UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
CURSO DE LICENCIATURA EM MATEMÁTICA

RAIZA NASCIMENTO DE ALMEIDA

CRIPTOGRAFIA RSA

BELÉM – PARÁ
2023

RAIZA NASCIMENTO DE ALMEIDA

CRIPTOGRAFIA RSA

Trabalho de Conclusão de Curso apresentado para obtenção do grau de Licenciatura Plena em Matemática pela Universidade Federal do Pará
Orientadora: Profa Dra Irene Castro Pereira

BELÉM – PARÁ
2023

CRIPTOGRAFIA RSA

Trabalho de conclusão de curso apresentado como requisito para a obtenção do título de Licenciado Pleno em Matemática pela Universidade Federal do Pará pela seguinte banca examinadora:

Orientadora: Profa. Dra. Irene Castro Pereira

Faculdade de Matemática - ICEN, UFPA

Prof. Dr. Juaci Picanço da Silva

Faculdade de Matemática - ICEN, UFPA

Prof. M.e Leonardo Rodrigues Pantoja

Faculdade de Matemática - ICEN, UFPA

DATA DE AVALIAÇÃO:

CONCEITO:

Para todos que me ajudaram nesta caminhada.

AGRADECIMENTOS

À minha orientadora, Irene Castro Pereira, por não hesitar uma vez se quer em continuar este trabalho. Obrigada pelo compromisso.

À minha família, em especial aos meus pais, Nazareno Dias e Maria Almeida, pelo apoio constante e a confiança em mim, sem eles nada seria possível. Aos meus irmãos pelo incentivo e força, Maria Nascimento, Jucele Almeida, Suelem Almeida, Eric Almeida e Aldo Almeida, que podem não perceber, mas fizeram toda diferença no meu emocional.

Não poderia deixar de agradecer imensamente meus amigos de graduação, Maridilce de Jesus, Jaqueline Valério, Enielson Gama, Socorro Ferreira e Erick Rodolfo, obrigada pelo maravilhoso companheirismo e aprendizados. Em especial a minha amiga Pamela Pantoja, que me mostrou que a lealdade é atemporal, obrigada pela cumplicidade.

A todos os meus professores, em especial a professora Nazaré Bezerra, que me mostrou que todo conhecimento pode ser repassado, mas que a Práxis pedagógica deve esta presente para que o aprendizado seja eficaz.

À minha noiva, Evelin Mesquita, pelo total apoio ao finalizar este trabalho, obrigada pelo incentivo e companheirismo.

À Universidade Federal do Pará, em especial a Faculdade de Matemática.

"Se você está atravessando o inferno, continue andando."

WINSTON CHURCHILL

Resumo

Neste trabalho estudaremos a criptografia RSA a partir do conjunto dos números inteiros. Faremos uma breve introdução à Teoria dos Números, com os conceitos necessários para entender a criptografia: Números primos, congruências, função de Euler. Desta forma, iremos compreender como funcionam as etapas de implementação do método RSA. Outrossim, com exemplos de aplicação, os quais mostram passo a passo de como codificar e decodificar uma mensagem.

Palavras-chave: criptografia, teoria dos números; números primos.

Sumário

INTRODUÇÃO **1**

1 INTRODUÇÃO A TEORIA DOS NÚMEROS **3**
1.1 Anel dos inteiros . . . 3
1.2 Relação de ordem . . . 5
1.2.1 Elemento Mínimo de um Conjunto . . . 5
1.2.2 Princípio da Boa Ordem . . . 6
1.3 Princípio da indução finita . . . 6
1.4 Divisibilidade em $\mathbb{Z}$ . . . 6
1.4.1 Definição e Propriedades . . . 6
1.5 Máximo Divisor Comum . . . 7
1.5.1 Existência de Máximo Divisor comum . . . 8
1.6 Algoritmo da Divisão . . . 8
1.7 Algoritmo de Euclides . . . 10
1.8 Inteiros Relativamente Primos . . . 12

2 TEOREMA FUNDAMENTAL DA ARITMÉTICA E NÚMEROS PRIMOS **13**
2.1 Números Primos . . . 13
2.1.1 Propriedades dos Números Primos . . . 14
2.1.2 Teorema fundamental da aritmética . . . 15

3 CONGRUÊNCIAS **17**
3.1 Inteiros Congruentes . . . 17
3.1.1 Propriedades da Congruência . . . 18
3.2 Teorema de Fermat, Euler e Wilson . . . 21
3.2.1 Teorema de Fermat . . . 21
3.2.2 Teorema de Wilson . . . 21
3.3 Função de Euler . . . 22
3.3.1 Cálculo de $\phi(n)$ . . . 23

4 CRIPTOGRAFIA RSA **26**
4.1 Pré-codificação . . . 26
4.2 Geração de Chave e Codificação em RSA . . . 27
4.3 Decodificação . . . 27
4.4 Aplicações . . . 28

Considerações Finais **34**

INTRODUÇÃO

Desde a antiguidade utilizava-se a criptografia para transmitir mensagens secretas, seguindo um método bem lógico. Este método era constituído pelo embaralhamento de uma mensagem, de modo que, apenas quem conhecesse o processo para desembaralhar conseguiria tornar a mensagem legível novamente.

Segundo o autor, "Nessa abordagem, um algoritmo utiliza uma chave para converter as informações naquilo que se parece com bits aleatórios. Assim, o mesmo algoritmo utiliza a mesma chave para recuperar os dados originais"(BURNETT, 2002). Este conceito é chamado de criptografia de chave simétrica, pois utilizar-se de apenas uma chave privada para codificar e decodificar uma mensagem.

A necessidade de uma criptografia mais segura e com maior domínio de chave, fez com que fosse criada em 1976, por Diffie e Hellman, a criptografia de chave assimétrica. Esta criptografia mudou os rumos do campo de codificação, ela inovou por utilizar duas chaves diferentes: uma pública e outra privada. O processo de codificar e decodificar uma mensagem ficou mais trabalhado, portanto, mais seguro. Visando isso, os cientistas, Ronald Rivest e Adi Shamir, que trabalhavam no MIT na década de 70, empenharam-se em criar um método de criptografia de chave assimétrica eficiente. Foram ajudados pelo matemático Leonard Adleman, que fazia validações pelo ponto de vista matemático, em 1977 o método RSA foi registrado pelos três.

Tratando-se dos métodos criptográficos de chave pública, o RSA é um dos mais conhecidos e atualmente o mais utilizado nas aplicações comerciais. Iremos abordar os processos para entendermos como codificar e decodificar uma mensagem em RSA. Este projeto irá**investigar** nos estudos dos números inteiros, focando-se nos primos, as propriedades necessárias para a implementação do método RSA.

A criptografia de chave RSA é o mais conhecido entre os métodos criptográficos de chave pública. Atualmente o mais usado, sobretudo em aplicações comerciais. Essa criptografia é muito útil para o comércio eletrônico via Internet, assim como para navegar nela. O RSA, por ser um método de chave pública, permite que qualquer usuário codifique mensagens, mas como a chave de decodificação é secreta, só o destinatário legítimo poderá decodificá-la.

O RSA é um método muito avançado e difícil de ser quebrado, mas não impossível, afinal nenhum algoritmo é inquebrável. O diferencial é que utilizando os números inteiros, especificamente os números primos, vemos como a matemática é bem trabalhada, com isso torna-se extremamente dificultoso decodificar o RSA. Desta forma, podemos dizer que números primos, envolvido com muitos caracteres é o segredo para este método ser tão eficiente. Desta maneira, destacamos que a matemática é utilizada para fazer todos os passos de criptografia de dados e todos os métodos serão mostrados neste trabalho.

No primeiro capítulo, há tópicos da Teoria dos Números, sendo essa a base para implementarmos a criptografia RSA. Como, por exemplo, o anel dos inteiros, primordial para trabalharmos com os números e suas propriedades. Por conseguinte, será apresentado um método de grande valia na teoria dos números, o princípio da indução finita. Em seguida, veremos algumas propriedades de divisibilidade, afinal teremos que tê-las em mente para usar nossos algoritmos, como o de Euclides. Esta introdução de teoria dos números dará total auxílio para implementação do método ao final deste trabalho.

O teorema fundamental da aritmética e números primos são elementos primordiais quando se trata de criptografia RSA, pois o resultado do teorema dará suporte para trabalhar diversos teoremas e propriedades que irão compor as etapas da criptografia. O segundo capítulo desde trabalho mostra a importância do conhecimento acerca dos primos, a criptografia RSA é forte justamente por ser feita através do uso destes números. Logo, saber sobre suas propriedades torna-se imprescindível.

As congruências modulares e suas propriedades é outra parte importante deste trabalho, mostrada no terceiro capítulo. Veremos que o uso destas propriedades nas etapas de codificação e decodificação torna o método RSA bem trabalhado. As relações de ordem, assim como os algoritmos trabalhados, são facilitadores para que este método cumpra todas as etapas. Desde a criação de uma tabela até a separação de uma mensagem em blocos aleatórios, de maneira semelhante, transportar uma mensagem que apenas quem tenha posse da chave de decodificação possa acessá-la, preservando assim a eficácia do método.

No último capítulo será trabalhada o método RSA, podemos não perceber, mas há criptografia em nosso dia a dia, como, por exemplo, nossos dados do celular, computador, dados de aplicativos de rede, são mascarados por criptografias específicas. Em particular, o RSA é um método muito avançado e difícil de ser quebrado. Notamos isso quando nos capítulos mostramos o passo a passo de cada propriedade, algoritmo, teorema e percebemos quão difícil é manipular os números. Este método abrange três etapas, então torna-se mais complicado uma saída rápida. Utilizando o que foi visto percebe-se que decodificar uma mensagem em RSA é difícil, não é impossível, porém demanda muito tempo para chegar a mensagem original, justamente, porque após embaralhar uma mensagem usa-se algorítimos diferentes para codificar e decodificá-la.

O RSA funciona com duas chaves, uma pública e outra privada. As chaves inicialmente estão com o destinatário da mensagem, quem envia a mensagem utiliza-se da chave pública para codificar e após enviar a mensagem codificada ao destinatário, para que este com a chave privada, que sempre está em sua posse, decodifique e retorne a mensagem original. A chave pública pode ser acessada por qualquer pessoa que queira enviar uma mensagem para quem possui da chave privada. Os recursos utilizados, como os números primos com dígitos de muitos caracteres, é o segredo para o método ser tão eficiente. O que vimos foi a parte da matemática utilizada para fazer todos os passos, codificar e decodificar, da criptografia de dados. Esses algoritmos serão mostrados neste capítulo seguidos de exemplos e aplicações.

Capítulo 1

INTRODUÇÃO A TEORIA DOS NÚMEROS

1.1 Anel dos inteiros

De acordo com, (FILHO, 1981), em teoria elementar dos números, o conjunto dos números inteiros define-se.

Definição 1.1. *Os números inteiros ou apenas os inteiros são:* $..., -3, -2, -1, 0, 1, 2, 3, ...$

cujo conjunto representa-se pela letra $\mathbb{Z}$*, isto é:* $\mathbb{Z} = \{..., -3, -2, -2, 0, 1, 2, 3, ...\}$.

Neste conjunto estão definidas duas operações:

1. **Adição:**
$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$(a, b) \ \to \ a + b$$

2. **Multiplicação:**
$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$(a, b) \ \to \ ab$$

Em seguida veremos as propriedades destas operações.

