"CRIPTOGRAFIA: A Importância da Álgebra Linear para Decifrá-la

Darlan da Silva Godinho, Grasiela de Lima Cesario, Juciane Neubert dos Reis, Rodrigo Soares Saraiva

Faculdade Cenecista de Osório (FACOS)
Rua 24 de Maio, 141 – 95.520-000 – Osório – RS – Brasil

darlan.godinho@uol.com.br, grasiela-cesario@bol.com.br,{jucyane-reis,rodrigosaraiva19}@hotmail.com

Resumo. *Criptografia é técnica de escrever mensagens em cifras ou códigos com o intuito de manter sigilo sobre as informações. Também é bastante utilizada como meio de conferir segurança às operações realizadas no cotidiano como acesso a Sistemas de caixas eletrônicos, home-banking, pay-per-view e páginas da internet, em especial as que pedem senha. Atualmente, a criptografia, dado o grau de sofisticação e embasamento teórico que envolve o seu estudo, é considerada uma ciência no campo das Ciências Exatas, sendo a Teoria dos Números, Álgebra Linear e a Matemática Discreta as responsáveis por toda a sua parte teórica, tornando-se indispensável a estudantes da área da computação.*

Palavras chaves: *criptografia, álgebra linear, segurança de dados*

Abstract. *Encryption is a technique of writing messages in code or cipher in order to maintain the confidentiality of the information. It is also widely used as a means of providing security to transactions in everyday systems such as access to ATMs, home banking, pay-per-view and websites, especially those that ask for your password. Currently, encryption, given the degree of sophistication and theoretical frameworks that involves his study, is considered a science in the field of Exact Sciences, and number theory, linear algebra and discrete mathematics are responsible for all its theoretical part, making it is essential that students in the area of computing.*

1. Introdução

O presente Artigo apresenta o tema Criptografia, sua história, aplicação e alguns resultados importantes da Teoria de Números que são utilizados nos mais diversos tipos de códigos e cifras, sendo este, um dos sistemas mais seguros de dados.

Embora os códigos secretos remontem os primórdios da comunicação escrita, tem havido um aumento recente no interesse pelo assunto devido à necessidade de manter a privacidade da informação transmitida ao longo de linhas públicas de comunicação.

Para codificar e decodificar mensagens utiliza-se a aritmética modular e a eliminação gaussiana, tornando a Criptografia uma introdução ao estudo de matrizes e sistemas lineares. Por ser basicamente formada pelo estudo dos algoritmos criptográficos que podem ser implantados em computadores, a álgebra linear é

de importância fundamental a estudantes das áreas da matemática, computação e profissionais que lidam com a segurança da informação.

De fato, este estudo cobre bem mais do que cifragem e decifragem, é um ramo especializado da teoria da informação com muitas contribuições de outros campos da matemática e do conhecimento científico, incluindo autores como Howard (2001), Marcacini (2002), Machado (2003) e Shokranian (2005).

2. Breve Histórico

Não existe uma precisão quanto à origem e pouco se sabe acerca de seu uso nos primórdios da História, mas acredita-se que a criptografia seja tão antiga quanto à própria escrita. Há indícios que, na Antiguidade, foi conhecida no Egito, Mesopotâmia, Índia e China. Na Roma Antiga, Júlio Cesar também utilizava um método para cifrar sua correspondência. Com a revolução industrial, a criptografia evoluiu no sentido de mecanização e automotização. O uso de códigos secretos, antes utilizados quase que exclusivamente por militares e diplomatas, foi-se difundindo e estende-se hoje a fichas médicas em hospitais, a empresas que necessitam preservar informações técnicas da sua laboração e de seus equipamentos, às atividades bancárias, ao tratamento e circulação de dados científicos bem como a salvaguarda de informações em redes de informática. Há 25 anos, aproximadamente, a criptografia tornou-se uma disciplina científica, ativamente estudada por matemáticos, especialistas em estatística e cientistas ligados a sistemas informáticos.

3. Métodos de Criptografia

3.1. Cifras de Substituição

Para converter textos comuns em cifrados utilizam-se códigos denominados cifras. As cifras mais simples, ou de substituição, são as que substituem as letras do alfabeto por outra letra. Por exemplo:

Texto Comum: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z,

Texto Cifrado: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C.

