UNIVERSIDADE FEDERAL DO AMAZONAS
PRÓ-REITORIA DE PESQUISA E PÓS GRADUAÇÃO
DEPARTAMENTO DE APOIO A PESQUISA
PROGRAMA INSTITUCIONAL DE INICIAÇÃO CIENTÍFICA

RIGOR CIENTÍFICO EM LÓGICA MATEMÁTICA E ÁLGEBRA - APLICAÇÕES À CRIPTOGRAFIA

Bolsista: Carla Almeida Rodrigues, CNPq

Manaus
2009

UNIVERSIDADE FEDERAL DO AMAZONAS
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO DE APOIO À PESQUISA
PROGRAMA INSTITUCIONAL DE INICIAÇÃO CIENTÍFICA

RELATÓRIO PARCIAL
PIB - E/0081/2008

Bolsista: Carla Almeida Rodrigues

Orientador: Prof. Dr. Nilomar Vieira de Oliveira

Manaus
2009

Sumário

Introdução

Neste relatório encontram-se estudos feitos em Lógica Matemática e Algebra, e alguns resultados em relação ao estudo principal do projeto, a Criptografia.

A *Criptografia* é a arte ou a ciência de escrever em cifra ou em códigos mensagens, de forma a permitir que somente o destinatário a decifre e a compreenda, ou seja, a Criptografia transforma textos originais em textos cifrados e ilegíveis. De uma forma mais estrita, a criptografia obtém métodos matemáticos de codificar e decodificar uma mensagem de modo que apenas seu destinatário, através do uso de uma chave de decodificação, possa interpretá-la.

Uma das primeiras técnicas criptográficas foi a cifra de César ou cifra por substituição usada pelo imperador romano Júlio César para transmitir mensagens aos seus exércitos. A técnica consiste em substituir letras do alfabeto por símbolos ou por outras letras. No ano de 1563, Blaise de Viginére criou um novo sistema que inicialmente não podia ser criptoanalisado por análise de frequência de símbolos. O sistema era baseado em mais de um alfabeto e conhecido como método de cifragem polialfabético. Em 1854 a Cifra de Viginére foi quebrada por Charles Babbage e, por muitos anos, nenhum outro método de criptografia foi desenvolvido de modo a apresentar relativa segurança. Antes do início da Segunda Gerra Mundial, no final da década de vinte, a Alemanha havia desenvolvido uma máquina de criptografia mecânica batizada de *Enigma* que utilizou métodos já conhecidos de substituição e transposição de forma tão complexa que a criptoanálise manual de suas mensagens era quase impossível. Quebrar o código da Enigma se tornou uma questão de vida ou morte. Um certo matemático inglês desempenhou papel fundamental para a quebra do código.

Na década de 70 surgiu um novo método criptográfico, o chamado algoritmo assimétrico. A idéia foi criada por Diffe e Hellman, e colocada em prática com o desenvolvimento do RSA criado por Ronald L. Rivest, Adi Shamir e Leonard Adleman, recebendo assim suas iniciais. O método tem base teórica na álgebra abstrata e na teoria dos números. Devido ao apelo matemático deste método, no decorrer deste projeto nos aprofundaremos mais nas técnicas da criptografia RSA.

Encontra-se também neste relatório o cronograma das atividades realizadas e as referências bibliográficas utilizadas.

Objetivos

Objetivo Geral:

Incentivar a participação dos estudantes de graduação em projetos de pesquisas, para que desenvolvam a prática e o pensamento científico com a orientação de grandes pesquisadores. Qualificar os profissionais desta área expandindo seus conhecimentos de forma rigorosa, tanto no projeto como em sua graduação ajudando os mesmos a terem um aprendizado e progresso de conhecimentos matemáticos. Capacitar os participantes para entrarem no mercado de trabalho ou na área de pesquisa.

