2014: Trabalho de Conclusão de Curso do Mestrado Profissional em Matemática - PROFMAT
Universidade Federal de São João del-Rei - UFSJ
Sociedade Brasileira de Matemática - SBM

CRIPTOGRAFIA RSA
TEORIA E PRÁTICA NUMA ABORDAGEM MOTIVACIONAL

Jorge Luiz Vares Raposo [1]
Juan Carlos Zavaleta Aguilar[2]

Resumo: Esse trabalho aborda conceitos da Teoria de Números como instrumentos da construção teórica da Criptografia RSA. Recursos computacionais, onde são implementados o sistema de criptografia RSA, são descritos com o intuito de motivar e complementar o aprendizado dos alunos da educação básica.

Palavras-chave: Teoria dos Números. Criptografia RSA. Maxima.

1 Introdução

A história da humanidade está permeada por avanços no conhecimento gerados por necessidades bélicas. Sendo, infelizmente, uma constante na evolução de todas as sociedades, a guerra traz em seu bojo a necessidade de um dos lados contendores sobrepujar a outra parte. Assim, a busca por inovações tecnológicas, práticas medicinais mais eficazes, equipamentos mais resistentes e meios de comunicações mais seguros, elementos perenes nos campos de batalha, sempre contribuíram para o desenvolvimento das ciências.
O primeiro relato do uso de técnicas de criptografia na história vem justamente da necessidade de se transmitir informações secretas no calor da guerra. Relatos dão conta que o Imperador Romano, Júlio César (13 de julho, 100 a.C. - 15 de março de 44 a.C), utilizava-se de um sistema de codificação para se comunicar com suas tropas em campanha na Europa. Baseado na troca das letras de uma palavra pelas suas respectivas correspondentes, escolhidas a partir de um posicionamento pré-definido, ou uma chave de codificação, esse código funciona da seguinte maneira: suponha que cada letra da palavra será substituída pela terceira letra na sequência das letras do alfabeto, admitido com 23 letras. Assim, o A será substituído pelo D, o B, pelo E, e assim sucessivamente. Por exemplo, a palavra ATACAR seria escrita, usando essa codificação, como DXDFDU.
Embora o código usado por César pode ser considerado hoje como um sistema de fácil decifragem, a idéia de se usar métodos de ocultação de informação prevaleceu e evoluiu ao ponto de chegar a ser, no presente, a principal ferramenta de segurança nas transações executadas no maior avanço tecnológico de comunicação das últimas décadas: a internet. Obviamente, tendo em vista a magnitude do alcance desse meio de comunicação, o sistema de codificação de

[1]Aluno de Mestrado Profissional em Matemática, Turma 2013
Instituição: Universidade Federal de São João del-Rei - UFSJ
E-mail: jorgelvr@ig.com.br
[2]Orientador do Trabalho de Conclusão de Curso
Departamento de Matemática e Estatística - DEMAT, UFSJ
E-mail: jaguilar@ufsj.edu.br

informações não poderia ser baseado em técnicas simplórias, passíveis de serem decodificadas indevidamente. É nesse contexto que surge o sistema de criptografia RSA, assim batizada em homenagem a seus desenvolvedores (Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman), baseado inteiramente na Teoria dos Números, ramo da Matemática que estuda as principais propriedades dos números inteiros [1].
Esse trabalho tem por objetivos principais a abordagem dos conceitos fundamentais envolvidos na elaboração da Criptografia RSA, os quais muitas vezes não recebem a devida relevância na educação básica e a utilização de recursos computacionais em atividades de sala de aula, envolvendo esse sistema de criptagem, com vistas à motivação dos alunos no ensino da Matemática.

2 Embasamento Teórico

O método de criptografia conhecido como RSA baseia-se, como já mencionado na introdução, na Teoria dos Números. Muitos conceitos tratados nessa teoria são abordados no ensino fundamental, sobretudo nos anos intermediários, 6º e 7º anos, sem, contudo, o aproveitamento desses conteúdos de forma mais elaborada. Muitas vezes, o que se observa é uma transmissão de regras, como para se calcular o mínimo múltiplo comum (mmc) ou o máximo divisor comum (mdc), meramente como ferramentas, sem a preocupação com a interpretação dos conceitos, bem como com a de suas utilizações no dia-a-dia. Há que se observar ainda que, em todo ensino médio, nada se trata sobre a Teoria dos Números, ficando relegada apenas àquelas séries intermediárias no ensino fundamental. Uma consequência imediata desse tratamento meramente algorítmico é a dificuldade dos alunos em lidar com conceitos relativamente simples como números primos e números compostos, divisores e múltiplos, entre outros.
A Teoria dos Números trata particularmente dos números inteiros e das propriedades que envolvem esses números. Não é o objetivo desse trabalho descrever toda essa teoria, mas, apenas aqueles conceitos indispensáveis à elaboração da criptografia RSA.

2.1 Divisores e Múltiplos de um número

Sejam a,b e c números inteiros, tais que $a = bc$. Nessas condições, diz-se que b e c dividem a (indica-se esse fato pela notação $b|a$, $c|a$) ou ainda, a é múltiplo de b ou de c. Chama-se também b e c de fatores de a. Assim, verifica-se, por exemplo, que $12 = 3.4$, onde 3 e 4 dividem 12. É interessante notar que 1 é fator de qualquer inteiro a, pois, $a = 1.a$.

2.2 Máximo Divisor Comum - Algoritmo de Euclides

O conceito de máximo divisor comum (mdc) entre números recebe um tratamento muito tecnicista na educação básica, deixando a compreensão relegada a um segundo plano. Veja, por exemplo, organizando-se em conjuntos distintos os divisores positivos de 90 e 24, encontrar-se-iam $D(90) = \{1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90\}$ e $D(24) = \{1, 2, 3, 4, 6, 8, 12, 24\}$. Assim, é imediatamente verificável que 6 é o maior divisor comum entre 24 e 90. É possível se explorar também o fato de que esses números possuem outros divisores comuns, levando-se em consideração inclusive, que quaisquer números que se tenham, sempre haverá pelo menos o número 1 como divisor comum.

O processo de se listar todos os divisores de cada um dos números envolvidos na operação pode ser bastante custoso, embora, nele se encerre o conceito de máximo divisor comum. Existem alguns processos que permitem encontrar o mdc entre números, dentre deles destaca-se o Algoritmo de Euclides. Esse algoritmo permite, além de encontrar o mdc entre os números analisados, escrevê-lo como uma combinação linear entre os números. Sejam a e b números inteiros e positivos. O máximo divisor comum entre a e b, utilizando-se Algoritmo de Euclides é processado da seguinte forma:

$$a = b.q_1 + r_1$$
$$b = r_1.q_2 + r_2$$
$$\vdots$$
$$r_{n-2} = r_{n-1}.q_n + r_n \ ,$$

onde $r_n = 0$. O $mdc(\ a,\ b) = r_{n-1}$

Observe o exemplo já citado. Encontrando o máximo divisor comum entre 90 e 24, utilizando o Algoritmo de Euclides, tem-se que

$$90 = 24.3 + 18$$
$$24 = 18.1 + 6$$
$$18 = 6.3 + 0$$

Assim, o mdc(90, 24) = 6.

Usando o tradicional processo prático para o cálculo do mdc entre 90 e 24, obtém-se

quocientes		3	1	3	
	90	24	18	6	mdc
restos	18	6	0		

Sejam a *e* b números inteiros e c o máximo divisor comum entre eles.

Então,

$$\text{mdc}(a,\ b) = c$$
$$c = s.a + t.b,$$

com s e t números inteiros.

O interesse está em encontrar os valores de s e t, tais que

$$s.a + t.b = \text{mdc}(a,\ b).$$

Voltando ao exemplo já tratado.

mdc(24, 90) = 6

18 = 6.3 e 24 = 18. 1 + 6,

onde 18 = 24 - 6.

90 = 24.3+ 18

90 = 24.3 + 24 - 6

90 = 24.4 - 6 = (-1).90 + 4.24

Logo, o mdc(24, 90) = 6 pode ser escrito como uma combinação linear entre 24 e 90, como se segue

6 = (- 1).90 + 4.24.

2.3 Números Primos e Números Compostos

Quando se busca escrever um número inteiro como um produto de fatores, procedimento conhecido como fatoração numérica, o que se está buscando é a decomposição desse número inteiro, em fatores chamados primos. Os primos representam uma classe de números que se caracterizam da seguinte forma: seja p um número primo, então $p \neq \pm 1$ e p é divisível apenas por ± 1 e $\pm p$. Por outro lado, se um número inteiro é diferente de ± 1 e não é primo, ou seja, possui outros divisores, então esse número é chamado composto. Os números 2, 17, - 29 são primos, porém, o número $12 = 3.4$, não é.