Axiomas da Adição:

1. A adição é chamada associativa quando para quaisquer $a, b, c \in \mathbb{Z}$ têm-se:
$$(a + b) + c = a + (b + c)$$

2. Existência do Elemento neutro:

   Existe um único elemento, pertencente ao conjunto dos inteiros, denominado o elemento neutro da adição ou zero, denotado por 0, tal que seja, $a \in \mathbb{Z}$ tem-se:

$$a + 0 \ = \ 0 + a = a;$$

3. Existência do oposto:

   Para cada inteiro a, existe um inteiro b, tal que.

$$a + b \ = \ b + a = 0$$

   O elemento b acima é chamado de **oposto ou inverso aditivo** de a e será denotado por $-a$. Desta forma:

$$a + (-a) \ = 0, \forall \ a \in \mathbb{Z}$$

4. A adição é chamada comutativa quando, para quaisquer $a, b \in \mathbb{Z}$, tem-se.

$$a + b \ = \ b + a$$

Axiomas da Multiplicação:

5. multiplicação é dita associativa quando, para quaisquer, $a, b, c \in \mathbb{Z}$ tem-se:

$$(ab)c \ = \ a(bc)$$

6. Existência do Elemento unidade:

   Em $\mathbb{Z}$ existe um único elemento, denominado o **neutro da multiplicação** ou **elemento unidade**, denotado por 1, $1 \neq 0$, tal que para quaisquer $a \in \mathbb{Z}$ têm-se:

$$a1 = 1a = a$$

7. A multiplicação é dita comutativa quando, para quaisquer $a, b \in \mathbb{Z}$, tem-se:

$$ab = ba$$

8. Distributividade da multiplicação em relação à adição:

   Isto é, para quaisquer $a, b, c \in \mathbb{Z}$, tem-se

$$a(b + c) = ab + ac$$

   Possuindo essas 8 propriedades juntamente com as operações de adição e multiplicação, dizemos que o conjunto $\mathbb{Z}$, isto é, o terno $(\mathbb{Z}, +,)$ é um anel

9. O conjunto $\mathbb{Z}$ é sem divisores de zero, isto é

$$\forall a, b \in \mathbb{Z}, \text{ Se } ab = 0, \text{ então } a = 0 \text{ ou } b = 0$$

   As seguintes notações serão usadas para os subconjuntos de $\mathbb{Z}$:

   $\mathbb{Z}^* = \mathbb{Z} - \{0\}$ (conjunto dos inteiros não nulos)

$\mathbb{Z}_+ = \{0, 1, 2, 3, ...\}$ (conjunto dos inteiros não negativos)

$\mathbb{Z}_+^*$ = $\{1, 2, 3, ...\}$(conjunto de inteiros positivos)

10. Para quaisquer $a, b \in \mathbb{Z}_+$ tem-se que $a + b \in \mathbb{Z}$ e $a, b \in \mathbb{Z}$

1.2 Relação de ordem

Definição 1.2. *Dados inteiros a e b, dizemos que a é menor que b (ou que b é menor que a) e escrevemos $a < b$ ou $b > a$* ***se existe um inteiro positivo*** *c tal que.*

$$b = a + c$$

Escreve-se $a \leq b$ (a é menor ou igual a b) se $a < b$ ou $a = b$, isto é,

$\exists\, c \in \{0, 1, 2, 3, ...\}$ tal que $b = a + c$.

A relação $\leq$ tem as seguintes propriedades:

(a) é **reflexiva**, isto é, $a \leq a \ \forall\, a \in \mathbb{Z}$;

(b) é **antissimétrica**, isto é, para qualquer $a, b \in \mathbb{Z}$, se $a \leq b$ e $b \leq a$, $\Rightarrow a = b$;

(c) é **transitiva**,isto é, para quaisquer a, b e $c \in \mathbb{Z}$,$a \leq b$ e $b \leq c \Rightarrow a \leq c$.

Com essas 3 propriedades dizemos que $\leq$ é uma **Relação de Ordem** em $\mathbb{Z}$ e que $\mathbb{Z}$ é um **Conjunto Ordenado**.

(A11) Tricotomia Dados inteiros a e b, apenas umas das condições abaixo se verifica:

(i) $a < b$.

(ii) $a = b$.

(iii) $b < a$.

1.2.1 Elemento Mínimo de um Conjunto

Definição 1.3. *Seja A um conjunto de inteiros, se existe um elemento $a \in A$, tal que, $a \leq x$, $\forall x \in A$. Então o chamamos de elemento mínimo de A.*
Representa-se pela notação "$minA$ ", que se lê: "mínimo de A, Portanto simbolicamente:
$minA = a \Leftrightarrow a \in A$ *e* $\forall x \in A \Rightarrow a \leq x$

Teorema 1.4. *Se a é elemento mínimo de A , então este elemento é único.*

Demonstração:

Por absurdo, vamos supor que exista outro elemento mínimo b de A, Teríamos:

(1) $a \leq b$, pois $a = minA$.

(2) $b \leq a$, pois $b = minA$.

Então pela propriedade antissimétrica da relação de ordem em $\mathbb{Z}$, logo.

$a = b$ Portanto, a é mínimo de A e é único.

1.2.2 Princípio da Boa Ordem

Todo conjunto não vazio A de inteiros não negativos possui o elemento mínimo. Em outros termos, todo subconjunto não vazio A do conjunto.

$\mathbb{Z}_+ = \{0, 1, 2, 3...\}$.

dos inteiros não negativos ($\emptyset \neq A \subset \mathbb{Z}_+$) possui o elemento mínimo, isto é, simbolicamente:

$(\forall A \subset \mathbb{Z}_+, A \neq \emptyset) \Rightarrow \exists \min A$.

1.3 Princípio da indução finita

Teorema 1.5. *Seja $R \subset \mathbb{Z}_+$ que satisfaz as duas seguintes condições:*

(1) $1 \in R$.
(2) $\forall n \in \mathbb{Z}_+$, *se* $n \in R \Rightarrow n + 1 \in R$.
Nessas condições, R é o conjunto $\mathbb{Z}$.

Demonstração:

Vamos supor, por absurdo, que R não é o conjunto $\mathbb{Z}_+$ e seja X o conjunto de todos os inteiros positivos que não pertencem a R isto é:

$$X = \{x/x \in \mathbb{Z}_+ \text{ e } x \notin R\} = \mathbb{Z}_+ \setminus R.$$

Então, X é um subconjunto não vazio de $\mathbb{Z}_+$ ($\emptyset \neq X \subset N$) e pelo"princípio da boa ordenação", existe o elemento mínimo x_0 de X ($\min X = x_0$).
Pela condição (1),$1 \in R$, de modo que $x_0 > 1$ e, portanto, $x_0 - 1$ é inteiro positivo que não pertence a X. Logo, $x_0 - 1 \in R$ e pela condição (2), segue-se que $(x_0 - 1+)1 = x_0 \in R$, o que é uma contradição, pois, $x_0 \in X = \mathbb{Z}_+ \setminus R$.

1.4 Divisibilidade em $\mathbb{Z}$

1.4.1 Definição e Propriedades

Definição 1.6. *Dados dois inteiros d e a, dizemos que d divide a e que a é um múltiplo de d e escrevemos $d \mid a$. se existe $q \in \mathbb{Z}$ com $a = qd$. Caso contrário, escrevemos $d \nmid a$.*

Por exemplo, temos que $-5 \mid 10$, mas $10 \nmid -5$

A seguir iremos introduzir algumas propriedades importantes da divisibilidade.

Lema 1.7. *Sejam*

$$a, b, c, d \in \mathbb{Z}$$

. Temos:

1. *Se $d \mid a$ e $d \mid b$, então $d \mid (ax + by)$ $\forall x, y \in \mathbb{Z}$.*
2. *Se $d \mid a$, então $a = 0$ ou $|d| \leq |a|$.*
3. *(Transitividade) Se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração:

1.

Se $d \mid a$, então existe $q_1 \in \mathbb{Z}$, tal que

$(1)\ a = dq_1$,

Se $d \mid b$, então existe $q_2 \in \mathbb{Z}$, tal que

$(2)\ b = dq_2$,

Sejam, x, y $\in \mathbb{Z}$, multiplicando a equação (1) por "x"e a equação (2) por "y", respectivamente, teremos.

$(3)\ ax = dq_1x$; e $(4)\ by = dq_2y$,

Em seguida, somando-se (3) e (4), teremos:

$ax + by = dq_1x + dq_2y$, colocando "d" em evidência, temos que $ax + by = d\ (q_1x + q_2y)$.

Como $q_1x + q_2y \in \mathbb{Z}$. Portanto, $d \mid ax + by$, como queríamos demonstrar.

Para demonstrar o 2, Vamos supor que $d \mid a$ e $a \neq 0$

$d \mid a$, então $\exists$ q $\in \mathbb{Z}$, tal que $a = dq$ com $q \neq 0$.

assim $\mid q \mid \geq 1$, Portanto, $\mid a \mid = \mid d \mid$ e $\mid q \mid \geq \mid$ d $\mid$, logo, $\mid a \mid \geq \mid d \mid$, como queríamos demonstrar.

Demonstração 3

Se $a \mid b$ e $b \mid c$, então, $\exists\ q_1, q_2 \in \mathbb{Z}$ tais que:

$i)\ b = aq_1$; e $ii)\ c = bq_2$

Substituindo $i)$ em $ii)$, temos que $c = aq_1q_2$, portanto, $a \mid c$, como queríamos demonstrar.

Definição 1.8. *Diz-se que um número $b \in \mathbb{Z}$ divide outro inteiro a, se existe $c \in \mathbb{Z}$, tal que, $a = b.c$.*

Escreve-se $b \mid a$ para simbolizar que "b divide a"e $b \nmid a$, para indicar que "b não divide a".

Se b divide a, dizemos que b é um divisor de a ou que b é um fator de a, ou ainda que a é um múltiplo de b.

1.5 Máximo Divisor Comum

Definição 1.9. *Seja a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Chama-se máximo divisor comum de a e b o inteiro positivo d, o qual satisfaz as seguintes condições:*
(1) $d \mid a$ e $d \mid b$
(2) Se $c \mid a$ e $c \mid b \Rightarrow c \mid d$.

Observação 1.10. *Pela condição (1), d é um divisor comum de a e b e pela condição (2), d é o maior dentre todos os divisores comuns de a e b.*

O máximo divisor comum de a e b indica-se pela notação $mdc(a, b)$

1.5.1 Existência de Máximo Divisor comum

Demonstraremos a seguir que para quaisquer dois inteiros tais que $a^2 + b^2 > 0$, o máximo divisor comum destes inteiros sempre existe.

Teorema 1.11 (Teorema de Bézout)**.** *Sejam a e b inteiros tais que $a^2 + b^2 > 0$, então existe e é único o $mdc(a, b)$, além disso, existem inteiros r e s tais que:*

$$mdc(a, b) = a.r + b.s$$

Isto é, o $mdc(a, b)$ é uma combinação linear inteira de a e b.

Demonstração:

Seja $\mathbb{A}$ o conjunto de todos os inteiros positivos da forma $au + bv$, com $u, v \in \mathbb{Z}$, isto é

$$\mathbb{A} = \{au + bv / au + bv > 0 \; e \; u, v \in \mathbb{Z}\}$$

Este conjunto não é vazio, por exemplo: se $a \neq 0$ então um dos inteiros $a = a.1 + b.0$ e $-a = a.(-1) + b.0$ é positivo e pertence a $\mathbb{A}$. E pelo princípio da boa ordem, existe e é único o elemento mínimo d de $\mathbb{A}$, $min\mathbb{A} = d > 0$. E também existem inteiros r e s tais que $d = ar+bs$.

Agora iremos demonstrar que $d = mdc(a, b)$. Usando o algoritmo da divisão, temos:

$a = dq + r_1$,com $0 \leq r_1 < d$, então $r_1 = a - dq = a - (ar + bs)q = a - aqr - qbs = a(a-qr)+(-qs)$, logo $r_1 = a(1-qr)+b(-qs)$. Portanto, o resto r_1 é uma combinação linear de a e b e como $0 \leq r_1 < d$ e $d > 0$ é o elemento mínimo de $\mathbb{A}$ então $r_1 = 0$ e isto implica que $a = dq$, assim concluímos que $d \mid a$.

Segue o mesmo raciocínio para concluir que $d \mid b$. Logo, d é um divisor comum positivo de a e b.

