CRIPTOGRAFIA DE DADOS UTILIZANDO MATRIZES

[1]**Eduardo Elias Pereira** – eduardo.pereira89@hotmail.com
[1]**Gláucio Barbosa de Souza** – glauciocomputacao@gmail.com
[1]**Rhuan Gonzaga da Cunha** – rhuangonzaga@gmail.com
[1]**Vinícius Spneli Forzan Silva** – viniciusspinelle@gmail.com
[2]**Fausto Rogério Esteves** – fausto-rogerio@hotmail.com
[2]**Patrícia Carolina de Souza Pereira** – patricia.souza@unifenas.br

RESUMO

A Criptografia surgiu da necessidade de guardar mensagens secretas, consideradas importantes, onde somente o remetente e o destinatário poderiam interpretá-las, tornando difícil o acesso por pessoas não autorizadas. Atualmente a criptografia é muito utilizada em situações nas quais é necessária uma comunicação confidencial (privada), como por exemplo: via internet, em caixas eletrônicos, em transações eletrônicas, entre outros. A criptografia atual é constituída por estudo de algoritmos criptográficos que podem ser implantados em computadores. As matrizes são usadas na criptografia para codificar e decodificar mensagens, sendo que o remetente usará uma chave para codificar e o destinatário usará outra chave para decodificar.

Palavras chave: Criptografia, Matrizes

ABSTRACT

Encryption arose from the need to keep secret messages, considered important, where only the sender and the recipient might interpret them, making it difficult for unauthorized persons. Currently encryption is often used in situations where a private communication is required (private), eg: via the Internet, at ATMs in electronic transactions, among others. The current encryption consists of study of cryptographic algorithms that can be deployed on computers. The arrays are used in cryptography to encode and decode messages, wherein the sender uses a key to encrypt and the recipient uses another key to decrypt. Keywords: Cryptography, Arrays

---

[1]Acadêmico do Curso Bacharelado em Ciência da Computação, UNIFENAS.
[2]Docente do Curso Bacharelado em Ciência da Computação, UNIFENAS.

1 INTRODUÇÃO

Desde a época do Antigo Egito, era necessário guardar mensagens secretas, onde somente algumas pessoas podiam decifrar.

A criptografia vem do Grego, *Kryptós*que, significa secreto e*gráphein*que 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.

O interesse pelo assunto tem aumentado significativamente devido a necessidade de manter a privacidade (MENEZES,2013).

Por ser formada por algoritmos criptográficos, a álgebra linear é de grande importância aos estudantes de computação, matemáticos, profissionais de segurança de informação e especialistas em estatística, diretamente ligados aos sistemas de informação (ZATTI,2010).

O desenvolvimento das matrizes ocorreu a partir do século XIX, apesar de ter representações de números semelhantes às matrizes modernas desde a Era Cristã, com matemáticos como Arthur Cayley, Augustin-Louis Cauchy e William Rowan Hamilton. Recentemente, com as planilhas eletrônicas de computador, podem ser feitos cálculos antes realizados à mão, de maneira cansativa e lenta. Essas planilhas, em geral, são formadas por tabelas que armazenam os dados utilizados (BARICHELLO,[2013?]).

Este artigo tem como objetivo analisar os métodos criptográficos existentes e demonstrar a utilização das matrizes para a criptografia.

2 REVISÃO DE LITERATURA

2.1 Tipos de criptografia

2.1.1 Criptografias Simétricas

É uma técnica muito antiga e também muito conhecida. Um número, uma palavra ou uma sequência de letras aleatórias pode ser uma chave secreta. É aplicada à mensagens pra alterá- las de alguma maneira(GUIMARÃES, 2001).

O remetente e o destinatário podem criptografar e descriptografar todas mensagens, contando que saibam a chave secreta. Os algoritmos usados na Criptografia Simétrica são menos complexos que na Criptografia Assimétrica pelo fato de que a mesma chave é usada tanto para criptografar quanto para descriptografar os dados, sendo este ponto uma grande desvantagem da Criptografia Simétrica (GALVÃO, 2007).

2.1.2 Criptografias Assimétricas

Neste caso existem duas chaves, sendo uma Pública e outra Privada. A chave pública é disponibilizada a qualquer pessoa que queira enviar algum tipo de mensagem e a chave privada é mantida em total sigilo (GALVÃO, 2007).

Qualquer mensagem que seja criptografada usando a chave privada somente poderá ser descriptografada fazendo o uso da chave pública correspondente e qualquer mensagem que seja criptografada usando a chave pública somente poderá ser descriptografada fazendo uso da chave privada (GALVÃO,2007).

Em conjunto essas chaves são conhecidas como Par de Chaves.

