CRIPTOGRAFIA: CONCEITO E EVOLUÇÃO ATRAVÉS DA MATEMÁTICA

Natalia Alves do Valle[1] e Marcella Medeiros Mascaro[2]

Resumo

Esta pesquisa consiste no estudo introdutório da criptografia, uma área de aplicação da matemática, que evoluiu nos últimos anos. Mostra seus aspectos mais fundamentais, destacando a matemática como ferramenta essencial para seu aperfeiçoamento.

1. Introdução

A criptografia surgiu devido à necessidade do homem em esconder informações. Com o surgimento da internet e a facilidade de transmitir dados que ela introduziu, a criptografia tornou-se indispensável, pois permite que somente pessoas autorizadas possam ter acesso a determinadas informações.

> *"O termo **criptografia** surgiu da fusão das palavras gregas "kryptós" e "gráphein", que significam "oculto" e "escrever", respectivamente. Trata-se de um conjunto de conceitos e técnicas que visam codificar uma informação de forma que somente o emissor e o receptor possam acessá-la, evitando que um intruso consiga interpretá-la. Para isso, uma série de técnicas são usadas e muitas outras surgem com o passar do tempo."*
>
> Escrito por Emerson Alecrim, em: *http://www.infowester.com/criptografia.php* - Publicado em 12/08/2005 - Atualizado em 11/07/2009

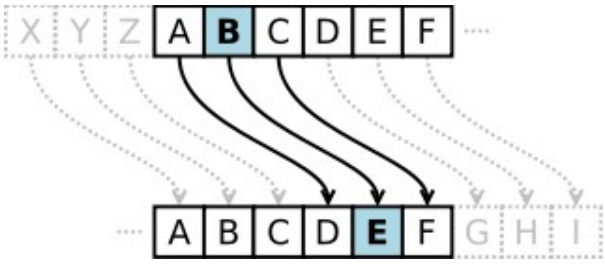
Palavras-chave: criptografia, codificar, algoritmo

[1] Universidade do Estado do Rio de Janeiro, natydovalle@hotmail.com

[2] Universidade do Estado do Rio de Janeiro, marcellamedeirosm@hotmail.com

Os primeiros métodos de criptografia foram utilizados em guerras, e para exemplificar, temos a Cifra de César. Na tentativa de se comunicar com os seus generais, o Imperador romano Júlio Cesar utilizava essa técnica de criptografia em suas mensagens. O algoritmo era simples: substituição monoalfabética. Cada letra da mensagem era substituída por outra, que se apresenta no alfabeto um número fixo de posições à frente dela, de forma cíclica. Este número fixo, chamado parâmetro de troca, é a chave da mensagem criptografada e por isso, deve ser transmitida ao receptor por um canal seguro.

Observe o esquema abaixo:



Neste caso, o parâmetro de troca é 3. Por exemplo, se fôssemos criptografar uma mensagem utilizando este parâmetro, teríamos:

De um modo geral, podemos escrever a Criptografia em Cifras de César da seguinte maneira:
Seja $k = \pi$, uma permutação de A, conjunto das letras do alfabeto:

$$y = C(k, x_i) = \pi(x_1)\pi(x_2)\pi(x_3) \dots \pi(x_n)\,,\ 1 < i < n,$$

onde $C(k, x_i)$ é a mensagem, k é o parâmetro de troca (a chave), x_i são as letras e n é o número de letras dessa mensagem.

Sendo assim, $\pi(x_i), 1 < i < n$, são as letras da mensagem criptografada.

Então, para decodificar esta mensagem, temos:

$$x = C^{-1}(k, y_i) = \pi^{-1}(y_1)\pi^{-1}(y_2)\pi^{-1}(y_3) \dots \pi^{-1}(y_n), 1 < i < n.$$

Por exemplo, como citado anteriormente, temos $k = 3$, e:

$$\pi(a) = d, \pi(b) = e, \pi(c) = f, \pi(d) = g, \dots, \pi(z) = c$$

Então,

$$y = C(3, As\ tropas\ chegaram) = DV\ WURSDV\ FKHJDUDP$$

A Criptografia em Cifras de César também pode ser representada matematicamente utilizando a aritmética modular.

Dentre as maneiras de decifrá-la, assim como qualquer outro tipo de cifra de substituição simples, existe a análise de frequência, que compara as frequências de distribuição das letras. Mas, a decodificação se torna altamente fácil quando temos o seguinte gráfico:

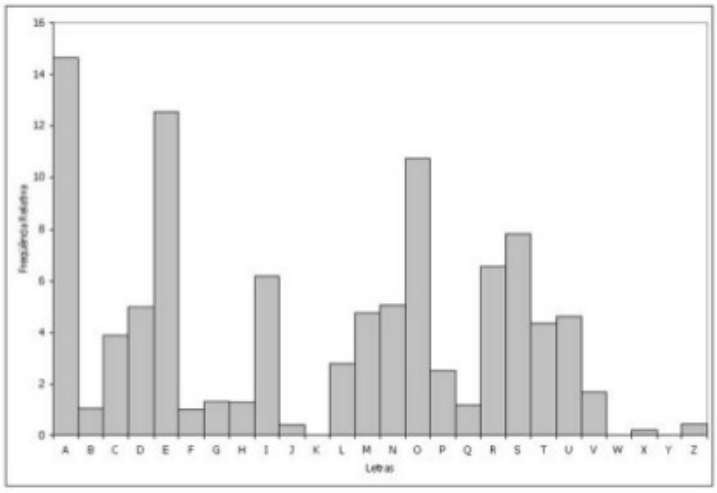


Gráfico da frequência de letras na língua portuguesa.

Hoje, qualquer tipo de troca de informações pode ser feitas através de uma rede de computadores. Empresas, escolas, qualquer estabelecimento se preocupa com a segurança de suas informações. Com isso, as técnicas de codificação foram estudadas cada vez mais, e novas técnicas desenvolvidas.

Exemplificando o avanço destas tecnologias, foi estudado também nesta pesquisa o método de criptografia mais conhecido e usado atualmente: o RSA.

Este código foi desenvolvido em 1978 por Ronald Rivest, Adi Shamir e Leonard Adleman, que na época trabalhavam no *Massachussets Institute of Technology (M.I.T.)*. As letras RSA correspondem às iniciais dos inventores do código. Esse método de criptografia atua diretamente na internet, em mensagens de emails, compras on-line.

O RSA envolve um par de chaves: uma chave pública, que pode ser conhecida por todos e uma chave privada, que deve ser mantida em sigilo. Toda mensagem cifrada, usando uma chave pública, só pode ser decifrada a partir da respectiva chave privada. A escolha destas chaves não se faz de forma aleatoria. Ela envolve um estudo avançado da matemática e da informática.

As chaves são geradas da seguinte maneira:

1. Escolhem-se dois números primos grandes p e q;
2. Considera-se $n = p.q$;
3. Computa-se a função totiente em n: $\varphi(n) = (p-1)(q-1)$;
4. Escolhe-se um inteiro e tal que $1 < e < \varphi(n)$, com $mdc(\varphi(n), e) = 1$;
5. Computa-se d tal que $de \equiv 1(mod\ \varphi(n))$.

No passo 5 é usado o algoritmo de Euclides estendido, e o conceito de inverso multiplicativo que vem da aritmética modular.

Logo, temos:

A chave pública: par de números n e e.

A chave privada: o par de números n e d.

Para criptografar devemos utilizar um método para trocar as letras por números. Mas isso não se faz de uma forma aleatória, utiliza-se o ASC II (acrônimo para *American Standard Code for Information Interchange*, que em português significa "Código Padrão Americano para o Intercâmbio de Informação") é uma codificação de caracteres de oito bits, baseada no alfabeto inglês. Os códigos ASCII representam texto em computadores, equipamentos de comunicação, entre outros dispositivos que trabalham com texto. Desenvolvida a partir de 1960, grande parte das codificações de caracteres modernas a herdaram como base.

O método é, basicamente, a troca de cada letra por um número específico.

Por exemplo: A=97, B=98 e assim por diante até que todas as letras do alfabeto possuam seu respectivo número.

Logo, a mensagem "casa", por exemplo, no ASCII ficará : "99 97 114 97"

Chamamos de bloco, cada número correspondente a apenas uma letra da mensagem que foi criptografada em ASCII.

Continuando o processo temos a seguinte fórmula para criptografar cada bloco da mensagem:

$$C_i = m_i^e (mod\ n), 1 < i < l,$$

onde m_i corresponde a cada bloco em ASCII a ser criptografado em RSA, l é a quantidade desses blocos e C_i cada bloco criptografado.

E para decodificar usamos:

$$M_i = c_i^d (mod\ n), 1 < i < l,$$

onde M_i corresponde a cada bloco em ASCII da mensagem original, l é a quantidade desses blocos e C_i cada bloco criptografado.

Através do que foi estudado, podemos concluir que a matemática é uma importante ferramenta, não só para se resolver problemas numéricos cotidianos, mas também para desenvolver algoritmos usados em estudos complexos e importantes atualmente, como a criptografia. O avanço

dessas pesquisas nos permite aperfeiçoar diversas de suas aplicações, na tentativa de responder às exigentes demandas da crescente sociedade.

Referências

COUTINHO, S. C., Números Inteiros e Criptografia, Série de Computação e Matemática, IMPA, Segunda Edição, 2003.

WAGA, C. Algebra I, UERJ , Agostode 2011.

SILVA, Elen Viviani P. Introdução à Criptografia RSA. 2006. Departamento de Matemática, Faculdade de Engenharia de Ilha Solteira. São Paulo.

NUMABOA, disponível em: http://www.numaboa.com.br/criptografia, visitado em: 12 jan. 2011