Agora vamos supor que c é um divisor comum positivo qualquer de a e b. Então, $c \mid a$ e $c \mid b$, com $c > 0$. Portanto, $c \mid (ar + bs)$, então $c \mid d$ e como $c \leq d$ concluí-se que d é o maior divisor comum positivo de a e b. Ou seja,

$$mdc(a, b) = d = ar + bs, com \; r, s \in \mathbb{Z},$$

como queríamos demonstrar.

1.6 Algoritmo da Divisão

Lema 1.12. *Para quaisquer inteiros a e b, com $b > 0$, existem inteiros q e r, com $0 \leq r < b$, tais que, $a = b.q + r$.*

Em que q e r chamam-se respectivamente o quociente e o resto na divisão de a por b.

Demonstração:

Seja S o conjunto abaixo:

$$S = \{a - b.x \geq 0 \mid x \in \mathbb{Z}\}.$$

Por construção $S \subset \mathbb{Z}_+$, como $b \geq 1$, tomando $x = -|a|$,

segue que $a - bx = a + b|a| \geq a + |a| \geq 0$.

$\Rightarrow\ a + b|a|\ \in S.$

$\Rightarrow S \neq \emptyset.$

e pelo princípio da boa ordenação,

$\exists\ r = \min S\ \Rightarrow\ r\ \in S\ \Rightarrow\ r = a - bq,$ para algum $\ q \in \mathbb{Z}.$

$\Rightarrow\ a = bq + r$, com $\ q, r \in \mathbb{Z}$ e $\ r \geq 0.$

Resta mostrar que $r < b.$

Suponha que isso seja falso, assim sendo $\ r \geq b,$

segue que $\ 0 \leq\ r - b = (a - bq) - b = a - b(q + 1).$

$\Rightarrow\ r - b\ \in S,$

uma contradição, pois $\ r - b < r = \min S$.

Corolário 1.13. *Se a e b são dois inteiros, com $\ b \neq 0$, existem e são únicos os inteiros q e r que satisfazem as condições:*

$$a = b.q + r \qquad e \qquad 0\ \leq r < |\ b\ |$$

Demonstração:

Nota-se que se $b > 0,$ não há nada para demonstrar, e se $b < 0$ então, $|\ b\ | > 0,$ e ,por conseguinte, existem e são únicos os inteiros q_1 e r tais que:

$$a = |\ b\ |\ q_1 + r \qquad \text{e} \qquad 0 \leq r < |\ b\ |$$

ou seja, por ser $|\ b\ | = -b$:

$$a = b(-q_1) + r \qquad \text{e} \qquad 0 \leq r < |\ b\ |$$

Portanto, existem e são únicos os inteiros $q = -q_1$ e r tais que:

$$a = bq + r \qquad \text{e} \qquad 0 \leq r < |\ b\ |$$

Exemplo 1.14. *Achar o quociente q e o resto r da divisão de $a = -79$ por $b = 11$ que satisfazem as condições do algoritmo da divisão.*

Efetuando a divisão usual dos valores absolutos de a e b, obtemos:

$79 = 11.7 + 2$; implica que

$-79 = 11(-7) - 2$
Mas o termo $r = -2 < 0$ não satisfaz a condição $\ 0 \leq r < 11,$ então se somarmos e subtrairmos 11 de b ao segundo membro da igualdade anterior, teremos:
$-79 = 11(-7) - 11 + 11 - 2$
$\Rightarrow -79 = 11[(-7) + (-1)] + 9$
$\Rightarrow -79 = 11(-8) + 9$
Com o $\leq 9 < 11.$

Logo, o quociente $q = -8$ e o resto $r = 9.$

1.7 Algoritmo de Euclides

Lema 1.15. *Se $a = bq + r$, então o $mdc(a, b) = mdc(b, r)$.*

Demonstração:

Se o $mdc(a, b) = d$, então, $d \mid a$ e $d \mid b$, o que implica $d \mid (a - bq)$ ou $d \mid r$, isto é, d é um divisor comum de b e $r(d \mid b$ e $d \mid r)$.

Por outro lado, se c é um divisor comum qualquer de b e r, então $c \mid (bq + r)$ ou $c \mid a$, isto é, c é um divisor comum de a e b, o que implica $c \mid d$. Assim sendo, o $mdc(b, r) = d$.

Sejam a e b dois inteiros tal que $a^2 + b^2 > 0$ cujo máximo divisor comum se deseja determinar.

É imediato:

$$(1) \text{ Se } a \neq 0, \text{ então o } mdc(a, 0) = |a|.$$

$$(2) \text{ Se } a \neq 0, \text{ então o } mdc(a, a) = |a|.$$

$$(3) \text{ Se } b \mid a, \text{ então o } mdc(a, b) = |b|.$$

Além disso, por ser $mdc(a, b) = mdc(|a|, |b|)$, a determinação do $mdc(a, b)$ reduz-se ao caso em que a e b são inteiros positivos, por exemplo, com $a > b$, tais que b não divide a, isto é, $a > b > 0$ e $b \nmid a$. Nestas condições, a aplicação repetida do $algoritmo$ da divisão dá-nos as igualdades.

$$a = bq_1 + r_1, 0 < r_1 < b$$

$$b = r_1q_2 + r_2, 0 < r_2 < b$$

$$r_1 = r_2q_3 + r_3, 0 < r_3 < b$$

$$r_2 = r_3q_4 + r_4, 0 < r_4 < b$$

....

Como os restos $r_2, r_2, r_2, r_2...$ são todos inteiros positivos tais que $b > r_2 > r_2 > r_2 > r_2...$

e existem apenas b-1 inteiros positivos menores que b, necessariamente se chega a uma divisão cujo resto $r_{n+1} = 0$, isto é, finalmente, teremos:

$$r_{n-2} = r_{n-1}q_n + r_n, 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_nq_{n+1} + r_{n+1}, r_{n+1} = 0$$

O último resto $r_n \neq 0$ que aparece nesta sequência de divisões é o máximo divisor comum procurado de a e b, isto é, o $mdc(a, b) = r_n$, visto que, pelo lema anterior, temos:

$mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = ... = mdc(r_{n-2}, r_{n-1}) = mdc(r_{n-1}, r_n) = r_n$.

Este processo prático para cálculo do máximo divisor comum de dois inteiros positivos a e b é denominado de $algoritmo\ de\ EUCLIDES$:

	q_1	q_2	q_3		q_n	q_{n+1}
a	b	r_1	r_2	...	r_{n-1}	r_n
r_1	r_2	r_3	r_4		0	

Que se traduz na seguinte REGRA: Para se achar o mdc de dois inteiros positivos, divide-se o maior pelo menor, este pelo primeiro resto obtido, o segundo resto pelo primeiro, e assim sucessivamente até se encontrar um resto nulo. O último resto não nulo é o máximo divisor comum procurado.

O algoritmo de EUCLIDES também é usado para achar a expressão do $mdc(a, b) = r_n$ como combinação linear de a e b, para o que basta eliminar sucessivamente os restos $r_{n-1}, r_{n-2}, ..., r_3, r_2, r_1$ entre as n primeiras igualdades anteriores.

Exemplo 1.16. *Achar o* $mdc(963, 657)$ *pelo algoritmo euclidiano.*

Resolução:

$963 = 657.1 + 306$

$657 = 306.2 + 45$

$306 = 45.6 + 36$

$45 = 36.1 + 9$

$36 = 9.4 + 0$

	1	2	6	1	4
963	657	306	45	36	9
306	45	36	9	0	

Portanto, o $mdc(963, 657) = 9$*. Que é o último resto não nulo da sequência de divisões.*

Exemplo 1.17. *Achar o* $mdc(252, -180)$ *pelo algoritmo euclidiano.*

Resolução:

$252 = 180.1 + 72$

$180 = 72.2 + 36$

$72 = 36.2 + 0$

Portanto, o $mdc(252, -180) = mdc(252, 180) = 36$*, que é o último resto não nulo da sequência de divisões.*

Exemplo 1.18. *Achar o* $mdc(1769, 2378)$ *pelo algoritmo euclidiano.*

$2378 = 1769.1 + 609$

$1769 = 609.2 + 551$

$609 = 551.1 + 58$

$551 = 58.9 + 29$

$58 = 29.2 + 0$

Portanto, o $mdc(1769, 2378) = 29$*, que é o último resto não nulo da sequência de divisões.*

1.8 Inteiros Relativamente Primos

Definição 1.19. *Dois inteiros a e b dizem-se relativamente primos (ou primos entre si) se* $mdc(a, b) = 1$

Teorema 1.20 (De Euclides)**.** *Sejam a, b e c inteiros, tais que $a \mid bc$. Se a e b são relativamente primos, então $a \mid c$.*

Demonstração:

Como a e b são relativamente primos, então existem $r, s \in \mathbb{Z}$, tais que $ar + bs = 1$. E se a e b são relativamente primos, então $mdc(a, b) = 1$ e $a \mid bc$, , logo existem x, y e $z \in \mathbb{Z}$, tais que;
$ax + by = 1$ e $bc = az$, Portanto,
$a(xc) + (bc)y = c \Rightarrow a(xc) + a(zy) = c \Rightarrow a(xc + zy) = c \Rightarrow a \mid c$. Como queríamos demonstrar.

Capítulo 2

TEOREMA FUNDAMENTAL DA ARITMÉTICA E NÚMEROS PRIMOS

O teorema fundamental da aritmética e o conjuntos dos números primos são primordiais quando se trata de criptografia RSA, pois, por meio do domínio de seus conhecimentos, nos será possível ter o suporte necessário para adentrarmos ao mundo da criptografia RSA. A base da criptografia RSA é considerada forte, justamente por ser feita através do uso de números primos. Portanto, saber sobre suas propriedades torna-se imprescindível. Nesse sentido, iremos trabalhar diversos teoremas abordados em (MARTINEZ et al., 2010) e (FILHO, 1981) como também propriedades que irão compor as etapas da criptografia.

2.1 Números Primos

Definição 2.1. *Um número p, pertencente ao conjunto dos números inteiros, diz-se primo se ele tem exatamente dois divisores positivos distintos, 1 e p.*

Denotado por $D^+(a)$ o conjunto de divisores positivos de um inteiro a, então $p \in \mathbb{Z}$ é primo se $D_+(p) = \{1, p\}$ é um conjunto com exatamente dois elementos distintos, 1 e p.

*Um inteiro $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ que não é primo, diz-se **composto**.*

Exemplo 2.2. *-7 é um número primo, pois $D^+(-7) = \{1, 7\}$.*

Exemplo 2.3. *11 é um número primo, pois $D^+(11) = \{1, 11\}$.*

Exemplo 2.4. *1 é não um número primo, pois $D^+(1) = \{1\}$.*

Exemplo 2.5. *4 é um número composto, pois $D^+(4) = \{1, 2, 4\}$.*

Teorema 2.6. *Se um primo p não divide um inteiro a, então a e p são primos entre si.*

Demonstração: Vamos demonstrar que
Se p é primo e $p \nmid a$, então $mdc(p, a) = 1$.

Considerando (d) o mdc de a e p teremos que.

$d \mid a$ e $d \mid p$.

Como $d \mid p$, então temos duas opções: $d = 1$ ou $d = p$

notamos que a segunda igualdade não é verdadeira, pois $p \nmid a$, conclui-se que $d = 1$.

Portanto, a e p são primos entre si. Como queríamos mostrar.

2.1.1 Propriedades dos Números Primos

Proposição 2.7. *Sejam a e p números inteiros. Se p é primo e $p \mid a$, então $mdc(p, a) = 1$*

Demonstração: Suponha $d = mdc(p, a) \Rightarrow d \mid p$.

Como $d > 0$ e p é primo, segue que $d = 1$ ou $d = p$.

E como $d \mid a$ e $p \nmid a \Rightarrow d \neq p$. Portanto, $d = 1$.

Proposição 2.8. *Sejam a, b e p números inteiros. Se p é primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração: Se $p \mid a$ então pelo **teorema 2.3**, verificamos que $p \mid b$.

