UNIVERSIDADE FEDERAL DO MARANHÃO
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
PROGRAMA DE MESTRADO PROFISSIONAL
EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

ADEILSON CARLOS DE LIMA ALVES

CRIPTOGRAFIA E SEGURANÇA RSA:
contextualização e aplicação

São Luís
2019

ADEILSON CARLOS DE LIMA ALVES

CRIPTOGRAFIA E SEGURANÇA RSA:
contextualização e aplicação

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal do Maranhão como requisito parcial para a obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. João de Deus Mendes da Silva

São Luís

2019

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).

Núcleo Integrado de Bibliotecas/UFMA

Alves, Adeilson Carlos de Lima

CRIPTOGRAFIA E SEGURANÇA RSA: contextualização e aplicação / Adeilson Carlos de Lima Alves. - 2019

53 p.

Orientador(a): João de Deus Mendes da Silva.
Dissertação (Mestrado) - Programa de Pós-graduação em Rede - Matemática em Rede Nacional/ccet, Universidade Federal do Maranhão, São Luís, 2019.

1. Algoritmo 2. Aritmética modular 3. Cifra de César 4. Criptografia RSA 5. Teoria dos Números. I. Silva, João de Deus Mendes da. II. Título.

ADEILSON CARLOS DE LIMA ALVES

CRIPTOGRAFIA E SEGURANÇA RSA:
contextualização e aplicação

Dissertação apresentada ao PROFMAT/ Universidade Federal do Maranhão como requisito parcial para a obtenção do grau de Mestre em Matemática.

Aprovado em: 9 de janeiro de 2019

BANCA EXAMINADORA

Prof. João de Deus Mendes da Silva (Orientador)
Doutor em Matemática
Universidade Federal do Maranhão

Prof. João Coelho Silva Filho
Doutor em Matemática
Universidade Estadual do Maranhão

Profa. Valeska Martins de Souza
Doutora em Matemática
Universidade Federal do Maranhão

Dedico este trabalho aos meus pais, Aldeides e Cleide, por serem muito mais que apenas pais e sim educadores da vida.

AGRADECIMENTOS

Agradeço primeiramente a Deus, criador do universo e dono de toda sapiência.

Ao meu orientador Prof. Dr. João de Deus Mendes da Silva pela singular orientação e dedicação neste trabalho.

Aos professores do PROFMAT, por contribuir na caminhada da busca de adquirir mais conhecimentos em minha profissão e para que esse objetivo fosse alcançado.

Ao PROFMAT, um programa de suma importância na qualificação de docentes do nosso País.

À CAPES, pela ajuda financeira (bolsa de estudo), a qual foi de uma importância singular.

A minha esposa Agizelle da Conceição Silva Alves, amiga de todas as horas, que me acompanhou nesta caminhada.

À minha família por sempre acreditar na capacidade do meu trabalho e nunca me deixar desistir desse sonho, em especial ao meu pai Aldeides Carlos Alves e minha mãe Cleide de Lima ALves, que sempre me mantiveram na linha da busca do conhecimento, onde acreditavam que o caminho da Educação seria o melhor e o mais honesto para uma vida mais digna.

Aos meus irmãos: Willian Lima Alves e Werbeth de Lima Alves, pelos incentivos e estarem sempre no apoio em minha trajetória.

Aos meus colegas de turma, os quais passamos por grandes dificuldades, mas que seguem com insistência e perseverança em busca de mais conhecimentos para poder retransmiti-los aos alunos.

"Meus filhos terão computadores, sim, mas antes terão livros. Sem livros, sem leitura, os nossos filhos serão incapazes de escrever, inclusive a sua própria história".

Bill Gates

RESUMO

O presente trabalho discorre sobre Criptografia e a Segurança RSA, fazendo uma contextualização do tema para estimular a aprendizagem da matemática através de aplicações práticas aos alunos do Ensino Fundamental e Ensino Médio. São abordados os conceitos de criptografia, seus métodos de encriptação, desencriptação e a importância da segurança na troca de informações. A pesquisa se fundamenta, sobretudo, na Teoria dos Números e na relação entre os números inteiros e o método de criptografia RSA. A importância do tema e sua escolha se justificam por ser o RSA, entre os métodos conhecidos atualmente, bastante utilizado em operações simples como envio de e-mails, transações bancárias, compras online e por satisfazer requisitos de segurança.

Palavras-chave: Algoritmo. Aritmética Modular. Cifra de César. Criptografia a RSA. Teoria dos Números.

ABSTRACT

The present paper deals with Cryptography and RSA (Rivest-Shamir-Adleman) Security, making a theme contextualization to stimulate the learning of mathematics through practical applications to Middle and High School students. This thesis discusses the cryptography concepts, its methods of encryption, decryption and the importance of security in the information exchange. The research is based mainly on the Numbers Theory and the relationship between integers and the RSA encryption method. The importance of the theme and its choice are justified by the fact that RSA, among the methods known nowadays, is widely used in simple operations, such as sending e-mails, banking transactions, online purchases and meeting security requirements.

Keywords: Algorithm. Modular Arithmetic. Caesar Cipher. Encryption to RSA. Numbers Theory

SUMÁRIO

Lista de Figuras

Lista de Tabelas

1 INTRODUÇÃO

A presente dissertação tem como objetivo despertar o interesse dos alunos para o aprendizado da Matemática, através da utilização de conceitos básicos deste componente curricular, em situações cotidianas que envolvam a segurança no envio e recebimento de dados e informações.

O momento que estamos vivendo, em que a comunicação e a tecnologia têm ganhado espaço, principalmente entre os jovens, através da grande quantidade de redes sociais, com a utilização em demasia da internet e a não menos importante exposição a que estão sendo submetidos.

Desde os tempos mais remotos a interceptação de dados sigilosos trazem ao ápice da discussão a espionagem. Atualmente a necessidade de proteger essas informações sigilosas é cada vez maior em um mercado altamente competitivo no mundo globalizado.

Historicamente, reis e imperadores utilizou-se da interceptação de informações para aumentar seus domínios. Surgiu então a ideia de ocultar mensagens, prática conhecida como esteganografia, palavra do grego que significa "escrita coberta". Os químicos se apropriam muito bem da esteganografia ao utilizar uma solução a base de suco de limão para escrever em uma folha de papel utilizando um pincel, mas quando aquecida a folha, a mensagem é revelada (também conhecida como tintas invisíveis).

Foi necessário garantir que não haveria intermediário nas informações trocadas entre o emissor e o receptor. Chamamos essa proteção de informações de confidencialidade, na qual um emissor troca informações com um ou mais destinatários. A problemática de garantir o sigilo da comunicação é o principal objeto de estudo da criptografia.

Em dias atuais, o artigo 3^o, inciso II, da Lei 12.965/14, a Lei 12.737/12, também conhecida como lei Carolina Dieckmann, e também o artigo 5^o, inciso X, da Constituição Federal de 1988, garantem a proteção da privacidade e mostra a importância que o Governo Brasileiro tem dado às questões relacionadas à violação e ao compartilhamento de informações privadas.

Logo, objetiva-se com esse trabalho, através de simples aplicações matemáticas e aliado ao que se pretende nos Parâmetros Curriculares Nacionais, fazer com que o aluno compreenda conceitos, procedimentos e estratégias matemáticas que permita o desenvolvimento e a obtenção de uma formação científica geral, além da aplicação de tais conhecimentos na vida cotidiana, na interpretação da ciência e da atividade tecnológica.

> No ensino da Matemática, destacam-se dois aspectos básicos: um consiste em relacionar observações do mundo real com representações (esquemas, tabelas, figuras); outro consiste em relacionar essas representações com princípios e conceitos matemáticos. Nesse processo, a comunicação tem grande importância e deve ser estimulada, levando-se o aluno a falar e a escrever sobre Matemática. [...] O significado da Matemática para o aluno resulta das conexões que ele estabelece entre ela e as demais disciplinas, entre ela e seu cotidiano e das conexões que ele estabelece entre os diferentes temas matemáticos. (BRASIL, 2007, p.19).

Unindo um tema moderno e a utilização de cálculos matemáticos que possibilitem entender a metodologia de codificação e decodificação existentes, é a receita ideal para que se consiga êxito dentro e fora da sala de aula. Afinal o objetivo do professor é despertar no aluno o desejo de transformar o mundo que o contorna. Cabe ao professor incentivar a pesquisa, o questionamento e a busca pelo conhecimento.

Para isso, apresentaremos no decorrer deste trabalho assuntos pertinentes à Criptografia, tratando de um breve histórico sobre os primórdios e a evolução da criptografia utilizamos o capítulo 2 para descrever sobre a Cifra de César e suas possíveis alterações e verificamos que ao saber em qual língua materna a cifra foi escrita originalmente, e fazendo uma análise de frequências dessas letras, o embaralhamento das letras fica facilmente decifrável.

No capítulo 3 são abordadas as principais metodologias e técnicas matemáticas. Trataremos sobre a fatoração de um número, introduzindo as definições e notações elementares.

Exemplos são abordados apenas para melhor entendimento da aplicabilidade dos tópicos, visando um fácil entendimento e abordagem prática para alunos da educação básica. Aritmética modular, inverso modular e o algoritmo do resto chinês, juntamente com a função de Euler e o Pequeno Teorema de Fermat, terá grande utilidade para o entendimento do RSA.

Faremos um estudo dos números inteiros e suas propriedades, dando ênfase aos números primos.

No capítulo 4 abordaremos sobre a criptografia RSA, descrevendo de forma rigorosa e fiel o algoritmo conforme descrito no livro titulado Criptografia e Segurança de Redes, escrito por Stalling, e ainda, dando exemplo de como tratar as informações e aplicando uma codificação e depois decodificando uma mensagem e, com isso, mostrar o que a torna tão segura e aplicável nos dias atuais.

Sabendo que não existem mecanismos totalmente seguros e visando a defesa de um possível ataque a essas trocas de informações é necessário garantir um tempo hábil que essas informações permanecerão seguras.

No capítulo 5 apresentaremos algumas atividades lúdicas para alunos na educação básica desenvolver na sala de aula ou mesmo em casa, visto que os conteúdos necessários para desenvolver tais atividades foram abordados nos capítulos anteriores.

A teoria dos números contribuiu, e ainda contribui, de forma significativa para a segurança dessas informações. Um sistema de criptografia específico chamado RSA é o mais utilizado dos métodos de criptografia e suas aplicações estão em simples mensagens de e-mails às compras on-line.