2.4 Fatoração de números inteiros

O sistema de criptografia RSA utiliza-se de números primos para a cifragem de mensagens, portanto, determinar se um número é primo ou não é de vital importância para a utilização do processo mencionado. Obviamente, dadas as definições de números primos e números compostos acima descritas, parece, numa primeira análise, que basta verificar que o número inteiro p é composto, ou seja, possui outros fatores primos além de ± 1 e de $\pm p$. Um processo bastante utilizado no ensino básico para se encontrar os fatores de um número inteiro, consiste em se verificar se esse número é divisível pelos números primos, na sequência crescente em que eles se apresentam, repetindo a operação até que o último quociente encontrado seja 1. Esse "algoritmo"pode ser visualizado no exemplo abaixo

$$\begin{array}{r|l} 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$$

Logo, o número 30 pode ser escrito como o produto de seus fatores primos, ou seja, $30 = 2.3.5$, portanto, um número composto.
Embora esse processo seja bastante prático ele carece de eficiência à medida que o número analisado é relativamente grande e, além disso, o número não seja divisível por nenhum dos números primos existentes entre 1 e 10. Isso torna a fatoração desse número um processo mais dificultoso, pois, não possuindo divisores entre os primos já mencionados, obviamente esse número possuirá, se possuir, fatores primos iguais ou superiores a 11. Veja o exemplo do número 403. Ao se verificar seus possíveis divisores entre os primos contidos entre 1 e 10, observa-se que nenhum deles é seu divisor, entretanto, $403 = 13.31$, ou seja, um número composto. O problema prático está justamente em se determinar se dado um número inteiro p, ele é primo ou não, quando o processo por fatoração utilizando os primos 2, 3, 5 e 7 como possíveis divisores de p falha. Nesse contexto, há um processo conhecido como Crivo de Eratóstenes que permite encontrar todos os números primos até um valor pré-determinado. Eratóstenes nasceu em Cirene, no ano 276 a.C. e morreu em 194 a.C., na cidade de Alexandria, ambas cidades da antiga Grécia. Atuou em várias áreas do conhecimento como Geografia, Astronomia e Matemática. É de sua autoria o cálculo da circunferência da Terra, usando noções de trigonometria e semelhança entre triângulos. Sua principal contribuição à Teoria dos Números está justamente na identificação dos números primos, utilizando-se de um processo prático cujo nome já foi mencionado acima.

O método de Eratóstenes para se encontrar os primos existentes até certo valor n definido consiste em se listar todos os números inteiros até n e, a partir do número 2, eliminar dessa lista todos os múltiplos de 2. De igual maneira procede-se com o próximo primo da lista, o número 3, eliminando-se todos seus múltiplos. Assim, segue-se utilizando os primos constantes da lista, até que sobre nela somente números primos.

Exemplo (1). Encontrar todos os números primos positivos existentes entre 1 e 100.

- 1º passo: lista-se todos os números de 1 a 100.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Tabela 1: números naturais de 1 a 100

- 2º passo: elimina-se o número 1 e todos os múltiplos de 2, excetuando-o.

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	
81		83		85		87		89	
91		93		95		97		99	

Tabela 2: exclusão do 1 e dos pares

- 3º passo: elimina-se todos os múltiplos de 3, excetuando-o.

	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	
		83		85				89	
91				95		97			

Tabela 3: exclusão dos múltiplos de 3 maiores que ele

- 4º passo: elimina-se todos os múltiplos de 5, excetuando-o.

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			

Tabela 4: exclusão dos múltiplos de 5 maiores que ele

- 5º passo: elimina-se todos os múltiplos de 7, excetuando-o.

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

Tabela 5: exclusão dos múltiplos de 7 maiores que ele

Observe que não há necessidade de se continuar o processo na sequência crescente dos números primos, ou seja, os próximos múltiplos a serem eliminados da tabela seriam os múltiplos de 11, que já foram eliminados naturalmente pelos passos anteriores. Dessa forma, chega-se à conclusão que os números primos existentes entre 1 e 100 são os que pertencem ao conjunto $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}$.
Obviamente esse processo prático torna-se laborioso à medida que o número pré-determinado é relativamente grande. Veja, por exemplo, determinar se o número 419 é primo, seguindo os passos anteriores "à risca"seria custoso. Então, pode-se simplificar os passos listados acima da seguinte forma: verifica-se se o número 419 é divisível pelos primos 2, 3, 5, 7 e 11, usando critérios de divisibilidade [1].
Se o número não for divisível por nenhum desses primos, deve-se prosseguir na verificação até o último número primo menor ou igual a $\sqrt{419}$, ou seja, 19, dado que $19 \leq \sqrt{419}$.

$$419 = 32.13 + 3 \qquad 419 = 24.11 + 17 \qquad 419 = 22.\boldsymbol{19} + 1$$

Logo, verifica-se que 419 é de fato um número primo, pois nenhum dos primos menores ou iguais a $\sqrt{419}$ é divisor dele. Há aqui duas questões que merecem um tratamento mais elaborado: por que se deve interromper a verificação ao se atingir o último número primo menor ou igual à raiz quadrada do número analisado? Por que o número 1 é excluído da lista de números primos?

Para responder a primeira pergunta, suponha n um número inteiro positivo e composto, tal que $n = p.c$, onde p é o menor fator primo de n. Assim, obviamente que $c \geq p$. Tratando convenientemente essa afirmação, tem-se que $p.c \geq p.p$, mas, como $n = p.c$, pode-se verificar que $n \geq p^2$, ou, por outro lado, $p \leq \sqrt{n}$. Portanto, como verificado no exemplo, se 419 não fosse um número primo, algum fator próprio dele seria encontrado antes da $\sqrt{419}$. Para o segundo questionamento, faz-se necessário enunciar o Teorema da Fatoração Única.

Teorema (1) (Teorema da Fatoração Única): dado um número inteiro positivo $n \geq 2$, pode-se sempre escrevê-lo, de modo único, na forma $n = p_1^{e_1} \cdot ... \cdot p_k^{e_k}$, onde $1 < p_1 < p_2 < ... < p_k$ são números primos e $e_1, ..., e_k$ são inteiros positivos [1].

Veja que o teorema afirma que todo número pode ser escrito de forma única pelo produto de fatores primos, devidamente acompanhados de suas potências necessárias. Dessa forma, se ± 1 fossem considerados números primos, a fatoração do número 2, por exemplo, poderia resultar em 2 ou 2.1^2. Na verdade, qualquer inteiro poderia ter uma infinidade de fatorações, caso não se excluíssem ± 1 dos números primos.

2.5 Números Primos entre si

Há números que não são primos, porém, quando se verifica a existência de divisores em comum entre eles e só se encontra o 1, diz-se que esses números são primos entre si.

Sejam a e b números inteiros e o mdc$(a,\ b) = 1$, então a e b são números primos entre si. Sejam os números compostos 14 e 15, por exemplo. O máximo divisor comum entre eles é igual a 1. É interessante notar que $14 = 2.7$ e $15 = 3.5$, ou seja, não possuem fatores primos em comum, então, pode-se enunciar que números que não possuem fatores primos em comum, possuem o 1 como máximo divisor comum e, portanto, são números primos entre si. Esse fato merece atenção, pois, o conceito de inverso modular está intimamente ligado ao do máximo divisor comum entre números e, sobretudo, números primos entre si.

2.6 Aritmética Modular

Um importante fenômeno observado na Teoria dos Números diz respeito à periodicidade com que os restos de uma divisão se apresentam. Para ilustrar esse fenômeno, observe a tabela abaixo, onde estão incluídos os números de 0 a 15, e seus respectivos restos, quando divididos por 5.

Inteiros	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Restos	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0

Tabela 6: restos da divisão por 5 dos inteiros positivos de 1 a 5

Observe que, na divisão por 5, os restos se repetem a cada 5 inteiros sucessivos, ou seja, nesse exemplo, pode-se afirmar que o período em que ocorrem os valores para o resto é igual a 5. Logo, na execução de uma divisão de um número inteiro positivo a por outro inteiro positivo n, obtem-se $a = nq + r$, com q e r inteiros e $0 \leq r < n$. Os restos r da divisão desse número inteiro positivo a repertir-se-ão com periodicidade igual a n. Por questões de clareza nos conceitos, evitando-se assim, confundir o termo periodicidade com a noção de tempo, usaremos o termo ***módulo*** para definir esses períodos. Assim, utilizando o exemplo acima, diz-se que 9 e 14 possuem o mesmo resto módulo 5.

Verificando na tabela 6, é possível ver que 9 e 14 possuem o mesmo resto quando divididos por 5, ou possuem o mesmo módulo. Nesses casos dizemos que 9 e 14 são congruentes módulo 5. Generalizando, sejam a e b números inteiros, e n um número inteiro e positivo, então, a será congruente a b, módulo n se $n|(a - b)$.

É fácil verificar a veracidade dessa afirmação, como se segue

$$a = n.q_1 + r_1 \text{ e } b = n.q_2 + r_2$$
$$n|(n.q_1 + r_1 - (n.q_2 + r_2))$$
$$n|(n.q_1 + r_1 - n.q_2 - r_2),$$

mas, como a e b são congruentes módulo n, implica que $r_1 = r_2$, portanto,

$$n|n(q_1 - q_2).$$

Para indicar que a e b são congruentes módulo n, usa-se a notação $a \equiv b \ (mod\ n)$ e, se não são congruentes, usa-se $a \not\equiv b \pmod{\text{n}}$

$$4 \equiv 9 \pmod{5}, \text{mas}, 4 \not\equiv 10 \pmod{\text{n}}$$

2.6.1 Propriedades da Congruência Modular

A congruência modular goza de propriedades semelhantes as da igualdade usual, ou seja, reflexiva, simétrica e transitiva. Entretanto, a forma como se demonstra a validade dessas propriedades requer um trabalho um pouco mais elaborado.

Reflexiva: todo número é congruente módulo n a ele mesmo.

$a \equiv a \ (mod\ n)$. Pela definição, $n|(a - a)$, ou seja, $n|0$.

Simétrica: se $a \equiv b \ (mod\ n)$ então $b \equiv a \ (mod\ n)$.

