook.com

3 *Universidade Federal do Semi-Árido*, monica.sousa@ufersa.edu.br

### Resumo:

Aplicativos móveis desonestos são responsáveis por 28% dos ataques de fraudes observados pela RSA (2018), Rivest Shamir Adleman, no segundo trimestre de 2018 e mais de 70% das transações fraudulentas foram originadas no canal de telecomunicação. Sabendo disso mostraremos um método bastante intuitivo, com operações fáceis, que pode ser utilizado por pessoas comuns para enviar e receber mensagens com mais segurança. Assim, visando um entendimento geral, porém simplificado, utiliza-se matrizes com um conjunto de números para simplificar a manipulação das transformações de letras para números e vice-versa. No procedimento o remetente utiliza uma matriz para codificar a mensagem e o destinatário usa uma outra matriz associada à anterior por uma relação de inversão para decodificá-la. Dada a mensagem, cada letra é associada a um número que são ordenados em uma matriz. Para codificar, a mensagem é multiplicada com a matriz do remetente e o resultando é enviado como a matriz resultante. Para decodificar, o destinatário utiliza sua matriz e multiplica pela matriz recebida, resultando na matriz original, assim podendo converter para suas letras associadas. Portanto, tem-se por finalidade mostrar a importância de divulgar um conhecimento científico que torna a tecnologia mais segura, já que a criptografia é um método aplicável em qualquer meio de comunicação, basta que haja os três objetos: o emissor, o transformador e o receptor, e que a segurança a partir da troca de informações ao utilizar esses métodos seja de forma discreta entre emissor e receptor, inclusive a existência de duas matrizes invertíveis em suas mensagens.

**Palavras chaves:** Criptografia; Matriz; Codificar, Decodificar

### Introdução

Aplicativos móveis desonestos são responsáveis por 28% dos ataques de fraude observados pela RSA (2018) (empresa de segurança virtual) no segundo trimestre de 2018 e mais de 70% das transações fraudulentas foram originadas no canal telemóvel. O envio e o recebimento de informações sigilosas são necessidades comuns entre a população, para suprir isso surgiu a criptografia e formas de aplicá-la. Mostraremos um método bastante intuitivo com operações de fácil manejo sendo projetado para pessoas comuns, que poderá utilizar para enviar e receber mensagens com total segurança, de origem grega ela define a arte ou ciência de escrever mensagens em códigos, de forma que pessoas autorizadas possam decifrá-las, tão antiga quanto à própria escrita, já estava presente no sistema de escrita hieroglífica dos egípcios e os romanos utilizavam códigos secretos para comunicar planos de batalha. Com a Segunda Guerra Mundial estabeleceu-se a importância da informação e da criptografia.

### Metodologia

Iniciamos nossos estudos em livros, artigos e sites, tendo em vista a importância das mensagens codificadas e o sigilo ao trocar mensagens, sabendo que três bilhões de pessoas estão conectados (DIG 2017), cerca de 40% da população mundial. A busca por mensagens mais seguras se torna frequente e além disso, em função da segurança de dados trocados entre a população, de acordo com Gomes (2013), os jovens estão a cada dia mais migrando para a troca de mensagens. Os dados contidos nesta pesquisa foram organizados e discutidos objetivando informar pessoas que não têm muito conhecimento com matrizes e operações matriciais.

Visando um entendimento geral e simplificado, mostrando ser um assunto atrativo e de fácil manipulação até mesmo para as pessoas sem prática no uso de operações matemáticas envolvendo matrizes, como a utilização de matriz para abranger um conjunto maior de números e simplificar a manipulação das transformações de letra para número e vice-versa, tendo em vista que dentre muitos métodos de criptografia esse é bem mais simples que alguns usados por grandes empresas para manter suas informações em sigilo, mas a garantia que queremos é de total compreensão e aplicação dessa técnica por qualquer pessoa que não tenha um conhecimento muito amplo com matrizes.

## Resultados e discussão

O procedimento envolve matrizes, onde uma matriz  $m \times n$ , com  $m$  e  $n$  números naturais não nulos, que são toda tabela composta por  $m \times n$  elementos dispostos em  $m$  linhas e  $n$  colunas, em geral, representada por uma letra maiúscula do nosso alfabeto ( $A, B, \dots, Z$ ), enquanto os seus termos são representados pela mesma letra, desta vez minúscula, acompanhada de dois índices ( $a_{11} \ a_{12} \ a_{13} \ \dots \ a_{mn}$ ), onde o primeiro representa a linha e o segundo a coluna em que o elemento está localizado.

