ALGUMAS APLICAÇÕES DA TEORIA DE NÚMEROS.

Amanda Caroline Gonçalves Paschoal (PIBIC/CNPq/FA/UEM), Rosali Brusamarello (Orientadora), e-mail: brusama@uem.br

Universidade Estadual de Maringá / Centro de Ciências Exatas, PR.

Área e subárea do conhecimento: Matemática/Álgebra

Palavras-chave: criptografia RSA, números primos, congruências.

Resumo:

Neste projeto iremos utilizar a teoria de números para descrever um método de envio de mensagens, o método de criptografia RSA.

Introdução

A criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. O método de criptografia RSA foi inventado em 1978 por R.L.Rivest, A.Shamir e L. Adleman, de onde vem o nome RSA. Para aplicar este método é preciso utitizar algumas noções de teoria de números, tais como: máximo divisor comum, números primos, fatoração, congruência, entre outras. A teoria dos números auxilia também para garantir a segurança do método.

Materiais e métodos

Por se tratar de um projeto de pesquisa básica, a metodologia empregada consiste de pesquisas bibliográficas, estudo do material coletado, apresentação de seminários e discussão do tema abordado.

Resultados e Discussão

Um dos mais importantes objetivos de nosso trabalho é entender como funciona a Criptografia e como podemos utilizá-la com segurança.

Para codificar uma mensagem pelo método RSA precisamos de um número natural *n* e da sua decomposição em números primos (em geral tomamos *n=p.q*). Para decodificar a mensagem é necessário conhecer esta fatoração em primos. Quanto maiores forem os números primos escolhidos, mas difícil será a fatoração de *n* e maior será a segurança do método.

A teoria dos números nos auxilia na busca de números primos bem grandes, com 60 ou mais algarismos. Dentre as fórmulas existentes para este fim, estudamos as fórmulas polinomiais, as fórmulas exponenciais (números de Mersenne e números de Fermat) e as fórmulas fatoriais.

Para codificar uma mensagem utilizaremos também a função de Euler Φ, que associa a cada número inteiro positivo *n* o número inteiro positivo *Φ(n)* que é o número de inteiros menores do que *n* que são primos com *n.* Utilizando a teoria de grupos, mostramos que *Φ(mn)= Φ(m)Φ(n)*, para *m,n* números inteiros positivos e que *Φ(p)=p-1* se *p* é um número primo.

Primeiramente, se desejamos usar o método RSA precisamos converter a mensagem em uma sequência de números. Chamaremos esse primeiro momento de *pré-codificação*. 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 duas palavras será substituído pelo número 99, quando for feita a conversão. Por exemplo, a palavras *Paraty é linda* é convertida no número:

2510271029349914992118231310.

Antes de continuar precisamos determinar os parâmetros do sistema RSA que vamos usar. Estes 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. Estes blocos devem ser números menores que *n*. Por exemplo, se escolhemos *p=11* e *q=13*, então *n=143*. Neste caso, a mensagem, cuja

conversão numérica foi feita anteriormente, pode ser quebrada nos seguintes blocos:

25 – 102 – 7 – 102 – 93 – 49 – 91 – 49 – 92 – 118 – 23 – 13 – 10.

Encerramos assim a pré-codificação, e podemos passar à etapa da codificação propriamente dita. Para codificar a mensagem precisamos de *n,* que é o produto dos primos, e de um inteiro positivo *e* que seja inversível módulo Φ*(n).* Em outras palavras, mdc*(e,* Φ*(n))*=1. Note que é fácil calcular Φ(*n*) se conhecemos *p e q;* de fato,

$$\Phi(n)=(p-1)(q-1).$$

Chamaremos o par (*n,e*) de *chave de codificação* do sistema RSA que estamos usando, esta chave é pública. Tendo submetido a mensagem à pré-codificação, temos uma sequência de números em blocos. Codificaremos cada bloco separadamente, e a mensagem codificada será a sequência de blocos codificados. Vamos denotar o bloco codificado por **C**(*b*). A fórmula para calcular **C**(*b*), é a seguinte:

C(*b*)= resto da divisão de b^e por *n.*

Vejamos o que aconteceria no exemplo que estamos tomando. Temos *n*=143 e Φ(*n*)=120. Ainda precisamos escolher *e*. Neste exemplo, o menor valor para *e* é 7, que é o menor primo que não divide 120. Assim, o bloco 102 da mensagem anterior é codificado como o resto da divisão de 102^7 por 143. Fazendo as contas, obtemos que **C**(102) = 119. E codificando toda a mensagem, obtemos a seguinte sequência de blocos:

64 – 119 – 6 – 119 – 102 – 36 – 130 – 36 – 27 – 79 – 23 – 117 – 10.

Vejamos então, como fazer para decodificar um bloco da mensagem codificada. A informação que precisamos para poder decodificar consiste de dois números: *n* e o inverso de *e* módulo Φ(*n*), que denotamos por *d.* Chamaremos o par (*n,d*) de *chave de decodificação*. Seja *a* um bloco da mensagem codificada, então **D**(*a*) será o resultado do processo de decodificação. A fórmula para calcular **D**(*a*) é a seguinte:

D(*a*)= resto da divisão de a^d por *n.*

Podemos calcular *d* facilmente, desde que Φ(*n*) e *e* sejam conhecidos. No exemplo que estamos acompanhando, temos que *n*=143 e *e*=7. Aplicando alguns algoritmos de teoria de números e congruências, obtemos que *d=103.* Assim, para decodificar o bloco 119 da mensagem codificada, calculamos a forma reduzida de 119^{103} módulo 143. Usando propriedades de congruências, podemos verificar que, de fato, $119^{103} \equiv 102 \pmod{143}$. Fazendo isso para todos os blocos da mensagem codificada, encontramos a mensagem decodificada, como queríamos.

Conclusões

A teoria de números é uma das teorias matemáticas mais antigas e vem sendo estudada até os dias de hoje com aplicações cada vez mais atuais. Vimos neste projeto que o método de codificação de mensagens RSA tem como base matemática a teoria de números, tanto para a sua formulação como para garantir a sua segurança.

Agradecimentos

Agradeço a Deus, por me dar saúde e força, a minha família, a minha orientadora e ao CNPq pela bolsa de estudos.

Referências

Coutinho, S.C., *Números inteiros e Criptografia RSA*, Série de Computação e Matemática, IMPA/SBM, Rio de Janeiro, 1997.

Santos, José Plínio de Oliveira,. *Introdução à Teoria dos Números,* Coleção Matemática Universitária, IMPA, Rio de Janeiro, 1998.