$a \equiv b \ (mod\ n)$, implica que $n|(a - b)$, ou, $a - b = k.n$, onde k é um número inteiro.

Multiplicando $a - b = k.n$ por (- 1), tem-se que

$$b - a = (-k).n, \text{ ou seja, } n|(b - a).$$

Transitiva: Se $a \equiv b \ (mod\ n)$ e $b \equiv c \ (mod\ n)$, então $a \equiv c \ (mod\ n)$.

$a \equiv b \ (mod\ n)$ implica que a - b = k.n e $b \equiv c \ (mod\ n)$ implica que $b - c = j.n$,

onde k e j são números inteiros.

Assim,

$$(a - b) + (b - c) = k.n + j.n$$
$$a - c = (k + j).n$$
$$a \equiv c \ (mod\ n).$$

2.6.2 O conceito de resíduos

Sejam a e n números inteiros, com $a > 0$. Dividindo a por n obtém-se

$$a = n.q + r \text{ e } 0 \leq r < n$$

$$a - r = n.q,$$

que, por definição, equivale a dizer que $a \equiv r \ (mod\ n)$.
Assim, pode-se afirmar que todo número inteiro positivo é congruente módulo n ao resto de sua divisão por n. Usa-se chamar r de o resíduo de a módulo n, e esse resíduo é único. De fato, suponha que

$$a \equiv r \ (mod\ n), \text{ com } 0 \leq r \leq n-1;$$

$$a \equiv r' \ (mod\ n), \text{ com } 0 \leq r' \leq n-1$$

pelas propriedades simétrica e transitiva, tem-se que

$$r \equiv r' \ (mod\ n).$$

supondo $r \geq r'$, $n|(r - r')$, mas r e r' são menores que n, logo, $0 \leq r - r' < n$. Dessa forma, $r - r'$ só pode ser múltiplo de n se $r - r' = 0$, ou seja, $r = r'$.
A utilização da designação resíduo no lugar de resto possui sua sutileza. Enquanto o termo resto aplica-se geralmente a números inteiros positivos, usa-se resíduo para qualquer inteiro. De fato, supondo $n = 8$ e $a = -23$. O objetivo é encontrar um resíduo r, com $0 \leq r < 8$, tal que $-23 \equiv r \ (mod\ 8)$.
Observe que $23 = 2.8 + 7$. Se multiplicar por (- 1) ambos os lados dessa igualdade, tem-se $-23 = (-2).8 - 7$, onde $-23 \equiv -7 \ (mod\ 8)$. Entretanto, como (- 7) não pertence ao intervalo $0 \leq r < 8$, não é o resíduo procurado. Contudo, $8 = 1 - (-7)$, donde se conclui que $-7 \equiv 1 \ (mod\ 8)$ e, pela propriedade da transitividade, $-23 \equiv 1 \ (mod\ 8)$. Logo, -23 possui resíduo 1 módulo 8.

2.6.3 Adição, Multiplicação e Congruência

Nesse texto já foi abordado que a congruência modular possui propriedades que se assemelham àquelas aplicadas à igualdade. É de se supor também, que certos resultados aplicados à soma e à multiplicação numa igualdade também podem ser aplicados à congruência.

Se $a \equiv a' \ (mod\ n)$ e $b \equiv b' \ (mod\ n)$, então

- $a + b \equiv a' + b' \ (mod\ n)$;
- $a.b \equiv a'.b' \ (mod\ n)$.

Utilizando o próprio conceito do módulo, tem-se que

$$a - a' = k.n \text{ e } b - b' = j.n.$$

Somando-se os termos dessas equações, obtém-se

$$(a - a') + (b - b') = k.n + j.n,$$

onde, arrumando convenientemente resulta em

$$(a + b) - (a' + b') = (k + j).n$$

ou, conforme se queria demonstrar

$$(a + b) \equiv (a' + b') \ (mod \ n).$$

Partindo do mesmo princípio de que

$$a - a' = k.n \text{ e } b - b' = j.n$$

e, arrumando convenientemente tem-se que

$$a = a' + k.n \text{ e } b = b' + j.n.$$

Multiplicando-se, membro a membro, essas duas equações, obtém-se

$$a.b = (a' + k.n)(b' + j.n) = a'.b' + n.(a'.j + b'.k + k.j.n),$$

ou seja,

$$a.b - a'.b' = n.(a'.j + b'.k + k.j.n),$$

que equivale a dizer que

$$a.b \equiv a'.b' \ (mod \ n),$$

como se queria demonstrar.

2.6.4 Inversos Modulares

O conceito de inversos modulares assemelha-se ao conceito do inverso de números reais diferentes de zero. Enquanto o inverso do número 2 é $\frac{1}{2}$, pois, $2.\frac{1}{2} = 1$, o inverso módulo 5 de 7 é 3. Observe, $7 \equiv 2 \ (mod \ 5)$ e $3 \equiv 3 \ (mod \ 5)$, entretanto, $7.3 \equiv 1 \ (mod \ 5)$. De forma intuitiva percebe-se que o inverso modular de um número é justamente aquele que resulta, por meio de um produto, a congruência com 1. Observe a tabela abaixo.

Resíduo	*Inverso Módulo 7*
1	1
2	4
3	5
4	9
5	10
6	6

Tabela 7: resíduo e inverso módulo 7

Sejam a, a' e n números inteiros. Se $a.a' \equiv 1\ (mod\ n)$, então a' é inverso de a módulo n, e vice-versa. Há aqui alguns questionamentos interessantes. Todo número inteiro a possui inverso modular n? O inverso modular de um número, se existir, é único?
Observe a tabela abaixo.

Resíduo	*Inverso Módulo 8*
1	1
2	-
3	3
4	-
5	5
6	-
7	7

Tabela 8: resíduo e inverso módulo 8

Na tabela 8 é possível verificar que 2, 4 e 6 não possuem inverso modulo 8. Em outras palavras, não há número inteiro que multiplique 2, 4 ou 6 e produza resto 1, quando dividido por 8. Observe que justamente esses números possuem fator primo comum com o 8. Esse fato está descrito no seguinte teorema.

Teorema (2): Sejam $a < n$ inteiros positivos. O resíduo a tem inverso módulo n se, e somente se, a e n não têm fatores primos em comum. Ou, descrito de outra forma, o resíduo a possui inverso módulo n, se a e n forem primos entre si, ou, mdc(a, n) = 1.

Sejam a e n dois números inteiros e positivos tais que $1 < a < n$. Além disso, admiti-se que a e n possuam um fator primo p, com $1 < p < n$, comum a ambos. Então, $n = p.c$ e $a = p.d$. É fácil verificar que $c = \frac{n}{p}$, onde $1 < c < n$. Como já definido acima, tem-se também que $1 < a < n$, logo, c não é congruente a 0 módulo n e a não é congruente a 0 módulo n.
Tratando convenientemente a congruência $a \equiv a\ (mod\ n)$, tem-se

$$a \equiv p.d\ (mod\ n)$$

$$c.a \equiv c.p.d\ (mod\ n),$$

mas,

$$c.p = n$$

$$c.a \equiv n.d\ (mod\ n),$$

mas,

$$c.p \equiv n \equiv 0\ (mod\ n),$$

portanto,

$$c.a \equiv c.p.d \equiv 0\ (mod\ n),$$

concluindo-se assim, que se a e n possuem fatores primos em comum, não existe inverso a' de a módulo n. Há aqui outra conclusão interessante. Sendo $n = p.c$ e $a = p.d$, demonstrou-se acima que $c.a \equiv 0\ (mod\ n)$.

Uma importante consequência da existência ou não do inverso modular de um número é a possibilidade de se realizar um cancelamento de fatores na congruência. Ou, de forma mais clara, verificar se é possível ou não realizar a seguinte operação $a.b \equiv b.c \ (mod \ n)$, implica que $a \equiv c \ (mod \ n)$.
Supondo que $n > 0$ e $1 \leq a \leq n-1$ são números inteiros que possuem um fator primo p em comum. Então, pode se escrever $n = p.c$ e $a = p.d$.

Sabe-se que $a.c \equiv a.0 \ (mod \ n)$, com a e c positivos e menores que n, o que garante que $a \not\equiv 0 \ (mod \ n)$ e $c \not\equiv 0 \ (mod \ n)$.
Assim, chega-se a seguinte conclusão: se a, b e $n > 1$ são inteiros que possuem fator primo em comum, então a não pode ser cancelado em congruências do tipo $a.b \equiv a.0 \ (mod \ n)$.
Se a admite um inverso módulo n e b e c são inteiros tais que $a.b \equiv a.c \ (mod \ n)$, então a pode ser cancelado, implicando em $b \equiv c \ (mod \ n)$, que é facilmente verificável, como se segue.
Seja a' o inverso de a módulo n. Trabalhando convenientemente a afirmação $a.b \equiv a.c \ (mod \ n)$, tem-se

$$a'.a.b \equiv a'.a.c \ (mod \ n)$$

$$(a'.a).b \equiv (a'.a).c \ (mod \ n),$$

com $a'.a \equiv 1 \ (mod \ n)$, conclui-se que

$$b \equiv c \ (mod \ n).$$

Dessa forma, pode-se enunciar o teorema a seguir.