Corolário 2.9. *Sejam $a_1.a_2.....a_n$ e p números inteiros, com $n \geq 2$. Se p é um número primo e $p \mid (a_1a_2....a_n)$, então $p \mid a_k$, para algum k, com $1 \leq k \leq n$.*

Demonstração:

Faremos a demonstração por indução em n.

(i)Base de Indução: $n = 2$

Já demonstrado na proposição 2.2

(ii)Passo Indutivo: Seja $n > 3$ um inteiro e considerando o resultado verdadeiro para $n - 1$ fatores. Vamos supor que $p \mid (a_1a_2....a_{n-1}a_n)$, isto é, $p \mid ba$. Onde b = $a_1a_2....a_{n-1}a_n$.
Por (i), isto implica que $p \mid b$ ou $p \mid a_n$. Se $p \neq a_n$, então $p \mid b$.
Mas pela hipótese de indução temos que,

se $p \mid b$, então, $p \mid a_i$ para algum $1 \leq i \leq n - 1$.
Juntando temos que $p \mid a_i$, para algum $1 \leq i \leq n$. Como queríamos mostrar

Teorema 2.10. *Seja $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Então p é primo, se e somente se, sempre que p divide um produto de dois inteiros, p divide ao menos um dos dois fatores.*

Demonstração: ($\Rightarrow$)
p é primo $\Rightarrow$ (se $p \mid ab$, $p \mid a$ ou $p \mid b$)
Já mostrado na proposição 2.2

($\Leftarrow$)
$p \in \mathbb{Z} \setminus \{-1, 0, 1\}$ é tal que para quaisquer inteiros a, b
Se $p \mid ab$, então $p \mid a$ ou $p \mid b \Rightarrow p$ é primo.
Vamos supor, por absurdo que p tem esta propriedade, mas não é um número primo. Então p é composto, logo existem inteiros positivos a e b, com $1 < a, b <\mid p \mid$, tais que $\mid p \mid = ab$.
Segue que

$$p \mid ab$$

porém $p \nmid a$ e $p \nmid b$, o que contraria a hipótese.

Teorema 2.11. *Todo número composto possui um divisor primo.*

Demonstração:

Seja a um inteiro composto. Consideramos o conjunto A de todos os divisores positivos de a, exceto os divisores triviais 1 e a, isto, $A = \{x/a \mid 1 < x < a\}$. Pelo princípio da boa ordem existe o elemento mínimo p de A, que iremos demonstrar ser primo. Então, se p fosse composto admitiria pelo menos um divisor d tal que $1 < d < p$, e então d $\mid p$ e $p \mid a$, o que implica que $d \mid a$, isto é, p não seria o elemento mínimo de A. Logo, p é primo.

2.1.2 Teorema fundamental da aritmética

Teorema 2.12. *$\forall n \geq 2 \in \mathbb{Z}$, n pode ser decomposto em um produto de fatores primos, isto é $n = p_1 p_2 p_3 ... p_n$.*

Demonstração: Se n é primo, então está demonstrado.

Se n não é primo, então n é composto, isto é

pelo Teorema 2.11 possui um divisor primo p_1(Abri explicação), desta forma:

(1) $n = p_1 n_1$, com $1 \leq n_1 \leq n$

Se n_1 é primo, teremos que n é um produto de fatores primos.

Se n_1 é composto, teremos que, pelo teorema Teorema 2.6

(2) $n_1 = p_2 n_2$, com $1 \leq n_2 \leq n_1$

Com p_2 primo, então por (1) e (2), teremos que

(3) $n = p_1 p_2 n_2$

Como em (1) e (2), da mesma forma acontece em (3)

Se n_2 é primo então n é um produto de fatores primos.

Caso contrário, para n_2 composto, teremos que

$\exists$ p_3,n_3 tal que, $n_2 = p_3 n_3$, com $1 \leq n_3 \leq n_2 \leq n_1 \leq n$

Portanto, $n = p_1 p_2 p_3 n_3$

Nota-se que temos uma sequência decrescente

$n > n_1 > n_2 > n_3 > ... > 1$

Provando que para quaisquer $n \geq 2$ teremos n decomposto em fatores primos.

Corolário 2.13. *A decomposição de um inteiro positivo $n \geq 2$ como produto de fatores primos é única, a menos da ordem dos fatores.*

Demonstração:

Por absurdo, vamos supor que n admite duas decomposições como produto de fatores primos, assim sendo

(1) $n = p_1 p_2 p_3 ... p_r = q_1 q_2 q_3 ... q_s$; onde os p_i e os q_j são inteiros primos tais que:

(2) $p_1 \leq p_2 \leq p_3 \leq ... \leq p_r \quad q_1 \leq q_2 \leq q_3 \leq ... \leq q_s$

Como $p_1 \mid q_1 ... q_s \Rightarrow \exists k; com\ 1 \leq k \leq S$

E pelo corolário 7.3 $\Rightarrow p_1 = q_k$, com $p_1 \geq q_1$

Portanto, pela propriedade antissimétrica da relação de ordem temos

$p_1 = q_1 \Rightarrow p_2 p_3 ... p_r = q_2 q_3 ... q_s$

Da mesma forma conclui-se que $p_2 = q_2$, então

$p_3 p_4 ... p_r = q_3 q_4 ... q_s$ e assim por diante

Assim sendo, se subsiste a desigualdade $r \leq s$, então se chega necessariamente a igualdade $1 = q_{r+1} q_{r+2} ... q_s$.

Porém é um absurdo, pois cada $q_j \geq 1$. Logo, $r = s$ e temos

$p_1 = q_1; p_2 = q_2, ..., p_r = q_s$

Isto é, as duas decomposições do inteiro positivo $n > 1$ como produto de fatores primos são idênticas, ou seja, n admite uma única decomposição como produto de fatores primos.

Lema 2.14. *Todo inteiro $a > 1$ tem divisor primo.*

Demonstração:

Vamos demonstrar pela segunda forma do princípio da indução finita.
(i) Base de Indução: $a = 2$, é verdadeiro, pois 2 é primo e $2 \mid 2$.
(ii) Passo indutivo: Seja $a \geq 2$ um inteiro e considere o resultado válido para todo inteiro k, com $1 < k < a$.
Se a é primo o resultado e imediato e se a é composto, então existem d, q, com $1 < d, q < a$, tais que $a = dq$. Como $1 < d < a$, segue da hipótese de indução que d tem um divisor primo p, e como $p \mid d \quad$ e $\quad p \mid a \Rightarrow p \mid a$.

Capítulo 3

CONGRUÊNCIAS

3.1 Inteiros Congruentes

Definição 3.1 (Congruência módulo m). *Dado um inteiro positivo m, dizemos que os inteiros a e b são congruentes módulo m, se eles deixam o mesmo resto na divisão euclidiana por m, ou seja, $m \mid (a-b)$.*

Para indicar que a e b são congruentes módulo m escrevemos:

$$a \equiv b(\text{mod } m)$$

E se $m \nmid (a-b)$ a negação da relação acima, é representada por:

$$a \not\equiv b(\text{mod } m)$$

(i) Observamos que para qualquer número inteiro o resto da divisão deste por 1 é sempre zero. Logo, para quaisquer inteiros a e b, tem-se:

$$a \equiv b(\text{mod } 1)$$

(ii) Se a $\not\equiv b(\text{mod } m)$, então ambos deixam o mesmo resto na divisão por **m**, isto é existem inteiros q_1, q_2 e r, com $0 \leq r <|\text{ m}|$, tais que:

$$a = mq_1 + r \text{ e } b = mq_2 + r$$

Segue que,

$$a = (-m)(-q_1) + r \text{ e } b = (-m)(-q_2) + r$$

Nota-se que **a** e **b** também deixam o mesmo resto na divisão por **-m**, então também temos $a \equiv b(\text{mod } (-m))$.

Conclui-se que:

$$a \equiv b(mod\text{ p}) \Leftrightarrow a \equiv b(\text{mod } (-m)).$$

Como visto em (i) e (ii) vamos seguir as demostrações restringindo ao caso inteiro $m > 1$

Proposição 3.2. *Seja $m > 1$ um inteiro. para quaisquer inteiros a, b tem-se que*

$$a \equiv b(\textit{mod } m) \Leftrightarrow m \mid (a-b).$$

Demonstração:

($\Rightarrow$)

$a \equiv b(\text{mod } m) \Leftrightarrow m \mid (a-b)$.

Se $a \equiv b(\text{mod } m)$, então $\exists q_1, q_2 \in \mathbb{Z}$, com $0 \leq r < m$, tais que

$a = mq_1 + r$ e $b = mq + r$. Subtraindo as equações teremos $\Rightarrow a - b = m(q_1 - q_2)$
$\Rightarrow m \mid (a-b)$

($\Leftarrow$)

$m \mid (a-b) \Rightarrow a \equiv b(\text{mod } m)$.

$m \mid (a-b)$ $\exists k \in \mathbb{Z}$. Como $a - b = mk$, então $a = b + mk$.

Seja r o resto da divisão de a por m, então $a = mq + r$, com $q \in \mathbb{Z}$. Assim.

$$a = b + mk = mq + r \Rightarrow b = m(q-k) + r$$

Como $0 \leq r < m$, da unicidade do resto tem-se que r é também o resto da divisão de b por m. Logo, $a \equiv b(\text{mod } m)$.

3.1.1 Propriedades da Congruência

Proposição 3.3. *Se a e b são inteiros, temos que $a \equiv b(mod\ m)$ se, e somente se, existe um inteiro k tal que $a = b + km$.*

Demonstração:

Se $a \equiv b(\text{mod } m)$, então.

Existe um número k tal que, $a - b = km$. Somando b de ambos lados da igualdade teremos a equação a seguir.

$$a = b + km.$$

A recíproca é trivial, veja que a existência de um k satisfazendo $a = b + km$, temos
$km = a - b$, ou seja, que $m \mid (a-b)$ isto é, $a \equiv b(\text{mod } m)$.

Definição 3.4. *Seja $m > 1 \in \mathbb{Z}$, a relação de congruência módulo m, definida em $\mathbb{Z}$ abaixo:*

$$a \equiv b(mod\ m) \Leftrightarrow m \mid (a-b).$$

têm as seguintes propriedades, sejam quaisquer $a, b, c \in \mathbb{Z}$.

(P1) Reflexiva: $a \equiv a(\text{mod } m)$.

Demonstração:

Como $m \mid 0$, então $\forall a \in \mathbb{Z}$. temos que $m \mid (a-a) \Rightarrow a \equiv a(\text{mod } m)$. ✓

(P2) Simétrica: Se $a \equiv b(\text{mod } m) \Rightarrow b \equiv a(\text{mod } m)$.

Demonstração:

$a \equiv b(\text{mod } m)$

$\Rightarrow m \mid (b-a)$

$\Rightarrow b \equiv a(\text{mod } m)$. Como queríamos demonstrar.✓

(P3) Transitiva: Se $a \equiv b(\text{mod}m)$ e $b \equiv c(\text{mod } m)$, então $a \equiv c(\text{mod } m)$.

Demonstração:

$a \equiv b(\text{mod } m)$ e $b \equiv c(\text{mod } m)$

$\Rightarrow\ m \mid (a-b)$ e $m \mid (b-c)$

$\Rightarrow\ m \mid [(a-b)+(b-c)]$

$\Rightarrow\ m \mid a-c$. Como queríamos demonstrar.✓

Portanto, $a \equiv c(\text{mod } m)$. É uma relação de equivalência.

(P4) Se $a \equiv b(\text{mod}m) \Rightarrow a+c \equiv b+c(modm) \Rightarrow ac \equiv bc(modm).\forall c \in \mathbb{Z}$.

Demonstração:

$a \equiv b(\text{mod } m)\ \Rightarrow\ m \mid (a-b)$. Das propriedades de divisibilidade, temos que:

(i) $m \mid [(a-b)+(c-c)]$

$\Rightarrow\ m \mid [(a+c)-(b+c)]$

$\Rightarrow\ a+c \equiv b+c(\text{mod } m)$.

