Método de Criptografia RSA

Eliani Magalhães Beloni, Antônio Aparecido de Andrade (orientador), Campus de São José do Rio Preto, Instituto de Biociências, Letras e Ciências Exatas, Matemática, elianimb2010@bol.com.br, PICME/CNPq.

Palavras Chave: *Criptografia, RSA, primos*

Introdução

A *criptografia* é uma área da Matemática que estuda os métodos para codificar e decodificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. Essa tarefa de escrever mensagens secretas é muito antiga. Nasceu com a diplomacia e com as transações militares e hoje em dia, o método de Criptografia RSA, que possui chave pública, é um dos mais utilizados na troca de informações sigilosas, como em transações financeiras e no uso seguro da internet. Para se utilizar tal método é necessário ter conhecimento de Teoria dos Números, pois são abordados assuntos como números primos, congruência, número inverso, teorema de Fermat e teorema Chinês do Resto.

Objetivos

Entender o funcionamento do método RSA, com o objetivo de analisar a dificuldade em se quebrar uma mensagem codificada no RSA.

Material e Métodos

O material utilizado neste trabalho foram livros didáticos e científicos e a metodologia utilizada foi a pesquisa individual e encontros quinzenais com supervisão do professor orientador.

Resultados e Discussão

O método RSA possui três etapas: Pré-codificação, Codificação e Decodificação.

Pré-codificação: Consiste em convertermos as letras em números, com base na tabela abaixo.

Tabela 1. Pré-codificação.

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

Exemplo: A palavra MATEMÁTICA é convertida no número: 22102914221029181210. Vamos agora determinar a chave pública n=pq, onde p e q são dois primos distintos muito grandes. Fazendo p=17 e q=23, temos n=391 e o número anterior pode ser quebrado nos blocos: 22-102-91-42-210-291-8-12-10, que são menores que n. Veja que tais blocos não correspondem a nenhuma unidade linguística, o que torna a decodificação por contagem de frequência impossível.

Codificação: Consiste em codificar cada bloco b separadamente, obtendo C(b), onde C(b)= resto da divisão de b^3 por n. No exemplo que estamos considerando, o bloco 22 é codificado como o resto da divisão de 22^3 por 391, que por congruência, C(22)=91. Assim, tem-se $22^3 \equiv 22^2 \cdot 22 \equiv 484 \cdot 22 \equiv 93 \cdot 22 \equiv 2046 \equiv 91 \pmod{391}$. Codificando todos os blocos, obtemos a mensagem codificada: 91-34-114-189-165-178-121-164-218.

Decodificação: Consiste em reconstruir o bloco original antes da codificação. Para isso precisamos de dois números: n e o inverso d>0 ,onde pela definição de inverso: $3d \equiv 1 \pmod{(p-1)(q-1)}$, e o par (n,d) é chamado de chave de decodificação que deve ser mantido em segredo. Mas como esse método pode ser tão eficaz se para quebrá-lo basta fatorar o número n? Acontece que n é um número muito grande e não existe nenhum algoritmo conhecido capaz de fatorar inteiros grandes de modo realmente eficiente. Assim, seja a um bloco codificado, denotamos D(a)= resto da divisão de a^d por n. No exemplo, temos $(p-1)(q-1)=16 \cdot 22=352$, com d=235, já que $3d \equiv 3 \cdot 235 \equiv 705 \equiv 1 \pmod{352}$. Aplicando a receita para a=91, segue que $91^{235} \equiv 6^{235} \equiv (6^{16})^{14} \cdot 6^{11} \equiv (6^2)^5 \cdot 6 \equiv 2^5 \cdot 6 \equiv (-2) \cdot 6 \equiv 5 \pmod{17}$ $91^{235} \equiv 22^{235} \equiv (-1)^{235} \equiv -1 \equiv 22 \pmod{23}$.

Observação: Usamos o **Teorema de Fermat:** Se p é número primo e a é um inteiro que não é divisível por p então $a^{p-1} \equiv 1 \pmod{p}$.

Agora, fazendo $x=91^{235}$, segue que $x \equiv 5 \pmod{17}$ e $x \equiv 22 \pmod{23}$. Pelo teorema Chinês do resto, x=23q+22. Deste modo, $23q+22 \equiv 5 \pmod{17}$, $6q \equiv 0 \pmod{17}$, $6 \cdot 3q \equiv q \equiv 0 \cdot 3 \equiv 0 \pmod{17}$. Assim $x=23 \cdot 0+22=22$, ou seja, D(91)=22. Fazendo isso com os demais blocos codificados chegaremos a mensagem inicial.

Conclusões

O método de chaves públicas RSA é muito eficaz e seguro, além de ser muito difícil de ser quebrado dada a dificuldade em se fatorar um número grande.

Agradecimentos

Agradeço ao meu orientador pelo apoio e incentivo e também ao CNPq pelo auxílio financeiro.

Bibliografia

[1]Coutinho, S.C. *Números inteiros e Criptografia RSA*. Rio de Janeiro: IMPA, **2009**

[2] Coutinho, S. C.*Criptografia*. Rio de Janeiro, **2008**