Teorema (3): Suponha que a possui inverso módulo n. Se $a.b \equiv a.c \ (mod \ n)$, para b e c inteiros, então $b \equiv c \ (mod \ n)$.
O problema agora resume-se a demonstrar que se um número inteiro possui inverso módulo n, esse inverso é único.
Seja a' o inverso de a módulo n. Admitindo que $a"$ também é um inverso de a módulo n. Então, pela definição, tem-se que

$$a.a' \equiv 1 \ (mod \ n) \text{ e } a.a" \equiv 1 \ (mod \ n)$$

$$a".a.a' \equiv a".1 \ (mod \ n)$$

$$(a".a).a' \equiv a".1 \ (mod \ n)$$

$$a' \equiv a" \ (mod \ n),$$

logo $n|(a' - a")$, mas a' e $a"$ são números inteiros positivos menores que n e, portanto, a única maneira de $a' - a"$ ser divisível por n é se $a' - a" = 0$, ou seja, $a' = a"$. Logo, o inverso modular de um número, se existir, é único.

2.7 Teorema Chinês do Resto

Uma importante aplicação da aritmética modular está na determinação de um número inteiro que deixa restos diferentes, quando dividido por números inteiros diferentes.
Exemplo (2). Determinar o menor número inteiro positivo que deixa resto 3 quando dividido por 5, e resto 2 quando dividido por 7.

Escrevendo essas situações em termos de equações, tem-se que

$$x = 5.q_1 + 3 \text{ e } x = 7.q_2 + 2$$

Obviamente, por tratar-se de números relativamente pequenos, há a possibilidade de se chegar a uma solução por tentativa, trabalhando n como uma variável, utilizando-se, por exemplo, de tabelas contendo as seguintes expressões: $q_1 = \frac{x-3}{5}$ *e* $q_2 = \frac{x-2}{7}$, até que os resultados para q_1 e q_2 fossem ambos inteiros e positivos. Ainda assim, há que se considerar o caráter meramente experimental dessa técnica, o que certamente demandaria muito trabalho a medida que os valores envolvidos tornam-se maiores.
Uma interpretação diferente desse problema pode ser feita utilizando-se a congruência modular. As equações acima descritas podem ser resumidas às seguintes congruências:

$$\begin{cases} x \equiv 3 \ (mod\ 5) \\ x \equiv 2 \ (mod\ 7) \end{cases}$$

Num primeiro momento, parece que essa interpretação só mudou a forma de se escrever as equações que podem levar ao valor de n, sem, contudo, trazer algum benefício à solução. Acontece que ao se introduzir o conceito de congruência modular, é possível, utilizando-se sistematicamente dos conceitos e propriedades aplicadas à aritmética modular, chegar a um conjunto de valores que satisfazem essa equação.
A sistematização a qual se refere o texto acima é denominada Teorema Chinês do Resto, cuja primeira menção é encontrada no livro Manual de Aritmética do Mestre Sun, escrito entre os anos 287 d.C . e 473 d.C [1].

Teorema (4) (Teorema Chinês do Resto). Sejam m e n inteiros positivos primos entre si. Se a e b são inteiros quaisquer, então o sistema

$$\begin{cases} x \equiv a \ (mod\ m) \\ x \equiv b \ (mod\ n) \end{cases}$$

sempre possui solução e qualquer uma de suas soluções pode ser escrita na forma

$$a + m.(m'.(b - a) + n.t),$$

onde t é um inteiro qualquer e m' é o inverso de m módulo n.

Seja o sistema

$$\begin{cases} x \equiv a \ (mod\ m) \\ x \equiv b \ (mod\ n) \end{cases}$$

Considere x_0 uma solução dessas congruências, ou seja

$$\begin{cases} x_0 \equiv a \ (mod\ m) \\ x_0 \equiv b \ (mod\ n) \end{cases}$$

Fazendo $x_0 = a + m.k$, com k inteiro, pode-se afirmar que

$$a + m.k \equiv b \ (mod\ n)$$

onde se conclui que

$$m.k \equiv (b-a)\ (mod\ n).$$

Como m e n são primos entre si, m possui inverso módulo n, e chamemos m' esse inverso. Logo

$$m.k \equiv (b-a)\ (mod\ n)\ .(m')$$

$$k \equiv m'.(b-a)\ (mod\ n).$$

Assim, pode-se concluir que

$$k = m'.(b-a) + n.t,\ \text{para algum } t \text{ inteiro.}$$

Substituindo $k = m'.(b-a) + n.t\ em\ x_0 = a + m.k$, tem-se

$$x_0 = a + m.(m'.(b-a) + n.t),$$

onde, qualquer que seja o inteiro t, a expressão $a + m.(m'.(b-a) + n.t)$ é solução do sistema

$$\begin{cases} x \equiv a\ (mod\ m) \\ x \equiv b\ (mod\ n) \end{cases}$$

Voltando ao exemplo (2) apresentado, o sistema

$$\begin{cases} x \equiv 3\ (mod\ 5) \\ x \equiv 2\ (mod\ 7) \end{cases}$$

Tem-se que 5 e 7 são primos entre si, mdc(5, 7) = 1 e que 3 é o inverso de 5 módulo 7, pois $3.5 \equiv 1\ (mod\ 7)$. Então, usando o Teorema Chinês do Resto, as soluções possíveis para o sistema são da forma

$$x = 3 + 5.(3.(2-3) + 7.t),$$

$$x = -12 + 35t,$$

com t inteiro qualquer, que representa todas as soluções possíveis para o sistema apresentado. O menor número inteiro positivo procurado será obtido quando $t = 1$, ou seja

$$x = -12 + 35.1$$

$$x = 23$$

O Teorema Chinês do Resto também pode levar à solução de sistema de congruências do tipo $\begin{cases} x \equiv a\ (mod\ m) \\ x \equiv b\ (mod\ n) \end{cases}$, onde m e n não são primos entre si. Nesse caso há que se observar a regra a seguir.
Considere o sistema de congruências

$$\begin{cases} x \equiv a\ (mod\ m) \\ x \equiv b\ (mod\ n) \end{cases}$$

Admitindo que o máximo divisor comum entre m e n é d, com $d \neq 1$.

- se $d|(b-a)$ então o sistema possui solução;
- se $d \nmid (b-a)$ então o sistema não possui solução.

2.8 Teorema de Fermat

Um problema interessante abordado pela aritmética modular consiste em encontrar os restos da divisão de uma potência por um número qualquer. Obviamente, operações dessa natureza que envolvam potências menores podem ser resolvidas sem maiores dificuldades. Por exemplo, deseja-se encontrar o resto da divisão de 12^2 por 5. É fácil verificar que $12^2 = 144$, e $144 = 28.5 + 4$, onde 4 é o resto procurado. Nesse exemplo, a operação é imediata, porém, a situação muda drasticamente se a potência envolvida torna o processo descrito acima proibitivo. Veja o exemplo a seguir.
Exemplo (3). Encontrar o resto da divisão do número 7^{231} por 11. É evidente que o processo utilizado no exemplo anterior seria inviável, dada a dimensão do trabalho envolvido. Uma vez mais, a aritmética modular oferece uma alternativa a esse desafio. Observe a congruência modular entre as potências de 7 e o número 11.

$$7^1 \equiv 7 \ (mod\ 11)$$
$$7^2 \equiv 5 \ (mod\ 11)$$
$$7^3 \equiv 2 \ (mod\ 11)$$
$$7^4 \equiv 3 \ (mod\ 11)$$
$$7^5 \equiv 10 \ (mod\ 11)$$
$$7^6 \equiv 4 \ (mod\ 11)$$
$$7^7 \equiv 6 \ (mod\ 11)$$
$$7^8 \equiv 9 \ (mod\ 11)$$
$$7^{10} \equiv 1 \ (mod\ 11)$$

E a partir de 7^{11} haverá a repetição periódica dos restos da divisão por 11.
Podemos escrever 7^{231} como $(7^{10})^{23}.7^1$, e como $7^{10} \equiv 1 \ (mod\ 11)$, aplicando as propriedades da congruência, tem-se

$$7^{231} \equiv (1)^{23}.7 \equiv 7 \ (mod\ 11).$$

Assim, o resto da divisão de 7^{231} por 11 é igual a 7.
Embora esse processo permitiu chegar ao resto da divisão sem que recorresse ao cálculo da potência de 7^{231}, o que obviamente seria impraticável, o trabalho ainda assim foi considerável, haja vista a necessidade de se buscar a potência $7^n \equiv 1 \ (mod\ 11)$, o que, no exemplo analisado obrigou ao cálculo das potências de 7 até a potência 7^{10}, a qual gerou a congruência 1 módulo 11. Pode-se diminuir esse trabalho consideravelmente utilizando-se de uma "ferramenta"espetacular: o Teorema de Fermat.

Teorema (5)(Teorema de Fermat) : se p é um número primo e a é um número que não é divisível por p, então:

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Multiplicando-se ambos os lados da congruência por a, temos

$$a.a^{p-1} \equiv a.1 \ (mod\ p)$$

$$a.a^{p-1} \equiv a \ (mod\ p).$$

Como mdc(a, p) =1, existe o inverso modular a' de a tal que

$$a.a' \equiv 1 \ (mod\ p).$$

Multiplicando-se ambos os lados da congruência por *a'*, temos

$$a'.a.a^{p-1} \equiv a'.a \ (mod \ p)$$

$$a^{p-1} \equiv 1 \ (mod \ p)$$

Voltando ao exemplo (3). Descobriu-se o resto da divisão de 7^{231} por 11, usando a congruência modular, ao custo de se verificar todos os resíduos da potência 7^n módulo 11, o que demandou relativo trabalho. Porém, é fácil verificar, pelo Teorema de Fermat que

$$7^{10} \equiv 1 \ (mod \ 11),$$

logo,

$$7^{231} = (7^{10})^{23}.7^1,$$

então,

$$7^{231} \equiv (7^{10})^{23}.7^1 \equiv 1^{23}.7^1 \equiv 7 \ (mod \ 11).$$

Portanto, o resto da divisão de 7^{231} por 11 é 7, conforme verificado acima.