Objetivo Específico:

Enriquecer o conteúdo com relação a Lógica Matemática e Álgebra, com ênfase em Criptografia, ilustrando de maneira simples os estudos e relatando a importância do projeto no desenvolvimento da matemática, ampliando os conhecimentos e dando ao bolsista maturidade em sua formação acadêmica, dando-lhe um maior grau de abstração, preparando-o para um nível mais avançado de estudo, por exemplo, curso de pós-graduação *Lato Sensu* e *Stricto Sensu* em Matemática.

Metodologia

O projeto tem ênfase em duas grandes áreas da matemática, a Lógica Matemática e a Álgebra. A metodologia utilizada está de acordo com as normas científicas. Nesse contexto, tivemos como fontes de pesquisa livros específicos das duas áreas já referidas, além de outros de áreas da Matemática que nos deram suporte ao estudo que estamos realizando, e serviram para o enriquecimento de conteúdos e exposição do projeto. O conhecimento adquirido foi assimilado através de aulas oferecidas pelo departamento de Matemática da UFAM, estudo individual e em grupo, e resoluções de exercícios.

Capítulo 1

Preliminares

1.1 Lógica Matemática

Definição 1 *Proposição é uma sentença declativa que é verdadeira ou falsa mas não ambas as situações.*

Ou seja, dada uma proposição, ela pode assumir um dos valores: ela é verdadeira ou ela é falsa.

Adotando assim os seguintes princípios:

Principio da não-contradição: uma proposição não pode ser falsa e verdadeira ao mesmo tempo.

Principio do terceiro excluído: uma proposição é verdadeira ou falsa, a terceira possibilidade não existe.

Definição 2 *Tautologia é uma proposição que é sempre verdade, independentemente dos valores lógicos das proposições que a compõe. Por outro lado uma contradição é sempre falsa.*

Definição 3 (Tabelas-Verdade) *A cada proposição supomos valores lógicos sempre associados: falso ou verdadeiro.*

1.2 Os Conectivos Lógicos

	símbolos	significados
conjunção	$\wedge$	*e*
disjunção	$\vee$	*ou*
negação	$\neg$	*não*

	Símbolos	Significados
condicional	$\Rightarrow$	(se...então)
bicondicional	$\Leftrightarrow$	(se e somente se)

Capítulo 2

Resultados

2.1 Introdução

Vamos retormar uma revisão de alguns aspectos históricos da Criptografia antes de apontarmos seus aspectos teóricos, fundamentados através da Teoria dos Números. O termo *Criptografia* surgiu da fusão das palavras gregas *Kriptós* e *gráphein* que significam *oculto* e *escrever*, ou seja, é uma *escrita escondida*. A Criptografia estuda os métodos de codificar uma mensagem de forma que só o destinatário possa interpretá-la. É a arte dos *códigos secretos*, o mais simples destes códigos é a técnica de trocar as letras do alfabeto. Uma técnica semelhante foi o usado pelo imperador *César* para comunicar-se com suas tropas em combate pela Europa. Todo código vem acompanhado de duas receitas, uma para codificar e outra decodificar uma mensagem. Decodificar é o que o usuário legítimo faz quando recebe uma mensagem e quer lê-la, já decifrar é ler uma mensagem sem ser o usuário legítimo, ou seja, para decifrar uma mensagem é necessário quebrar o código. Os códigos como o de César são muito fáceis de decifrar, devido a frequência de cada letra em uma palavra, por exemplo: na língua portuguesa as vogais são mais frequentes que as consoantes e a vogal mais frequente é o A, tornando-se assim um método não muito confiável.

Assim, foi necessário inventar novos códigos, que fossem difíceis de decifrar, mesmo com a ajuda de um computador. Estes códigos foram criados para o uso em aplicações comerciais, e não na comunicação entre espiões, por isso os códigos são todos de *chave pública*. Esta foi uma idéia introduzida em 1976 por *Diffie* e *Hellman* da Universidade de Stanford. No código usado por César, se você sabe codificar então sabe decodificar, já em um código de *chave pública* saber codificar não significa saber decodificar. Isto

parece impossível, pois se sei codificar para decodificar é só desfazer o que fiz, mas nesse método desfazer o processo de codificação pode não ser tão fácil quanto parece.

O método de criptografia de chave pública mais conhecido é o RSA. Este foi um código inventado em 1978 por R.L.Rivest, A.Shamir e L. Adleman. As letras RSA correspondem às iniciais dos inventores do código, esse é atualmente o método mais usado nas aplicações comerciais.

O RSA é um grande exemplo de criptografia de chave assimétrica. Isto é, há uma chave pública, que todos conhecem e serve para codificar a mensagem. Porém, há uma chave privada, que é usada para decodificar a mensagem.

Exemplo: Para codificar uma mensagem utiliza-se um número $n = pq$, produto de dois primos. Essa é a chave pública. A chave privada é constituida pelos primos p e q.

A segurança do método vem do fato de que é difícil fatorar n para descobrir p e q, já que são números muito grandes (de 150 algarismos ou mais). Mas:

Como fatorar um número inteiro de maneira eficiente?

Como determinar se um dado inteiro é primo?

E a parte da matemática que estuda as propriedades dos números inteiros é a teoria de números, a qual enfocaremos sucitamente na seção seguinte.

2.2 Teoria dos Números Básica

Definição 4 *Sejam $a, b \in \mathbb{Z}$, dizemos que $a \mid b$ se existir um $k \in \mathbb{Z}$ tal que $b = ak$. Se a não divide b denotamos $a \nmid b$.*

Proposição 1 *Seja a, b e $k \in \mathbb{Z}, a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração Se $a \mid b$ e $b \mid c$ então existem k_1 e $k_2 \in \mathbb{Z}$ que $b = k_1 a$ e $c = k_2 b$, substituindo b na equação $c = k_2 b$ temos $c = k_1 k_2 a$ logo $a \mid c$.

Exemplo 1 (a) $3 \mid 12$ e $12 \mid 48$, então $3 \mid 48$. (b) $5 \,|\, 25$ e $25 \,|\, 125$, então $5 \,|\, 125$.

Proposição 2 *Se a, b, c, m e $n \in \mathbb{Z}$, $c \mid a$ e $c \mid b$ então $c \mid (ma + nb)$.*

Demonstração Se $c \mid a$ e $c \mid b$ então $a = k_1 c$ e $b = k_2 c$, multiplicando por m e n respectivamente temos $ma = mk_1 c$ e $nb = nk_2 c$, somando-se temos $ma + nb = (mk_1 + nk_2)c$ logo $c \mid (ma + nb)$.

Exemplo 2 $4 \,|\, 28$ e $4 \,|\, 32$ então $4 \,|\, (3 \times 28 + 7 \times 32) = 4 \,|\, (84 + 224) = 4 \,|\, 308$.

Propriedades da Divisibilidade

(i) $n \mid n$

(ii) $d \mid n \Rightarrow ad \mid an$

(iii) $ad \mid an$ e $a \neq 0 \Rightarrow d \mid n$

(iv) $1 \mid n$

(v) $n \mid 0$

(vi) $d \mid n$ e $n \neq 0 \Rightarrow |d| \leq |n|$

(vii) $d \mid n$ e $n \mid d \Rightarrow |d| = |n|$

(viii) $d \mid n$ e $d \neq 0 \Rightarrow (n/d)|n$.

Teorema 1 (Eudoxius) *Dados a, b inteiros com $b \neq 0$ então a é multiplo de b ou se encontra entre dois multiplos consecutivos de b, isto é, para cada par de inteiros a e $b \neq 0$ existe um inteiro q tal que, para $b > 0$,*

$$qb \leq a < (q+1)b$$

e para $b < 0$,

$$qb \leq a < (q-1)b.$$

Exemplo Se $a = 7$ e $b = 3$, tomamos $q = 2$
$qb \leq a < (q+1)b$
$2 \times 3 \leq 7 < (2+1) \times 3$
$6 \leq 7 < 9$

Se $a = 7$ e $b = -3$, tomamos $q = -2$
$qb \leq a < (q-1)b$
$(-2) \times (-3) \leq 7 < (-2-1) \times (-3)$
$6 \leq 7 < 9$

Teorema 2 (Algoritmo da Divisão) *Sejam $a, b \in \mathbb{Z}, b > 0$, existe um único par de inteiros q e r tais que*

$$a = qb + r, \ \textit{com } 0 \leq r < b \qquad (r = 0 \Leftrightarrow b \,|\, a).$$

Demonstração (*Existência*) Pelo teorema de Eudoxius, como $b > 0$, existe q que satisfaz a seguinte desigualdade

$$qb \leq a < (q+1)b,$$

e isso nos diz que $a - qb \geq 0$ e $a - qb < b$. Assim, se chamarmos $r = a - qb$, então teremos garantido a existência de q e r.

(*Unicidade*) Suponhamos que existam r e r_1, q e q_1 tais que:

$$a = qb + r \qquad \text{com} \qquad 0 \leq r < b$$

e

$$a = q_1 b + r_1 \qquad \text{com} \qquad 0 \leq r_1 < b.$$

Assim, das duas desigualdades acima, podemos deduzir que

$$(qb + r) - (q_1 b + r_1) = 0 \Rightarrow b(q - q_1) = r_1 - r,$$

donde $b|(r_1 - r)$. Agora, como $r_1 < b$ e $r < b$, devemos ter $|r_1 - r| < b$ e, conseqüentemente, como $b|(r_1 - r)$ devemos ter $r_1 - r = 0$, o que implica que $r = r_1$. E, deste fato, concluímos que $q_1 b = qb \Rightarrow q_1 = q$, pois $b \neq 0$.

Definição 5 *O Maximo Divisor Comum de $a, b \in \mathbb{Z}$ (a ou b diferente de zero), denotado por (a, b), é o maior inteiro que divide a e b.*

Teorema 3 *Seja d o máximo divisor comum de a e b, então existem n_0 e $m_0 \in \mathbb{Z}$ tais que $d = n_0 a + m_0 b$.*

Demonstração Seja B o conjunto de todas as combinações lineares $\{na + mb\}$ e d o menor entre todos os elementos estritamente positivos de B. Portanto, $d = n_0 a + m_0 b$. Mostraremos que d é o máximo divisor comum de a e b. Assim temos $d \geq 0$. Aplicando o algoritmo da divisão em a e d, o que é possível, pois $d > 0$: $a = qd + r$ $(0 \leq r < d)$, ou $a - qd = r$, e substituindo o valor de d temos: $r = a - q(n_0 a + m_0 b) = (1 - qn_0)a + (-qm_0)b$. Isto mostra que $r \in B$. Então, r não pode ser estritamente positivo, pois é menor que d(= mínimo de B).Logo, $r = 0$ e, portanto, $a = dq$. Ou seja $d|a$ e de forma análoga se prova que $d|b$. Como c é um divisor comum de a e b $(c|a \ e \ c|b, \ c > o)$, existem inteiros k_1 e k_2 tais que $a = k_1 c$ e $b = k_2 c$ e, portanto, $d = n_0 a + m_0 b = n_0 k_1 c + m_0 k_2 c = c(n_0 k_1 + m_0 k_2)$, o que implica que $c|d$. Pela propriedade da divisibilidade (vi), temos que $d \geq c$, isto é, d é o divisor comum positivo de a e b, concluímos que $d = n_0 a + m_0 b$.

Teorema 4 *O máximo divisor comum d de a e b é o divisor positivo de a e b o qual é divisível por todo divisor comum.*

Demonstração Do teorema anterior e pela Proposição 2 da divisão concluímos que se d_1 é divisor comum de a e b, então $d_1|d$. Portanto não podem existir dois números tendo cada um a propriedade de ser divisível por todo divisor comum. Isto por causa da Propriedade (vii) que, no caso de números positivos d_1 e d, nos diz que d_1 deve ser igual a d.

Proposição 3 *Para todo inteiro positivo t, $(ta, tb) = t(a, b)$.*

Demonstração Pelo Teorema 3 (ta, tb) é o menor valor positivo de $(mta + ntb)$, com m, n são números inteiros, que é igual a t vezes o menor valor positivo de $ma + nb = t.(a, b)$.

Proposição 4 *Se $c > 0$ e a e b são divisíveis por c, então*

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}(a, b)$$

Demonstração Como a e b são divisiveis por c, temos que a/c e b/c são inteiros, então substituindo na Proposição 3 "a" por "a/c" e "b" por "b/c" tomando $t = c$.

Corolário 1 *Se $(a, b) = d$, temos que $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.*

Demonstração Pela demonstração anterior temos que c é o divisor comum de a e b. Se tomarmos c como sendo o máximo divisor comum d, temos o resultado desejado.

Definição 6 *Sejam $a, b \in \mathbb{Z}$ são relativamente primos quando $(a, b) = 1$.*

Teorema 5 *Para a, b e x números inteiros temos $(a, b) = (a, b + ax)$.*

Demonstração Sejam $d = (a, b)$ e $f = (a, b + ax)$. Pelo Teorema 3 existem n_0 e $m_0 \in \mathbb{Z}$ tais que $d = n_0a + m_0b$ e como esta expressão pode ser escrita como $d = a(n_0 - xm_0) + (b + ax)m_0$, concluímos que o máximo divisor f de a e $b + ax$ é o divisor de d. Tendo mostrado que $f|d$, mostraremos que $d|f$. Pela Proposição 2 da divisão, $d|(b + ax)$ e pelo Teorema 4 sabemos que todo divisor comum de a e $b + ax$ é um divisor de f. Tendo, assim provado que $d|f$, uma vez que ambos são positivos.

Teorema 6 *Se $a|bc$ e $(a, b) = 1$, então $a|c$.*

Demonstração Como $(a, b) = 1$ pelo teorema 1 existem inteiros n em tais que $na + mb = 1$. Multiplicando - se os dois lados desta igualdade por c temos: $n(ac)+m(bc) = c$. Como $a|ac$ e, por hipótese, $a|bc$ então, pela Proposição 2 da divisão, $a|c$.

Teorema 7 *Se a e b são inteiros e $a = qb + r$ onde q e r são inteiros, então $(a, b) = (b, r)$.*

Demonstração Da relação $a = qb + r$ podemos concluir que todo divisor de b e r é um divisor de a (Proposição 2). Esta mesma relação, escrita na forma $r = a - qb$, nos diz que todo divisor de a e b é um divisor de r. Logo o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e r, o que nos garante o resultado $(a, b) = (b, r)$.

Definição 7 (Números Primos) *Diz - se que um inteiro positivo $p > 1$ é um número primo ou apenas um primo, se e somente se 1 e p são os seus únicos divisores positivos. Um inteiro positivo maior que 1 e que não é primo diz - se composto.*

Proposição 5 *Sejam a, b, c $\in \mathbb{Z}$ e suponhamos que mdc(a,b) = 1.*
1. Se b|ac então b|c.
2. Se a|c e b|c então ab|c.

Teorema 8 (Algoritmo Euclidiano) *Sejam a, b $\in \mathbb{Z}_+$, n$\neq$0, a$\geq$b. Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$r_{j-2} = r_{j-1}q_j + r_j, \qquad 0 \leq r_j < r_{j-1}$$

para j = 0, 1, 2, ..., n e $r_n = 0$ então mdc(a, b) = r_{n-1}, o último resto não nulo.

Teorema 9 (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*

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

Definição 8 (Congruência) *Se a e b são inteiros dizemos que a é congruente a b módulo m (m > 0) se m $|(a - b)$. Denotamos isto por $a \equiv b \mod m$.*
Se m $\nmid$ (a - b) dizemos que a é incongruente a b módulo m.

Exemplo: $11 \equiv 3 \mod 2$, pois 2 | (11 - 3).

Proposição 6 *Se a e b são inteiros, temos que $a \equiv b \mod m$ se, e somente se, existir um inteiro k tal que $a = b + km$.*

Demonstração Se $a \equiv b \mod m$, então m divide $(a-b)$ e, então existe um $k \in \mathbb{Z}$ tal que $a - b = km$, logo $a = b + km$. A recíproca também é verdade.

Proposição 7 *Se a, b, m e d são inteiros, $m > 0$, as seguintes sentenças:*

1. $a \equiv a \mod m$
2. *Se* $a \equiv b \mod m$, *então* $b \equiv a \mod m$
3. *Se* $a \equiv b \mod m$ *e se* $b \equiv c \mod m$, *então* $a \equiv c \mod m$.

Demonstrações

1. Esta propriedade é imediata, pois $a - a = 0 = m \times 0$
2. Se $a \equiv b \mod m$ então m divide $(a-b)$ e, consequentemente, $a - b = km$ para algum $k \in \mathbb{Z}$. Mas, $b - a = -mk = m \times (-k)$, de forma que m divide $(b-a)$, isto é, $b \equiv a \mod m$
3. Se $a \equiv b \mod m$, então existe algum $k_1 \in \mathbb{Z}$ tal que $a - b = k_1 m$. Semelhantemente, como $b \equiv c \mod m$, então existe algum $k_2 \in \mathbb{Z}$ tal que $b - c = k_2 m$ e, consequentemente, $(a-c) = (a-b) + (b-c) = (k_1 + k_2)m$. Assim, $(a-c)$ é múltiplo de m e, portanto, $a \equiv c \mod m$.

Teorema 10 *Se a, b, c e m são inteiros tais que $a \equiv b \mod m$, então*

1. $a + c \equiv b + c \mod m$
2. $a - c \equiv b - c \mod m$
3. $ac \equiv bc \mod m$

Demonstrações

1. Como $a \equiv b \mod m$ então $a - b = km$ para algum $k \in \mathbb{Z}$, e $(a-b) = (a+c) - (b+c) = km$, de onde $a + c \equiv b + c \mod m$.
2. Como $a \equiv b \mod m$ então $a - b = km$ para algum $k \in \mathbb{Z}$, e $(a-b) = (a-c) - (b-c) = km$, de onde $a - c \equiv b - c \mod m$.

3. Como $a \equiv b \mod m$ então $a - b = km$ para algum $k \in \mathbb{Z}$, implicando que $(a-b)c = (km)c = (kc)m$, isto é, $(a-b)c$ é múltiplo de m, pois $kc \in \mathbb{Z}$, e então $ac \equiv bc \mod m$.

Teorema 11 (Teorema do Resto Chinês) *Sejam m_1, $m_2, ...$, m_r números inteiros positivos tais que o $mdc(m_i, m_j) = 1$, se $i \neq j$. Então, sistema de congruências*

$$\begin{cases} x & \equiv & a_1 \ (mod \ m_1) \\ x & \equiv & a_2 \ (mod \ m_2) \\ & \vdots & \\ x & \equiv & a_r \ (mod \ m_r) \end{cases}$$

admite única solução côngruas módulo $m_1 m_2 ... m_r$.

Teorema 12 (Pequeno Teorema de Fermat) *Seja p um número primo e a um número inteiro, então.*
$a^p \equiv a \ (mod \ p)$

Definição 9 (Função ϕ de Euler) *Chama - se função de Euler a função aritmética $\phi(fi)$ assim definida para todo inteiro positivo n:*

$\phi \ (n)$ = *número de inteiros positivos que não superam n e que são primos com n.*

Teorema 13 ($\phi \ (n)$) *Se o inteiro n>1, então $\phi \ (n) = n - 1$ se e somente se n é primo.*

2.3 Criptografia

Pré-codificação

A mensagem a ser criptografada será *matemática.*
O primeiro passo é, converter as letras em números usando a seguinte tabela.

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

Obs: Os espaços entre as palavras será substituido pelo numero 99, mas neste caso especifico não utilizaremos.

A pré-codificação ficará assim:

22102914221029181210

Agora, os numeros acima devem ser quebrados em blocos, a forma de escolher os blocos não é única, mas cada bloco deve ser menor que n. Não pode começar um bloco por *0* e também deve-se tomar o cuidado para que eles não correspondam a nenhuma unidade linguística, para impossibilitar a decifração por contagem de frequência.

Assim tomemos $p = 17$ e $q = 23$ dois primos quaisquer, logo $n = p \times q = 17 \times 23 = 391$. Os blocos ficarão assim:

22 - 102 - 91 - 42 - 210 - 2 - 91 - 81 - 210

Codificação

A chave de codificação é o par *(n,e)* sendo e um inteiro positivo que é inversível $\phi(n)$ ou seja o $mdc(e, \phi(n)) = 1$, na verdade e é o menor primo que não divide $\phi(n)$, neste caso escolhemos *e=3*. Para codificar um bloco b, sendo que b é um inteiro positivo menor que n. Denotaremos o bloco codificado por *C(b)*.

C(b)= resto da divisão de b^e por n.

Codificando cada bloco separadamente:
$22^3 \equiv 93.22 \equiv 91 \mod 391$

$102^3 \equiv 238.102 \equiv 34 \mod 391$
$91^3 \equiv 70.91 \equiv 114 \mod 391$
$42^3 \equiv 200.42 \equiv 189 \mod 391$
$210^3 \equiv 308.210 \equiv 165 \mod 391$
$2^3 \equiv 8 \mod 391$
$91^3 \equiv 70.91 \equiv 114 \mod 391$
$81^3 \equiv 305.81 \equiv 72 \mod 391$
$210^3 \equiv 308.210 \equiv 165 \mod 391$

Logo a mensagem codificada fica assim:

91 - 34 - 114 - 189 - 165 - 8 - 114 - 72 - 165

Decodificação

Para decodificar um bloco da mensagem codificada. Precisamos de n e o inverso de e em $\phi(n)$, que chamaremos de d, ou seja, a chave de decodificação é o par *(n,d).*

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

Sendo que a é o bloco codificado e que $\phi(n) = (p-1).(q-1)$, então
$\phi(n) = 16.22 = 352$
Para calcular d iremos aplicar o algoritmo euclidiano estendido.
Dividindo ϕ (391) = 352 por 3.

$$352 = 117.3 + 1$$

onde

$$1 = 352 + (-117).3$$

Logo o inverso de 3 módulo 352 é -117, como iremos usar d como expoente de potências é necessário que d seja positivo. Portanto $d = 352 - 117 = 235$, que é o menor inteiro positivo congruente a $-117 \mod 352$. Para decodificar dividiremos cada bloco

a pelos primos 17 e 23, que são os primos em que n se fatora.

Como:

$$91 \equiv 6 \mod 17$$

$$91 \equiv 22 \mod 23$$

Assim

$$91^{235} \equiv 6^{235} \mod 17$$

$$91^{235} \equiv 22^{235} \mod 23$$

Aplicando o teorema de Fermat, temos:

$$6^{235} \equiv (6^{16})^{14}6^{11} \equiv 6^{11} \equiv 5 \mod 17$$

$$22^{235} \equiv (22^{22})^{10}22^{15} \equiv 22^{15} \equiv 22 \mod 23$$

$$x \equiv 5 \mod 17$$

$$x \equiv 22 \mod 23$$

Aplicando o Teorema do Resto Chinês no sistema acima, temos:

$M = 17.23 = 391$

$$m_1 = \frac{391}{17} = 23$$
$$m_2 = \frac{391}{23} = 17$$

Colocando na forma de congruência

$23x \equiv 1 \mod 17$ e $17x \equiv 1 \mod 23$

mas $x_1 = 3$ e $x_2 = 19$

Logo $x = 5 \times 23 \times 3 + 22 \times 17 \times 19 = 345 + 7106 = 7451$

Como $7451 \equiv 22 \mod 391$, então $x \equiv 22 \mod 391$

22 corresponde ao primeiro bloco. E procedendo da mesma forma com os outros blocos voltaremos a mensagem original.

Por que o RSA é seguro?