(ii) $m \mid (a-b)c$

$\Rightarrow m \mid (ac-bc)$

$\Rightarrow ac \equiv bc(modm).$✓

(P5) Cancelamento da adição:

Se $a+c \equiv b+c(\text{mod } m)$, então $a \equiv b(\text{mod } m)$

Demonstração:

$a+c \equiv b+c(\text{mod } m)$

$\Rightarrow\ m \mid [(a+c)-(b+c)]$

$\Rightarrow\ m \mid (a-b)$

$\Rightarrow\ a \equiv b(\text{mod } m).$✓

(P6) Cancelamento da multiplicação:

Se $ac \equiv bc(\text{mod } m)$ e $mdc(c,m)=1$, então $\equiv b(\text{mod } m)$.

Demonstração:

$ac \equiv bc(\text{mod } m)$

$\Rightarrow\ m \mid ac-bc$

$\Rightarrow\ m \mid (a-b)c$

$\Rightarrow\ m \mid (a-b), pois\ mdc(m,c)=1.$✓

(P7) Se $a \equiv b(\text{mod } m)$ e $c \equiv d(\text{mod } m)$, então $a+c \equiv b+d(modm)$, e $ac \equiv bd(modm)$

Demonstração:

Se $a \equiv b(\text{mod } m)$ e $c \equiv \Rightarrow m \mid (a-b)$ e $m \mid (c-d)$.

Segue das propriedades de divisibilidade que:
(i) $m \mid [(a-b)+(c-d)]$

$\Rightarrow m \mid [(a+c)-(b+d)]$

$\Rightarrow\ a+c \equiv b+d(\text{mod } m)$;

(ii) $m \mid sc-bc$ e $m \mid bc-bd$

$\Rightarrow \mid [(ac-bc)+(bc-bd)]$

$\Rightarrow\ m \mid (ac-bd)$

$\Rightarrow\ ac \equiv bd(\text{mod } m)$. ✓

(P8) Se $a \equiv b(\text{mod } m)\ \Rightarrow\ a^n \equiv b^n(\text{mod } m), \forall n \in \mathbb{Z}^*$

Demonstração: Por indução temos que:

Por hipótese tem-se (i) $n = 1$:

(ii) Seja $n \geq 1$ e suponha que $a^n \equiv b^n(\text{mod } m)$:

Por (P7), segue que $a^n.a \equiv b^n.b(\text{mod } m) \equiv a^{n+1} \equiv b^{n+1}(\text{mod } m)$, como queríamos demonstrar.

Teorema 3.5. *Sejam a, b e m inteiros tais que $m > 0$ e $(a, m) = d$. No caso em que $d \nmid b$ a congruência $ax \equiv b(mod\ m)$ não possui nenhuma solução e quando $d \mid b$, possui exatamente d soluções incongruentes módulo m.*

Demonstração: x só é solução de $ax \equiv b(\text{mod } m) \Leftrightarrow \exists y$, tal que, $ax = b + my$; ou ainda $ax = my = b$, pelo teorema anterior sabemos que está equação não possui nenhuma solução caso $d \nmid b$ e que se $d \mid b$ ela possui infinitas solução dadas por $x = x_0 - (\frac{m}{d})k$ e $y = y_0 - (d\frac{a}{d})k$

Definição 3.6. *Dizemos que a solução x_0 de $ax \equiv b(mod\ m)$ é única módulo m quando qualquer outra solução x_1 for congruenteax_0 módulo m.*

Definição 3.7. *Uma solução$= a$ de $ax \equiv 1(mod\ m)$ é chamada de inverso de a módulo m.*

Proposição 3.8. *Seja p um número primo. O inteiro positivo a é seu próprio inverso módulo p se, e somente se, $a \equiv 1(mod\ p)$ ou $a \equiv -1(mod\ p)$.*

Demonstração: ($\Rightarrow$)

Se a é seu próprio inverso, segue que:

$a^2 \equiv 1(\text{mod } p)$, portanto,

$\Rightarrow\ p \mid (a^2-1) \Rightarrow\ p \mid (a-1)(a+1)$, e como p é primo.

$\Rightarrow\ p \mid (a-1)\ \ ou\ \ p \mid (a+1)$

o implica que a $\equiv 1(\text{mod } p)$ ou $a \equiv -1(\text{mod } p)$✓

($\Leftarrow$)

Se $a \equiv 1(\text{mod } p)$ ou $a \equiv -1(\text{mod } p)$

$\Rightarrow\ p \mid (a-1)$ ou $p \mid (a+1)$.

Portanto, $p \mid (a-1)(a+1)$.

$\Rightarrow\ a^2 \equiv 1(\text{mod } p)$.✓

3.2 Teorema de Fermat, Euler e Wilson

3.2.1 Teorema de Fermat

Lema 3.9. *Dados inteiros a e p, com p primo, considere os conjuntos;*

$S = a, 2a, 3a, ...(p-1)a$ *o conjunto dos primeiros* $(p-1)$ *múltiplos positivos de* a *e* $R = \{r_1, r_2, ...r_t\}$ *o conjunto dos restos da divisão de cada um dos elementos de* S *por* p*.*

Se $p \nmid a \Rightarrow$

(i) Quaisquer dois elementos distintos de S são incongruentes módulo p;

(ii) nenhum elemento de S deixa resto na divisão por p.

Demonstração:

(i) Quaisquer dos elementos distintos $m, n \in \{1, 2, ...p-1\}$ tais que$ma \equiv na(\text{mod } p)$, uma vez que p é primo e $p \nmid a$, segue de **Proposição 5** que o $mdc(a, p) = 1$. Assim, pelo cancelamento da **multiplicação(P6)**, tem-se que $m \equiv n(\text{mod } p)$.

Portanto, para quaisquer $m, n \in \{1, 2, ..., p-1\}$ distintos.

$$ma \not\equiv na(\text{mod } p)$$

(ii) Nenhum elemento de S deixa resto zero na divisão por p:

De fato, suponha existir ma $\in S$.

com $ma \equiv 0(\text{mod } p) \Rightarrow p \mid ma$

$\Rightarrow p \mid m$,

um absurdo, pois $m < p$.

Assim sendo, cada um dos inteiros $a, 2a, 3a, ...(p-1)a$ é congruente $(modp)$ a um único inteiro $1, 2, ...p-1$, considerando numa certa ordem, e por conseguinte multiplicado ordenadamente todas essas $p-1$ congruências, teremos:

$a, 2a, 3a, ...(p-1)a \equiv 1, 2, ...p-1(mod\, p)$, ajeitando esta congruência teremos $a^{p-1}(p-1)! \equiv (p-1)!(mod\, p)$. Cancelando o fator comum teremos como resultado a congruência o teorema de FERMAT

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

3.2.2 Teorema de Wilson

Teorema 3.10. *Seja $n > 1$. então $n \mid (n-1)! + 1$ se, e só se, n é primo. Mais precisamente,*

$(n-1)! \equiv -1(modn)$*, se n é primo*

0 $(mod\, n)$ se n é composto e $n \neq 4$.

Demonstração: Se n é composto, mas não é quadrado de um primo podemos escrever $n = ab$ com $1 < a < b < n$.

Neste caso, tanto a quanto b são fatores de $(n-1)!$ e, portanto

$(n-1)! \equiv 0(\text{mod } n)$.

Se $n = p^2, p > 2$, entãop e $2p$ são fatores de $(n-1)!$
e novamente $(n-1)! \equiv 0(\text{mod } n)$;

isto demonstra que $\forall n \neq 4$ composto temos:

$(n-1)! \equiv 0(\text{mod } n)$.
Se n é primo podemos escrever $(n-1)! \equiv -2.3.....(n-2)(\text{mod } m)$;
Mas pelo lema anterior podemos juntar os inversos aos pares no produto do lado direito, onde $(n=1)! \equiv -1(\text{mod } n)$. Como queríamos mostrar.

3.3 Função de Euler

Definição 3.11. *Chama-se função de Euler a função aritmética $\phi(fi)$ assim definida para todo inteiro positivo n:*

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

Em outros termos: $\phi(n) =$ composição do conjunto $\{x \in \mathbb{N}/1 \leq x \leq n$ e $mdc(x,n) = 1\}$.

Exemplo 3.12. *Se $n + 12$, então o conjunto $\{x \in \mathbb{N}/1 \leq x \leq 12$ e $mdc(x,12)\} = \{1,5,7,11\}$*

tem 4 elementos, de modo que $\phi(12) = 4$.

Exemplo 3.13. *Calcular $d(\phi(15))$ e $\phi(d(15))$ Temos $d(\phi(15)) = d(8) = 4$*

$\phi(d(15)) = \phi(4) = 2$

A tabela abaixo apresenta os valores de $\phi(n)$ para os dez primeiros inteiros positivos:

n	1	2	3	4	5	6	7	8	9	10
$\phi(n)$	1	1	2	2	4	2	6	4	6	4

Teorema 3.14. *A função $\phi(n)$ de EULER é uma função aritmética multiplicativa.*

Demonstração: Sejam r e s dois inteiros positivos tais que o $mdc(r,s) = 1$. Iremos demonstrar que

$$\phi(rs) = \phi(r)\phi(s)$$

.

A proposição é verdadeira se r ou s é igual a 1, pois, teríamos:

$$(1.s) = \phi(s) = 1.\phi(s) = \phi(1)\phi(s)$$

.

$$(r.1) = \phi(r) = \phi(r).1 = \phi(r)\phi(1)\phi(s)$$

.

Suponhamos, pois, $r > 1$ e $s > 1$. Neste caso os inteiros de 1 a rs podem ser dispostos em r colunas com s inteiros em cada uma delas, do seguinte modo:

$$\begin{array}{cccc} 1 & 2... & \text{h} ... & \text{r} \\ r+1 & r+2 & r+h & 2r \\ 2r+1 & 2r+2 & 2r+h & 3r \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ (s-1)r+1 & (s-1)r+2 & (s-1)r+h & sr \end{array}$$

Por ser o $mdc(qr+h, r) = mdc(h, r)$, os inteiros da h-ésima coluna são primos com r se e somente se h é primo com r. E como a primeira linha o número de inteiros primos com r é igual a $\phi(r)$, segue que existem somente $\phi(r)$ formadas com inteiros que são todos primos com r. Por outro lado, em cada uma destas $\phi(r)$ colunas existem precisamente $\phi(s)$ inteiros primos com s, porque na progressão aritmética:

$$h, r+h, 2r+h, ..., (s-1)r+h$$

onde o $mdc(h, r) = 1$, número de termos que são primos com s é igual a $\phi(s)$, assim sendo, o número total de inteiros primos com r e com s, isto é, primos com rs é igual a $\phi(r)\phi(s)$, e isto significa que $\phi(rs) = \phi(r)\phi(s)$.

3.3.1 Cálculo de $\phi(n)$

Teorema 3.15. *Se o inteiro $n > 1$, então $\phi(n) = n - 1$, se e somente se n é primo.*

Demonstração: Se $n > 1$ é primo, então cada um dos inteiros positivos menores que n é primo com n e, portanto,

$$\phi(n) = n - 1$$

.

Reciprocamente, se $\phi(n) = n - 1$, com $n > 1$, então n é primo, se n fosse composto, teria pelo menos um divisor d tal que $1 < d < n$, de modo que pelo menos dois dos inteiros $1, 2, 3, ..., n$ não seriam primos com n, den. Isto é, $\phi(n) \leq n - 2$. Logo, n é primo.

Teorema 3.16. *Se p é primo e se k é um inteiro positivo então:*

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

Demonstração: O $mdc(n, p^k) = 1$, se e somente se p não divide $n (p \nmid n)$, e como existem p^{k-1} inteiros entre 1 e p^k que são divisíveis por p, os inteiros:

$$p, 2p, 3, p, ..., (p^{k-1})p$$

Segue que o conjunto $\{1, 2, ..., p^k\}$ contém exatamente $p^k - p^{k-1}$ inteiros primos com p^k, de modo que, pela definição da função ϕ de EULER, temos:

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

. Assim, p.ex:

$$\phi(16) = \phi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$$

isto é, existem 8 inteiros menores que 16 e primos com 16, que são os inteiros $1, 3, 5, 5, 7, 9, 11, 13$ e 15.