2.9 Teorema de Euler

Embora o Teorema de Fermat permita cálculos de congruências envolvendo potências, há uma restrição importante em sua utilização: o módulo deve ser primo. Na verdade, é possível utilizar o Teorema de Fermat para cálculo de congruências envolvendo potências, em determinadas condições, combinando-o com o Teorema Chinês do Resto.
Entretanto, há uma poderosa ferramenta que pode oferecer o mesmo resultado, ao custo da redução do trabalho.

2.9.1 Função de Euler

Seja n um número inteiro positivo. A função de Euler é dada pelo total de números inteiros positivos menores ou iguais a n que são primos entre si com n. Para efeito de notação, indica-se a função de Euler como $\phi(n)$. Assim, por exemplo, o número 16 possui os seguintes números menores ou iguais a ele que são primos entre si com 16: 1, 3, 5, 7, 9, 11, 13, 15, logo, $\phi(16) = 8$.
É evidente que se p for um número primo, $\phi(p) = p - 1$. Também é interessante calcular $\phi(p^k)$. Observe o exemplo a seguir

Exemplo (4). Calcular $\phi(7^2)$.
Como $7^2 = 49$, pode-se, facilmente encontrar todos o números inteiros positivos n , tais que o mdc $(n, 49) \neq 1$, ou seja, os elementos que pertençam ao conjunto $A = \{7, 14, 21, 28, 35, 42, 49\}$. Portanto, há 7 números menores ou iguais a 49 que não são primos entre si com ele. Logo, $\phi(49) = 49 - 7 = 42$.
Faz-se necessário generalizar esse resultado, de forma que seja possível se encontrar $\phi(p^k)$, quaisquer que sejam p e k.
Considere a como um número inteiro que divide p^k, tal que $0 < a \leq p^k$. Então,

$$p = a.b \text{ onde } 0 < b \leq p^{k-1}.$$

Portanto, há p^{k-1} inteiros positivos menores que p^k que são divisíveis por p. Logo, há $p^k - p^{k-1}$ números inteiros que não são divisíveis por p.

Assim

$$\phi(p^k) = p^{k-1}.(p-1).$$

É fácil verificar que essa generalização aplica-se ao exemplo (4).

$$\phi(7^2) = 7^{2-1}.(7-1) = 7.6 = 42$$

Há ainda outro teorema que apenas será enunciado aqui, antes de se abordar o Teorema de Euler.

Teorema (6). Se m ,n são inteiros positivos, com mdc(m, n) = 1, então

$$\phi(m.n) = \phi(m).\phi(n) \text{ [2].}$$

Exemplo. $\phi(144) = \phi(2^4.3^2) = \phi(2^4).\phi(3^2) = (2^3.1).(3.2) = 48$

Assim, pelo teorema acima temos que, se $n = p_1^{e_1} \cdot ... \cdot p_k^{e_k}$, então

$$\phi(n) = p_1^{e_1-1} \cdot ... \cdot p_k^{e_k-1}.(p_1-1) \cdot ... \cdot (p_k-1)$$

Teorema (7)(Teorema de Euler): Se n é um inteiro positivo e a é um inteiro tal que mdc(a, n) = 1, então

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

Seja $U(n)$ o conjunto de todos os números m, inteiros positivos menores que n tais que mdc(m, n) = 1.
Escrevendo $U(n) = \{m_1, m_2, ..., m_{\phi(n)}\}$, temos que

$$(a.m_1) \cdot ... \cdot (a.m_{\phi(n)}) \equiv m_1.m_2 \cdot ... \cdot m_{\phi(n)} \ (mod\ n)$$

logo,

$$a^{\phi(n)}.m_1.m_2 \cdot ... \cdot m_{\phi(n)} \equiv m_1.m_2 \cdot ... \cdot m_{\phi(n)} \ (mod\ n)$$

e, sabendo que mdc$(m_1, m_2, ..., m_{\phi(n)}, n) = 1$, podemos fazer o cancelamento dos dois lados da congruência, portanto,

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

Exemplo (5). Determinar o resto da divisão de 7^{242} por 12.

O que se quer encontrar aqui é um número x tal que $7^{242} \equiv x \ (mod\ 12)$. Veja que nesse caso o módulo é um número composto, o que torna a utilização do Teorema de Fermat dificultoso, como já mencionado no presente texto. Porém, $7^{\phi(12)} \equiv 1 \ (mod\ 12)$, de acordo com o Teorema de Euler.
Como $\phi(12) = 4$, temos $7^4 \equiv 1 \ (mod\ 12)$.
Trabalhando convenientemente a potência 7^{242}, temos $(7^4)^{60}.7^2 \equiv 1^{60}.7^2 \equiv 49 \equiv 1 \ (mod\ 12)$.
Portanto, o resto da divisão de 7^{242} por 12 é 1.

3 Criptografia RSA

A criptografia pode ser definida como a arte de se ocultar informações, de forma que somente quem as ocultou e a quem elas se destinam tenham conhecimento de seus reais conteúdos. Nesse mister, alguns processos foram desenvolvidos ao longo da história.

Contudo, se por um lado idéias simples, porém, interessantes foram criadas, como o Código de César nesse trabalho já mencionado, por outro, a relativa simplicidade dos processos permitiam, por meio de processos lógicos matemáticos decifrar os códigos utilizados. Alia-se a esse fator, o fato de que códigos como o de César ou da máquina Enigma, utilizado pelos alemães na 2ª Guerra Mundial para cifragem de mensagens, usarem um sistema de chave particular, ou seja, o processo de codificação só podia ser conhecido pelo emissor e pelo receptor da mensagem [3].
Com o avanço da tecnologia, a ponto de se permitir realizar transações financeiras por meios eletrônicos diversificados, um sistema de codificação que utilizasse somente chaves privadas se tornaria inviável, pois, cada pessoa que necessitasse realizar uma transferência de valores entre contas, por exemplo, teria que possuir uma chave privada fornecida pela instituição com a qual mantinha relações. Imagine a quantidade de chaves que uma única instituição apenas teria que criar para distribuir a seus clientes, sem falar que lojas não poderiam implementar tais sistemas, dada a dimensão do trabalho executado.
Em 1977, R. L. Rivest, A. Shamir e L. Adleman criaram um método de cifragem de mensagens utilizando um sistema de chave pública, ou seja, um código que pode ser de conhecimento público, usado para codificar a mensagem. Esse processo recebeu o nome de Criptografia RSA, em homenagem a seus idealizadores. É interessante notar também que, a base teórica desse processo de codificação, já abordada nesse trabalho, é a Teoria dos Números, que antes desse evento era tratada pela comunidade cientifica como sendo de pouca ou nenhuma aplicação prática. A criptografia RSA usa uma chave pública para codificar a mensagem e uma chave particular para a decodificação [1].

3.1 Pré-codificação

O processo de codificação de mensagens por RSA consiste basicamente em calcular uma potência módulo n, portanto, mensagens compostas por textos devem ser convertidas em números inteiros para que se possa usar a aritmética modular mencionada.
Na pré-codificação converte-se letras de um texto em números usando uma tabela de conversão, como a exemplificada 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	*0*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
23	*24*	*25*	*26*	*27*	*28*	*29*	*30*	*31*	*32*	*33*	*34*	*35*

Tabela 9: tabela para pré-codificção

Para codificar um texto, o espaço entre duas palavras deve ser preenchido com o número 99. Exemplo (6). A frase: *"penso, logo existo"* , atribuída à René Descartes (31 de março de 1596 - 11 de fevereiro de 1650), seria pré-codificada, excluindo-se a vírgula, da seguinte forma

25142328249921241624991433282924.

A escolha de se substituir as letras das palavras por números com pelo menos dois algarismos tem o propósito de se evitar ambiguidades tais como, por exemplo, se a letra A correspondesse ao número 1 e B, ao número 2, o número 12 poderia ser decodificado como AB ou a letra L.

Deve-se encontrar agora n, tal que $n = p.q$, onde p e q são dois números primos. Adotando-se, como exemplo, $p = 29$ e $q = 41$, tem-se $n = 29.41 = 1189$.

Por fim, o número gerado pela substituição das letras deve ser particionado em blocos, de tal forma que cada bloco represente um número menor que n. Então, considerando $n = 1189$, consegue-se os seguintes blocos:

$$251 - 423 - 282 - 499 - 212 - 416 - 249 - 914 - 332 - 829 - 24.$$

A única exigência com relação aos blocos diz respeito ao número gerado ser menor que n, não importando a quantidade de algarismos que possuam. Esse fato encerra uma aparente vantagem, a forma de se gerar os blocos não é única. Há que se observar também que os blocos assim gerados não correspondem a nenhuma unidade logística evitando-se assim uma possível decodificação por contagem de frequência [1].

