DESENVOLVIMENTO DE SOFTWARE PARA CODIFICAR MENSAGENS UTILIZANDO CONCEITOS DE ALGEBRA LINEAR

Douglas Araujo Silveira Modesto[1]
Danielle Cecilia Caldas Santos[2]
Aislan Silva Primo[3]

cadernos de graduação
ciências exatas e tecnológicas

Engenharia Elétrica

ISSN IMPRESSO 1980-1777
ISSN ELETRÔNICO 2316-3135

RESUMO

Desde o princípio da civilização os povos sentiam a necessidade de enviar mensagens com informações importantes, que caso caíssem em mãos erradas, poderiam trazer perdas no processo que aquela mensagem estaria informando e, muitas vezes, esta mensagem era interceptada por terceiros. Desta forma era necessário desenvolver uma forma de garantir que mesmo a mensagem caindo em mãos erradas, somente o destinatário poderia ser capaz de decifrá-la. Com base neste problema, foi desenvolvida a criptografia, que é representada por um conjunto de técnicas e princípios que permitem transformar uma informação em algo ilegível, de tal forma que somente possa ser entendida por seu destinatário, este, possuidor de uma chave. O presente trabalho visa a construção de um sistema que emprega conceitos de álgebra linear para realizar a codificação de mensagens entre um remetente e um destinatário, a fim de garantir que caso a mensagem seja interceptada durante sua transmissão, será impossível descobrir seu conteúdo, garantindo assim a segurança da informação.

PALAVRAS-CHAVES

Mensagem. Criptografia. Segurança.

ABSTRACT

From the beginning of civilization people felt the need to send messages with important information that should fall into the wrong hands, could bring losses in the process that this message would be telling, and often, this message was intercepted by others. Thus it was necessary to develop a way to ensure that the message even falling into the wrong hands, only the recipient might be able to decipher it. Based on this problem, the encryption was developed, which is represented by a set of techniques and principles for transforming an information into something unreadable, so that can only be understood by its recipient, this, possessor of a key. The present study aims to construct a system that employs linear algebra concepts to perform encoding of messages between a sender and a recipient in order to ensure that the same message being intercepted during transmission, it is impossible to find out its contents, thereby ensuring information security.

KEYWORDS

Message. Encryption. Security.

1 INTRODUÇÃO

Atualmente é difícil imaginar como seriam nossas vidas sem os meios de comunicação, utilizamos diversas formas de nos comunicar diariamente, sejam mensageiros, e-mails, redes sociais, dentre muitos outros, esta importância não se iniciou nos tempos atuais, por exemplo, na primeira guerra mundial, eram utilizados pombos-correios, pessoas para enviar mensagens e documentos secretos de um ponto para outro, sempre houve a comunicação, mesmo que em meios diferentes de propagação em relação aos dias atuais.

Porém, com a necessidade de se comunicar, surge também a preocupação com a segurança das informações passadas, porque muitas vezes precisamos enviar mensagens com informações sigilosas, como por exemplo, informações de documentos pessoais, senhas de banco, e-mails, contendo informações importantes, segredos pessoais, dentre muitos outros.

A segurança tratada se divide em duas partes essenciais, a primeira trata de dificultar o acesso à mensagem por terceiros e a segunda é garantir que caso alguma pessoa intercepte a mensagem durante seu trajeto, seja muito difícil de decifrar seu real conteúdo, ou até impossível. A esta segunda forma de segurança é chamada de criptografia, que é o tema chave deste trabalho.

A criptografia é a ciência que estuda formas de mascarar uma determinada mensagem, isto quer dizer que uma mensagem como "O clima está bom" poderia ser escrito de forma totalmente diferente e difícil de entender, algo como "121,124,490,2,345", de forma que somente o destinatário possuidor de uma chave e

do algoritmo utilizado poderia retomar ao conteúdo original da mensagem. Então, supondo que a mensagem caia em mãos erradas, seu conteúdo ainda assim estaria protegido, graças à criptografia empregada.

2 MÉTODOS DE CODIFICAÇÃO

Imaginemos que seja necessário criptografar a mensagem "vida" com a chave 1234, de conhecimento do remetente e destinatário, por meio do método de chave simétrica. De forma manual, deveremos seguir os passos demonstrados abaixo.

