

# TEORIA DOS NÚMEROS E CRIPTOGRAFIA: Introdução ao Método RSA



Universidade Estadual Paulista  
Faculdade de Ciências e Tecnologia  
Campus de Presidente Prudente

Douglas Azevedo Sant Anna  
UNESP - Curso de licenciatura em matemática - 2º ano  
E-mail: dgs.nvn@gmail.com  
Orientador: Professor Dr Jose Roberto Nogueira  
E-mail: jrnog@prudente.unesp.br

## INTRODUÇÃO

A aplicação de métodos matemáticos estudados na teoria dos números na área computacional, não é algo novo, tem por volta de 20 anos, mas muitos desses métodos já eram conhecidos há mais de 200 anos na Grécia. Esses métodos que estudam as propriedades dos números inteiros estão totalmente relacionados a áreas de grande interesse comercial atualmente, especificamente, à parte que diz respeito a segurança de computadores e sistemas de criptografia.

A criptografia estuda os métodos de codificar uma mensagem de modo que só seu destinatário legítimo possa interpretá-la. A criptografia tem uma "irmã gêmea" na arte de decifrar códigos ou, *criptoanálise* pois, naturalmente todo código vem acompanhado de duas receitas: uma para codificar a mensagem; outra para decodificá-la. Assim apesar desta pesquisa estar direcionada em estudar primeiramente métodos simples de criptografia, iniciamos estudando a Criptografia RSA, que atualmente é um dos métodos mais utilizados e seguros também é o mais conhecido método de chave pública. O RSA foi inventado em 1978 por R.L.Rivest, A. Shamir e L. Adleman, que trabalhavam no MIT (Massachusetts Institute of Technology), o RSA é atualmente o método mais usado em aplicações comerciais.

## PRÉ-CODIFICAÇÃO

A primeira coisa a fazer se desejamos usar o método RSA é converter a mensagem em uma seqüência de números. Suporemos, para simplificar, que a mensagem original é um texto onde não há números, apenas palavras. Portanto, em última análise, a mensagem é constituída pelas letras que formam as palavras e pelos espaços entre as palavras. Chamaremos esta primeira etapa de pré-codificação, para distingui-la do processo de codificação propriamente dito.

Na pré-codificação convertemos as letras em números usando a seguinte tabela de conversão:

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

O espaço entre as palavras será substituído pelo número 99, quando for feita a conversão. Por exemplo, a frase: "Paraty é linda" é convertida no número:

2510271029349914992118231310

Antes de continuar precisamos determinar os parâmetros do sistema RSA que vamos usar. Esses parâmetros são dois primos distintos, que vamos denotar por  $p$  e  $q$ . Ponha  $n = pq$ . A última fase do processo de pré-codificação consiste em quebrar em blocos o longo número produzido anteriormente. Esses blocos devem ser números menores que  $n$ . Por exemplo, se escolhemos  $p=11$  e  $q=13$ , então  $n=143$ . Nesse caso, a mensagem, cuja conversão numérica foi feita acima, pode ser quebrada nos seguintes blocos:

25-102-7-102-93-49-91-49-92-118-23-13-10

A maneira de escolher os blocos não é única, mas certos cuidados devem ser tomados. Por exemplo, é necessário evitar que o bloco comece por 0 porque isto traria problemas na hora de decodificar.

## CODIFICANDO E DESCODIFICANDO

Para codificar precisamos de  $n$ , ( $n = p \cdot q$ ), e de um inteiro  $e$  positivo que seja inversível módulo  $\Phi(n)$  (a função totiente), ou seja,  $\text{mdc}(e, \Phi(n))=1$ . Note que  $\Phi(n)=(p-1)(q-1)$ . Chamamos o par  $(n, e)$  de chave do RSA. Codificaremos cada bloco separadamente, e a mensagem codificada será uma seqüência de blocos codificados. Assim a chave de codificação  $e$  e denotando cada bloco por  $b$ , onde  $b$  é um inteiro menor que  $n$  e, ainda, chamamos  $C(b)$  de bloco codificado. O cálculo de  $C(b)$  é o seguinte:  $C(b)$  é o resto de divisão de  $b^e$  por  $n$ . Aplicando o exemplo analisado, com  $p=11$  e  $q=13$  então  $n=143$  e  $\Phi(n)=120$ . Ainda precisamos escolher  $e$ . Para este exemplo usamos  $e=7$  que é o menor primo que não divide 120. Assim o bloco 102 da mensagem é codificado como resto da divisão de  $102^7$  por 143, ou seja:

$102^7 = (-41)^7 = -81.138 = -24 = 119 \pmod{143}$ . A mensagem codificada fica:

64-119-6-119-102-36-130-27-79-23-117-10

Para a decodificação de cada bloco a informação que precisamos consiste de 2 números:  $n$  e o inverso de  $e$  módulo  $\Phi(n)$  que denotaremos por  $d$ , ou seja, a chave de decodificação é  $(n, d)$ . Seja  $a$  um bloco codificado, então  $D(a)$  será o resultado da decodificação, que calculamos assim:  $D(a) = \text{resto da divisão de } a^d \text{ por } n$ . Para o cálculo de  $d$  basta aplicarmos o algoritmo estendido de Euclides:  $120+7(-17)=1$ , como  $d$  é positivo pois é um expoente de potências fazemos:  $-17 = 103 \pmod{120}$ , assim  $d=103$ . Logo decodificando o bloco de valor 119, calculamos a forma reduzida de  $119^{103}$  módulo 143, neste caso apoiado num sistema de computação algébrica calculamos o resultado que é, e podemos verificar:  $119^{103} = 102 \pmod{143}$ .

## POR QUE É SEGURO?

O RSA é um método de chave pública, o par  $(n, e)$  dita chave de codificação é acessível para qualquer usuário, assim o RSA só será seguro se for difícil calcular  $d$  quando apenas  $(n, e)$  são conhecidos. Na prática, só conseguimos quebrar o código se fatorarmos  $n$ , mas se  $n$  é grande, este é um problema muito difícil, devido a ineficiência dos algoritmos de fatoração conhecidos, se alguém inventasse um algoritmo rápido para calcular  $\Phi(n)$ , a partir de  $n$  e  $e$  teríamos na verdade obtido um algoritmo rápido de fatoração. Mas não adianta uma maneira de achar  $\Phi(n)$  sem fatorar  $n$ . E se alguém inventar um algoritmo que ache  $d$  diretamente a partir de  $n$  e  $e$ , temos que como:  $ed = 1 \pmod{\Phi(n)}$ , isto implica que conhecemos um múltiplo de  $\Phi(n)$ , o que é suficiente para fatorar  $n$ , mas a demonstração está fora do alcance matemáticos abordado até este ponto da pesquisa.

Diante destes fatos, acredita-se que quebrar o RSA e fatorar  $n$  sejam tarefas semelhantes, embora até agora não se tenha demonstrado.

## CONCLUSÃO

A partir das pesquisas, observamos que é muito difícil separar os dois tópicos "criptografia e teoria dos números" e, baseado no sistema de criptografia RSA que é de enorme importância comercial, aplicado em sistemas de segurança de transações financeiras, por navegadores de internet entre outros, entendemos que a resolução de problemas na área de teoria dos números, tem vasta aplicação para os sistemas de criptografia, tanto que o mais conhecido destes problemas é a busca pela equação geradora de primos que, se ocorresse de sua descoberta, o sistema RSA se tornaria obsoleto.

BIBLIOGRAFIA S.C.Coutinho-Números inteiros e criptografia RSA