O produto de uma matriz  $A = (a_{ij})_{m \times p}$  e  $B = (b_{ij})_{p \times n}$ , que gera a matriz  $C = (c_{ij})_{m \times n}$ , onde o número de colunas de  $A$  tem que ser igual ao número de linhas de  $B$ , em que cada elemento  $c_{ij}$  é obtido por meio da soma dos produtos dos elementos correspondentes da  $i$ -ésima linha de  $A$  pelos elementos da  $j$ -ésima coluna de  $B$ .

$$A_{m \times p} \cdot B_{p \times n} = C_{m \times n}, \text{ onde } c_{ij} = a_{i1} \cdot b_{1j} + a_{i2} \cdot b_{2j} + \dots + a_{ip} \cdot b_{pj}.$$

E as matrizes inversas ou matriz invertível, aquelas que dada  $A$ , quadrada (número de linhas igual a colunas), de ordem  $n$ , existir uma matriz  $A'$ , de mesma ordem, tal que

$$A \cdot A' = A' \cdot A = I_n,$$

onde o produto de uma inversa com a matriz resulta na matriz identidade de ordem  $n$  (indicada por  $I_n$ ) quando os elementos da diagonal principal são todos iguais a 1 (um) e os elementos restantes são iguais a 0 (zero), sendo assim  $A'$  é matriz inversa de  $A$ . Representamos a matriz inversa por  $A^{-1}$ .

Assim, para a criptografia, primeiro converte-se as letras em números e depois se agrupa-se os números  $k$  a  $k$ , onde  $k$  é um número natural, e multiplicando-se cada grupo por uma matriz quadrada de ordem  $n$  invertível (ou seja, determinante diferente de zero). Os números resultantes são novamente passados para letras, e assim tem-se a mensagem codificada.

Descrevemos abaixo um método bastante simples, para codificar e decodificar mensagens, que envolve apenas um par de matrizes de tamanho  $n$ ,  $A$  e  $A^{-1}$ , cujos elementos

devem ser números inteiros. Primeiramente ilustramos o método utilizando uma matriz  $A$  e a sua inversa  $A^{-1}$ .

Sejam uma matriz  $A_{2 \times 2}$  cuja primeira linha é formada pelos números 3 e 1, já a segunda os números 2 e 1, e  $A^{-1}_{2 \times 2}$  cuja primeira linha é formada pelos números 1 e  $-1$ , já a segunda os números  $-2$  e 3, tal que

$$AA^{-1} = A^{-1}A = I.$$

A matriz  $A$  é apropriada, pois seus elementos são números inteiros, assim como os da matriz  $A^{-1}$ .

O remetente vai usar a matriz  $A$  para *codificar* a mensagem, e o destinatário vai usar a matriz  $A^{-1}$  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 alternativas não ajudem em nada a um decodificador não amigável.

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

<i>A ou Ã</i>	<i>B</i>	<i>C ou Ç</i>	<i>D</i>	<i>E</i>	<i>F</i>	<i>G</i>	<i>H</i>	<i>I</i>	<i>J</i>	<i>K</i>	<i>L</i>
01	02	03	04	05	06	07	08	09	10	11	12
<i>M</i>	<i>N</i>	<i>O ou Õ</i>	<i>P</i>	<i>Q</i>	<i>R</i>	<i>S</i>	<i>T</i>	<i>U</i>	<i>V</i>	<i>W</i>	<i>X</i>
13	14	15	16	17	18	19	20	21	21	22	23
<i>Y</i>	<i>Z</i>	<i>.</i>	<i>,</i>	<i>#</i>							
25	26	27	28	29							

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, e entre outros).