3.2 Codificação

Com a pré-codificação executada, pode-se realizar a codificação. Para realizar essa ação precisa-se de $n = p.q$ e de um número positivo e que seja inversível módulo $\phi(n)$.
Ou seja,

$$mdc(e, \phi(n)) = mdc(e, (p-1).(q-1)) = 1.$$

Esse par $(n,\ e)$ é a chave de codificação e ela pode ser de conhecimento público.
Chamando b um bloco qualquer dentre os formados na pré-codificação e usando a chave de codificação $(n,\ e)$, codificá-lo é executar a operação abaixo,

$$C(b) \equiv b^e \ (mod\ n),$$

onde $0 \leq C(b) < n$ é o bloco b codificado.
No exemplo analisado, já se conhece n ($n = 1189$). Precisamos encontrar e. É fácil determinar que $\phi(1189) = (29-1).(41-1) = 1120$. Se observarmos que mdc (e, 1120) = 1, concluímos que o menor valor positivo para e é 3.
Logo, chamando $b_1 = 251$, devemos encontrar o resto da divisão de 251^3 por 1189. O caminho natural para se efetuar essa operação seria $251^3 = 15813251$, portanto, $15813251 = 13299.1189 + 740$, ou seja, C(251) = 740. Entretanto, é nesse ponto que a aritmética modular fará a diferença, pois, o que estamos procurando é um número r, tal que $251^3 \equiv r\ (mod\ 1189)$. Ou seja,

$$C(251) \equiv 251^3 \equiv 251^2.251 \equiv 1173.251 \equiv 740\ (mod\ 1189)$$

Procedendo de modo análogo para cada um dos demais blocos obtidos na pré-codificação, obteremos

$$\begin{aligned}
&C(423) = 1172\\
&C(282) = 39\\
&C(499) = 999\\
&C(212) = 671\\
&C(416) = 913\\
&C(249) = 273\\
&C(914) = 1113\\
&C(332) = 515\\
&C(829) = 360\\
&C(24) \ = 745
\end{aligned}$$

Portanto, a mensagem *penso, logo existo* apresenta-se codificada como

$$740 - 1172 - 39 - 999 - 671 - 913 - 273 - 1113 - 515 - 360 - 745$$

É importante observar que se os valores obtidos na codificação forem agrupados em um único bloco a decodificação tornar-se-á impossível, por isso, mantém-se os blocos codificados separados na sequência original obtida na pré-codificação.

3.3 Decodificação

Para a codificação, utiliza-se como chave pública o par $(n,\ e)$. A decodificação deve ser um processo secreto e, para tanto, utilizar-se-á uma chave privada composta pelo par $(n,\ d)$, onde d é o inverso de e módulo $\phi(n)$. Chamando $D(c)$ o resultado do processo de decodificação do bloco b codificado $C(b) = c$, tem-se que

$$D(c) = b, \text{ tal que } c^d \equiv b \ (mod\ n)$$

onde $0 \leq D(c) < n$.
Voltando ao exemplo já codificado. A primeira coisa que devemos encontrar é d. Sabemos que $n = 1189$, $e = 3$ e $\phi(1189) = 1120$. Usando o algoritmo de Euclides para encontrar d, temos

$$1120 = 373.3 + 1 \Rightarrow 1 = 1120 + (-373).3$$

Assim, o inverso de 3 modulo 1120 é (- 373). Porém, d deve ser um número positivo, pois, será utilizado como potência na congruência $D(c) \equiv c^d \ (mod\ n)$ então, $d = 1120$ - $373 = 747$.

Logo,

$$\begin{aligned}
D(740) &= b\\
740^{747} &\equiv b \ (mod\ 1189)\\
b &= 251
\end{aligned}$$

3.4 Funcionamento do processo de criptografia RSA

A pergunta óbvia que se deve fazer é: sempre será possível se decodificar uma mensagem codificada pelo método RSA? Pois, caso contrário, o processo é passível de falha naquilo que é sua principal função: codificar e decodificar uma mensagem.

Todo o processo, como já detalhado anteriormente, depende primeiramente da escolha adequada dos números primos p e q, os quais geram n ($n = p.q$). O que se deve provar é que $D(C(b)) \equiv b \ (mod\ n)$, quaisquer que sejam p, q e b, tal que $b < n$. Sabe-se que

$$D(C(b)) \equiv (b^e)^d \equiv b^{e.d} \ (mod\ n),$$

onde d é o inverso de e módulo $\phi(n)$. Portanto, existe um número inteiro k tal que $e.d = 1 + k.\phi(n)$.
Assim,

$$b^{e.d} \equiv b^{1+k.\phi(n)} \equiv (b^{\phi(n)})^k.b \ (mod\ n).$$

A partir dessas congruências há duas possibilidades a serem analisadas.

- Se mdc(b, n) = 1, então o Teorema de Euler fornece a prova necessária, ou seja,

$$b^{e.d} \equiv (b^{\phi(n)})^k.b \equiv b \ (mod\ n)$$

- Se b e n não são primos entre si e considerando $n = p.q$, com p e q primos e distintos entre si.
  Assim,

$$b^{e.d} \equiv b^{1+k.\phi(n)} \equiv (b^{(p-1)})^{k.(q-1)}.b \ (mod\ p)$$

Se mdc(b, p) = 1, usando o Teorema de Fermat ($b^{p-1} \equiv 1 \ (mod\ p)$).
Se b e p não são primos entre si, então $p|b$ e, portanto,

$$b^{e.d} \equiv b \equiv 0 \ (mod\ p).$$

Logo,

$$b^{e.d} \equiv b \ (mod\ p).$$

Tratando de forma análoga com o número primo q, chega-se a

$$b^{e.d} \equiv b \ (mod\ q).$$

Portanto,

$$b^{e.d} \equiv b \ (mod\ p.q).$$

3.5 Vantagens e desvantagens do sistema de criptografia RSA

Todo processo de codificação possui vantagens e desvantagens que pesam no momento da escolha de sua implementação. É fato que o grau de segurança e confiabilidade das operações de criptografia influenciará na escolha de um processo ou outro. O sistema RSA possui como principais vantagens:

- É um processo cuja codificação é relativamente simples, pois, depende da escolha de dois números primos que geraram a chave pública $n = p.q$. Somente n é conhecido, sendo p e q de conhecimento privado. É justamente esse fato que gera a segurança do processo, uma vez que os números primos utilizados são extremante grandes. Na verdade, utilizam-se primos com pelo menos 100 algarismos, em operações na internet, por exemplo. Dessa forma, o número n possuirá cerca de 200 algarismos. Fatorar um número dessa grandeza é um trabalho hercúleo. Estudos apontam que para se fatorar um número composto por 200 algarismos seriam necessários aproximadamente 4 bilhões de anos, ou seja, a segurança está ligada diretamente à escolha dos números primos e suas dimensões em termos de quantidade de algarismos que possuem [4].

- A mesma base teórica (Teoria dos Números) utilizada na implementação da codificação e decodificação de mensagens nesse sistema também permite a elaboração de assinaturas digitais. Codificar uma mensagem usando uma chave pública pode gerar um problema de confiabilidade no que concerne à autoria da mensagem. Utilizando-se novamente da aritmética modular, pode-se implementar uma certificação privada, de tal forma que quem emite uma mensagem agregue a ela essa certificação e quem a recebe tem a capacidade de reconhecer a autenticidade do remetente [2].

- A escolha de números primos relativamente grandes não é de fato um problema. O Teorema de Euclides afirma que existem infinitos números primos [1].

A principal desvantagem desse sistema de criptografia consiste na magnitude dos cálculos envolvidos. O processamento computacional demanda equipamentos potentes, o que limita a implementação de chaves muito maiores dos que as já utilizadas, assim, o aumento da segurança nesse sistema que depende do tamanho dos números primos envolvidos, dependerá da evolução da capacidade de processamento de dados dos computadores disponíveis.

4 RSA em sala de aula

Já foi abordado nesse trabalho que os conceitos tratados na Teoria dos Números na educação básica restringem-se às operações fundamentais da aritmética e, assim mesmo, de forma bastante tecnicista. Talvez, por ter sido a aritmética modular encarada sob uma ótica puramente conceitual durante tanto tempo, só vindo a ter realmente aplicações práticas a partir dos anos 1970 com a implementação da criptografia RSA, esse assunto não galgou tanto destaque na educação básica, como outros conceitos tradicionalmente trabalhados nesse nível educacional.

O grande desafio que se impõe ao professor em sala de aula hoje, mais do que em qualquer outra época, é a competição que ele enfrenta com os meios tecnológicos à disposição dos alunos. A abordagem puramente conceitual de conteúdos, sobretudo matemáticos, encontra cada vez mais resistência num ambiente onde a perspectiva de se obter informação à velocidade de toques de dedos é real. Uma pesquisa sobre *resto da divisão de potências* no principal site de buscas na internet resulta em 437000 sites com possíveis informações sobre o assunto. Cabe aqui uma colocação que se crê ser consenso entre profissionais de educação: informação não é sinônimo automático de conhecimento, ou, posto de outra forma, obter uma resposta pronta, sem a análise necessária de sua construção, não significa decisivamente ganho de conhecimento.

