UNIVERSIDADE DO ESTADO AMAZONAS
ESCOLA NORMAL SUPERIOR
LICENCIATURA EM MATEMÁTICA

KAREN STEPHANE NOGUEIRA PACHECO

A FUNÇÃO ϕ DE EULER E APLICAