Criptografia como aplicação da Álgebra Linear: Construção de um programa para a execução da Cifras de Hill

Camila Santos Correa*[1], Rafael Brito Teixeira[1], Ricardo da Silva Reis[1], Polyane Alves Santos[2].

1. Estudante de Engenharia Elétrica do Instituto Federal de Educação, Ciência e Tecnologia da Bahia, campus Vitória da Conquista; *camilacorreacs.cs@gmail.com
2. Professora de Matemática no Instituto Federal de Educação, Ciência e Tecnologia da Bahia- IFBA.
Palavras Chave: *Criptografia, Álgebra Linear, Matrizes.*

Introdução

O envio e o recebimento de informações sigilosas são necessidades antigas, que existem há milhares de anos. Com o surgimento da globalização e da rede mundial de computadores que propõe facilidade de transmitir dados de maneira precisa e rápida, a criptografia tornou-se uma área de fundamental estudo para garantir melhor segurança no acesso e transmissão da informação.

A criptografia é um conjunto de técnicas que visa camuflar informação de acesso não autorizado. O principal objetivo é transformar um conjunto de dados legíveis em uma sequência desordenada de caracteres, impossibilitando a compreensão do seu conteúdo.

Antigamente, a criptografia era realizada através dos métodos de substituição e transposição das letras que compunha a mensagem. O Código de César, por exemplo, funciona deslocando as letras do alfabeto de acordo com a chave. No entanto, este método não é tão seguro, pois o número de possibilidades é pequeno.

Na criptografia, existem dois métodos pelos quais podem ser feitos o processo de cifragem e decifragem dos sistemas criptográfico. São eles: o método de chaves públicas e o método de chave privada. A ideia básica da utilização de chave pública é a eliminação da necessidade de utilização de um canal eficiente e de alta segurança para a distribuição de chaves.

Esse trabalho objetivou um estudo sobre criptografia e os métodos utilizados no decorrer de sua história. Especificamente, esse artigo visa a aplicação da álgebra linear como ferramenta para o funcionamento do criptosistema chamado Cifras de Hill, que foi proposta pelo matemático norte americano Lester S. Hill em 1929.

Resultados e Discussão

Para o desenvolvimento deste trabalho, foi elaborado um programa em linguagem C para a execução da criptografia de uma informação através dos procedimentos das Cifras de Hill. A forma básica de se criptografar, parte da transformação dos caracteres da mensagem através de matrizes. Para a realização desse estudo e da construção do programa foi utilizado a metodologia [1]FIARRESGA.

A cifras de Hill é uma classe de sistemas poligráficos que são baseados em transformações matriciais, que consistem em transformações lineares de R^n em R^m. A condição para uma transformação ser matricial é se, e somente se, as seguintes relações valem para todos os vetores u e v em R^n e qualquer escalar c.

(a) $T(u + v) = T(u) + T(v)$
(b) $T(cv) = cT(v)$

Após a verificação dessa condição o primeiro procedimento a realizar é converter as letras que compõe a mensagem em números, depois agrupa-se os números n a n e multiplica-se por uma matriz quadrada A 3x3, exemplo utilizado no programa. Esta matriz quadrada é a chave e deve-se ser invertível, ao digitar uma matriz quadrada qualquer no programa, ele calculará seu determinante se det A ≠ 0, então a matriz admite inversa.

A matriz que representa a informação será multiplicada pela matriz quadrada. Assim quando a matriz resultante for transformada em letras, de acordo com a Tabela 1, a mensagem estará diferente e ilegível, concluindo a codificação da mensagem.

Tabela 1. Correspondência entre letras e números.

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Para acesso a informação codificada é necessário a chave para a decodificação. A chave no criptosistesma em estudo é a matriz inversa da matriz digitada pela pessoa. Note que a chave que codifica é diferente da que decodifica.

Para decifrar utilizando as cifras de Hill, usamos a inversa da matriz codificadora. No programa criado, ao digitar a chave ocorrerá a multiplicação da matriz codificada pela matriz inversa, obtendo assim acesso à informação desejada. Os resultados podem ser observados na Figura1.

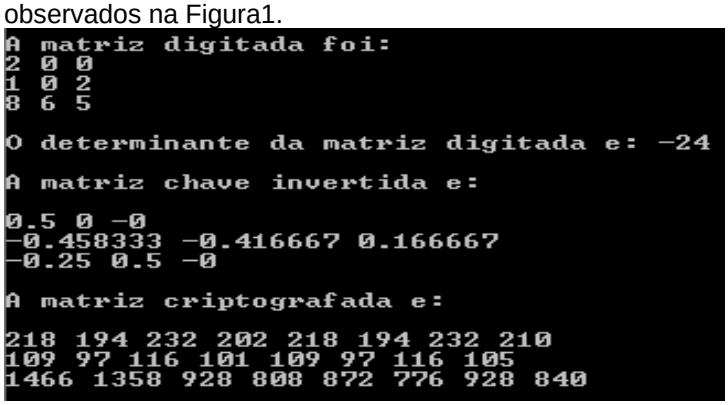

Figura 1. Compilação do Programa para codificadar.

Conclusões

A partir desse breve estudo é perceptível a importância e as contribuições da matemática para o avanço da criptografia. Os métodos que envolvem a álgebra se tornaram imprescindíveis para o aprimoramento e execução segura de determinadas tarefas. A aplicação destes conhecimentos tornou possível e mais eficaz a forma como as pessoas se comunicam e garantem a integridade de informações.

Agradecimentos

Ao IFBA e a Professora Polyane pelo seu suporte e incentivo.

[1]FIARRESGA, V. M. C. *Criptografia e Matemática* .2010. 161 f. Dissertação (Mestrado em matemática) – Faculdade de ciências da Universidade de Lisboa. Setembro 2010.