É nesse sentido que a utilização de recursos tecnológicos em sala de aula, como meios complementares à prática pedagógica, pode conduzir à tão desejada motivação dos discentes.
Motivações educacionais surgem sob formas diferentes em indivíduos diferentes. Em 1983, ano em que cursava a antiga 8ª série do ensino fundamental (atual 9º ano) esse mestrando que ora desenvolve esse texto, deparou-se com o seguinte problema: encontrar o resto da divisão do número 342^{41} por 5 [5].
Com a base matemática que possui àquela época, sabia que a solução não passaria pela operação de se elevar 342 a 41. Não possuindo mais recursos para "desvendar"o mistério, recorreu ao professor que propôs a seguinte solução:

$342 = 5.68 + 2$
2^1 produz 2 como resto na divisão por 5
2^2 produz 4 como resto na divisão por 5
2^3 produz 3 como resto na divisão por 5
2^4 produz 1 como resto na divisão por 5
2^5 produz 2 como resto na divisão por 5

Como a partir de 2^5 os restos repetir-se-ão de 4 em 4 blocos, bastava verificar o resto da divisão de 41 por 4, ou seja,

$$41 = 4.10 + 1$$

logo,

$$342^{41} = (5.68 + 2)^{41},$$

cujo resto da divisão por 5 será o mesmo obtido da divisão de 2^1 por 5, ou seja, 2.
Sem explicações mais elaboradas sobre o porquê daquele resultado, esse mestrando aprendeu a operacionalizar esse tipo de cálculo sem, no entanto, absorver o conhecimento necessário à interpretação da solução. Evidentemente, com o contato com outros conceitos matemáticos, como o Binômio de Newton, ficou mais claro o algoritmo utilizado pelo professor para solucionar o problema. A verdade, porém, é que o problema em si suscitou a motivação necessária para que a absorção de outros conteúdos pudessem ser aproveitados em prol do conhecimento utilizado em sua solução, como a aritmética modular.
É nesse mister que o uso da criptografia com todo seu embasamento matemático, aliado à possibilidade de implementá-la em sala de aula com o apoio de softwares gratuitos, pode criar nos discentes a motivação necessária não só ao ensino da Matemática, mas, sobretudo a busca pela construção do conhecimento e não apenas por respostas prontas.
A implementação do sistema de criptografia RSA não é simples, do ponto de vista de programação, dada a complexidade das linguagens envolvidas na técnica. Há que se observar também que esse não é o principal objetivo ao se propor a utilização de técnicas computacionais em sala de aula para a elaboração desse processo de codificação. O que se busca é, por meio de programas matemáticos gratuitos, a interação entre o conceito apresentado e sua possível aplicação prática que, nesse contexto, refere-se à aplicação da Teoria dos Números.
Há três programas matemáticos gratuitos, baseados no sistema de álgebra computacional (CAS), que permitem a realização de cálculos envolvidos na elaboração da criptografia RSA.

4.1 Maxima

Maxima é um sistema de manipulação de expressões simbólicas e numéricas, incluindo diferenciação, integração, expansão em série de Taylor, transformadas de Laplace, equações diferenciais ordinárias, sistemas de equações lineares, vetores, matrizes e tensores, aritmética modular, entre outros. O Maxima produz resultados de alta precisão usando frações exatas, números inteiros e números irracionais. Pode ainda traçar gráficos de funções e dados em duas ou três dimensões. Pode ser obtido gratuitamente no site http://maxima.sourceforge.net/. É possível utilizar o Maxima, como apoio didático, para se implementar o RSA [6].

Exemplo (6). Utilizando a frase: *"penso, logo existo"*, já pré-codificada no item 3.1, encontrou-se o número 25142328249921241624991433282924, separado nos seguintes blocos

$$251 - 423 - 282 - 499 - 212 - 416 - 249 - 914 - 332 - 829 - 24$$

Para codificar o bloco 251, utilizando o Maxima, deve-se seguir o algoritmo definido na tabela abaixo.

Ação	***Comando no Maxima***
Definir os primos p *e* q	p:29; q:41; (ctrl + enter) 29 41
Encontrar $n = p.q$	$n : (p * q)$; (ctrl + enter) n:1189
Encontrar $r = \phi(n) = (p-1).(q-1)$	$r : totient(n)$; (ctrl + enter) 1120
Encontrar e, *tal que mdc(*e,r*) = 1 Obs: dado o valor de* r, *deve-se testar, a partir do menor número primo* e *possível, que produza mdc(*e,r*) = 1. O par (*n, e*) é a chave pública da criptografia implementada.*	$gcd(3, r)$; (ctrl + enter) 1 e:3; (ctrl + enter) e:3
Definir b = *bloco a ser codificado*	$b : 251$; (ctrl + enter) $b : 251$
Codificar o bloco b, *tal que* $C(b) \equiv b^e \pmod n$, *onde* C *é o bloco codificado.*	$power\_mod(b, e, n)$; (ctrl + enter) 740 C:740; (ctrl + enter) C:740
Encontrar d, *tal que* d *é o inverso de* e *módulo* $\phi(n)$ *(Função de Euler).* *Obs: o par (*n, d*) é a chave privada da criptografia implementada.*	$inv\_mod(e, r)$; (ctrl + enter) 747 d:747; (ctrl + enter) d:747
Decodificar o bloco C *para se obter o bloco* b *original.*	$power\_mod(C, d, n)$; (ctrl + enter) 251
De posse da tabela de conversão de letras em números, retornar ao texto original.	

Tabela 10: comandos no Maxima para implementar o RSA

Nas figuras 1 e 2, é possível se verificar as linhas de comando necessárias à implementação do RSA para o exemplo realizado.

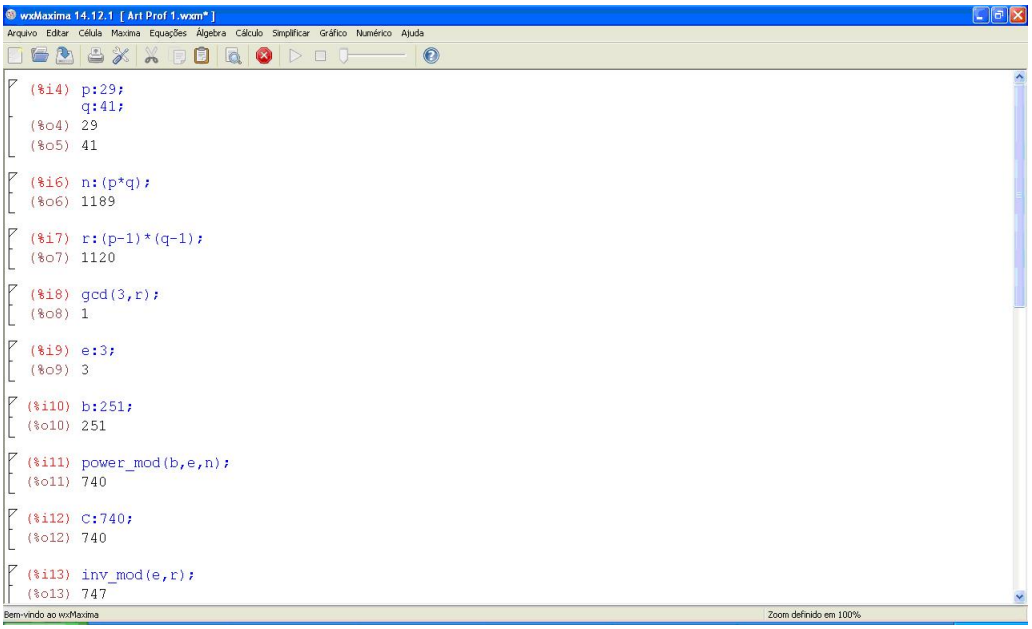

Figura 1: tela do Maxima com comandos para o RSA

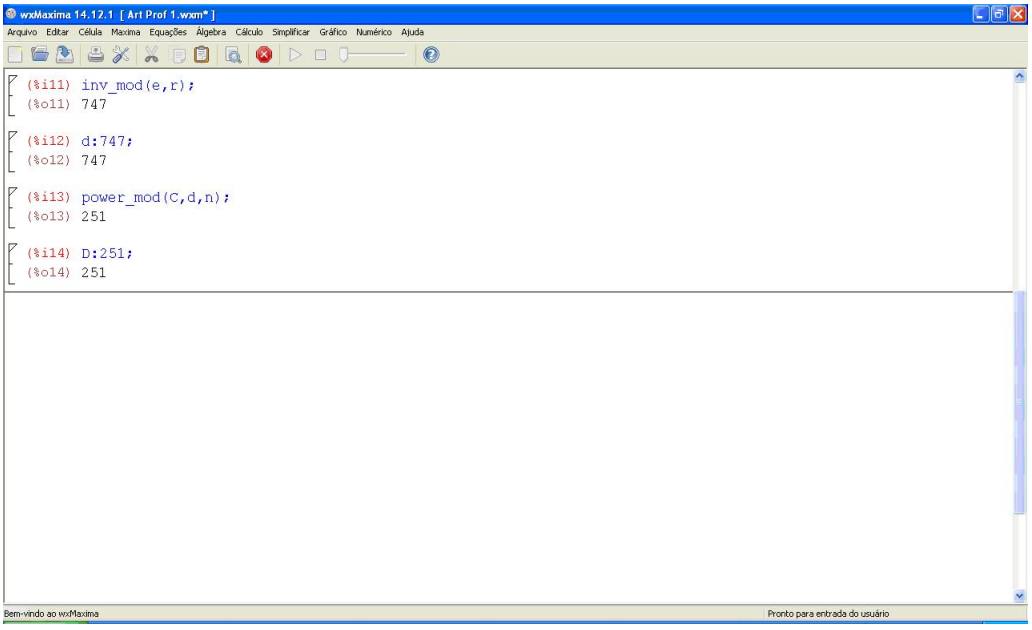

Figura 2: continuação da tela do Maxima com comandos para o RSA

Algumas considerações importantes.