Teorema 3.17. *Se* $n = p_1^{k_1}p_2^{k_1}...p_r^{k_r}$ *é a decomposição canônica do inteiro positivo* $n > 1$*, então:*

$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})...(p_r^{k_r} - p_r^{k_r-1}) = n(1 - 1/p_1)(1 - 1/p_2)...(1 - 1/p_r)$.

Ou seja, $\phi(n) = (p_i^{k_i}) - p_i^{k_i-1}) = n(1 - 1/p_i)$

Demonstração: Usaremos o "Teorema da Indução Matemática"sobre r, número de fatores distintos de n.

A proposição é verdadeira para $r = 1$. Suponhamos, então, que a proposição é verdadeira para $r = i$. Como o $mdc(p_1^{k_1}p_2^{k_2}...p_i^{k_i}p_{i+1}^{k_{i+1}})$ e $\phi(n)$ é uma função aritmética multiplicativa, temos:

$$\phi[(p_1^{k_1}p_2^{k_2}...p_i^{k_i})p_{i+1}^{k_{i+1}}] = \phi(p_1^{k_1}p_2^{k_2}...p_i^{k_i})\phi(p_{i+1}^{k_{i+1}})$$

Ou seja,

$$\phi[(p_1^{k_1}p_2^{k_2}...p_i^{k_i})p_{i+1}^{k_{i+1}}] = \phi(p_1^{k_1}p_2^{k_2}...p_i^{k_i})(p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1}-1})$$

pela hipótese de indução:

$\phi(p_1^{k_1}p_2^{k_2}...p_i^{k_i}p_{i+1}^{k_{i+1}}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})...(p_i^{k_i} - p_i^{k_i-1})(p_{i+1}^{k_i+1} - p_{i+1}^{k_{i+1}-1})$.

Isto significa que a proposição é verdadeira para $r = i + 1$. Logo, a proposição é verdadeira para todo inteiro positivo r.

Exemplo 3.18. *Calcular* $\phi(7865)$.

Como a decomposição de fatores primos de $7865 = 5.11^2.13$*, então temos:* $\phi(7865) = (5 - 1)(11^2 - 11)(13 - 1) = 4.110.12 = 5280$

Exemplo 3.19. *Calcular* $\phi(1350)$.

Como a decomposição de fatores primos de $1350 = 2.3^3.5^2$*, então temos:* $\phi(1350) = 1350(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 1350.\frac{1}{2}.\frac{2}{3}.\frac{4}{5} = 360$.

Lema 3.20. *Sejam* a *e* $n > 1$ *inteiros tais que o* $mdc(a, n) = 1$*. Se* $a_1, a_2, ..., a_{\phi(n)}$ *são inteiros positivos menores que* n *e que são primos com* n*, então cada um dos inteiros:* $aa_1, aa_2, ..., aa_{\phi(n)}$ *é congruente módulo* n *a um dos inteiros* $a_1, a_2, ..., a_{\phi(n)}$ *(não necessariamente nesta ordem).*

Demonstração:

Dois quaisquer dos inteiros $aa_1, aa_2, ..., aa_{\phi(n)}$ *são incongruentes módulo* n*, se fosse, teríamos:*

$aa_i \equiv aa_j(mod\ n)$*,com* $1 \leq i < j \leq \phi(n)$*, após cancelar o fator comum* a*, teríamos:*

$a_i \equiv a_j(mod\ n)$ *o que é uma contradição.*

Por outro lado, como o $mdc(a_i, n) = 1(i = 1, 2, ..., \phi(n))$ *e o* $mdc(a, n) = 1$.

Segue que o $mdc(aa_i, n) = 1$*. Assim sendo, para cada* aa_i *existe um único inteiro* b_i*, com* $0 \leq b_i < n$*, tal que,* $aa_i \equiv b_i(mod\ n)$*. Além disso, por ser* $mdc(b_i, n) = mdc(aa_i, n) = 1$*, então* b_i *é um dos inteiros* $a_1, a_2, ..., a_{\phi(n)}$*, isto é, os inteiros:*

$aa_1, aa_2, ..., aa_{\phi(n)}$ *e* $a_1, a_2, ..., a_{\phi(n)}$ *são idênticos (módulo n) numa certa ordem, e a proposição fica demonstrada.*

Teorema 3.21. *Se* n *é um inteiro positivo e se o* $mdc(a, n) = 1$*, então:* $a^{\phi(n)} \equiv 1(mod\ p)$.

Demonstração:

Vamos supor por indução que para $n = 1$ a proposição é verdadeira, pois, temos: $a^{\phi(1)} = a \equiv 1(mod\ 1)$ suponhamos, pois, $n > 1$. Sejam $a_1, a_2, ..., a_{\phi(n)}$ os inteiros positivos menores que n e que são primos com n. com o $mdc(a, n) = 1$, então, pelo lema anterior, os inteiros $aa_1, aa_2, ..., a_{\phi(n)}$ são congruentes módulo n, não necessariamente nesta ordem, aos inteiros $a_1, a_2, ..., a_{\phi(n)}$, isto é:

$$aa_1 \equiv a_1^*(mod\ n)$$

$$aa_2 \equiv a_2^*(mod\ n)$$

.....

$$aa_{\phi(n)} \equiv a_{\phi(n)}^*(mod\ n)$$

Onde $a_1^*, a_2^*, ..., a_{\phi(n)}^*$ são os inteiros $a_1, a_2, ..., a_{\phi(n)}$..numa certa ordem.

multiplicando ordenadamente essas $\phi(n)$ congruências, obtemos:

$$(aa_1)(aa_2)...(aa_{\phi(n)}) \equiv a_1^*, a_2^*, ..., a_{\phi(n)}^*(mod\ n)$$

$$\equiv a_1a_2, ..., a_{\phi(n)}(mod\ n)$$

Ou seja:

$a^{\phi(n)}(a_1a_2...a_{\phi(n)} \equiv, a_1a_2...a_{\phi(n)}(mod\ n)$ como o $mdc(a_i, n) = 1 para i = 1, 2, 3, ..., \phi(n)$
então o $mdc(a_1a_2...a_{\phi(n)}, n) = 1$

e, portanto, podemos cancelar o fator comum

$$a_1a_2...a_{\phi(n)}$$

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

Nota-se que, se p é primo, então $\phi(p) = p - 1$, e se o $mdc(a, p) = 1$:

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

Que é o teorema de FERMAT. Assim, o teorema de EULER é uma generalização do teorema de FERMAT.

Exemplo 3.22. *Verificar o teorema de EULER com $n = 9$ e $a = -4$*

O $mdc(-4, 9) = 1$ e $\phi(9) = 6$. Portanto: $(-4)^{\phi(9)} = (-4)^6 = 4096$

e como $9 \mid (4096 - 1)$, segue-se que $4096 \equiv 1(mod\ 9)$, isto é: $(-4)^{\phi(9)}$

Capítulo 4

CRIPTOGRAFIA RSA

O RSA é um método muito avançado e difícil de ser quebrado, mas não impossível, afinal nenhum algoritmo é inquebrável. O diferencial é que utilizando tudo que vimos nos capítulos anteriores, principalmente por meio dos números primos, vemos como a matemática é bem trabalhada, com isso torna-se extremamente dificultoso decodificar o RSA. Desta forma, podemos dizer que números primos, envolvido com muitos caracteres é o segredo para este método ser tão eficiente. Desta maneira, destacamos que a matemática é utilizada para fazer todos os passos de criptografia de dados e todos os métodos serão mostrados no capitulo a seguir.

4.1 Pré-codificação

O primeiro passo para a codificação pelo método RSA é fazer a conversação de letras por números e/ou números por letras, da mensagem dada. Por exemplo, vamos supor que a mensagem original contém somente letras, portanto, a composição da mensagem é constituído por letras, as que formam as palavras, e pelos espaços que existem entre as palavras. Então, utilizando a tabela abaixo, realizamos a converção de letras por números.

A	B	C	D	E	F	G	H	I	J	K	L	M
12	13	14	15	16	17	18	19	20	21	22	23	24
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
25	26	27	28	29	30	31	32	33	34	35	36	37

De acordo com (COUTINHO, 1997), para que possamos evitar ambiguidades na conversão, é preferível que utilizemos um número composto por dois algarismos para corresponder a cada letra. Caso contrário, poderíamos obter alguns equívocos na codificação por não saber qual correspondência seria a mais adequada. Vejamos, se correspondermos a letra A ao número 1 e a letra b ao número 2, e assim sucessivamente, como resultado teríamos duas opções, AB que corresponde a 1 e 2 ou L, que corresponde ao número 12, pela ordem alfabética. Contudo, não teríamos como saber qual seria a escolha correta para compor a mensagem.

Por exemplo a PALAVRA "TCC"é convertida no número.

$$311414$$

4.2 Geração de Chave e Codificação em RSA

Agora vamos determinar os parâmetros do sistema RSA, vamos chamá-los de p e q dois primos distintos, em situações reais, esses números são astronômicos (algo no mínimo da ordem de 10^{100}), o que impossibilita qualquer tentativa de decodificação sem a chave. Após, determinamos o produto desses dois números e o denotamos por n que é nossa chave de codificação. Portanto, $n = pq$.

Para exemplificar usaremos $p = 7$ e $q = 13$, como $n = pq$, então $n = 7.13 \Rightarrow n$=91.

Agora podemos separar em blocos a mensagem. Só precisamos seguir uma condição, cada bloco formado terá que ser menor que nossa chave de codificação, ou seja, cada bloco terá que que ser menor que 91. Desta forma iremos formar os seguintes blocos.

$$3 - 32 - 61 - 41 - 6 - 1 - 6 - 1 - 72 - 6 - 29 - 31 - 16$$

A codificação segue a seguinte regra:

$b^e \equiv a(\text{mod } n)$, onde:

- b é cada bloco formado.
- e é um inteiro positivo inversível modulo $\varphi(n)$
- a é o resto da divisão de b^e por n

Agora iremos codificar cada bloco. Como o inteiro positivo e tem que ser inversível módulo $\varphi(n)$, então eles têm que ser relativamente primos, como foi visto no capitulo 2.6, ou seja, $mdc(e, \varphi(n)) = 1$. Portanto, iremos escolher e, neste exemplo será o número 7, pois ele é o menor número primo que não divide $\varphi(n) = 72$.

Então o bloco 3 da mensagem anterior é codificado como o resto da divisão de 3^7 por 91. Assim denotaremos o número codificado por $C(b)$ sendo

$C(b) =$ Resto da divisão de b^e por n .

Fazendo as contas obtemos que $C(3) = 3$ e $C(32) = 46$, assim por diante. Após a codificação de toda a mensagem vamos obter a seguinte sequencia de blocos.

$$3 - 46 - 61 - 76 - 20 - 1 - 20 - 1 - 58 - 20 - 29 - 73 - 16$$

4.3 Decodificação

O que precisamos para decodificar uma mensagem em RSA são dois números: n e o inverso de e em $\varphi(n)$, que denotaremos por d. Deste modo, seja a um bloco da mensagem codificada, denotaremos por $D(a)$ o resultado após a decodificação desta mensagem. Portanto $D(a)$ define-se como:

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

Neste caso, teremos que encontrar d, como mostrado no Lema 1.12, do Capítulo 1. Sendo assim, aplicaremos o algoritmo euclidiano estendido a e e $\varphi(n)$. Então, dividindo $\varphi(n) = 72$ por 7 fica

7 = 72.0 + 7

$x = (+1) - (+1).(+0) = 1$

$y = (+0) - (+0).(+0) = 0$

72 = 7.10 + 2

$x = (+)0 - (-10).(+10) = -10$

$y = (-1) - (+1).(+10) = 1$

7 = 2.3 + 1

$x = (+1) - (+31).(+3) = 31$

$y = (+0) - (+3).(+3) = -3$

2 = 1 . 2 + 0 (Parar)

$x = (-10) - (-72).(+2) = -72$

$y = (+1) - (+7).(+2) = 7$

Como teremos o par $x = 31$ e $y = -3$, com $mdc(31, -3) = 1$, então $d = 31$.