2.2 Métodos criptográficos

2.2.1 Cifras de HILL

O processo de cifras de Hill consiste em transformar pares sucessivos de texto em texto cifrado, através da escolha de uma matriz 2x2 A, e uma tabela com valores numéricos para todas as letras do alfabeto. Cada par de letras do texto se transforma em um vetor-coluna p através do seu correspondente valor numérico, e o produto Ap é convertido em seu equivalente alfabético. Como o alfabeto possui 26 letras, e a multiplicação de Ap pode resultar em um vetor coluna com números maiores que 26, é utilizado a teoria dos conjuntos dos resíduos módulo 26 para fazer a correspondência da tabela. O processo de decodificação que tem que ser realizado pelo receptor é semelhante ao de codificação, com apenas uma diferença, usando a inversa da matriz de codificação na multiplicação pelas matrizes colunas dos pares de letras do texto codificado (ZATTI,2010).

2.2.2 Cifras de substituição

Consiste em um método onde unidades de texto são substituídas por unidades de textos cifrados, sendo regulares e pré-determinados, podendo ser números, letras, par de letras, trilhas de letras ou simplesmente uma combinação de todos. O receptor deve fazer a substituição inversa para recuperar uma mensagem cifrada. Se a unidade de substituição tiver frases ou palavras inteiras o sistema é habitualmente dito ser um código, não uma cifra (SARAIVA *et al*, 2011).

Tipos de cifras de substituição: Substituição simples (Opera com letras isoladas), Substituição poligráfica (opera com grupos de letras), entre outras (SARAIVA *et al*,2011).

2.2.3. Método Matriz

Semelhante ao de substituição e transposição, com ênfase diferente. Tem como objetivo tornar o algoritmo mais complexo e pode ser aplicado como introdução às Matrizes (SARAIVA *et al*,2011).

2.2.4 Método Permutacional

O mais utilizado antes da existência do computador, este era o método que mais se utilizava. Para gerar uma cifra permutacional bastava aplicar uma das 26! Permutações das letras do alfabeto. Este método pode ser aplicado na introdução de Análise Combinatória ou em Funções (SARAIVA 2011).

2.2.5 Método RSA

Atualmente é o método mais utilizado e conhecido em aplicações comerciais na internet. Permite a identificação do documento, criptografar dados, criar e verificar assinaturas digitais. Este método é baseado no problema do logaritmo discreto (OLIVEIRA,2012).

2.2.6 SSL e TLS

O *TransportLayer Security* (TLS) e o seu predecessor *Secure Sockets Layer (*SSL), são protocolos criptográficos que fornecem segurança para comunicação em redes inseguras, como a Internet. Estes protocolos cifram na camada de aplicação, os segmentos que trafegam nas conexões de rede, garantindo assim um tráfego seguro no nível de camada de transporte. O TLS é especificado pela RFC 5246, enquanto o SSL foi especificado pela Netscape. O TLS utiliza segurança baseada no algoritmo assimétrico RSA com chave de 1024 e 2048 bits. Após a conexão ser estabelecida, o cliente e o servidor negocia uma suíte de cifração baseada em criptografia simétrica (COSTA, 2010).

2.3 Matrizes e criptografia

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

Segue um exemplo abaixo de matrizes onde a matriz A irá codificar a mensagem e o destinatário usará a matriz B para descodificar (ZATTI,2010).

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

Figura 1 - Matriz A e B

O primeiro passo para codificar a mensagem é fazer sua conversão da forma alfabética para forma numérica.

Utilizaremos a tabela abaixo:

Tabela 1 – Tabela alfanumérica

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10
K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20
U	V	W	X	Y	Z	.	!	#	
21	22	23	24	25	26	27	28	29	30

Tanto o remetente quanto o destinatário devem estar cientes desta tabela. Vamos codificar a seguinte frase: “MEU FUTURO DEPENDE DE MIM”.

MEU#FUTURO#DEPENDE#DE#MIM

13 5 21 29 6 21 20 21 18 15 29 4 5 16 5 14 4 5 29 4 5 29 13 9 13

O símbolo # serve para não haver erros de leitura na língua portuguesa após a decodificação da mensagem.

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.

$$M = \begin{pmatrix} 13 & 5 & 21 & 29 & 6 & 21 & 20 & 21 & 18 & 15 & 29 & 4 & 5 \\ 16 & 5 & 14 & 4 & 5 & 29 & 4 & 5 & 29 & 13 & 9 & 13 & 30 \end{pmatrix}$$

Figura 2 - Matriz M

Para codificar a mensagem, multiplicamos a matriz A por M, tal que N=AM:

$$N = \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 13 & 5 & 21 & 29 & 6 & 21 & 20 & 21 & 18 & 15 & 29 & 4 & 5 \\ 16 & 5 & 14 & 4 & 5 & 29 & 4 & 5 & 29 & 13 & 9 & 13 & 30 \end{bmatrix}$$

$$N = \begin{bmatrix} 55 & 20 & 77 & 91 & 23 & 92 & 64 & 68 & 83 & 58 & 96 & 25 & 45 \\ 42 & 15 & 56 & 62 & 17 & 71 & 44 & 47 & 65 & 43 & 67 & 21 & 40 \end{bmatrix}$$

Figura 3 - Matriz resultante A*M

A matriz N apresenta a mensagem codificada**: 55, 20, 77, 91, 23, 92, 64, 68, 83, 58, 96, 25,**

45, 42, 15, 56, 62, 17, 71, 44, 47, 65, 43, 67, 21, 40.