1º - Obviamente, a segurança do sistema de criptografia RSA está baseada na dificuldade de se fatorar números relativamente grandes, da ordem de 200 algarismos. No exemplo analisado, usaram-se números primos pequenos (29 e 41), apenas para se facilitar os cálculos. Querendo-se trabalhar com valores mais próximos da realidade, o Maxima oferece a possibilidade de se utilizar números primos grandes. Por exemplo, deseja-se utilizar o número 3555736890013, caso seja primo, para definir as chaves pública e privada da criptografia elaborada.
Digita-se no Maxima
primep(3555736890013)*; (ctrl+enter)*
false
Como retornou *false*, digita-se
next_prime(3555736890013)*; (ctrl+enter)*
3555736890089
Deve-se testar agora se 3555736890089 é primo. Digita-se
primep(3555736890089)*; (ctrl+enter)*
true
Como retornou *true*, 3555736890089 é primo com muita probabilidade.
Para se definir um outro primo basta-se digitar
next_prime(3555736890089); (ctrl+enter)
3555736890119
Assim, muito provavelmente haverá dois números primos "grandes"para gerarem n.

2º - Uma vez que a escolha dos valores de p e q no exemplo realizado produziu $n = 1189$, isso obrigou a utilizar o texto pré-codificado em blocos, os quais deveriam formar números menores que n. A desvantagem dessa abordagem está no fato de se ter que "rodar"o algoritmo criado para cada bloco formado. É possível se evitar essa repetição de rotinas, escolhendo-se adequadamente os valores dos primos p e q, de tal forma que o $n = p.q$ gerado seja maior que o número gerado na pré-codificação do texto.

4.2 GP/Pari

GP/Pari é um sistema de álgebra computacional amplamente utilizado e projetado para cálculos rápidos na teoria dos números (fatoração, curvas elípticas ...). Contém também um grande número de outras funções úteis para cálculos matemáticos, tais como matrizes, polinômios, série de potência, entre outros. Pode ser obtido gratuitamente no site $http://pari.math.u-bordeaux.fr/$[7].
É possível se implementar a criptografia RSA no GP/Pari, como se segue.

Usando o exemplo (6), criptografar a frase: *"penso, logo existo"*, já pré-codificado nos blocos abaixo.

$$251 - 423 - 282 - 499 - 212 - 416 - 249 - 914 - 332 - 829 - 24$$

Ação	***Comando no GP/Pari***
Definir n = 29.41 = 1189	?$n = 29 * 41(enter)$ %1 = 1189
Encontrar $\phi(n) = (p-1).(q-1)$	? fi = eulerphi(n) (enter) %2 = 1120
Definir e *= 3* *Obs:* e*, tal que mdc(*e*,1120) = 1*	?$e = 3$ (enter); %3 = 3
Definir $a = Mod(e, fi)$	?a = Mod(e,fi) (enter) %4 = Mod(3,1120)
Encontrar a inversa de 3 (mod 1120)	?$1/a(enter)$ %5 = (747, 1120) ?d = 747 (enter) %6 = 747
Definir P *= 251 (bloco original pré-codificado)*	?P = Mod(251,n) (enter) %7 = Mod(251,1189)
Encontrar o bloco criptografado C	?C = P^ e (enter) %8 = Mod(740,1189) ?C = 740 (enter) %9 = 740
Decodificar o bloco C *para se obter o bloco* b *original.*	?D = C^ d (enter) %10 = Mod(251,1189) ?D = 251 (enter) % = 251
De posse da tabela de conversão de letras em números, retornar ao texto original.	

Tabela 11: comandos no GP/Pari para implementar o RSA

4.3 SAGE

SAGE é um software matemático livre e de código aberto (open-source), desenvolvido sob a licença GPL (General Public License) por uma comunidade de programadores e matemáticos, que busca ser uma alternativa para os principais sistemas proprietários de software matemático como o Magma, Maple, Mathematica e Matlab. Ele engloba e se utiliza de um grande número de pacotes pré-existentes como Maxima, GAP, Pari/GP, softwares de renderização de imagens e muitos outros, integrando-os em uma interface única que busca ser amigável e de fácil assimilação. Todos os principais pacotes são instalados juntamente com o SAGE e muitos outros pacotes existem para extensões em áreas específicas. Por este motivo O SAGE é adequado para uso em ensino e pesquisa [8].
Pode ser obtido gratuitamente no site *http://www.sagemath.org/pt/.*
É possível se observar um exemplo da implementação da criptografia RSA, no site *http* : *//www.uam.es/personal_pdi/ciencias/pangulo/doc/laboratorio/b6RSA.html.*

4.4 Conclusão

É notório o fascínio que os avanços tecnológicos exercem, sobretudo, nos jovens. Quer seja se divertindo, comunicando-se, buscando informações de seu interesse, o aluno, hoje, mais do que nunca, está imerso num mundo de estímulos rápidos e facilmente acessíveis. Assim, a sala de aula encerra em seu interior jovens cujas motivações em prol da educação precisam estar alinhadas com essa realidade contemporânea. Buscar o casamento do conceito teórico com a implementação prática parece ser um bom caminho a seguir, na busca dessa tão desejada motivação. Ao se implementar um sistema de criptografia RSA usando softwares gratuitos, por exemplo, o que se pretende não é criar "hackers" capazes de quebrar códigos na internet, mas, sim pessoas que enxerguem o acoplamento da teoria com o mundo real em que vivem, conseguindo assim construir um conhecimento com significância para suas vidas e, consequentemente, para a sociedade à qual estão inseridos.
A Matemática nunca decepciona. Oferece sempre desafios àqueles que nela se aventuram. Aliás,

"a Matemática é o alfabeto com o qual Deus escreveu o universo".
Galileu Galilei

5 Agradecimentos

Ao término dessa empreitada, é por consciência e total reconhecimento que não posso deixar de expressar meus mais profundos agradecimentos àqueles que certamente tornaram essa realização pessoal possível.
Ao Prof Dr Juan Carlos Zavaleta Aguilar, pela sua competência, constante disponibilidade, orientações oportunas e pela forma cordial com que sempre nos tratou. Reconheço também sua compreensão pelas vezes que não consegui corresponder às suas expectativas.
Ao corpo docente da UFSJ que nos concedeu parcela do seu tempo ministrando aulas e disponibilizando meios diversos para nos orientar nas disciplinas que cursamos durante essa jornada.
À UFSJ, pela acolhida e pela oportunidade que nos ofereceu de aprimorarmos nossos conhecimentos e práticas, na busca por uma educação básica com mais qualidade para os alunos desse nível de ensino.
Ao Comando do Colégio Militar de Belo Horizonte, nas pessoas do Cel Cav Nilton José Batista Moreno Júnior, Comandante e Diretor de Ensino e do Cel Art Éverton Duarte, Subdiretor de Ensino, pelo inestimável apoio concedido à realização desse curso.
Ao Maj QCO Fernando Carvalho Ramos, Professor e Mestre, Chefe da cadeira de Matemática do Colégio Militar de Belo Horizonte, pelo incentivo e pelas sugestões sempre pertinentes.
À minha família, especialmente aos meus pais, Jorge e Dilza, pela formação que me proporcionaram e a minha esposa Eliane e a meu filho Luiz Felipe pelo incentivo em continuar e pela compreensão para com minhas ausências rotineiras, devido à necessidade dos estudos. Sem eles, certamente não teria a base necessária para a conclusão dessa etapa de minha vida.
Ao meu antigo Professor de Matemática, Kenji Nishio, inspiração constante em minha vida e exemplo de homem correto. Muito do pouco que sei, devo às incontáveis horas em que passei estudando com ele, há mais de 30 anos.
Aos meus amigos de curso, especialmente Vilmar e Maurício, pelo convívio agradável e pela preciosa troca de experiências. Sentirei falta desse convívio.
Finalmente, a Deus, por tudo.

Referências

[1] COUTINHO, S. C. *Criptografia*. Programa de Iniciação Cientifica OBMEP n. 7. Rio de Janeiro, 2008.

[2] PIMENTEL, E. G. *Teoria de Números e Criptografia RSA*. 2006.
Disponível em *www.mat.ufmg.br/∼ elaine/OBMEP/criptografia.pdf*
Acesso em 12 jan. 2015

[3] Disponível em https://www.lume.ufrgs.br/bitstream/handle/10183/66106/000870987.pdf?sequence=1
Acesso em 20 jan. 2015

[4] Disponível em *http://www.batebyte.pr.gov.br/modules/conteudo/conteudo.php?conteudo=1384.*
Acesso em 29 jan. 2015

[5] BEZERRA, J. B. *Questões de Matemática*. São Paulo: Companhia Editora Nacional.

[6] LUZ, W. B. *Introdução à Matemática do Criptossistema RSA*.
Disponível em *http://bit.profmat-sbm.org.br/xmlui/handle/123456789/494*
Acesso em 4 fev. 2015

[7] COSTA, C. ; SILVA DE FIGUEIREDO, *L. M.Instrumentação para o Ensino da Matemática. Tópicos de Matemática e Atualidade*. Rio de Janeiro, Universidade Federal Fluminense. Centro de Estudo de Pessoal do Exército Brasileiro. 2006

[8] Disponível em *http://www.uam.es/personal_pdi/ciencias/pangulo/doc/laboratorio/b6RSA.html.*
Acesso em 6 fev. 2015