Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Criptografia: Um Estudo da Aritmética Modular por meio de Códigos

Matias Zimmermann¹

Universidade do Vale do Rio dos Sinos, São Leopoldo, RS

Alessandra Fabian Sostisso²

Faculdade Mário Quintana, Porto Alegre, RS

Resumo

A palavra Criptografia vem do grego, *kriptós*: escondido, *oculto* e *grápho*: grafia. Sendo uma forma de escrever em códigos mensagens de forma que somente o destinatário possa decodificá-la ou compreendê-la. Assim, para criptografar uma mensagem, o texto deve ser adaptado a um sistema numérico. Esta primeira etapa é denominada pré-codificação, que consiste em considerar uma correspondência biunívoca de todos os grafemas (letras) usados na mensagem e um conjunto finito, sequencial e adequado de números. Codificar o conteúdo de uma mensagem de forma a que se torne imperceptível a estranhos designa-se por encriptação. À mensagem criptografada chama-se de texto cifrado. Para criptografar e descriptografar usa-se uma chave, que dita a transformação do texto original em um texto criptografado. Uma chave é uma informação restrita que controla toda a operação dos algoritmos de criptografia.

Segundo Singh (2003), atualmente os meios de comunicação podem ser interceptados facilmente, ameaçando nossa privacidade, além disso, à medida que mais transações comerciais são realizadas por meio da Internet, necessitam ser instaladas medidas de proteção para a segurança das empresas e de seus clientes. A criptografia é o único meio de proteger a privacidade e garantir o sucesso do mercado digital. O mais conhecido e utilizado código de criptografia de chave pública, inventado em 1977 por Rivest, Shamir e Adleman, o RSA. A implementação deste algoritmo baseia-se, principalmente, nos seguintes resultados:

Teorema 1 (Teorema Fundamental da Aritmética). *Todo inteiro $a \geq 2$ pode ser escrito como produto de números primos. Esta decomposição é única exceto pela ordem dos fatores primos.*

Teorema 2 (Divisão Euclidiana). *Sejam a e b dois números inteiros com $a > 0$. Existem dois únicos números inteiros q e r que são chamados o quociente e resto da divisão de b por a , tais que: $b = a.q + r$, com $0 \leq r < a$.*

¹matias_znp@hotmail.br - Bolsista CNPq

²alesostisso@gmail.com

Algoritmo Euclidiano: Dados dois números inteiros positivos a e b tais que $a \geq b$, divide-se a por b , encontrando resto r_1 . Se $r_1 \neq 0$, dividimos b por r_1 , obtendo resto r_2 . Se $r_2 \neq 0$, dividimos r_1 por r_2 e assim por diante. O último resto diferente de zero dessa sequência de divisões é o $mdc(a, b)$.

Teorema 3 (Algoritmo Euclidiano Estendido). *Sejam a e b inteiros positivos e seja d o máximo divisor comum entre a e b . Existem inteiros α e β tais que $\alpha a + \beta b = d$.*

Definição 1. Seja n um inteiro positivo. A função de Euler $\varphi(n)$ é definida como o número de inteiros positivos não excedendo n que são relativamente primos com n .

Definição 2: Diremos que d é um máximo divisor comum mdc de a e b se possuir as seguintes propriedades:

- d é um divisor comum de a e de b , sendo a e b não simultaneamente nulos;
- d é divisível por todo divisor comum de a e b .

Teorema 4 (Função de Euler). *Se m, n são inteiros positivos tais que $mdc(m, n) = 1$, então $\varphi(mn) = \varphi(m - 1) \cdot \varphi(n - 1)$.*

Se $n = p_1^{k_1} \dots p_r^{k_r}$, onde os p_j são os fatores primos de n , então, pode-se determinar o valor da função em n , por: $\varphi(n) = (p_1 - 1)p_1^{k_1 - 1} \dots (p_r - 1)p_r^{k_r - 1}$

Teorema 5 (Teorema de Euler). *Se n é um inteiro positivo e a é um inteiro tal que $mdc(a, n) = 1$, então $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Processo de cifragem por meio de RSA

1. Atribuímos valores numéricos as letras do alfabeto;
2. Escolhemos dois primos distintos p e q e definimos seu produto por $n = p \cdot q$, que pelo Teorema 1, garante-se que é único;
3. Aplicamos o Teorema 4 em n para obter $\varphi(n)$.
4. Escolhemos um número r em que $1 < r < \varphi(n)$, de forma que $mdc(\varphi(n), r) = 1$. Neste passo, criamos a chave-pública, que permite cifrar a mensagem.
5. Aplicando a fórmula $c = m^r \pmod{n}$, onde m é o valor numérico de cada letra. Assim, ciframos a mensagem.

Processo de decifragem

Para decifrar a mensagem deve-se utilizar a chave privada que obtém-se por meio de:

1. Para decifrar a mensagem, deve-se encontrar o inverso multiplicativo de r . Ou seja, $\alpha \cdot r = 1 \pmod{\varphi(n)}$. Para isso, aplica-se o Teorema 3, para encontrar α , tal que $\alpha \cdot r + \beta(\varphi(n)) = mdc(\varphi(n), r) = 1$.
2. Por fim, aplicamos a seguinte equação: $m = c^\alpha \pmod{n}$

Para o processo de cifragem e decifragem de uma mensagem foram utilizados alguns teoremas e resultados da aritmética. O que mostra uma possibilidade de por meio da criptografia elaborar um material de apoio didático que contemple tais conteúdos.

Referências

- [1] A. Hefez. *Elementos de Aritmética*. SBM, Rio de Janeiro, 2006.
- [2] S. Singh. *O Livro dos Códigos*. Record, Rio de Janeiro, 2003.