O destinatário, no momento em que receber a mensagem codificada, usará a matriz B para decodificar e ler a mensagem.

Sabendo que B.N=B.A.M=I.M = M, temos que M = B.N.

Multiplicamos a matriz B por N, assim, obteremos o seguinte resultado:

$$M = \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 55 & 20 & 77 & 91 & 23 & 92 & 64 & 68 & 83 & 58 & 96 & 25 & 45 \\ 42 & 15 & 56 & 62 & 17 & 71 & 44 & 47 & 65 & 43 & 67 & 21 & 40 \end{bmatrix}$$

$$M = \begin{bmatrix} 13 & 5 & 21 & 29 & 6 & 21 & 20 & 21 & 18 & 15 & 29 & 4 & 5 \\ 16 & 5 & 14 & 4 & 5 & 29 & 4 & 5 & 29 & 13 & 9 & 13 & 30 \end{bmatrix}$$

Figura 4 - Matriz resultante B*M

Enfim chegamos à matriz M=B.N do remetente que é a mensagem original.

Em seguida é só reverter os números utilizando novamente a tabela alfanumérica**. 13 5 21 29 6 21 20 21 18 15 29 4 5 16 5 14 4 5 29 4 5 29 13 9 13**

MEU#FUTURO#DEPENDE#DE#MIM

3 CONCLUSÃO

A criptografia permite ou possibilita evitar violações nas informações que são consideradas secretas, principalmente por meios onde são utilizadas senhas, garantindo com segurança que as informações não serão copiadas ou modificadas.

A criptografia é hoje considerada de extrema importância para as áreas de computação, matemática, profissionais de informação e especialistas em estatística.

A criptografia assimétrica é mais segura que a simétrica podendo ser utilizada em assinatura digital, porém, há uma grande desvantagem sendo mais lenta que a simétrica.

A cifra de Hill juntamente com os métodos criptográficos são opções muito importantes dentro da criptografia porque são de fácil entendimento e muito utilizados na área de computação.

Concluímos que é possível utilizar criptografia com matrizes sendo uma forma muito segura de criptografar mensagens com chaves de segurança, para que somente o remetente e o destinatário tenham acesso às mensagens originais.

REFERÊNCIAS

BARICHELLO, L. **Mensagens Secretas com Matrizes**. Unicamp. Campinas. SP. [2013?]. Disponível em: <http://m3.ime.unicamp.br/recursos/1020>. Acesso em: 25 de Out. 2015.

COSTA, B.M. **Segurança na Internet/ Protocolos SSL/TSL**. Rio de Janeiro.2010. Disponível em: <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2010_2/bernardo/tls.html>. Acesso em: 25 de Out. 2015.

GALVÃO,J. **Diferenças entre chaves simétrica e assimétrica para criptografia**. Sorocaba.2007. Disponível em: <https://pedrogalvaojunior.wordpress.com/2007/11/16/diferencas-entre-chaves-simetrica-e-assimetrica-para-criptografia/>. Acesso em: 25 de Out. 2015.

GUIMARÃES, C.R.**Criptografia para Segurança de Dados**. Uberlândia. 2001. Disponível em:<http://www.computacao.unitri.edu.br/downloads/monografia/79431146079328.pdf>. Acesso em: 25 de Out. 2015.

MENEZES, S**. Mensagens Secretas com Matrizes-Criptografia**. Rio De Janeiro. 2013. Disponível em: <http://www.ime.unicamp.br/~olimpiada/OficinaPrimavera/AtividadeFinal_Criptografia28092013.pdf>. Acesso em: 25 de Out. 2015.

SARAIVA,R.S.;et al.**Criptografia**:**A Importância Da Álgebra Linear para Decifrá-la**. Ozório.2011.Disponível em:<http://www.facos.edu.br/old/galeria/130072011050939.pdf>. Acesso em: 25 de Out. 2015.

OLIVEIRA, R. L. **Introdução à Criptografia RSA**. Presidente Prudente. 2012. Disponível em:<http://www.unoeste.br/site/enepe/2012/suplementos/area/Exactarum/Exatas%20e%20da%20Terra/Matem%C3%A1tica/INTRODU%C3%87%C3%83O%20A%20CRIPTOGRAFIA%20RSA.pdf>. Acesso em: 25 de Out. 2015.

ZATTI, S.B.**A Presençada Álgebra Linear e Teoria dos Números na Criptografia**. Santa Maria.2006. Disponível em:<http://www.unifra.br/eventos/jornadaeducacao2006/2006/pdf/artigos/matem%C3%A1tica/A%20PRESEN%C3%83A%20DA%20-LGEBRA%20LINEAR%20E%20TEORIA%20DOS%20N+MEROS%20NA%20CRIPT%C3%A0.pdf>. Acesso em: 25 de Out. 2015.