A letra do texto comum *A* é substituída pela letra do cifrado *D*, a letra do texto comum *B* pelo *E*, e assim sucessivamente. Com esta cifra, a mensagem comum ROMA NÃO FOI CONSTRUÍDA EM UM DIA fica URPD QDR IRL FRKVWUXLGD HP XP GLD. Este tipo de cifra preserva a freqüência de letras individuais, tornando fácil a resolução dos códigos por métodos estatísticos. Uma forma de superar tal problema seria dividir o texto em grupos de letras e criptografar o texto comum por grupo, em vez de uma letra de cada vez.

3.2 Cifras de Hill

O sistema de criptografia polialfabética chamada cifra de Hill foi inventada em 1929 por Lester S. Hill. Este sistema consiste em fazer $\boldsymbol{m}$ combinações lineares dos $\boldsymbol{n}$ caracteres do texto plano, produzindo os $\boldsymbol{m}$ caracteres do texto criptografado. As cifras de Hill são baseadas em transformações matriciais.

Cada letra do texto comum e do texto cifrado, excetuando o $\boldsymbol{Z}$, tem o valor

numérico que especifica sua posição no alfabeto padrão (Tabela 1). Por motivos que ficarão claros mais tarde, dá-se a ***Z*** o valor de **0**.

Tabela 1: Alfabeto

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

Nos casos mais simples, transformam-se pares sucessivos de textos cifrados pelo procedimento a seguir:

1 – Escolhe-se uma matriz de ordem 2x2 com entradas inteiras para efetuar a codificação.

Ex: $AI = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$

2 – Agrupam-se letras sucessivas do texto comum em pares, adicionando uma letra fictícia para completar o último par, se o texto tem um número ímpar de letrassubstitui-se cada letra de texto comum pelo seu valor numeric.

3 – Converte-se cada par sucessivo $\boldsymbol{p}_1\ \boldsymbol{p}_2$ de letras de texto comum em um vetor coluna e forma-se o produto ***A.p***. Chama-se ***p*** de vetor comum e ***A.p*** o correspondente vetor cifrado.

Ex: $p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$

4 – Converte-se cada vetor cifrado em seu equivalente alfabético. Substitui-se os inteiros maiores que 25 pelo resto da divisão dele por 26. Esta é uma técnica matemática chamada Aritmética Modular.

Para decifrar as cifras de Hill, utiliza-se a inversa da matriz codificadora.

3.3 Método Matriz

O método utilizado é 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.

Ex: Para criptografar a mensagem "EU TE AMO", forma-se uma matriz de ordem 3x3, que usando a correspondência numérica da cifra matriz torna-se

$$A=\begin{bmatrix} E & U & - \\ T & E & - \\ A & M & O \end{bmatrix}=\begin{bmatrix} 5 & 21 & 0 \\ 20 & 5 & 0 \\ 1 & 13 & 15 \end{bmatrix}$$

Suponha que a chave para esta codificação é a palavra "PACIÊNCIA" e **B** uma matriz qualquer de ordem 3x3 inversível, que descreve esta chave:

$$B=\begin{bmatrix} P & A & C \\ I & E & N \\ C & I & A \end{bmatrix}=\begin{bmatrix} 16 & 1 & 3 \\ 9 & 5 & 14 \\ 3 & 9 & 1 \end{bmatrix}$$

Multiplica-se a matriz mensagem **A** pela secreta **B** obtendo-se a matriz resultante **C**:

$$C=\begin{bmatrix} 5 & 21 & 0 \\ 25 & 5 & 0 \\ 1 & 13 & 15 \end{bmatrix}\times\begin{bmatrix} 16 & 1 & 3 \\ 9 & 5 & 14 \\ 3 & 9 & 1 \end{bmatrix}=\begin{bmatrix} 269 & 110 & 309 \\ 365 & 45 & 130 \\ 178 & 201 & 200 \end{bmatrix}$$

A mensagem codifica que será enviada é uma cadeia de números: 269, 110, 309, 365, 45, 130, 178, 201, 200.

Para decodificar a mensagem recebida, o receptor deverá multiplicá-la pela matriz inversa $A \times B \times B^{-1} = A$, ou seja,

$A \times B = C \Rightarrow A \times B \times B^{-1} = C \times B^{-1} \Rightarrow A \times C \times B^{-1}$ e posterior transcrição dos numerous para as letras:

$$\begin{bmatrix} 269 & 110 & 309 \\ 365 & 45 & 130 \\ 178 & 201 & 200 \end{bmatrix}\times\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}=\begin{bmatrix} 5 & 21 & 0 \\ 20 & 5 & 0 \\ 1 & 13 & 15 \end{bmatrix}=\begin{bmatrix} \grave{E} & U & - \\ T & E & - \\ A & M & O \end{bmatrix}$$

3.4 Método Permutacional

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.