Como encontramos d, teremos que decodificar cada bloco a basta o resto da divisão de a^{31} por 91. Para o primeiro bloco teremos $3^{31} \equiv C(a) (\text{mod } 91)$

4.4 Aplicações

A seguir vamos exemplificar com detalhes o que foi visto.

Exemplo 4.1. *Será um exemplo numérico prático, simples, para entendimento do conceito.*

*Vamos supor que queremos codificar uma mensagem, seguindo a tabela vista anteriormente. Iremos codificar a mensagem **RSA**.*

O primeiro passo é a pré-codificação onde iremos transformar letras em números.

293012

O segundo passo é codificar a mensagem, mas para isso precisamos de dois números primos p e q para podermos criar a chave pública de codificação n. Para este exemplo teremos $p = 2$ e $q = 17$. Portanto, $n = 2.17 = 34$

Agora podemos separar em blocos, relembrando que cada bloco deve ser menor que $n = 34$. Após separado fica assim.

$$29 - 30 - 12$$

Após a formação podemos codificar. Usando a fórmula mostrada no capítulo anterior. $b^e \equiv a \ mod \ n$.

Neste exemplo vamos escolher $e = 7$. Após isso, codificar cada bloco.

$29^7 \equiv [(29^2)]^3.29 \equiv 25^2.25.(-5) \equiv (-9)^2.(-9).(-5) \equiv 81.45 \equiv 13.11 \equiv 143 \equiv 7$ *mod* 34

$30^7 \equiv [30^2)]^3.30 \equiv [(-4)^2]^3.(-4) \equiv (16)^2.16.(-4) \equiv 256.(-64) \equiv 18.4 \equiv 72 \equiv 4$ *mod* 34

$12^7 \equiv [12^2)]^3.12 \equiv 144^2.144.12 \equiv (8)^2.8.12 \equiv 64.96 \equiv (-4).(-6) \equiv 24$ *mod* 34

Terceira etapa é decodificar a mensagem, para isso temos que verificar quem é d, sendo d o inverso de $7\ mod\varphi(n)$. *sendo*$\varphi(n) = (p-1)(q-1) = (2-1).(17-1) = 16$. *Encontrando* $\varphi(n)$ *podemos encontrar* d. *Sendo* $7d \equiv 1\ mod 16$, *logo* $d = 7$, *pois deixa resto* 1 *na divisão por* 16. *Seguindo a formula,* $a^d \equiv b\ mod\ n$, *para decodificar a mensagem teremos.*

$7^7 \equiv [7^2)]^3.7 \equiv 49^2.49.7 \equiv (15)^2.105 \equiv 225.105 \equiv (-13).3 \equiv -39 \equiv 29$ *mod* 34

$4^7 \equiv [4^2)]^3.4 \equiv 16^2.16.4 \equiv 256.64 \equiv 18.(-4) \equiv -72 \equiv 30$ *mod* 34

$24^7 \equiv [24^2)]^3.24 \equiv [-10^2)]^3.(-10) \equiv 100^2.100.(-10) \equiv (-2)^2(-2).(-10) \equiv 4.20 \equiv 80 \equiv 12$ *mod* 34

Retornando assim a mensagem original, RSA.

Exemplo 4.2. *Suponha que PAM queira mandar uma mensagem para sua amiga RAI, utilizando o método RSA.*

Pam, utilizará a mesma tabela vista anteriormente, porém acrescentando "?" como número 38 *da tabela. Ela quer enviar a mensagem "Acabou o TCC?". Convertendo as letras em números ficará assim*

$$121412132632 - 26 - 31141438$$

em seguida Pam vai separar em blocos, após separados

$$12 - 14 - 12 - 13 - 26 - 32 - 26 - 31 - 14 - 14 - 3 - 8$$

PAM pede a RAI uma chave pública. Então RAI envia sua chave pública (e, n) *que são* $(7, 35)$ *não revelando a chave privada* d. *Seguindo a regra mostrada em 3.0.2,* $b^e \equiv a(mod\ n)$, *em cada bloco, teremos*

$12^7 \equiv a(mod\ 35)$

$12^7 \equiv [(12^2)]^3.12 \equiv 4^3.12 \equiv (-6).12 \equiv -2 \equiv 68 \equiv 33$ *mod* 35

$14^7 \equiv [(14^2)]^3.14 \equiv 196^3.14 \equiv (-14)^2.(-14).14 \equiv 196.(-196) \equiv (-14).14 \equiv -196 \equiv 14$ *mod* 35

$13^7 \equiv [(12^2)]^3.13 \equiv 169^3.13 \equiv (-6)^2.(-6).13 \equiv 1.(-6).13 \equiv -78 \equiv 27$ *mod* 35

$26^7 \equiv [(26^2)]^3.26 \equiv (-9)^3. - 9 \equiv (81)^3. - 9 \equiv (11)^3. - 9 \equiv (11)^2.11.(-9) \equiv 16.11.(-9) \equiv 16(-99) \equiv 16.6 \equiv -9 \equiv 26$ *mod* 35

$32^7 \equiv [(32^2)]^3.32 \equiv [(-3^2)]^3. - 3 \equiv (9)^3. - 3 \equiv 81.9.(-3) \equiv 11.9.(-3) \equiv 11.27 \equiv 11.8 \equiv 18$ *mod* 35

$31^7 \equiv [(31^2)]^3.26 \equiv [(-4)^2]^3.-4 \equiv (16)^2.16.-4 \equiv 256.16.(-4) \equiv 11.16.(-4) \equiv 176.(-4) \equiv 1(-4) \equiv 31$ *mod* 35

$3^7 \equiv [(3^2)]^3.3 \equiv (9)^2.9.3 \equiv (81).9.3 \equiv 11.27 \equiv 11. - (8) \equiv -88 \equiv -18 \equiv 17$ *mod* 35

$8^7 \equiv [(8^2)]^3.8 \equiv (64)^3.8 \equiv (-6)^3.8 \equiv (-6)^2.(-6).8 \equiv 36.(-6).8 \equiv 1.(-6).8 \equiv -48 \equiv 22$ *mod* 35

Após codificado cada bloco ficou assim

$$33 - 14 - 33 - 27 - 26 - 18 - 26 - 31 - 14 - 14 - 17 - 22$$

Então PAM envia a RAI a mensagem codificada. Com a Chave privada (n, d) *neste caso (35,7), RAI vai decodificar a mensagem.*

$33^7 \equiv [(33^2)]^3.33 \equiv [(-2)^2]^3.(-2) \equiv (-4)^3.(-2) \equiv 64.(-2) \equiv (-6).(-2) \equiv 12$ *mod* 35

$14^7 \equiv [(14^2)]^3.14 \equiv 196^3.14 \equiv (-14)^2.(-14).14 \equiv 196.(-196) \equiv (-14).14 \equiv -196 \equiv 14$ *mod* 35

$27^7 \equiv [(27^2)]^3.27 \equiv [(-8)^2]^3.(-8) \equiv (64)^2.64.(-8) \equiv (-6)^2.(-6).(-8) \equiv 36.48 \equiv 1.13 \equiv 13$ *mod* 35

$26^7 \equiv [(26^2)]^3.26 \equiv (-9)^3. - 9 \equiv (81)^3. - 9 \equiv (11)^3. - 9 \equiv (11)^2.11.(-9) \equiv 16.11.(-9) \equiv 16(-99) \equiv 16.6 \equiv -9 \equiv 26$ *mod* 35

$18^7 \equiv [(18^2)]^3.18 \equiv (324)]^3.(-8) \equiv (9)^2.9.18 \equiv 81.9.18 \equiv 11.9.18 \equiv 99.18 \equiv (-6).18 \equiv 108 \equiv -3 \equiv 32$ *mod* 35

$31^7 \equiv [(31^2)]^3.26 \equiv [(-4)^2]^3.-4 \equiv (16)^2.16.-4 \equiv 256.16.(-4) \equiv 11.16.(-4) \equiv 176.(-4) \equiv 1(-4) \equiv 31$ *mod* 35

$17^7 \equiv [(17^2)]^3.17 \equiv (289)]^3.17 \equiv (9)^2.9.17 \equiv 81.9.17 \equiv 11.9.17 \equiv 99.17 \equiv (-6).17 \equiv -102 \equiv 3$ *mod* 35

$22^7 \equiv [(22^2)]^3.22 \equiv [(-13)]^2]^3.(-13) \equiv (169)^3.(-13) \equiv (-6)^2.(-6).(-13) \equiv 36.(-6).(-13) \equiv 1.78 \equiv 8$ *mod* 35

Após decodificar a mensagem RAI consegue retornar a mensagem original. "ACABOU O TCC?

No exemplo vemos que $p = 5$ *e* $q = 7$*, após fatorar* 35*. E para determinar o valor de* d*, é só achar o* $\varphi(35) = (5-1).(7-1) = 24$*. em seguida dividir* $e = 7$ *por* $\varphi(35)$*. pelo teorema estendido é igual a* 7*. Detalhando a seguir.*

7 = 24 .0 + 7

$x = (+1) - (+1).(+0) = 1$

$y = (+0) - (+0).(+0) = 0$

24 = 7.3 + 3

$x = (+0) - (-3).(+3) = -3$

$y = (+1) - (+1).(+3) = 1$

7 = 3.2 + 1

$x = (+1) - (+7).(+2) = 7$

$y = (+0) - (-2).(+2) = -2$

3 = 1 . 3 + 0 *(Parar)*

$x = (-3) - (-24).(+3) = -24$

$y = (+1) - (+7).(+3) = 7$

Vimos que é bem fácil decodificar quando os primos são números pequenos. Porém quando os números são astronômicos isso muda. O caso não é dizer que é impossível quebrar uma chave assim, mas demanda muito tempo, anos e até séculos, o que se torna inviável a tentativa, fazendo com que o RSA seja uma Criptografia segura de ser usada.

Exemplo 4.3. *Agora vamos para um exemplo mais difícil, assim veremos como é praticamente impossível quebrar a chave RSA.*

Escolhendo os Primos $p = 461$ *e* $q = 691$*, teremos que* $n = pq$*, assim sendo* $n = 461.691 = 318.551$*. Então, phi de* n *é*

$\varphi(n) = (p-1).(q-1) = 1 => \varphi(n) = (461-1).(691-1) = 460.690 = 317.400$*. Iremos escolher o* e *este numero deve ser inversível modulo* $\phi(n)$*, ou seja o* $mdc(e, \phi(n)) = 1$*. Portanto, vamos escolher nosso* $e = 7$

Com essas chaves iremos criptografar os seguintes blocos, pois $b^e \equiv a(mod\ n)$*, sendo* b *cada bloco.*

$123116 - 142 - 62931 - 12 - 2926 - 30272 - 92627 - 292026 - 301516 - 17 - 162031 - 26 - 302 - 72 - 61516301629 - 271629 - 201826 - 302625 - 322514 - 123016 - 301 - 213 - 16283 - 21223 - 16261 - 51617 - 162031 - 26 - 28 - 3216 - 30 - 32303 - 116253 - 112252 - 53030 - 26 - 161520 - 172014 - 2026 - 20253 - 11620 - 2926$

Iremos começar com o bloco 1,o número 123116

Seja $b_1^e \equiv C(b_1)(mod\ n)$ *;* $C(b_1) =$ *mensagem criptografada.*

$123116^7 \equiv C(b_1)(mod\ 318551) = 123116^2 * 123116^2 * 123116^2 * 123116 \equiv 255774 * 255774 * 255774 * 123116 \equiv 157308 * 149781 \equiv 124833 \mod 318551$*. então,* $123116^7 \equiv 124833 \mod 318551$*. Portanto,* $C(b_1) = 124833$*.*