2 A HISTÓRIA DA CRIPTOGRAFIA

Ao longo da história, reis e rainhas e seus generais de guerra, sempre buscaram formas seguras de se comunicar e de comandar seus exércitos. A necessidade de não revelar táticas e estratégias aos inimigos, motivou o desenvolvimento de códigos e técnicas para mascarar a mensagem, possibilitando apenas ao destinatário ler o conteúdo. Uma corrida intelectual foi posta desde então, de um lado, nações criaram departamentos para elaborar códigos e, do outro lado, surgia os decifradores de códigos.

Observa-se então que a matemática teve seu papel primordial ao longo do tempo para a evolução dos códigos, e "evolução" é um termo bem apropriado, já que todo código sempre está sob o ataque dos decifradores e no decorrer da história, os códigos foram fundamentais para a decisão que influenciaram no resultado das batalhas.

2.1 Cifra de substituição ou Cifra de César

Um dos códigos mais simples consiste em substituir uma letra do alfabeto pela letra seguinte. Utilizava-se um alfabeto cifrado apenas rearranjando o alfabeto original, mas também empregavam alfabetos que continham outros símbolos, a essa cifra se dá o nome de Cifra de substituição. Segundo COUTINHO (2014, p. 2) "um código semelhante a este foi usado, por exemplo, pelo ditador romano Júlio César para se comunicar com seus soldados romanos em combate pela Europa. Este parece ser o primeiro exemplo de código secreto de que se tem notícia" e por ser um dos primeiros métodos de codificação relatados na história é que recebeu o nome do imperador. Esta cifra permaneceu invulnerável por séculos.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
B	C	D	E	F	G	H	I	J	K	L	M	N
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Tabela 2.1: Alfabeto cifrado.

Era comum deslocar as letras do alfabeto, por exemplo, como descrito na

Tabela 2.1, o alfabeto utilizado para cifrar uma mensagem tem início na letra b.

Utilizando-se da Tabela 2.1, podemos codificar a mensagem "**Esta é a cifra de césar**" e após codificação se torna "**Ftub f b djgsb ef dftbs**".

2.2 Cifra de Vigenère

A cifra levou o sobrenome de Blaise de Vigenère, não por ter inventado, mas por ter difundido. Vigenère foi um diplomata e criptógrafo francês que viveu entre 1523 e 1596. Iniciou sua carreira diplomática aos 17 anos e com o passar dos anos conheceu criptologistas e tomou contato com livros de criptografia.

Foi autor de vários livros na qual ganha destaque a obra *Traité des Chiffres* ou *Secrètes manières d'escrire* (1586), onde explica detalhadamente seu código de cifra de substituição polialfabética com palavras-chave.

A imagem das Carreiras de Vigenère, Figura 2.1, é similar ao Código de César. Consiste em ter uma palavra-chave, que será usada para codificar, e a posição de cada símbolo codificado é encontrado ao associar as letras da colunas (mensagem original) com as letras das linhas (palavra-chave), fazendo uma espécie de batalha-naval com as letras.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figura 2.1: Carreiras de Vigenère.

Exemplo 2.1. Utilize a Figura 2.1 e codifique a seguinte mensagem: **ESTUDE MATEMATICA** com a palavra-chave: **AMOR**.

Como resultado da codificação dessa mensagem teremos:

EEHLDQARTQARTUQR

2.3 Análise de frequências

Os códigos baseados na Cifra de César sofrem de um grande problema: são muito fáceis de decifrar (quebrar). Decifrar ou quebrar códigos significa ter capacidade de ler a mensagem, ainda que não seja o verdadeiro destinatário. Para COUTINHO (2014, p. 2), "qualquer código que envolva substituir cada letra sistematicamente por outro símbolo qualquer sofre do mesmo problema".

Essa facilidade ocorre porque a frequência média com que cada letra aparece em um determinado texto de uma dada língua é razoavelmente constante. A Tabela 2.2 faz referência a frequência média, em porcentagem, de cada letra em relação às palavras na língua portuguesa.

Letra	%	Letra	%	Letra	%	Letra	%
A	14,64	G	1,30	M	4,75	S	7,81
B	1,04	H	1,28	N	10,73	T	4,64
C	3,88	I	6,18	O	10,73	U	4,64
D	4,10	J	0,40	P	2,52	V	1,70
E	12,5	K	0,70	Q	1,20	X	0,21
F	1,02	L	2,78	R	6,53	Z	0,47

Tabela 2.2: Frequência das letras no idioma português (Brasil).

O sistema consiste em: conhecendo o idioma texto, encontrar um texto diferente, na mesma língua, suficientemente longo para preencher uma página. Então contar a frequência com que cada letra aparece. Em seguida examinar a tabela de frequência das letras que se deseja decifrar e correlacioná-las (SINGH, 2001).

É importante fazer uma correspondência entre as letras e os símbolos mais frequentes. Entretanto, podemos observar que esse método utilizado para quebrar códigos só funciona bem se o texto for longo, pois a existência da facilidade de escrever um texto curto na qual a contagem de frequência seja totalmente diferente da média, pode colocar a utilização da metodologia em xeque.

2.4 Disco de Cifras

Disco de cifras é um misturador de códigos que transforma a letra do texto original em letra do texto cifrado, uma técnica criptográfica que faz uso de dois discos para cifrar e decifrar mensagens. Seu inventor sugeriu que a disposição do disco fosse alterada durante uma mensagem, gerando uma cifra polialfabética, dificultando ainda mais a sua decodificação ao mudar o modo de mistura durante o processo de cifragem.

Sua concepção básica consiste de dois discos com diâmetros diferentes que são montados de forma concêntrica, conforme ilustra a Figura 2.2, onde as escalas com o alfabeto são gravados e, ao movê-los em torna do eixo comum, relacionam-se entre si, permitindo a mudança de cifras de uma forma prática e fácil.

Figura 2.2: Disco de Cifras.

3 INTRODUÇÃO À TEORIA DOS NÚMEROS

O estudo das propriedades dos números inteiros positivos é o objetivo central da Teoria dos Números. Apresentamos algumas propriedades elementares dos números inteiros na qual serão necessárias para entender o funcionamento do algoritmo RSA.

3.1 Números inteiros

Neste tópico serão abordadas algumas propriedades e características dos números inteiros que garantem a segurança do RSA no que diz respeito ao envio e recebimento de informações e na qual terá extrema necessidade para aplicação da criptografia.

3.1.1 Divisor e Múltiplo

Definição 3.1. Um número inteiro b divide outro número inteiro a se existe um terceiro número inteiro c tal que $a = b \cdot c$

Podemos dizer que b é um *divisor* ou *fator* de a, ou também que a é *múltiplo* de b . Todas essas formas de se expressar tem o mesmo significado (COUTINHO, 2000).

Nas condições da definição 3.1, se $1 < b < a$, dizemos que b é um fator ou divisor *próprio* de a. De forma natural, podemos afirmar que só temos dois divisores que não são próprios, 1 e o próprio a. O número c, descrito na definição é chamado de *cofator* de b em a, ou seja, determinamos que um número b divide um número a efetuando a divisão e verificando se o resto é zero.

O cofator é o quociente da divisão. Dois números inteiros quaisquer sempre terão, pelo menos, o número 1 como fator comum, ou seja, o número 1 divide qualquer número inteiro. Se o número 1 for o único fator comum a dois números, diremos que *não existe fator próprio comum*, ou ainda, os dois números *são primos entre si*.

Coutinho (2015) cita propriedades dos múltiplos. Se a, b, c e d são números inteiros, então:

1. d divide 0;

2. Se d divide a e b, então também divide $a + b$;

3. Se d divide a, então divide $a \cdot c$.

3.1.2 Primo e Composto

Definição 3.2. Um número inteiro a $(a > 1)$ é chamado de *primo* se possui somente dois divisores inteiros positivos, a e 1. Se $a > 1$ não é primo dizemos que a é composto.

Proposição 3.1. *Se* $\boldsymbol{a}$ *for composto, o menor fator próprio de* $\boldsymbol{a}$ *é menor ou igual a raiz quadrada de* $\boldsymbol{a}$*. Desta forma, buscando fatorar o número* $\boldsymbol{a}$*, se* $\boldsymbol{a}$ *for composto, algum fator deverá ser encontrado antes da busca ultrapassar* $\sqrt{\boldsymbol{a}}$ *.*

3.1.3 Algoritmo

A origem da palavra algoritmo é de certa forma curiosa. No princípio a palavra era escrita "algorismo" que vem da palavra árabe Al-khowarazmi, "o homem de khowarazm", pelo qual o matemático árabe Ibn Musa ficou conhecido. Ele foi o responsável por fazer chegar o sistema de numeração, usado na Índia, na Europa Medieval, quando escreveu o livro **Al-jabr wa'l muqabalah**, no século IX. Por este motivo que falamos em algarismos indo-arábicos e as palavras algorismo e algarismo são variações da mesma palavra que significavam numerais indo-arábicos.

Observamos que a palavra algoritmo é muito antiga, mas que ganhou um novo significado por volta de 1800.

Coutinho (2000) afirma que esse novo significado, os matemáticos chamam de algoritmo qualquer método sistemático utilizado para fazer alguma coisa.

Através da Proposição 3.1 podemos, então, criar um algoritmo que descreverá suas etapas afim de verificar se um número é primo ou composto. Chamaremos: Algoritmo ACHAR-FATOR.

Devemos ter uma **entrada**: um número inteiro positivo a; e uma **saída**: um fator próprio de a ou a conclusão de que a é primo.

Procedimento: tentar dividir por 2. Se for divisível pare, pois descobrimos que 2 é fator de a, se não, tente dividir por 3. Se for divisível pare, pois descobrimos que 3 é

fator de a, se não, tente dividir por 5. Continuar desta maneira até encontrar um número que divida a ou até que o candidato a divisor seja maior que $\sqrt{a}$. Se esse candidato a divisor for maior que $\sqrt{a}$ pare, pois descobrimos que a é primo.

Proposição 3.2. *O fator de um número inteiro* $\boldsymbol{a > 1}$ *encontrado pelo algoritmo ACHAR-FATOR citado anteriormente é sempre um número primo menor ou igual a raiz quadrada de* $\boldsymbol{a}$.

3.1.4 Custo da Fatoração

Apesar da facilidade de entender e de utilizar o algoritmo ACHAR-FATOR, ele é muito ineficiente, mesmo quando usamos um supercomputador. Há uma certa facilidade de ilustrarmos se estimarmos o tempo que um computador levaria para achar um fator de um número grande usando o algoritmo ACHAR-FATOR.

Vale lembrar que, tendo um número a por entrada, ACHAR-FATOR executa na máquina $\sqrt{a}$ tentativas de divisão antes de encontrar um fator para a, sendo o pior caso possível ocorrendo quando executado exatamente $\sqrt{a}$ tentativas de divisão, o que corresponde a dizer que a é primo.

É neste pior caso que teremos que trabalhar para estimar o tempo de resposta de um computador para retornar a resposta: a é primo.

Consideremos um número primo p, de 100 ou mais algarismos. Isto é $p \geq 10^{100}$ e, portanto, $\sqrt{p} \geq 10^{50}$. Desta forma, precisaremos executar, pelo menos, 10^{50} divisões para garantir que o numero p é primo, utilizando o algoritmo ACHAR-FATOR. Para transformar isso em tempo de cálculo, precisamos ter uma ideia de quantas divisões um computador é capaz de executar em um segundo.

Vamos utilizar, para nosso exemplo, o supercomputador adquirido pela USP (Universidade de São Paulo) que faz cerca de 20 trilhões de cálculos por segundo, de acordo com reportagem feita pelo sítio PlantãoNERD.com (PAIVA, 2012). Suponhamos conseguir extrair cem por cento da capacidade desse supercomputador, ou seja, capaz de executar $2 \cdot 10^{13}$ divisões por segundo. Então precisaríamos de, pelo menos,

$$\frac{10^{50}}{2 \cdot 10^{13}} = 0,5 \cdot 10^{37} = 5 \cdot 10^{36} \text{ segundos}$$

para determinar que certo número a, usando o algoritmo ACHAR-FATOR, é primo.

Supondo que um ano tem 365 dias (para efeito de contas), cada dia tem 24 horas, cada hora tem 60 minutos e cada minuto tem 60 segundos, então:

$$365 \cdot 24 \cdot 60 \cdot 60 = 31536000 \text{ segundos},$$

isto é, 1 ano tem 31536000 segundos, então:

$$\frac{5 \cdot 10^{36}}{31536000} \cong 158548959918823000000000000000 \text{ anos}$$

Calculando essa estimativa de tempo (em anos) que o supercomputador adquirido pela USP leva para fatorar um número relativamente grande (100 algarismos), concluímos que demoraria um pouco mais que 158,5 octilhões de anos.

Podemos afirmar que, é impossível confirmar que um número de 100 ou mais algarismos é primo usando este algoritmo ACHAR-FATOR. No entanto, não significa que o algoritmo seja inútil, visto que vamos fatorar um número inteiro que nada sabemos sobre, há sempre possibilidade que tenha um fator primo pequeno (menor que um milhão) e para esses casos o algoritmo ACHAR-FATOR encontrará um fator rapidamente.

3.1.5 Fatorando um número

Consideremos o número inteiro 12105. Vamos aplicar o algoritmo ACHAR-FATOR a este número inteiro e achamos o fator 3,

$$\frac{12105}{3} = 4035,$$

assim

$$12105 = 3 \cdot 4035.$$

Os fatores encontrados pelo algoritmo ACHAR-FATOR sempre são primos, assim, 3 é primo. É necessário aplicar o algoritmo ACHAR-FATOR ao cofator 4035 de 3 em 12105. Aplicando ACHAR-FATOR a 4035, observamos que 3 também é fator deste número. Como

$$\frac{4035}{3} = 1345,$$

tem-se que

$$12105 = 3 \cdot 4035 = 3 \cdot (3 \cdot 1345) = 3^2 \cdot 1345.$$

Aplicando o algoritmo ACHAR-FATOR novamente, teremos achado o cofator de 1345, e encontramos o fator 5, pois

$$\frac{1345}{5} = 269,$$

de modo que

$$12105 = 3^2 \cdot 1345 = 3^2 \cdot (5 \cdot 269).$$

No entanto, aplicando o algoritmo ACHAR-FATOR teremos $\sqrt{269} = 16,4012194...$, ou seja, teremos que testar se 269 é divisível por números menores que 16 e pela Definição 3.2 verificamos que 269 não é divisível por nenhum número menor que 16. Esses resultados nos permitem observar que o número 269 é primo.

Então, podemos concluir que, usando o algoritmo ACHAR-FATOR a fatoração do número 12105 em potencias de números primos é:

$$12105 = 3^2 \cdot 5 \cdot 269.$$

3.2 Aritmética Modular

Definição 3.3. Se a e b são inteiros dizemos que a é congruente a b módulo $n(n > 0)$ se $n|(a-b)$. Denotamos isto por $a \equiv b(mod\ n)$. Caso contrário, dizemos que a é incongruente a b módulo n.

Semelhante às propriedades dos números inteiros, congruência modular também possui um rol de propriedades dessas. Considerando que n é um inteiro positivo.

1. Reflexiva, todo número é congruente módulo n a si próprio;
2. Simétrica, se $a \equiv b(mod\ n)$ então $b \equiv a(mod\ n)$;
3. Transitiva, se $a \equiv b(mod\ n)$ e $b \equiv c(mod\ n)$, então $a \equiv c(mod\ n)$.

Demonstração. Para mostrar que a congruência módulo n é reflexiva, devemos verificar que $a \equiv a(mod\ n)$. Mas, pela definição, isto é o mesmo que dizer que $a - a = 0$ é múltiplo de n. Contudo, zero é múltiplo de qualquer inteiro n, uma vez que $0 \cdot n = 0$. Passemos à simétrica. Pela definição de congruência módulo n, $a \equiv b(mod\ n)$, é o mesmo que dizer que $a - b$ é múltiplo de n. Em outras palavras, se $a \equiv b(mod\ n)$ então existe algum inteiro k tal que $a - b = k \cdot n$.

Multiplicando esta equação por -1, obtemos: $b - a = (-k) \cdot n$; isto é, $b - a$ é múltiplo de n, ou ainda, $b \equiv a(mod\ n)$.

Para a propriedade transitiva, tomamos por hipótese que: $a \equiv b(mod\ n)$ e que $b \equiv c(mod\ n)$. Mas estas duas congruências se traduzem, por definição, nas igualdades: $a - b = k_1 \cdot n$ e $b - c = k_2 \cdot n$, onde k_1 e k_2 são inteiros escolhidos de maneira adequada. Somando estas duas últimas equações, $(a - b) + (b - c) = k_1 \cdot n + k_2 \cdot n$.

Cancelando o b à esquerda e usando a distributividade da direita, obtemos: $a - c = (k_1 + k_2) \cdot n$, que é equivalente à congruência $a \equiv c(mod\ n)$. □

As três propriedades que provamos correspondem às propriedades dos múltiplos, no entanto, podemos ir bem mais longe que isto. Digamos que a é um inteiro positivo. Dividindo a por n temos: $a = n \cdot q + r$, com $r \in [0,\ n[$.

Logo, $a - r = n \cdot q$; que é equivalente a dizer que $a \equiv r(mod\ n)$.

Verificamos com isto que todo inteiro positivo é congruente módulo n ao resto de sua divisão por n, que é um número entre 0 e n. Podemos generalizar desta forma: se $a \equiv r(mod\ n)$ e $0 \leq r < n$, dizemos que r é o resíduo de módulo n.

Isto porque cada número só pode ter um resíduo módulo n. De fato, se:

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

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

então, pelas propriedades simétrica e transitiva, $r \equiv r'(mod\ n)$. Digamos que $r \geq r'$. Pela definição da congruência, isto significa que $r - r'$ é um múltiplo de n. Mas tanto r, quanto r' são menores que n, de modo que $0 \leq r - r' \leq n$. Isto significa que $r - r'$ só pode ser múltiplo de n se o cofator correspondente for zero; o que nos dá $r = r'$, mostrando que os dois resíduos, r e r' têm que ser iguais.

Aparentemente a única coisa que fizemos ao introduzir os resíduos foi inventar um nome novo para o resto, mas não é bem assim. Note que o termo resíduo se aplica a qualquer inteiro, positivo ou negativo, ao passo que o resto geralmente é usado quando dividimos um inteiro positivo por n. O que ocorre, então, se a for negativo? Para tornar o argumento mais claro, convém começar com um exemplo.

Exemplo 3.1. Seja $n = 6$ e $a = -55$. Nosso objetivo é calcular o resíduo de -55 módulo

6; em outras palavras, queremos achar um inteiro $0 \leqslant r < 6$ tal que:

$$-55 \equiv r(mod\ 6).$$

Poderíamos proceder por tentativa, mas vamos tratar o problema de maneira mais sistemática para podermos lidar mesmo com o caso em que o n for grande. Para isto, dividimos 55 por 6, obtendo quociente 9 e resto 1, ou seja, $55 = 9 \cdot 6 + 1$. Multiplicando tudo por -1, teremos $-55 = (-9) \cdot 6 - 1$, de forma que $-55 \equiv -1(mod\ 6)$. Observe que -1 não é o resíduo de -55 módulo 6 porque -1 é negativo. Contudo, como $6 = 5 - (-1)$, obtemos $-1 \equiv 5(mod\ 6)$; e a propriedade transitiva da congruência nos permite concluir que $-55 \equiv 5(mod\ 6)$. Portanto, -55 tem resíduo 5 módulo 6.

3.2.1 Algoritmo resíduo-mod-n

Para tratar o caso geral, podemos fazer um pequeno algoritmo seguindo as etapas do Exemplo 3.1.

Primeiramente, estamos supondo que a é negativo, então $-a$ deve ser positivo. Dividindo-o por n, $-a = n \cdot q + r$ e $0 \leq r < n$, onde q e r são o quociente e o resto da divisão respectivamente.

Multiplicando esta equação por -1, obtemos $a = n \cdot (-q) - r$ e $0 \leq r < n$, isto é, $a \equiv -r(mod\ n)$ e $0 \leq r < n$.

Se $r = 0$, então $a \equiv 0(mod\ n)$ e já achamos o resíduo. Se $r \neq 0$, então $(n - r) - (-r) = n$ nos diz que $-r \equiv n - r(mod\ n)$, de modo que a transitividade da congruência nos permite concluir que $a \equiv n - r(mod\ n)$. Ainda precisamos nos certificar que $n - r$ é um resíduo, mas, para isto, basta verificar que está entre 0 e $n - 1$. Como $r \geq 0$ e $r \neq 0$, temos que $r > 0$. Logo $n - r < n$. Entretanto, $r < n$, e assim, concluímos que $n - r > 0$.

3.3 Inversos modulares

Nesta seção serão discutidos alguns tópicos de suma importância para entendermos o funcionamento do RSA.

3.3.1 Definindo inverso modular

Vejamos a congruência $2 \cdot 3 \equiv -1(mod\ 7)$.

Utilizando a linguagem elementar dos números racionais, dizemos que -1 "dividido" por 2 é igual a 3. Ao multiplicar a congruência por -1 obtemos $2 \cdot (-3) \equiv 1(mod\ 7)$ e também $(-2) \cdot 3 \equiv 1(mod\ 7)$.

Como $-3 \equiv 4(mod\ 7)$ e $-2 \equiv 5(mod\ 7)$, podemos concluir que

$$2 \cdot 4 \equiv 1(mod\ 7) \text{ e } 5 \cdot 3 \equiv 1(mod\ 7).$$

Também, para este caso, dizemos que 1 dividido por 2 módulo 7 resulta em 4, e 1 dividido por 3 resulta 5. Ocorrendo isto, dizemos que 2 e 4 são inversos módulo 7, e o mesmo se dá com os números 3 e 5.

Sistematicamente, dizemos que a e a' são inversos módulo n se $a \cdot a' \equiv 1(mod\ n)$.

Para este caso, dizemos que a' é o inverso de a módulo n, ou também que a é o inverso de a' módulo n.

3.3.2 A existência de inverso modular

Enumeramos, na Tabela 3.1, cada um dos resíduos diferentes possíveis módulo 11, indicando o resíduo e seu respectivo inverso módulo 11. Notemos que zero não tem inverso módulo n não importando qual valor n assuma, já que $0 \cdot b \equiv 0(mod\ n)$ qualquer que seja $b \in \mathbb{Z}$. Com isso, não listamos o número 0 entre os resíduos na Tabela 3.1.

Podemos utilizar mais que simples tentativa, porque se nos restringimos aos inteiros entre 1 e $n-1$, então cada um destes números tem apenas um inverso neste mesmo intervalo. Com efeito, se a' e a'' são inversos de a módulo n, e estão entre 1 e $n-1$, então,

$$a \cdot a' \equiv 1(mod\ n) \text{ e } a \cdot a'' \equiv 1(mod\ n),$$

podemos concluir que,

$$a'' \cdot (a \cdot a') \equiv a'' \cdot 1 \equiv a''(mod\ n),$$

Resíduo	Inverso Módulo 11
1	1
2	6
3	4
4	3
5	9
6	2
7	8
8	7
9	5
10	10

Tabela 3.1: Resíduo inverso modular 11.

e também que,

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

No entanto fizemos apenas aplicar a propriedade associativa, não alterando o resultado e, desta forma,

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

Então significa que a subtração $a' - a''$ é divisível por n. Só que, a' e a'' são maiores que zero e menores que n, de tal forma

$$-n < a' - a'' < n.$$

Assim, a única forma da subtração $a' - a''$ ser múltiplo de n é se for igual ao número 0; concluímos que $a' = a''$.

Essa conclusão ajuda muito na hora de calcular a tabela. Quando calculamos, observamos que 2 e 6 são inversos, um do outro, módulo 11, então nem o número 2 e muito menos o número 6 podem ser inversos de 3 módulo 11. Assim, procuramos pelo resíduo do inverso de 3 apenas entre os inteiros 3, 4, 5, 7, 8, 9 e 10. Por isso, quanto mais inversos determinamos, mais rápido fica determinar os que ainda faltam.

3.3.3 A inexistência de inverso modular

Propomos calcular uma outra tabela de inversos, desta vez calcularemos os inversos dos resíduos diferentes módulo 8. Sabendo que 1 é seu próprio inverso, começaremos do número 2;

$$2 \cdot 2 \equiv 4 \not\equiv 1 (mod\ 8)$$

$$2 \cdot 3 \equiv 6 \not\equiv 1 (mod\ 8)$$

$$2 \cdot 4 \equiv 0 \not\equiv 1 (mod\ 8)$$

$$2 \cdot 5 \equiv 2 \not\equiv 1 (mod\ 8)$$

$$2 \cdot 6 \equiv 4 \not\equiv 1 (mod\ 8)$$

$$2 \cdot 7 \equiv 6 \not\equiv 1 (mod\ 8)$$

Após efetuarmos os cálculos verificamos que 2 não tem inverso módulo 8. Por Coutinho (2014, p.85) sabemos que "todo inteiro é congruente módulo n ao seu resíduo". Modificaremos a frase para adaptar ao nosso exemplo: todo inteiro é congruente módulo 8 ao seu resíduo. Como devemos calcular se um número ou se seu resíduo produz iguais resultado módulo 8, não podendo haver nenhum número inteiro que inverta 2, já que tal número inteiro não existe entre os números inteiros de 1 a 8. Não sendo suficiente apareceram resultados muito estranhos nos cálculos feitos acima: embora saibamos agora que 2 e 4 não sejam congruentes a 0 módulo 8, o produto deles dois é 8, e este é congruente a 0 módulo 8. Fazendo uma alusão com a multiplicação, é como se estivéssemos dizendo que a multiplicação de 2 números diferentes de 0 deu 0, o que é extremamente estranho.

Enumeramos todos os inversos módulo 8, apresentados na Tabela 3.2.

Observamos, na Tabela 3.2, que os números 2, 4 e 6 não tem inverso módulo 8.

A existência de uma forte ligação entre não ter inverso módulo n e ser anulado módulo n pelo produto com um resíduo não nulo. A prova que isso de fato ocorre é dada por Hefez (2005).

Demonstração. Supondo que n e $1 < a < n$ são inteiros positivos e que têm um fator primo comum entre 1 e n, ou seja, $1 < p < n$. Então, podemos escrever: $n = p \cdot c$ e $a = p \cdot e$, onde c e e são os cofatores similares. Como $1 < p < n$, tem-se $c = \dfrac{n}{p}$ também

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

Tabela 3.2: Resíduo inverso modular 8.

satisfaz $1 < c < n$. Por outro lado, como $1 < a < n$ por hipótese, temos que nem c, nem a são congruentes a 0 módulo n. Contudo,

$$c \cdot a \equiv c \cdot p \cdot e (mod\ n).$$

Por sua vez $n = c \cdot p$, e desta forma,

$$c \cdot p \equiv n \equiv 0 (mod\ n);$$

na qual,

$$c \cdot a \equiv c \cdot p \cdot e \equiv 0 (mod\ n). \tag{3.1}$$

Mas, como usaremos essa informação para verificar que a não tem inverso módulo n? De fato que estes cálculos exibem que a não pode ter inverso módulo n. Para entender por que, procederemos por contradição.

Suponha que a tivesse inverso a' módulo n. Para isso, deveríamos ter,

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

Multiplicando ambos os lados da congruência por c, obteremos,

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

Associando os parênteses teremos,

$$(c \cdot a) \cdot a' \equiv c(mod\ n) \tag{3.2}$$

Entretanto, pela Equação (3.1),

$$c \cdot a \equiv 0(mod\ n);$$

de forma que

$$(c \cdot a) \cdot a' \equiv 0 \cdot a' \equiv 0(mod\ n).$$

Comparando o resultado com a Equação (3.2), obtemos,

$$c \equiv 0(mod\ n);$$

ou seja, n divide c. Só que não é verdade, pois, vimos acima que, $1 < c < n$. Obtendo, desta forma, uma conclusão absurda. Ocorreu isso porque fizemos uma afirmação falsa ao supor que a tem inverso módulo n. Logo, a não tem inverso módulo n, como havíamos afirmado antes. Em resumo, mostramos o que queríamos. □

3.4 Algoritmo Chinês do Resto

Para enunciar o Teorema Chinês do Resto, vamos inicialmente considerar o seguinte exemplo para facilitar nosso entendimento.

Exemplo 3.2. Determinar o menor inteiro positivo que satisfaz a seguinte condição: deixar resto 1 quando dividido por 3 e resto 2 quando dividido por 5.

Observe que o Exemplo 3.2 é muito simples, o suficiente para que possamos resolvê-lo sem precisar fazer contas. Entretanto, nas aplicações do RSA, vamos encontrar exemplos parecidos, mas, com números muito maiores, que só será possível resolver procedendo de maneira metódica, que é outra forma de dizer que resolvemos aplicando um algoritmo. Enunciaremos um teorema que será de grande valia mais adiante.

Teorema 3.4.1. *Suponha que a tenha inverso módulo n. Se $a \cdot b \equiv a \cdot c(mod\ n)$, para a, $b \in \mathbb{Z}$, então $b \equiv c(mod\ n)$.*

Vamos iniciar descrevendo a aplicação do algoritmo ao nosso exemplo.

Chamaremos de n o inteiro que procuramos. Podemos escrever as equações correspondentes à divisão de n por 3 e por 5 na seguinte forma:

$$n = 3q_1 + 1$$

$$n = 5q_2 + 2.$$

Usaremos simbologias diferentes (q_1 e q_2) para denotar os quocientes das divisões, e usando a mesma simbologia, automaticamente, implicaria na incorreta igualdade. Veja que temos um sistema que apresenta três variáveis (n, q_1 e q_2) e duas equações. Como queremos determinar uma solução inteira torna isso um problema ainda mais complicado. Contudo, as linhas desse sistema de equações podem ser reescritas usando congruência. Ao fazer, obtemos:

$$n \equiv 1(mod\ 3),$$

$$n \equiv 2(mod\ 5).$$

O problema é achar uma forma de usar congruências para determinar o número procurado usando apenas uma variável. No entanto, quando temos um sistema de equações, tentamos isolar uma incógnita de uma equação e substituir em outra equação para achar a resposta procurada. Mas, o problema apresenta duas congruências que têm módulos diferentes e, portanto, não podemos substituí-las diretamente.

Vamos usar uma saída estratégica e híbrida: substituiremos a equação $n = 5q_2 + 2$ não na equação $n = 3q_1 + 1$ mas, usaremos essa equação para substituir na congruência $n \equiv 1(mod\ 3)$. Fazendo a substituição, tem-se:

$$5 \equiv 2(mod\ 3)$$

Acontece que $5q_2+2 \equiv 1(mod\ 3)$, de forma que a congruência pode ser reescrita na forma

$$2q_2 + 2 \equiv 1(mod\ 3).$$

Subtraindo 2 de ambos os membros da congruência, obteremos:

$$2q_2 \equiv -1(mod\ 3);$$

sendo $-1 \equiv 2(mod\ 3)$, também podemos escrever:

$$2q_2 \equiv 2(mod\ 3).$$

Como 2 é inversível módulo 3, podemos cancelá-lo na congruência acima pelo Teorema 3.4.1, e obtemos:

$$q_2 \equiv 1(mod\ 3),$$

ou seja, q_2 deixa resto 1 na divisão por 3, de modo que reescrevemos como:

$$q_2 = 3q_3 + 1,$$

sendo, q_3 correspondente ao quociente da divisão. Então, agora temos, a partir das equações:

$$n = 3q_1 + 1,$$
$$n = 5q_2 + 2$$

originais, obtemos uma nova equação:

$$q_2 = 3q_3 + 1,$$

que explicita q_2, mesmo que tenhamos introduzido outra variável q_3, contudo essa ultima equação nos permite substituir o valor de q_2 diretamente na linha 2 das duas equações originais. Fazendo

$$n = 5q_2 + 2 = 5(3q_3 + 1) + 2.$$

Tem-se que

$$n = 15q_3 + 7.$$

Entretanto, se dividirmos $15q_3 + 7$ por 3, teremos $15 = 3 \cdot 5$, tal que:

$$15q_3 + 7 = 3 \cdot 5q_3 + 7.$$

Como $7 \geq 3$ precisaremos escrever essa equação de outra forma. Se 7 fosse menor que 3, automaticamente seria o resto da divisão. Então:

$$7 = 3 \cdot 2 + 1$$

Substituindo as equações obtidas e colocando o número 3 em evidência, temos:

$$15q_3 + 7 = 3 \cdot (5q_3 + 2) + 1;$$

desta forma $15q_3+7$ deixa resto 1 na divisão por 3, como o que pretendíamos que ocorresse com o n a ser determinado em nosso exemplo, para qualquer valor inteiro escolhido para q_3.

De forma mais direta, na divisão por 5 teremos:

$$15q_3 + 7 = 5 \cdot 3q_3 + 5 + 2 = 5(3q_3 + 1) + 2;$$

na qual $5q_3+7$ deixa resto 2 na divisão por 5, resultando no que pedia o exemplo a solução como sendo $n = 15q_3 + 7$.

No entanto, não obtivemos apenas uma solução. O resultado nos leva a uma família de soluções, na qual, cada valor q_3 inteiro que escolhermos, levará a uma solução distinta. Veja na Tabela 3.3 alguns valores para q_3.

$15q_3 + 7$	q_3
-53	-4
-38	-3
-23	-2
-8	-1
7	0
22	1
37	2
52	3
67	4
82	5

Tabela 3.3: Soluções do exemplo.

A partir da fórmula $n = 15q_3 + 7$, obtemos qualquer possível solução deste problema. Basta escolher adequadamente o valor de q_3. Para verificar o menor inteiro n positivo para as duas sentenças, podemos avaliar, de forma mais detalhada, a Tabela 3.3:

i) Se $q_3 < 0$, então $n = 15q_3 + 7 < 0$;

ii) Se $q_3 > 0$, então $n = 15q_3 + 7 > 7$;

de tal forma que o menor inteiro positivo procurado é $n = 7$.

3.4.1 O Teorema Chinês do Resto

As técnicas utilizadas anteriormente para resolver sistemas de congruências são conhecidas como Algoritmo do Resto Chinês (SANTOS, 2006) ou Algoritmo Chinês do Resto (COUTINHO, 2014). Recebeu esse nome, segundo Coutinho (2014, p.113-114) "porque um dos primeiros lugares em que aparece é o livro Manual de aritmética do mestre Sun, escrito entre 287 d.C. e 473 d.C." encontrado na China. No entanto, Coutinho (2014, p.114) também descreve que, "o mesmo resultado é mencionado na Aritmética de Nicômaco de Gerasa, escrita por volta de 100 d.C.".

Considere o seguinte sistema (1):

$$x_0 \equiv a(mod\ m),$$
$$x_0 \equiv b(mod\ n),$$

onde m e n são números inteiros positivos diferentes e vamos supor que o inteiro x_0 é uma solução deste sistema de congruência. Significa que x_0 satisfaz as congruências ao mesmo tempo:

$$x_0 \equiv a(mod\ m),$$
$$x_0 \equiv b(mod\ n).$$

Sabendo que os módulos são distintos, só podemos substituir uma congruência na outra, se modificar uma delas em uma igualdade de números inteiros. Fazendo-o com a linha 1 do sistema, verificamos que:

$$x_0 = a + m \cdot k \tag{3.3}$$

onde k é um número inteiro qualquer, tal que:

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

ou também,

$$m \cdot k \equiv (b - a)(mod\ n). \tag{3.4}$$

Vamos supor que m e n sejam primos entre si, então m é inversível módulo n. Digamos que m' é o inverso de m módulo n. Multiplicando a Equação (3.3) por m', teremos:

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

ou seja,

$$k \equiv m'(b - a) + n \cdot t,$$

para algum número inteiro t. Trocando a expressão para k na Equação (3.3), teremos:

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

Então, verificamos que se x_0 é uma solução do sistema (1), então:

$$x_0 = a + m(m'(b - a) + n \cdot t). \tag{3.5}$$

É facilmente verificado que, atribuindo um valor inteiro qualquer a t, uma expressão da forma $a + m(m'(b - a) + n \cdot t)$ é obrigatoriamente solução do sistema (1). Basta ver que, $a + m(m'(b - a) + n \cdot t)$ é congruente a a módulo m. Por outro lado,

$$a + m(m'(b - a) + n \cdot t) \equiv a + m \cdot m'(b - a)(mod\ n)$$

Como $m \cdot m' \equiv 1(mod\ n)$, tem-se

$$a + m(m'(b - a) + n \cdot t) \equiv a + 1 \cdot (b - a) \equiv b(mod\ n);$$

comprovando que $a + m(m'(b - a) + n \cdot t)$ é uma solução do sistema (1). O que fizemos está resumido no Teorema Chinês do Resto.

Santos enuncia o Teorema Chinês do Resto da seguinte forma:

> Sejam m e n inteiros positivos primos entre si. Se a e b são inteiros quaisquer, então o sistema
>
> $$x \equiv a(mod\ m),$$
> $$x \equiv b(mod\ n).$$
>
> sempre tem solução e qualquer uma de suas soluções pode ser escrita na forma
>
> $$a + m(m'(b - a) + n \cdot t),$$
>
> onde t é um inteiro qualquer e m' é o inverso de m módulo n. (SANTOS, 2006, p.44).

Vamos generalizar o Teorema Chinês do Resto proposto por Santos apresentando o Teorema 3.4.2 e uma aplicação dessa generalização no Exemplo 3.3:

Teorema 3.4.2. *Sejam $m_1, m_2, ..., m_r$, inteiros positivos primos entre si, dois a dois, e sejam $a_1, a_2, ..., a_r$; inteiros quaisquer. Então, o sistema de congruência:*

$$X \equiv a_1(mod\ m_1)$$

$$X \equiv a_2(mod\ m_2)$$

$$... \ ... \ ...$$

$$X \equiv a_r(mod\ m_r)$$

admite uma solução X. Além disso, as soluções são únicas módulo $M = m_1 \cdot m_2 \cdot ... \cdot m_r$

Exemplo 3.3. Determinar qual número deixa resto 2, 3 e 2, quando dividido por 3, 5 e 7.

Inicialmente observamos que o problema é equivalente ao sistema:

$$X \equiv 2(mod\ 3)$$

$$X \equiv 3(mod\ 5)$$

$$X \equiv 2(mod\ 7)$$

No intuito de achar as soluções módulo M, multiplicaremos os $m_1, m_2, ..., m_r$ existentes.

$$M = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105,$$

desta forma,

$$M_1 = \frac{M}{m_1} = 35$$
$$M_2 = \frac{M}{m_2} = 21$$
$$M_3 = \frac{M}{m_3} = 15.$$

Por outro lado as soluções das congruências:

$$35Y \equiv 1(mod\ 3)$$

$$21Y \equiv 1(mod\ 5)$$

$$15Y \equiv 1(mod\ 7)$$

são respectivamente, $y_1 = 2$, $y_2 = 1$ e $y_3 = 1$. Portanto, uma solução módulo $M = 105$ é dada por:

$$x = M_1 y_1 a_1 + M_2 y_2 a_2 + M_3 y_3 a_3 = 233$$

Como $233 \equiv 23(mod\ 105)$, segue que 23 é uma solução e qualquer outra solução é do tipo $23 + 105t$, $t \in Z$.

3.5 Potências

Estamos caminhando para a parte final sobre o que precisamos para apropriarmos do RSA de forma adequada. Embora trabalhado de forma elementar, vimos o quão importante a matemática tem-se mostrado. Vamos enunciar algumas definições e *o Pequeno Teorema de Fermat* para prosseguir.

3.5.1 Funções Aritméticas

Santos (2006, p.69) define "função aritmética a função definida para todos os inteiros positivos. A função ϕ de Euler é um exemplo de função aritmética".