O primeiro passo é desenvolver uma tabela de conversão, que irá transformar cada caractere da mensagem em um número, esta tabela deverá ser de conhecimento do remetente e destinatário. Tomemos inicialmente como base a tabela de conversão abaixo:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	w	y	z
2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97	101

Desta forma, convertendo a mensagem em formato numérico, ficaria:

v	i	d	a
79	23	7	2

Como a matriz chave estará no formato 2x2, necessitamos que a matriz a ser codificada esteja no formato 2xN, onde N é o número de coluna. Esta condição deve ser seguida a fim de possibilitar a multiplicação entre as matrizes. Organizando o resultado obtido por meio da conversão, obtemos a seguinte matriz:

$$M = \begin{bmatrix} 79 & 23 \\ 7 & 2 \end{bmatrix}$$

Devemos também arrumar a matriz chave, para que ela esteja no formato ideal para a multiplicação das matrizes, como fizemos com a matriz M:

$$C = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

O próximo passo é realizar a multiplicação entre as matrizes C e M, onde o resultado será Mc, que é a matriz M em sua forma codificada:

$$Mc = C \times M = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 79 & 23 \\ 7 & 2 \end{bmatrix} = \begin{bmatrix} 93 & 27 \\ 265 & 77 \end{bmatrix}$$

A matriz Mc, será separada por vírgula, ficando no formato 93,27,265,77 que é a mensagem cifrada e protegida a ser enviada ao destinatário.

Para o destinatário descobrir o real conteúdo da mensagem "93,27,265,77", ele deverá estar portando a chave combinada anteriormente, neste caso a 1234 e a tabela de conversão. Primeiramente, ele deverá arrumar a matriz chave como o remetente fez, ficando no formato 2x2, como demonstrado abaixo:

$$C = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

Agora, deverá ser obtida a inversa de C, para isso devemos realizar uma multiplicação de C por uma matriz genérica (C^{-1}) de mesma ordem, cujo produto será igual à matriz identidade, conforme a demonstração abaixo:

$$C \times C^{-1} = I$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

O produto acima gera os seguintes sistemas de equações:

$$\begin{cases} a + 2c = 1 \\ 3a + 4c = 0 \end{cases}$$

$$\begin{cases} b + 2d = 0 \\ 3b + 4d = 1 \end{cases}$$

Ao resolver os sistemas lineares descritos acima, encontraremos o seguinte resultado:

$$C^{-1} = \begin{bmatrix} -2 & 1 \\ 1{,}5 & -0{,}5 \end{bmatrix}$$

De posse da chave inversa (C^{-1}), o destinatário deverá realizar a multiplicação entre C^{-1} pela matriz codificada Mc, e o resultado será exatamente a matriz anterior à codificação.

$$C^{-1} \times Mc = M$$

$$\begin{bmatrix} -2 & 1 \\ 1{,}5 & -0{,}5 \end{bmatrix} \times \begin{bmatrix} 93 & 27 \\ 265 & 77 \end{bmatrix} = \begin{bmatrix} 79 & 23 \\ 7 & 2 \end{bmatrix}$$

O último passo é converter a matriz M para o formato 79,23,7,2 e comparar com a tabela padrão e obter as letras correspondentes aos números.

v	i	d	a
79	23	7	2

Desta forma, a transferência da mensagem "vida" de forma segura foi concluída.

Agora imaginemos que seja necessária a codificação de uma mensagem com mais de mil letras, é facilmente perceptível que o trabalho manual seria imenso e demoraria várias horas, ou até dias e, considerando que as mensagens precisam ser passadas com velocidade, realizar a criptografia de forma manual para mensagens de tamanho considerável, é inviável.

Para resolver esta problemática, foi desenvolvido o software nomeado *HiddenCrip*, que possui a capacidade de realizar os processos da criptografia por chave simétrica de forma automática e rápida, englobando diversas melhorias e relação ao processo manual como, por exemplo:

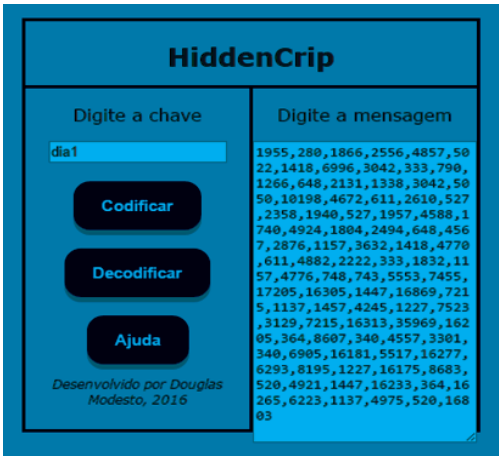
- Tabela de conversão mais complexa que engloba a maioria dos caracteres utilizados nas mensagens;
- Velocidade e praticidade na criptografia das mensagens;
- A chave de criptografia pode englobar não somente números, mas caracteres de diversos tipos;
- É possível realizar a criptografia diversas vezes, desta forma a mensagem ficará cada vez mais difícil de decifrar.

