CRIPTOGRAFIA: MÉTODO R.S.A.

Yasmin Iandária de Oliveira Garcia
Lúcia De Fátima De Medeiros Brandão Dias
Departamento Acadêmico de Matemática e Estatística, Universidade Federal de Rondônia, Ji-Paraná, Brasil — 2020

Introdução

Criptografia é um sistema de algoritmos matemáticos que codificam dados do usuário para que somente o destinatário possa decifrá-la.

A criptografia foi muito utilizada nas guerras para o envio de mensagens secretas das ações contra os inimigos.

Com a evolução tecnológica houve-se a necessidade de melhorar o método de criptografia afim de proteger o usuário. Dessa forma, surgiu a criptografia de chave pública onde é usado dois tipos de chaves: sendo uma pública para criptografar a mensagem e a chave de decodificação onde somente o usuário pode visualizar a mensagem original codificada.

Objetivos

- Estudar o conteúdo teórico fundamental;
- Estudar e apresentar o método de criptografia R.S.A.

Apresentação e discussão dos dados

Alguns resultados e definições importantes para a implementação e análise do R.S.A. são:

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:

$$\alpha.a + \beta.b = d$$

Congruência Modular: Sejam a e b números inteiros positivos. Dizemos que a e b são congruentes módulo m quando $a - b$ é múltiplo de m, escrevemos $a \equiv b\,(mod\, m)$.

Pequeno Teorema de Fermat: Seja p um número primo e a um número inteiro, então: $a^p \equiv a\ (mod\ p)$

Teorema 1. Se m, n são inteiros positivos tais que mdc$(m, n) = 1$, então $\phi(mn) = \phi(m).\phi(n)$

Teorema de Euler Sejam $n > 0$ e a números inteiros. Se mdc $(a, n) = 1$

$$a^{\phi(n)} \equiv 1(mod\, n)$$

Criptografia método R.S.A.

Para implementar esse método de criptografia é necessário ter dois números inteiros primos distintos p e q.

Pré codificação: é converter a mensagem em uma sequência de números. Denote por b cada bloco obtido após a etapa de pré-codificação.

Codificação: Para codificar uma mensagem usamos n e e tais que o mdc $(e, \phi(n)) = 1$. Chamamos(n, e) a chave de codificação ou chave pública. Sendo $C(b)$ cada bloco b codificado para calcular $C(b)$ é definido como o resto da divisão de b^e por n.

Decodificação: Seja a o bloco codificado e $D(a)$ o bloco decodificado. $D(a)$ é definido como sendo o resto da divisão de a^d por n. Para calcular d basta aplicar o Algoritmo euclidiano estendido que será uma tarefa fácil desde que $\phi(n)$ seja conhecido.

Suponha que se queira criptografar a seguinte palavra PERSISTA, então usando a tabela de correspondência abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

obtém-se a seguinte sequência de números 2514272818282910. Essa sequência deve ser quebrada em blocos de números obedecendo duas regras:
1) Cada bloco não pode ser maior do que o número n obtido. O número n é o produto de dois números primos cuidadosamente escolhidos.
2) Cada bloco não pode iniciar pelo dígito zero.

Considere $p = 11$ e $q = 17$, dessa forma $n = p.q = 187$ e $e = 3$. O cálculo de $\phi(n)$ se torna fácil quando sabemos a fatoração em números primos de n (essa fatoração não é uma informação pública). Pelo Teorema 1 sabemos que, nesse caso, $\phi(n) = (p - 1).(q - 1) = 160$. Como $e = 3$, tem-se que $mdc(e, \phi(n)) = 1$. Escolhido os números primos p e q e satisfeitas as condições teóricas para a implementação do método quebra-se a sequência numérica 2514272818282910, obtida acima. A mensagem deve ser quebrada em blocos menores que $n = 187$, como por exemplo:

$$25 - 142 - 7 - 28 - 182 - 8 - 29 - 10$$

O bloco codificado é: $104 - 131 - 156 - 73 - 62 - 138 - 79 - 65$

Quando calculamos o resto da divisao de 25^3 por 187 obtemos 104, ou seja, $25^3 \equiv 104\,(mod\, 187)$

Fazendo alguns cálculos, obtemos $d = -53+160$

A decodificação do bloco 79:
$79^7 \equiv 139\,(mod\, 187)$
$(79^7)^5 \equiv (139)^5\,(mod\, 187)$
$(79^{35}) \equiv 175\,(mod\, 187)$
$(79^{35})^3 \equiv (175)^3\,(mod\, 187)$
$(79^{105}) \equiv 142\,(mod\, 187)$
$(79^{105}).79^2 \equiv 79^2.142\,(mod\, 187)$
$(79^{107}) \equiv 29\,(mod\, 187)$

Dessa forma, a sequência de blocos decodificados é: $25-142-7-28-182-8-29-10$. E assim, utilizando a tabela de correspondência obtém-se a palavra que foi criptografada: PERSISTA.

Por que funciona o método R.S.A.?

O método R.S.A. somente funciona se um bloco decodificado volta ao bloco codificado, mostrando sua mensagem original. Dessa forma, precisa-se verificar que se b é um inteiro, C é a função codificação e D é a função decodificação então $DC(b) = b$.

É necessário que b esteja no intervalo de $1 \leq b \leq n - 1$ para que a função C seja injetora. Vejamos um exemplo, considere $n = 3, e = 3$, dessa forma tem se:

$$2^3 \equiv 2\,(mod\, 3)$$
$$5^3 \equiv 2\,(mod\, 3)$$

Se os números 2 e 5 fossem os blobos b a serem codificados teríamos que $C(2) = 2$ e $C(5) = 2$. Logo, ao decodificar, quem seria $DC(2)$?

Observe que se a função C não é injetora torna-se impossível obter a mensagem decodificada. A função C será injetora se considerarmos seu domínio sendo todos os números naturais b tais que $1 \leq b \leq n - 1$.

Por que o RSA é seguro?

Tornar-se fácil quebrar o sistema R.S.A. quando:

- p e q forem muito pequenos pois pode à mão ou mesmo usando um computador é possível fatorar n rapidamente e achar seus fatores primos p e q;
- p e q são grandes mas $|p-q|$ é pequeno. Nesse caso podemos achar p e q facilmente a partir de n utilizando o algoritmo de Fermat.

Considerações finais

Com esse trabalho podemos apresentar aplicações da matemática, discutir o conceito de função e de divisibilidade, entre outros com os alunos da rede pública ou privada de ensino para despertar interesse pela ciência além de mostrar como a matemática é utilizada no nosso dia a dia.

Referência

COUTINHO, S.C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro : IMPA/SBM, 1997.

RIBENBOIM, P. **Números Primos, amigos que causam problemas**. Rio de Janeiro : IMPA/SBM, 2015.

SANTOS, J.P.O. **Introdução à teoria dos números**. Rio de Janeiro : IMPA/SBM, 2007.

SANTIAGO, Emerson. Criptografia.**InfoEscola**, 7 de Agosto de 2012. Disponível em: <https://www.infoescola.com/informatica/criptografia/>. Acessado em 1 de Agosto de 2020.