Também nos utilizamos da simbologia $\tau(n)$ para representar o número de divisores positivos de n (SANTOS, 2006), em outras palavras, se $n = p_1^{a_1}\ p_2^{a_2}\ p_3^{a_3} \cdot\ ...\ \cdot p_r^{a_r}$, então:

$$\tau(n) = (a_1 + 1)\ (a_2 + 1)\ (a_3 + 1) \cdot\ ...\ \cdot (a_r + 1).$$

Podemos utilizar uma aplicação rápida e fácil: $12 = 2^2 \cdot 3$, logo:

$$\tau(12) = (2 + 1)(1 + 1) = 6.$$

A função ϕ de Euler é apresentada da seguinte forma: dado um número inteiro positivo n, essa função é definida como o número de inteiros positivos não excedendo n que são relativamente primos com ele próprio, ou seja,

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

Exemplificando $\phi(27) = 3^3 - 3^{3-1} = 3^3 - 3^2 = 27 - 9 = 18$. Em um caso geral se $n = p_1^{a_1}\ p_2^{a_2}\ p_3^{a_3} \cdot ... \cdot p_r^{a_r}$, teremos:

$$\phi(n) = n(1 - \tfrac{1}{p_1})(1 - \tfrac{1}{p_2})(1 - \tfrac{1}{p_3}) \cdot ... \cdot (1 - \tfrac{1}{p_r}).$$

3.5.2 Teorema de Fermat

Coutinho (2000) enuncia o Pequeno Teorema de Fermat da seguinte forma. Se p é um número primo e a é um número inteiro que não é divisível por p, então

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

Iremos mostrar a veracidade do Teorema de Fermat que foi proposto por Euler, por ser mais elementar. Enumerando possíveis resíduos módulo p, que são

$$1,\ 2,\ 3,\ 4, ...,\ p - 1$$

e pegando cada resíduo desse, vamos multiplicá-lo por a, teremos então,

$$a \cdot 1,\ a \cdot 2,\ a \cdot 3,\ a \cdot 4, ...,\ a \cdot (p - 1).$$

Suponhamos que r_1 é o resíduo de $a \cdot 1$, que r_2 é o resíduo de $a \cdot 2$ e assim sucessivamente, até r_{p-1}, que terá o resíduo, por generalização de suposição $a \cdot (p - 1)$. Iremos calcular esse produto

$$r_1 \cdot r_2 \cdot r_3 \cdot r_4 \cdot ... \cdot r_{p-1}.$$

módulo p de duas formas distintas.

Demonstração. Levando em conta que

$$r_1 \equiv a \cdot 1 (mod\ p),$$

$$r_2 \equiv a \cdot 2 (mod\ p),$$

$$r_3 \equiv a \cdot 3 (mod\ p),$$

$$... \quad ... \quad ... \quad ...$$

$$r_{p-1} \equiv a \cdot (p-1) (mod\ p),$$

podemos concluir que

$$r_1 \cdot r_2 \cdot r_3 \cdot r_4 \cdot ... \cdot r_{p-1} \equiv (a \cdot 1) \cdot (a \cdot 2) \cdot (a \cdot 3) \cdot (a \cdot 4) \cdot ... \cdot (a \cdot (p-1)) (mod\ p).$$

Contudo,

$$(a \cdot 1) \cdot (a \cdot 2) \cdot (a \cdot 3) \cdot (a \cdot 4) \cdot ... \cdot (a \cdot (p-1)) = a^{p-1} \cdot (1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot (p-1)).$$

de forma que

$$(r_1 \cdot r_2 \cdot r_3 \cdot r_4 \cdot ... \cdot r_{p-1} \equiv a^{p-1} \cdot (1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot (p-1)) (mod\ p).$$

□

Demonstração. Sabe-se que não podemos ter dois resíduos iguais dentre os resíduos $r_1,\ r_2,\ r_3,\ r_4,\ ...,\ r_{p-1}$.

Suponhamos por absurdo, que $r_k = r_l$, k e l inteiros entre 1 e $p-1$. Aplicando a definição de resíduos, teremos

$$a \cdot k \equiv r_k \equiv r_l \equiv a \cdot l (mod\ p);$$

ou seja,

$$a \cdot k \equiv a \cdot l (mod\ p).$$

No entanto, como a não é divisível por p e este por sua vez é primo, eles não têm fator próprio comum. Mas isto implica que a é inversível módulo p tal que, podemos cancelá-lo na última congruência, resultando

$$k \equiv l(mod\ p).$$

Mas k e l são números inteiros positivos, pela qual são menores que p, e só serão congruentes se forem iguais. Desta forma, se $r_k = r_l$, então teremos $k = l$.

Isto nos mostra que os resíduos $r_1,\ r_2,\ r_3,\ r_4,\ ...,\ r_{p-1}$ são, em números, $p-1$ resíduos, todos diferentes de zero e todos distintos entre si. Entretanto só há $p-1$ resíduos não nulos distintos módulo p, e esses são

$$1,\ 2,\ 3,\ 4,\ ...,\ p-1,$$

o que deduzimos que a sequência de números

$$r_1 \cdot r_2 \cdot r_3 \cdot r_4 \cdot ... \cdot r_{p-1}.$$

é apenas uma mistura de

$$1,\ 2,\ 3,\ 4,\ ...,\ p-1,$$

Um caso particular,

$$r_1 \cdot r_2 \cdot r_3 \cdot r_4 \cdot ... \cdot r_{p-1} = 1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot (p-1).$$

Concluímos, de uma forma genérica que, da primeira forma que efetuamos os cálculos, a multiplicação dos resíduos resulta em

$$r_1 \cdot r_2 \cdot r_3 \cdot r_4 \cdot ... \cdot r_{p-1} \equiv a^{p-1} \cdot (1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot (p-1))(mod\ p)$$

e da segunda forma, resulta em

$$r_1 \cdot r_2 \cdot r_3 \cdot r_4 \cdot ... \cdot r_{p-1} = 1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot (p-1).$$

Portanto,

$$a^{p-1} \cdot (1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot (p-1)) \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot (p-1)(mod\ p).$$

Contudo, $1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot (p-1)$ é a multiplicação de inversíveis módulo p. Logo o número inversível módulo p, é o próprio p. Então podemos cancelá-lo de ambos os membros da congruência, na qual resulta:

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

□

O próximo exemplo mostra uma aplicação do *Pequeno Teorema de Fermat*.

Exemplo 3.4. Calcular o resto da divisão de 3^{68} por 31.

Sabendo que:

$$3^{30} \equiv 1(mod\ 31),$$

pelo Teorema de Fermat e tendo em vista que $68 = 2 \cdot 30 + 8$, teremos:

$$3^{68} \equiv (3^{30})^2 \cdot 3^8 \equiv 1 \cdot 6561 \equiv 20(mod\ 31).$$

4 CRIPTOGRAFIA RSA

Reunindo os artifícios e as técnicas matemáticas apresentadas até agora, podemos adentrar no mundo do RSA. O tópico 4.1 descreve o algoritmo desenvolvido por Ronald Rivest, Adi Shamir e Leonard Adleman, e, como se pode observar, levou o título pelas iniciais dos sobrenomes de seus desenvolvedores. É extremamente necessário explicitá-lo para entender como funciona o procedimento e suas técnicas.

4.1 Algoritmo RSA

O esquema desenvolvido por Rivest, Shamir e Adleman utiliza uma expressão com exponenciais. O texto claro é criptografado em blocos, com cada bloco tendo um valor binário menor que algum número n; ou seja, o tamanho do bloco precisa ser menor ou igual a $log_2(n)$. Na prática, o tamanho do bloco é de i bits, onde $2^i < n \leq 2^{i+l}$. A criptografia e a descriptografia têm a seguinte forma, para algum bloco de texto claro M e bloco de texto cifrado C:

$$C = M^e \ mod \ n$$

$$M = C^d \ mod \ n = (M^e)^d \ mod \ n = M^{ed} \ mod \ n.$$

Tanto o emissor quanto o receptor precisam conhecer o valor de n. O emissor conhece o valor de , e somente o receptor conhece o valor de d. Assim, esse é um algoritmo de criptografia de chave pública com uma chave pública $PU = \{e, \ n\}$ e uma chave privada $PR = \{d, \ n\}$. Para que esse algoritmo seja satisfatório para a criptografia de chave pública, os seguintes requisitos precisam ser atendidos:

1. Ser possível encontrar valores de $e, \ d, \ n$ tais que $M^{ed} \ mod \ n = M$ para todo $M < n$.
2. Ser relativamente fácil calcular $M^e \ mod \ n$ e $C^d \ mod \ n$ para todos os valores de $M < n$.
3. Ser inviável determinar d dados e e n.

Por enquanto, focalizamos o primeiro requisito e consideremos as outras questões mais adiante. Precisamos encontrar um relacionamento na forma

$$M^{ed} \ mod \ n = M$$

O relacionamento a seguir se mantém se e e d forem inversos multiplicativos módulo $\phi(n)$, onde $\phi(n)$ é a função de Euler. O relacionamento entre e e d pode ser expresso como

$$ed \ mod \ \phi(n) = 1$$

Isso equivale dizer

$$ed \equiv 1 mod \ \phi(n)$$

$$d \equiv e^{-1} \ mod \ \phi(n)$$

Ou seja, e e d são inversos multiplicativos $mod \ \phi(n)$. Observe que, de acordo com as regras da aritmética modular, isso é verdadeiro somente se d (e, portanto, e) for relativamente primo a $\phi(n)$. De modo equivalente, $mdc(\phi(n), \ d) = 1$.

Agora, estamos prontos para formular o esquema RSA. Os ingredientes são os seguintes:

$p, \ q$, dois números primos	(privados, escolhidos)
$n = pq$	(público, calculado)
e, com $mdc(\phi(n), \ e) = 1$; $1 < e < \phi(n)$	(público, escolhido)
$d \equiv e^{-1} \ (mod \ \phi(n))$	(privado calculado)

A chave privada consiste em {d, n} e a chave pública consiste em {e, n} . Suponha que o **usuário A** tenha publicado sua chave pública e que o **usuário B** queira enviar a mensagem M para **A**. Então, **B** calcula $C = B^e \ mod \ n$ e transmite C. Ao receber esse texto cifrado, o **usuário A** descriptografa calculando $M = C^d \ mod \ n$.

4.2 Pré-Codificação

O que devemos fazer para encriptar uma mensagem no RSA é calcular sua potência módulo comparando a um expoente escolhido. No entanto, para ser viável, o texto deve ser um número inteiro. Entretanto não é isto o que ocorre em geral: a grande parte das mensagens é um texto. Então, a primeira coisa que devemos fazer, se queremos usar RSA, é descobrir um modo de converter o texto em uma sequência de números inteiros.

Vamos supor, para deixar simples, que o texto de origem é uma mensagem, de tal forma que, ela não contém números, apenas letras, e todas as suas letras são maiúsculas. Por fim, vamos supor, também que, no texto original tem apenas letras sem acentos, formando as palavras, e seus espaços entre as palavras. Vamos chamar esta etapa de *pré-codificação*, para diferenciar do processo de codificação propriamente dito. Então, na *pré-codificação* transformaremos as letras do texto original, em números usando a Tabela 4.1 para converter as letras em números.