O RSA é um método de chave pública. Sendo p e q os parâmetros desse sistema e $n = pq$. A chave de codificação é a chave pública, portanto o par n,e é conhecido por qualquer usuário, sendo que o RSA só será considerado seguro se for difícil calcular d quando apenas n e e são conhecidas, mas só sabemos calcular d aplicando o algoritmo euclidiano estendido a $\phi(n)$ e e, por outro lado para calcular $\phi(n)$ sem fatorar n de forma a obter p e q é muito difícil. Portanto só é possível quebrar o código se coseguirmos fatorar n, mas se n for muito grande isso será quase impossível.

Conclusão

A Lógica Matemática é um dos campos mais fascinantes e revolucionários do conhecimento humano.

A lógica preocupa-se com o relacionamento entre as premissas e a conclusão, com a estrutura e a forma de raciocínio. De maneira geral pode-se considerar que a lógica possui sempre os mesmos princípios básicos: a lei do terceiro excluído, a lei da não-contradição. Entretanto, a Lógica depois que foi expandida pela invenção da Lógica Matemática relacionou-se com a elucidação de idéias como referências, previsão, identidade, verdade, quantificação, existência, e outras. Diante disso, a Lógica Filosófica está muito mais preocupada com a conexão entre a liguagem natural e a Lógica.

A álgebra tem como objetivo dotar o aluno dos conceitos fundamentais das teorias de grupos. No entanto, apenas conceitos não são suficientes para dar ao aluno uma visão da disciplina, para isto são necessários alguns resultados estruturais, que justificam o trabalho desprendido no estudo de teorias básicas, como por exemplo: A Teoria dos Números. Alguns desses estudos relacionados a teoria dos números são essenciais para o estudo da criptografia RSA.

A Criptografia, por sua vez, é uma técnica muito interessante em toda a sua forma prática. Através dela podemos nos comunicar livremente com segurança. Este é um método usado particularmente pelos bancos para a proteção dos dados de seus clientes.

Cronograma

O desenvolvimento do projeto obedece o seguinte cronograma:

Atividades	Ago	Set	Out	Nov	Dez	Jan	Fev	Mar	Abr	Mai	Jun	Jul
Noções Sucintas de Lógica Matemática		X	X	X	X	X	X					
Apresentação Oral Parcial				X								
Grupos								X				
Propriedades de Grupos								X				
Elaboração do Relatório Parcial				X	X	X						
Subgrupos Normais							X		X			
Congruências								X				
Teorema do Resto Chinês									X			
Pequeno Teorema de Fermat									X			
Criptografia RSA										X	X	
Elaboração do Relatório Final										X	X	
Apresentação Final												X

Referências Bibliográficas

[1] Andrade, Doherty. Elementos de Lógica, Departamento de Matemática, Universidade Estadual de Maringá.

[2] Morais Filho, Daniel Cordeiro de. Um convite à matemática: fundamentos lógicos, com técnicas de demonstração, notas históricas e curiosidades. 2ª edição (revista e ampliada). Campina Grande, EDUFCG, 2007.

[3] Lima, Elon Lages. Curso de Análise; v.1. 12 edição. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2008.

[4] Santos, José Plinio de Oliveira. Introdução à Teoria dos Números. Segunda Edição. Rio de Janeiro: IMPA, CNPq, 2000.

[5] Coutinho, S. C. Números Inteiros e Criptografia RSA. Segunda Edição. Rio de Janeiro: IMPA/SBM, 2000.

[6] Alencar Filho, Edgar de. Teoria dos números. Segunda edição. São Paulo: Nobel, 1985.

[7] Milis, Francisco César Polcino. Coelho, Sônia Pitta. Números: Uma Introdução à Matemática. São Paulo: Editora da universidade de São Paulo, 2000.

[8] Domingues, Hygino H. Iezzi, Gelson. Álgebra Moderna. Quarta edição reform. São Paulo: Atual, 2003.

[9] Wikipédia, disponível em: http://pt.wikipedia.org/wiki/rsa. Acesso no dia 22/09/2008.