Este software funciona em qualquer dispositivo que possua um navegador de internet instalado, já que foi desenvolvido na linguagem HTML, junto com javascript e CSS, abrangendo, desta forma diversos tipos de dispositivos.

Vejamos o funcionamento do software desenvolvido por meio de um exemplo:

Mensagem a ser criptografada: "Pensar é apenas seguir, raciocinar é juntar dados, e refletir é avaliar o que vale a pena", chave utilizada: "dia1".

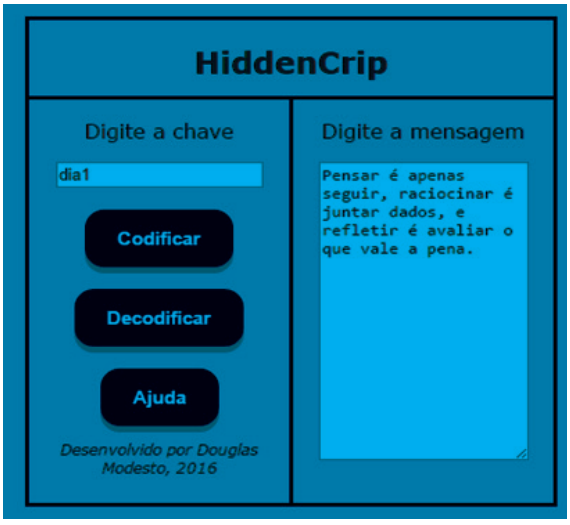
Figura 1 – Exemplo de funcionamento do HiddenCrip



Fonte: Autores.

O procedimento é inserir a mensagem no campo mensagem e a chave no campo da chave, conforme demonstrado na Figura 1:

Figura 2 – Exemplo de funcionamento do HiddenCrip



Fonte: Autores.

Após a inserção o usuário deverá clicar no botão "Codificar" e no campo onde estava a mensagem digitada ela aparecerá em sua forma criptografada. O resultado obtido pode ser visto na Figura 2:

Agora basta que o usuário copie a mensagem gerada e envie para seu destinatário, assim que o mesmo receber a mensagem deverá inseri-la a chave e a mensagem recebida, em seguida clicar em "Decodificar". O resultado obtido será a real mensagem, conforme a Figura 1.

Desta forma o processo de transmissão da mensagem de forma segura estará completo.

3 CONCLUSÃO

A criptografia é uma grande ferramenta para garantir a segurança nos meios de comunicação, este trabalho demonstrou somente uma forma de aplicação desta ciência, que é bastante abrangente e aperfeiçoada a cada dia, com a construção desse sistema foi possível entender o funcionamento da criptografia, em especial o método da chave simétrica, bem como aplicar diversos conceitos aprendidos na disciplina de álgebra linear, o que contribuiu de forma significativa para nossa evolução acadêmica.

REFERÊNCIAS

CALLIOLI, C.A; DOMINGUES, H.H.; COSTA, R.C.F. **Álgebra linear e aplicações.** 4.ed. São Paulo: Atual, 1983.

STEINBRUCH, A; WINTERLE, P. Álgebra **Linear**. 2.ed. São Paulo: Pearson Makron Books, 2008.

Data do recebimento: 3 de Dezembro de 2017
Data da avaliação: 5 de Dezembro de 2017
Data de aceite: 12 de Dezembro de 2017

1 Graduando em Engenharia Elétrica na Universidade Tiradentes – UNIT. E-mail: douglasmodesto10@hotmail.com
2 Graduanda em Engenharia Elétrica na Universidade Tiradentes – UNIT. E-mail: ceciliacaldas2014@gmail.com
3 Professor Especialista do Curso de Engenharia Elétrica da Universidade Tiradentes – UNIT. E-mail: aislanprimo14@gmail.com