Adotaremos que os espaços entre as palavras serão substituídos por 99. Utilizaremos como exemplo a frase AMO O PITAGORAS e usando a Tabela 4.1 para converter a frase em números teremos:

$$1022249924992518291016242710 28$$

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

Tabela 4.1: Conversor de letra em número.

Previamente, vamos precisar de parâmetros para determinar o sistema RSA que vamos usar. Dois primos distintos serão os parâmetros que denotaremos por p e q, de forma que o resto na divisão por 6 tem que ser 5. A escolha desse parâmetro é explicada no próximo tópico.

Escolha n que satisfaça $n = p \cdot q$. E por último vamos quebrar a frase convertida de número longo em blocos menores. Cada bloco tem que conter números menores que n. Exemplificando, escolhendo $p = 17$ e $q = 23$, então $n = 391$. Aplicando a quebra do número longo em blocos menores teremos:

$$102 - 224 - 99 - 249 - 92 - 51 - 82 - 9 - 101 - 62 - 42 - 7 - 102 - 8$$

Devemos tomar alguns cuidados ao quebrar o número longo em blocos menores para não haver ambiguidade, por exemplo, se tomarmos o conversor começando do número 1 haveria problema, pois se tivermos a letra B (seu número correspondente 2) e a letra A juntas não saberíamos distinguir da letra V (de número correspondente 21). Além disso,

os blocos não devem começar por 0, pois seria um problema, também, distinguir o bloco 071 do bloco 71. Vale ressaltar que o texto numérico não corresponde a uma unidade linguística e isso é bom, pois torna a análise de frequência impossível.

4.3 Codificando e Decodificando

Assim que encerrada a fase de pré-codificação, podemos iniciar a etapa de codificação. Vamos precisar de n para codificar a mensagem. Chamaremos n de *chave* do RSA e ela pode ser tornada pública, ou seja, sem se preocupar em manter n em segredo, pode-se enviar n a todos que queiram enviar uma mensagem. Stallings (2010) afirma que esse tipo de chave de codificação é conhecido como *chave pública*.

Com os blocos pré-codificados, codificaremos bloco a bloco de forma separada. A mensagem codificada aparecerá na ordem em que os blocos forem codificados e essa sequencia não pode ser modificada, pois ficaria impossível decodificar a mensagem original.

4.3.1 Codificação

Para codificar escolheremos um número inteiro positivo e, de modo que o $mdc(n,\ e) = 1 \quad \text{e} \quad 1 < e < n$, como destacado na Seção 4.1 no Algoritmo RSA. Chamaremos $C(b)$ de codificador de bloco e a fórmula para calculá-lo é:

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

Escolheremos $e = 3$ para nossa codificação de forma que, pegando bloco a bloco e codificando-os.

$$C(102) \equiv 102^3 \equiv 102^2 \cdot 102 \equiv 24276 \equiv 34 (mod\ 391);$$

$$C(224) \equiv 224^3 \equiv 224^2 \cdot 224 \equiv 128 \cdot 224 \equiv 129 (mod\ 391);$$

$$C(99) \equiv 99^3 \equiv 99^2 \cdot 99 \equiv 29 \cdot 99 \equiv 228 (mod\ 391);$$

$$C(249) \equiv 249^3 \equiv 249^2 \cdot 249 \equiv 223 \cdot 249 \equiv 5 (mod\ 391);$$

$$C(92) \equiv 92^3 \equiv 92^2 \cdot 92 \equiv 253 \cdot 92 \equiv 207 (mod\ 391);$$

$$C(51) \equiv 51^3 \equiv 51^2 \cdot 51 \equiv 255 \cdot 51 \equiv 102 (mod\ 391);$$

$$C(82) \equiv 82^3 \equiv 82^2 \cdot 82 \equiv 77 \cdot 82 \equiv 58 (mod\ 391);$$

$$C(9) \equiv 9^3 \equiv 9^2 \cdot 9 \equiv 81 \cdot 9 \equiv 338(mod\ 391);$$

$$C(101) \equiv 101^3 \equiv 101^2 \cdot 101 \equiv 35 \cdot 101 \equiv 16(mod\ 391);$$

$$C(62) \equiv 62^3 \equiv 62^2 \cdot 62 \equiv 325 \cdot 62 \equiv 209(mod\ 391);$$

$$C(42) \equiv 42^3 \equiv 42^2 \cdot 42 \equiv 200 \cdot 42 \equiv 189(mod\ 391);$$

$$C(7) \equiv 7^3 \equiv 7^2 \cdot 7 \equiv 49 \cdot 7 \equiv 343(mod\ 391);$$

$$C(102) \equiv 102^3 \equiv 102^2 \cdot 102 \equiv 238 \cdot 102 \equiv 34(mod\ 391);$$

$$C(8) \equiv 8^3 \equiv 8^2 \cdot 8 \equiv 64 \cdot 8 \equiv 121(mod\ 391);$$

Então temos a mensagem codificada, após aplicar nosso codificador de bloco e é:

$$34 - 129 - 228 - 5 - 207 - 102 - 58 - 338 - 16 - 209 - 189 - 343 - 34 - 121$$

4.3.2 Decodificando

Para decodificar precisaremos da chave pública e de um bloco codificado para podermos reconstruir o bloco antes da codificação. Então o que realmente precisamos é ter o número n e ter o número inverso $d > 0$ de 3 módulo $(p-1)(q-1)$, ou seja, $3d \equiv 1(mod\ (p-1)(q-1))$. A chave privada $\{d,\ n\}$ precisa manter-se em segredo, caso contrário, quem a tiver poderá decodificar as mensagens enviadas para você.

Chamaremos o bloco codificado de $D(a)$, onde a é o bloco codificado e a fórmula para decodificá-lo é:

$$D(a) \equiv a^d(mod\ n)$$

No tópico 4.2 supomos que p e q deixam resto 5 na divisão por 6, logo:

$$p \equiv 5(mod\ 6) \quad \text{e} \quad q \equiv 5(mod\ 6)$$

Desta forma,

$$(p-q)(q-1) \equiv 4 \cdot 4 \equiv 16 \equiv 4 \equiv -2(mod\ 6);$$

e

$$(p-q)(q-1) \equiv 6 \cdot k - 2,$$

para algum número inteiro k positivo. Aplicando nossos conhecimentos do tópico 3.3 descobrimos que o inverso de 3 módulo $6 \cdot k - 2$ é $4 \cdot k - 1$, assim, tomaremos

$$d = 4 \cdot k - 1.$$

Como $p = 17$ e $q = 23$, temos que:

$$(p-1)(q-1) = (17-1)(23-1) = 16 \cdot 22 = 352 = 6 \cdot 58 + 4$$

na qual,

$$(p-1)(q-1) = 6 \cdot 59 - 2.$$

Logo, $k = 59$ e

$$d = 4 \cdot 59 - 1 = 235.$$

De posse do número $d = 235$ podemos aplicar $D(a)$ e usaremos $a = 34$, desta forma teremos $D(34) \equiv 34^{235}(mod\ 391)$. Para resolvermos essa congruência, recorreremos aos tópicos 3.4.1 (Teorema Chinês do Resto) e 3.5.2 (Teorema de Fermat) na qual calcularemos 34^{235} módulo 17 e módulo 23, pois $n = 391 = 17 \cdot 23$.

$$\begin{cases} 34 \equiv 0(mod\ 17) \\ 34 \equiv 11(mod\ 23) \end{cases},$$

temos que $34^{235} \equiv 0^{235} \equiv 0(mod\ 17)$. Por outro lado, pelo Teorema de Fermat,

$$11^{235} \equiv (11^{22})^{10}11^{15} \equiv 11^{15}(mod\ 23).$$

Só que,

$$11 \equiv -12 \equiv -4 \cdot 3(mod\ 23)$$

então

$$11^{235} \equiv 11^{15} \equiv -4^{15} \cdot 3^{15}(mod\ 23);$$

Assim,

$$4^{11} \equiv 1(mod\ 23),$$

$$3^{11} \equiv 1(mod\ 23),$$

de modo que

$$4^{15} \equiv 2^{30} \equiv (2^{11})^2 \cdot 2^8 \equiv 2^8 \equiv 3(mod\ 23),$$

$$3^{15} \equiv 3^{11} \cdot 3^4 \equiv 3^4 \equiv 12(mod\ 23).$$

Desta forma concluímos que

$$11^{235} \equiv -4^{15} \cdot 3^{15} \equiv -3 \cdot 12 \equiv 10(mod\ 23).$$

Portanto

$$\begin{cases} 34^{235} \equiv 0(mod\ 17) \\ 34^{235} \equiv 10(mod\ 23) \end{cases},$$

corresponde a

$$\begin{cases} x \equiv 0(mod\ 17) \\ x \equiv 10(mod\ 23) \end{cases}.$$

Usaremos o Teorema Chinês do Resto para resolver esse sistema de congruência. Da linha 2 do sistema obtemos, $x = 10 + 23y$. Substituindo na linha 1 obtemos,

$$10 + 23y \equiv 0(mod\ 17).$$

Desta forma $6y \equiv 7(mod\ 17)$. No entanto 6 possui inverso 3 módulo 17, de madeira que $y \equiv 3 \cdot 7 \equiv 4(mod\ 17)$. Logo,

$$x = 10 + 23y = 10 + 23 \cdot 4 = 102;$$

e já era esperado esse resultado, já que decodificamos 34, e este é correspondente a codificação do bloco 102.

4.4 Segurança RSA

Vejamos então porque funciona. Como já vimos, existe a função $\phi(n)$ que calcula a quantidade de mdc entre dois números será igual a 1 e também vimos que $\phi(n) = \phi(pq) = (p-1)(q-1)$. Outro fator se deve ao Teorema de Fermat, que Euler generalizou, e afirma que, se pegarmos a e n de maneira que o máximo divisor comum seja igual a 1, então $a^{\phi(n)}$ quando dividimos por n possui resto da divisão igual a 1, ou seja:

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

Escolhendo n, sendo n o produto de dois números primos p e q, aplicando o Teorema de Fermat Euler teremos:

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

Fazendo algumas manipulações teremos $a^{1+m(p-1)(q-1)}$, pela qual, pegando esse número e dividindo por $p \cdot q$, o resto dessa divisão é igual a a, ou seja:

$$a^{1+m(p-1)(q-1)} \equiv a \; mod \; (pq),$$

e esta é a chave do método RSA. Reunindo as informações e inicialmente escolhemos o número e, de maneira que $mdc(e,\ (p-1)(q-1)) = 1$, também foi escolhido o número d, de maneira que $e \cdot d \equiv 1(mod\ (p-1)(q-1))$ e foi feito os cálculos fazendo $a^e \equiv b(mod\ n)$, ou seja, $b^d = (a^e)^d = a^{ed} = a^{1+m(p-1)(q-1) \equiv a(mod\ n)}$, e é justamente essa ultima linha que garante que a codificação e a decodificação funciona.