Definição: Uma permutação de um conjunto ***X*** é uma função bijetora $f : X \rightarrow X$.

Vamos supor que X é um conjunto finito, digamos que tenha n elementos denotados por $a_1, a_2, a_3, \ldots a_n$. Por exemplo, $n = 1$ temos uma permutação, a função $f = a_1 = a_1$. Se $n = 2$ então teremos duas permutações.

$$f_1 : \begin{cases} f_1 & a_1 = a_1 \\ f_1 & a_2 = a_2 \end{cases} \qquad f_2 : \begin{cases} f_2 & a_1 = a_2 \\ f_2 & a_2 = a_1 \end{cases}$$

O teorema a seguir mostra a quantia de permutações de um conjunto de *n* elementos:

Teorema 2.1: O número das permutações de um conjunto de *n* elementos é **n**.

Vamos supor que um conjunto $X_1 = \{a_1, a_2, a_3, \ldots, a_{n-1}\}$ de *n-1* elementos tenha $(n-1)!$ Permutações. Denotamos essas permutações por $f_1, f_2, \ldots f_{n-1}$. Consideramos um conjunto $X = X_1 \cup \{a_n\}$ de *n* elementos. Podemos estender as permutações f_1 do conjunto X_1 ao conjunto *X*, supondo que as f_i mantenham fixo o element funções a_n. A cada permutação f_i do conjunto *X*, associaremos *n* permutações $F_1, F_2, \ldots, F_n$ do conjunto *X* da seguinte maneira:

$$f_i \quad a_j \quad = \{$$

Portanto, no total existem $(n-1)!.n=n!$ permutações no conjunto *X*.

3.5 Método RSA

Atualmente é o método mais utilizado e conhecido em aplicações comerciais e na internet. Permite a identificação do documento, criptografar dados, criar e verificar assinaturas digitais. Foi inventado em 1978 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T). As letras RSA correspondem às iniciais dos inventores do código. Este método é baseado no problema do logaritmo discreto.

As etapas para a utilização do RSA:

1 – São escolhidos dois numerous primos extensos ***p*** e ***q*** (geralmente maiores que 10^{100})

Calcula-se

$n = p \times q$

$\phi\, n = p - 1 \,.\, q - 1$

2 – Escolhe-se um número ***d*** que seja co-primo a $\phi\, n$, isto é, $MDC\ d, \phi\, n = 1$.

3 – Encontra-se *e* de forma que $e.d \equiv 1 \bmod \phi\, n$

4 – O texto simples é dividido em blocos, de modo que cada mensagem, *M*, fique no interval $0 \leq M \leq$ n.

Para criptografar a mensagem, *M*, é calculado:

$C \equiv M^e \mod n$

5 – Para descriptografar C, é calculado:

$C \equiv M^d \mod n$

Para todo M na faixa especificada, as funções de cifragem e decifragem são inversas entre si. Para realizar a cifragem, é necessário conhecer o valor de **"e"** e o de **"n"**. Para decifrar a mensagem, são necessários os valores de **"d"** e **"n"**. Logo, a

chave pública consiste no par **(e,n)** e a chave privada consiste em **(d,n)**.

4. Considerações Finais

A criptografia é uma maneira eficaz de enviar dados sigilosos. Com o desenvolvimento da tecnologia e a inserção das redes públicas no cotidiano, é de extrema importância encontrar uma forma de codificar e decodificar mensagens de forma rápida e segura seja para enviar um e-mail ou para realizar transações comerciais. Em virtude das aplicações de segurança, a Álgebra Linear torna-se indispensável na área da computação, pois, aliada a Teoria dos Números, serve de estrutura para o desenvolvimento de programas capazes de manter o sigilo das mensagens e informações transmitidas ao longo das redes públicas.

References

Howard, A. e Rorres, C. (2001). Álgebra Linear com Aplicações. 8ª ed. Porto Alegre: Ed. Bookmann.

Machado, S. D. A. (Org.). (2003). Aprendizagem em Matemática. Registro de Representação Semi-ótica. Campinas. Ed. Papirus.

Marcacini, A. T. R. (2002). Direito e Informática – Uma Abordagem Jurídica sobre Criptografia. Rio de Janeiro. Ed. Forense.

Shokranian, S. (2005). Criptografia para Iniciantes. Editora: Universidade de Brasília.