O bloco 2, terá o número 142*.*

Seja $b_2^e \equiv C(b_2)(mod\ n)$ *;* $C(b_2) =$ *mensagem criptografada.*

$142^7 \equiv C(b_2)(mod\ 318551) = 142^3 * 142^3 * 142 \equiv 314880 * 314880 * 142 \equiv 314880 * 115820 \equiv 90365$*. então,* $142^7 \equiv 90365 \mod 318551$*. Portanto,* $C(b_2) = 90365$*.*

O bloco 3, terá o número 62931*.*

Seja $b_3^e \equiv C(b_3)(mod\ n)$ *;* $C(b_3) =$ *mensagem criptografada.*

$62931^7 \equiv C(b_3)(mod\ 318551) = 62931^2 * 62931^2 * 62931^2 * 62931 \equiv 84729 * 84729 * 84729 * 62931 \equiv 138105 * 174061 \equiv 198843$*. então,* $62931^7 \equiv 198843 \mod 318551$*. Portanto,* $C(b_3) = 198843$*.*

O bloco 4, terá o número 12*.*

Seja $b_4^e \equiv C(b_4)(mod\ n)$ *;* $C(b_4) =$ *mensagem criptografada.*

$12^7 \equiv C(b_4)(mod\ 318551) = 12^5 * 12^2 \equiv 248832 * 144 \equiv 35831808 \equiv 154096$ *então,* $12^7 \equiv 154096 \mod 318551$*. Portanto,* $C(b_4) = 154096$*.*

O bloco 5, terá o número 2926*.*

Seja $b_5^e \equiv C(b_5)(mod\ n)$ *;* $C(b_5) =$ *mensagem criptografada.*

$2926^7 \equiv C(b_5)(mod\ 318551) = 2926^2 * 2926^2 * 2926^2 * 2926 \equiv 279150 * 279150 * 279150 * 2926 \equiv 139778 * 28136 \equiv 281713$*. então,* $2926^7 \equiv 281713 \mod 318551$*. Portanto,* $C(b_5) = 281713$*.*

O bloco 6, terá o número 30272*.*

Seja $b_6^e \equiv C(b_6)(mod\ n)$ *;* $C(b_6) =$ *mensagem criptografada.*

$30272^7 \equiv C(b_6)(mod\ 318551) = 30272^2 * 30272^2 * 30272^2 * 30272 \equiv 241308 * 241308 * 241308 * 30272 \equiv 20819 * 182795 \equiv 198859$. *então,* $30272^7 \equiv 198859 \mod 318551$. *Portanto,* $C(b_6) = 198859$.

O bloco 7, terá o número 92627.

Seja $b_7^e \equiv C(b_7)(mod\ n)$ *;* $C(b_7) =$ *mensagem criptografada.*

$92627^7 \equiv C(b_7)(mod\ 318551) = 92627^2 * 92627^2 * 92627^2 * 92627 \equiv 227046 * 227046 * 227046 * 92627 \equiv 51990 * 171373 \equiv 129351$. *então,* $92627^7 \equiv 129351 \mod 318551$. *Portanto,* $C(b_7) = 129351$.

O bloco 8, terá o número 292026.

$292026^7 \equiv C(b_8)(mod\ 318551) = 292026^2 * 292026^2 * 292026^2 * 292026 \equiv 215017 * 215017 * 215017 * 292026 \equiv 48006 * 11179 \equiv 219190$. *então,* $292926^7 \equiv 219190 \mod 318551$. *Portanto,* $C(b_8) = 219190$.

O bloco 9, terá o número 301516.

$301516^7 \equiv C(b_9)(mod\ 318551) = 301516^2 * 301516^2 * 301516^2 * 301516 \equiv 309815 * 309815 * 309815 * 301516 \equiv 1184007 * 54443 \equiv 184007$. *então,* $30516^7 \equiv 184007 \mod 318551$. *Portanto,* $C(b_9) = 184007$.

O bloco 10, terá o número 17. $17^7 \equiv C(b_{10})(mod\ 318551) = 17^5 * 17 * 17 \equiv 145653 * 17 * 17 \equiv 245244 * 17 \equiv$. *então,* $30516^7 \equiv 184007 \mod 318551$. *Portanto,* $C(b_{10}) = 184007$.

O bloco 11, terá o número 162031.

$162031^7 \equiv C(b_{11})(mod\ 318551) = 162031^2 * 162031^2 * 162031^2 * 162031 \equiv 27194 * 27194 * 27194 * 162031 \equiv 156765 * 73582 \equiv 31969$. *então,* $162031^7 \equiv 31969 \mod 318551$. *Portanto,* $C(b_{11}) = 31969$.

O bloco 12, terá o número 26.

$26^7 \equiv C(b_{11})(mod\ 318551) = 26^3 * 264 \equiv 138425 * 26 * 26 \equiv 94989 * 26 * 26 \equiv 2469714 \equiv 239857 * 26 \equiv 6236282 \equiv 183813 \mod 318551$. *Então,* $26^7 \equiv 183813 \mod 318551$. *Portanto,* $C(b_{12}) = 183813$.

Fazendo as mesmas operações para os demais blocos teremos

13) $302^7 \equiv C(b_{13})(mod\ 318551) => 26^7 \equiv 78243 mod\ 318551$

14) $72^7 \equiv C(b_{14})(mod\ 318551) => 26^7 \equiv 115640 mod\ 318551$

15) $61516^7 \equiv C(b_{15})(mod\ 318551) => 61516^7 \equiv 78243 mod\ 318551$

16) $301629^7 \equiv C(b_{16})(mod\ 318551) => 301629^7 \equiv 19418 mod\ 318551$

17) $271629^7 \equiv C(b_{17})(mod\ 318551) => 271629^7 \equiv 267985 mod\ 318551$

18) $201826^7 \equiv C(b_{18})(mod\ 318551) => 201826^7 \equiv 193763 mod\ 318551$

19) $302625^7 \equiv C(b_{19})(mod\ 318551) => 302625^7 \equiv 216149 mod\ 318551$

20) $322514^7 \equiv C(b_{20})(mod\ 318551) => 322514^7 \equiv 75354 mod\ 318551$

21) $213016^7 \equiv C(b_{21})(mod\ 318551) => 213016^7 \equiv 39836 mod\ 318551$

22) $301^7 \equiv C(b_{22})(mod\ 318551) => 301^7 \equiv 213862 mod\ 318551$

23) $213^7 \equiv C(b_{23})(mod\ 318551) => 213^7 \equiv 127912 mod\ 318551$

24) $16283^7 \equiv C(b_{24})(mod\ 318551) => 16283^7 \equiv 57010 mod\ 318551$

25) $21223^7 \equiv C(b_{25})(mod\ 318551) => 21223^7 \equiv 227541 mod\ 318551$

26) $16261^7 \equiv C(b_{26})(mod\ 318551) => 16261^7 \equiv 282435 mod\ 318551$

27) $51617^7 \equiv C(b_{27})(mod\ 318551) => 51617^7 \equiv 135667 mod\ 318551$

28) $162031^7 \equiv C(b_{28})(mod\ 318551) => 162031^7 \equiv 731969 mod\ 318551$

29) $26^7 \equiv C(b_{29})(mod\ 318551) => 26^7 \equiv 78243 mod\ 183813$

30) $28^7 \equiv C(b_{28})(mod\ 318551) => 28^7 \equiv 63805 mod\ 318551$

31) $3216^7 \equiv C(b_{31})(mod\ 318551) => 3216^7 \equiv 21427 mod\ 318551$

32) $30^7 \equiv C(b_{32})(mod\ 318551) => 30^7 \equiv 199646 mod\ 318551$

33) $32303^7 \equiv C(b_{33})(mod\ 318551) => 32303^7 \equiv 297607 mod\ 318551$

34) $116253^7 \equiv C(b_{34})(mod\ 318551) => 116253^7 \equiv 31886 mod\ 318551$

35) $112252^7 \equiv C(b_{35})(mod\ 318551) => 112252^7 \equiv 303058 mod\ 318551$

36) $53030^7 \equiv C(b_{36})(mod\ 318551) => 53030^7 \equiv 9087 mod\ 318551$

37) $26^7 \equiv C(b_{37})(mod\ 318551) => 26^7 \equiv 183813 mod\ 318551$

38) $161520^7 \equiv C(b_{38})(mod\ 318551) => 161520^7 \equiv 7387 mod\ 318551$

39) $172014^7 \equiv C(b_{39})(mod\ 318551) => 172014^7 \equiv 257801 mod\ 318551$

40) $2026^7 \equiv C(b_{40})(mod\ 318551) => 2026^7 \equiv 195075 mod\ 318551$

41) $20253^7 \equiv C(b_{41})(mod\ 318551) => 20253^7 \equiv 103304 mod\ 318551$

42) $11620^7 \equiv C(b_{42})(mod\ 318551) => 11620^7 \equiv 146544 mod\ 318551$

43) $2926^7 \equiv C(b_{43})(mod\ 318551) => 29260^7 \equiv 281713 mod\ 318551$

Tendo feito isso, teremos que saber quem é d*. Pois* d *é necessário para decodificação da mensagem, sendo* d *o inverso de* $7\ mod \varphi(318551)$*. sendo* $\varphi(n) = (p-1)(q-1) = (461-1).(691-1) = 317400$*. Encontrando* $\varphi(318551)$ *podemos encontrar* d*. Sendo* $7d \equiv 1\ mod 317400$*, logo* $d = 45343$*, pois deixa resto* 1 *na divisão por* 317400*. Seguindo a fórmula,* $C(b_x)^d \equiv b_x\ mod\ n$*, para decodificar cada bloco de mensagem teremos.*

Decodificando:

$C(b_1) = 124833 => 124833^{45343} \equiv b_1\ mod\ 318551 => b_1 = 123116$*. Retornando a mensagem original.*

$C(b_2) = 90365 => 124833^{45343} \equiv b_2\ mod\ 318551 => b_2 = 142$*. Retornando assim a mensagem original.*

$C(b_3) = 198843 => 124833^{45343} \equiv b_3\ mod\ 318551 => b_3 = 62931$*. Retornando a mensagem original.*

$C(b_4) = 154096 => 124833^{45343} \equiv b_4\ mod\ 318551 => b_4 = 12$*. Retornando a mensagem original.*

Estamos trabalhando com primos de 3 *algoritmos e há calculadoras que não fazem estas operações das divisões de* n *e* $\phi(n)$ *a partir deles. Alguns aplicativos e sites online fazem, porém ao colocar para dividir o site congela e tem que ser reiniciado para posteriormente colocar o próximo bloco, o que dificultou as decodificações. Imagine para mais de* 3 *algoritmos como será o* n*,* e *e* d*?*

Fazendo o mesmo processo nos demais blocos retornaremos a mensagem original de cada um.

Considerações Finais

Este trabalho procurou entender o comportamento dos números inteiros desde seus conceitos básicos até chegar as operações mais profundas, para enfim, implementar o RSA como ferramenta eficaz na segurança de dados.

Tendo como objetivo mostrar as operações matemáticas no conjunto dos números inteiros e que através de definições, teoremas, lemas e corolários serão incrementadas nas etapas do método RSA.

As demonstrações mostradas neste trabalho são cruciais para o entendimento da matemática que está por trás do método e visualmente entender o porquê do RSA ser uma ferramenta eficaz na segurança de dados.

A segurança do RSA é verificada quando estudamos sobre algoritmos de fatoração. Por fim, conseguimos compreender a segurança do método, que está baseada no quanto é trabalhoso fatorar números grandes. Entendendo também que devemos ficar atentos ao escolher quem será p e q, para que o método seja seguro.

Referências Bibliográficas

BURNETT, S. *Criptografia e segurança: o guia oficial RSA*. Rio de Janeiro: Gulf Professional Publishing, 2002.

COUTINHO, S. C. *Números inteiros e criptografia RSA*. Rio de Janeiro: IMPA, 1997.

FILHO, E. A. *Teoria elementar dos números*. São Paulo: Nobel, 1981.

MARTINEZ, F. B. et al. Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro. 2010.