5 APLICAÇÕES DE CRIPTOGRAFIA NA SALA DE AULA

O objetivo desse capítulo é propor atividades em que alguns conteúdos abordados neste texto sejam trabalhados em sala de aula com alunos do Ensino Fundamental ou Ensino Médio.

5.1 Atividade 1

Cifra de César - *Um dos primeiros sistemas de Criptografia conhecido foi elaborado pelo general Júlio César, no Império Romano. Júlio César substituiu cada letra pela terceira letra que a segue no alfabeto, como ilustrado na Figura 5.1.*

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Q	R	S	T	U	V	W	X	Y	Z
T	U	V	W	X	Y	Z	A	B	C

Figura 5.1: Sistema Criptográfico de Júlio César.

Baseado nesse critério:

a) **Codifique a frase: Eu gosto de Matemática**;

b) **Decifre a mensagem: OHJDO FRQVHJXL**;

c) **Em vez de caminhar três letras para frente, podemos andar outro número de letras e teremos um novo método de cifrar mensagens. Esse número é chamado de chave ou senha do sistema criptográfico, o qual, por motivos óbvios, só deve ser conhecido por quem envia a mensagem e por quem a recebe. Estabeleça agora o seu critério de codificação avançando mais do que três letras. Escreva uma palavra para a outra pessoa da sua dupla e peça a ela para tentar decodificar sua mensagem. Se ela não conseguir, conte o seu critério e peça para ela tentar novamente**.

5.2 Atividade 2

Disco de Cifras - *Podemos transformar letras em números, no processo de substituição de letras para criptografar uma mensagem. No quadro a seguir (Figura 5.2), temos um exemplo de como podemos fazer essa associação.*

A=0	B=1	C=2	D=3	E=4	F=5	G=6	H=7
I=8	J=9	K=10	L=11	M=12	N=13	O=14	P=15
Q=16	R=17	S=18	T=19	U=20	V=21	W=22	X=23
Y=24	Z=25						

Figura 5.2: Sistema Criptográfico associando letras a números.

Desse modo, a letra codificada é obtida da letra original, somando-se três ao número correspondente. Mas, como vimos, podemos somar outros números. A partir dessas informações, resolva o problema a seguir, retirado de uma prova da Olimpíada Brasileira de Matemática das Escolas Públicas - OBMEP[1] 2007, Nível 2.

Um antigo método para codificar palavras consiste em escolher um número de 1 a 26, chamado *chave* do código, e girar o disco interno do aparelho ilustrado na figura até que essa chave corresponda à letra A. Depois disso, as letras da palavra são substituídas pelos números correspondentes, separados por tracinhos. Por exemplo, na Figura 5.3, a chave é 5 e a palavra PAI é codificada como 20-5-13.

a) **Usando a chave indicada na figura, descubra qual palavra foi codificada como: 23-25-7-25-22-13**;

b) **Codifique OBMEP usando a chave 20**;

c) **Chicó codificou uma palavra de 4 letras com a chave 20, mas esqueceu-se de colocar os tracinhos e escreveu 2620138. Ajude Chicó colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele codificou**;

d) **Em uma outra chave, a soma dos números que representam as letras A, B e C é 52. Qual é essa chave?**

[1]Encontrado no endereço eletrônico: $< http://www.obmep.org.br/provas\_static/pf2n2-2007.pdf >$. Acesso em 22 de fevereiro de 2017.

Figura 5.3: Disco de cifra.

5.3 Atividade 3

Carreiras de Vigenère - *Atribuído erroneamente ao francês Blase Vigenère a Cifra de Vigenère ou Carreiras de Vigenère foi um marco histórico na segurança de informações pois acreditavam que a cifra fosse inquebrável por ser um sistema criptográfico polialfabético na qual utiliza-se palavras-chave.*

Chicó, ao estudar Vigenère, observou que Blase Vigenène aperfeiçoou uma técnica existente e então decidiu criar as Carreiras de Chicó ou Cifra de Chicó (Figura 5.4) que consiste em substituir palavras-chave por deslocamento numérico para cifrar uma mensagem. A Tabela 5.1 exemplifica Chicó cifrando a mensagem: ATACAR

mensagem original	A	T	A	C	A	R
deslocamento	3	7	12	20	23	14
mensagem codificada	D	A	M	W	X	F

Tabela 5.1: Codificação de Chicó.

Usando deslocamento 15 - 12 - 15 - 1 e suas repetições:

0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Figura 5.4: Carreiras de Chicó.

a) **Codifique TECNOLOGIA**;

b) **Decodifique SUVB CMD BH PGPVMH**

c) **É possível decodificar uma mensagem utilizando as Carreiras de Chicó sem saber os deslocamentos utilizados?**

5.4 Reflexões sobre a Atividade 1

– ***Cifra de César***:

a) Codifique a frase: Eu gosto de Matemática. $HX\ JRVWRGH\ PDWHPDWLFD$;

b) Decifre a mensagem $OHJDO\ FRQVHJXL$. LEGAL CONSEGUI;

c) Este item dessa atividade gera respostas pessoais dos alunos, dependendo da senha que escolherem.

5.5 Reflexões sobre a Atividade 2

– ***Disco de Cifras***:

a) A partir da figura do enunciado temos $23 = S$, $25 = U$, $7 = C$, $22 = R$ e $13 = I$. Logo, a palavra codificada como 23-25-7-25-22-13 é $SUCURI$;

b) Para a chave 20 temos a figura abaixo, na qual vemos que $O = 8$, $B = 21$, $M = 6$, $E = 24$ e $P = 9$.

Assim, a codificação de $OBMEP$ é 8-21-6-24-9. Alternativamente, ao passar da chave 5 para a chave 20 devemos somar 15 aos números da figura do enunciado, lembrando que se a soma for maior do que 26 devemos subtrair 26.

Assim, temos: em que $OBMEP$ é codificada como 8-21-6-24-9;

c) Como não existe letra codificada como 0, um dos números associados a letras na sequência 2620138 é o 20. À sua direita há três dígitos, mas como não há letra codificada como 138 ou 38, os números associados a letras são o 13 e o 8. Isto dá um total de três letras. Portanto, à esquerda de 20 só podemos admitir o 26. Logo, a codificação da palavra é 26-20-13-8, a qual, na chave 20, corresponde a $GATO$;

d) Quando somamos três números consecutivos, obtemos um número divisível por 3; por exemplo, $14 + 15 + 16 = 45$. Ao somar os números que representam as letras A, B e C nessa certa chave, obtemos 52, que não é um número divisível por 3. Isso mostra que os três números não são consecutivos e isso somente é possível se um dos números for 26 e outro for 1. Como a soma é 52, o terceiro número é $52 - 27 = 25$. A única codificação de ABC, nesse caso, é 25-26-1, ou seja, a chave é 25.

5.6 Reflexões sobre a Atividade 3

– ***Carreiras de Vigenère***:

a) IQRODXDHXM

b) DIGA NAO AS DROGAS

c) Sim. As Carreiras de Chicó acompanham a metodologia das cifras polialfabéticas e ao fazer análise de frequência vai-se verificar um padrão e quanto maior a mensagem mais fácil se torna a decodificação.

6 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo compreender os conceitos matemáticos envolvidos que desencadearam na criação da Criptografia RSA, e segundo algumas análises é predominantemente aplicado em compras pela internet, com cartões de pagamento e assinatura digital.

Primeiramente foi trabalhada uma visão histórica na qual a necessidade de manter as informações em sigilo era fator primordial e decisivo em batalhas. Verificamos que a criptologia, no decorrer do tempo, passou por muitas mutações para obter a segurança perfeita, no entanto, pesquisas bibliográficas apontaram a não existência dessa solução íntegra e ótima.

Sabendo que não existem mecanismos totalmente seguros e visando a defesa de um possível ataque a essas trocas de informações é necessário garantir um tempo hábil que essas informações permanecerão seguras.

Apresentar ao aluno a perspectiva de envio e recebimento de mensagem usando materiais básicos como lápis e papel dar-se-á uma motivação maior ao aprendizado contextualizado, pois tem-se aprendizagem quando compreendemos conhecimento teórico aliada a visualização através da prática, e é o que torna o processo mais interessante.

A Teoria dos Números foi e é o alicerce do algoritmo RSA. A criptografia RSA baseia-se na dificuldade de obter números primos como fatores de decomposição de um número relativamente grande, e essa é a principal segurança deste modelo.

REFERÊNCIAS

COUTINHO, S. C. **Números inteiros e criptografia RSA**. Série de Computação e Matemática n.2, IMPA e SBM, segunda edição (revista e ampliada), 2000.

_____. **Criptografia**. Programa de Iniciação Científica da OBMEP. IMPA/OBMEP, 1 ed. (décima impressão), Rio de Janeiro - RJ: IMPA, 2014.

_____. **Criptografia**. Programa de Iniciação Científica da OBMEP. IMPA/OBMEP (www.obmep.org.br), 1 ed. (décima primeira impressão), Rio de Janeiro - RJ: IMPA, 2015.

FRANÇA, Milena Cristina. **Rede de Computadores**. Florianópolis ? SC: Publicações do IFSC, 2010.

HEFEZ, A. **Elementos de Aritmética**. Sociedade Brasileira de Matemática. 2005.

PAIVA, S. PlantãoNERD.com. **Supercomputador faz 20 trilhões de cálculos por segundo**, 2012. Disponível em: $< http://www.plantaonerd.com/blog/2012/03/15/supercomputador-faz-20-trilhoes-de-calculos-por-segundo/ >$ Acesso em: 20 de maio de 2016.

SANTOS, J. Plínio de O. **Introdução à Teoria dos Números**. 3 ed. (terceira impressão). Rio de Janeiro - RJ: IMPA, 2006.

SINGH, S. **O livro dos códigos**. São Paulo: Editora Record. 2001.

STALLINGS, W. **Criptografia e Segurança de Redes**. Tradução de Daniel Vieira. 4 Ed. Editora Pearson, São Paulo - SP, 2010.