Suponha que “TECNOLOGIA DA INFORMAÇÃO” é a mensagem a ser codificada e transmitida. Para convertê-la para a forma numérica, usamos a correspondência entre letras e números exibida acima:

<i>T</i>	<i>E</i>	<i>C</i>	<i>N</i>	<i>O</i>	<i>L</i>	<i>O</i>	<i>G</i>	<i>I</i>	<i>A</i>	<i>#</i>	<i>D</i>	<i>A</i>	<i>#</i>	<i>I</i>	<i>N</i>	<i>F</i>	<i>O</i>	<i>R</i>	<i>M</i>	<i>A</i>	<i>Ç</i>	<i>Ã</i>	<i>O</i>
20	05	03	14	15	12	15	07	09	01	29	04	01	29	09	14	05	15	18	13	01	03	01	15

Uma vez que a matriz codificadora  $A$  é uma matriz  $2 \times 2$ , arrumamos nossa sequência de números como os elementos de uma matriz com duas linhas formando uma matriz  $M_{2 \times 12}$ .

Caso a mensagem tem um número ímpar de elementos, completamos o fim da segunda linha com o número 29 que está associado ao símbolo #. Para codificação da mensagem multiplicamos a matriz  $M$  à esquerda pela matriz codificadora  $A$ :

$$N = AM$$

Os elementos de  $N$  constituem a mensagem codificada, e utilizaremos vírgulas entre esses elementos para maior clareza: 61, 44, 18, 56, 50, 51, 63, 34, 28, 6, 88, 27, 41, 39, 15, 42, 35, 39, 48, 27, 19, 5, 59, 23.

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

$$A^{-1}N = A^{-1}AM = IM = M.$$

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

Vejam os:

$$M = A^{-1}N$$

ou seja, resulta em  $M_{2 \times 12}$  cuja a primeira linha é formada pelos números 20, 05, 03, 14, 15, 12, 07, 09, 01, 29 e 04, já a segunda os números 01, 29, 14, 05, 15, 18, 13, 01, 03, 01 e 15.

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

20	05	03	14	15	12	07	09	01	29	04	01	29	09	14	05	15	18	13	01	03	01	15	
T	E	C	N	O	L	O	G	I	A	#	D	A	#	I	N	F	O	R	M	A	Ç	Ã	O

## Conclusões

Sendo assim, a partir do estudo de matrizes é perceptível que a álgebra linear, e a matemática, sempre estiveram muito presente nas áreas tecnológicas, gerando um avanço substancial nos últimos séculos. Os métodos utilizados nessas áreas são indispensáveis para a execução e o aprimoramento de tarefas diversificadas já que, segundo o G1 (2018), 75 bilhões de pessoas em todo o mundo usam o serviço de bate-papo, e a aplicação destes conhecimentos tornou possível e mais eficaz a forma como se comunicam garantindo a integridade das informações.

Assim, popularizar esse conhecimento científico que fundamenta a tecnologia permite orientar que as informações estão cada vez mais importantes e a descobertas desses dados podem ocasionar riscos um vez que há pessoas com atitudes ilícitas (crackers) cada vez mais preparados. A criptografia é um método viável e aplicável em qualquer meio de comunicação basta que haja os três objetos o emissor, o transformador e o receptor, e que a segurança a partir da troca de informações ao utilizar esses métodos seja de forma discreta entre emissor e receptor, inclusive a existência de duas matrizes invertíveis em suas mensagens.

## Referências

- DIG. **3 bilhões de pessoas no mundo usam redes sociais ativamente.** 2017. Disponível em: <<https://www.digai.com.br/2017/08/3-bilhoes-pessoas-mundo-usam-redes-sociais/>>. Acesso em: 17 ago. 2018.
- G1. **WhatsApp bate recorde de mensagens trocadas no Ano Novo.** 2018. Disponível em: <<https://g1.globo.com/economia/tecnologia/noticia/whatsapp-bate-recorde-de-mensagens-trocadas-no-ano-novo.ghtml>>. Acesso em: 10 ago. 2018.
- GOMES, Helton Simões. **Jovens brasileiros trocam Facebook por aplicativos de mensagens.** 2013. Disponível em: <<http://g1.globo.com/tecnologia/noticia/2013/11/jovens-brasileiros-trocam-facebook-por-aplicativos-de-mensagens.html>>. Acesso em: 17 ago. 2018.
- RSA. **Security Solutions to Address Cyber Threats.** Disponível em: <<https://www.rsa.com/>>. Acesso em: 18 ago. 2018.