XIX Congresso Nacional de Estudantes de Engenharia Mecânica - 13 a 17/08/2012 – São Carlos-SP
Artigo CREEM2012

A CRIPTOGRAFIA COMO UMA APLICAÇÃO DA TEORIA DE ÁLGEBRA LINEAR

Valéria Bueno Nascimento, Leonardo Conti, Ligia Laís Fêmina*
UFU, Universidade Federal de Uberlândia, Curso de Engenharia Mecânica
Campus Santa Mônica – Av. João Naves de Ávila, n°2121 - Bairro Santa Mônica – CEP 38.408-100 – Uberlândia - MG
E-mail para correspondência: valeria_buenonascimento@hotmail.com
* Professora Orientadora, Faculdade de Matemática- UFU

Introdução

Criptografia, basicamente, são códigos secretos, que seguem um padrão preestabelecido e que a partir desse padrão (denominado "chave" na linguagem da criptografia), é possível se comunicar com certo nível de segurança. Os primeiros relatos do uso de uma escrita secreta foram na Grécia antiga. Posteriormente, em Roma, nas guerras de Gália de Júlio César, passou se a usar um tipo simples de Criptografia, chamado substituição. A partir desse momento, a criptografia se destacou sendo utilizada com fins militares ou em situações que envolviam pessoas importantes e informações extremamente sigilosas.

Objetivos

O objetivo desse trabalho é explicar um método específico da Criptografia: As Cifras de Hill, que foi inventado em 1929 por Lester S. Hill. O presente trabalho mostra como é composto esse método, suas etapas de codificação e decodificação.

Metodologia

Para explicar o procedimento de codificação das Cifras de Hill, é necessário basear-se em ferramentas da Álgebra Linear e da Aritmética Modular.

Da Álgebra Linear são utilizadas as matrizes e operações matriciais (multiplicação de matrizes e conhecimentos a respeito de matrizes inversas). Além de conceitos sobre independência linear e transformações lineares.

A seguir, alguns conceitos da Aritmética Modular utilizado nesse trabalho:

Definição 1: Dado um número inteiro positivo *m* e dois inteiros *a* e *b* quaisquer, dizemos que *a* é equivalente a *b* módulo *m*, e escrevemos $a = b (\text{mod } m)$ se $a - b$ é um múltiplo inteiro de *m.*

Dado um módulo *m*, qualquer inteiro *a* é equivalente, módulo *m*, a exatamente um dos inteiros $0, 1, 2, \ldots, m-1$. Esse inteiro é chamado o resíduo de *a* módulo *m* e $Z_m = \{0, 1, 2, \ldots, m-1\}$ é o conjunto dos resíduos de *a* módulo *m*.

Definição 2: Dado um número inteiro *a* em Z_m, dizemos que um número a^{-1} em Z_m é um inverso multiplicativo de *a* módulo *m* se $a a^{-1} = 1 (\text{mod } m)$.

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, usa-se a inversa da matriz de codificação na multiplicação pelas matrizes colunas dos pares de letras do texto codificado.

Resultado

Seguindo a tabela de correspondência de letras e números abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

Considere o texto DIA ALEGRE e a matriz $A=\begin{bmatrix}1 & 3\\ 2 & 1\end{bmatrix}$

Vamos iniciar o processo de codificação:

1° - Agrupam-se as letras duas a duas sucessivamente. Caso haja um número ímpar de letras, coloca-se uma última letra fictícia para completar o último par e forma se a matriz-coluna de cada par.

D I A A L E G R E E* *esta última é a letra fictícia.

$\begin{bmatrix}4\\9\end{bmatrix}\quad\begin{bmatrix}1\\1\end{bmatrix}\quad\begin{bmatrix}12\\5\end{bmatrix}\quad\begin{bmatrix}7\\18\end{bmatrix}\quad\begin{bmatrix}5\\5\end{bmatrix}$

2º - Em seguida, fazemos a multiplicação da matriz escolhida para a codificação por cada matriz-coluna. Obteremos:

$\begin{bmatrix}1 & 3\\ 2 & 1\end{bmatrix}\begin{bmatrix}4\\9\end{bmatrix}=\begin{bmatrix}31*\\17\end{bmatrix}=\begin{bmatrix}5\\17\end{bmatrix}$ $\quad\begin{bmatrix}1 & 3\\ 2 & 1\end{bmatrix}\begin{bmatrix}1\\1\end{bmatrix}=\begin{bmatrix}4\\3\end{bmatrix}$ $\quad\begin{bmatrix}1 & 3\\ 2 & 1\end{bmatrix}\begin{bmatrix}12\\5\end{bmatrix}=\begin{bmatrix}27*\\29*\end{bmatrix}=\begin{bmatrix}1\\3\end{bmatrix}$

$\begin{bmatrix}1 & 3\\ 2 & 1\end{bmatrix}\begin{bmatrix}7\\18\end{bmatrix}=\begin{bmatrix}61*\\32*\end{bmatrix}=\begin{bmatrix}9\\6\end{bmatrix}$ $\quad\begin{bmatrix}1 & 3\\ 2 & 1\end{bmatrix}\begin{bmatrix}5\\5\end{bmatrix}=\begin{bmatrix}20\\15\end{bmatrix}$

**Observação:* Seguindo a teoria de Aritmética Modular, quando a matriz-coluna encontrada de cada par contiver números maiores que 25, usa-se o resto da divisão deste por 26.

Feito isso, substitui-se os números, por seus correspondentes na tabela dada acima.

Assim, encontramos o seguinte texto codificado: *EQDCACIFTO*.

Conclusões

A Cifra de Hill é uma opção muito interessante dentro da criptografia. Por ser baseado em princípios básicos da Álgebra Linear, esse método se torna de fácil entendimento e é muito utilizado na elaboração de programas computacionais. Aplicações como a Cifra de Hill despertam o interesse para o aprendizado de Álgebra Linear, uma vez que embora a Álgebra Linear seja um campo abstrato da Matemática, ela tem um grande número de aplicações dentro e fora da mesma. Assim a Álgebra Linear aplicam-se a várias áreas, em especial às Engenharias.

Referências Bibliográficas

Anton, H., Rorres, C., "Àlgebra Linear com Aplicações", Bookman Companhia Editora, Porto Alegre, RS, 2001.

Callioli, C., Domingues, H.H., Costa, R.C.F., "Álgebra linear e aplicações.", Editora Atual, São Paulo, SP, 1983.

Domingues, H. H., Iezzi, G., "Álgebra Moderna", Atual, São Paulo, SP, 2003.

Kolman, B.; Hill, D.R., "Introdução à Álgebra Linear com Aplicações", Tradução:Alesandra Bosquilha. Rio de Janeiro: LTC, 8ª ed, 2006.

Konheim, A. G., "Cryptography: a Primer", Wiley-Interscience, New York , USA, 1981.

Lima, E. L., "Álgebra Linear". Coleção Matemática Universitária, SBM, Rio de Janeiro,1995.

Sinkov, A., "Elementary Cryptanalysis: a Mathematical Approach", Mathematical Association of America,Washington, USA, 1966.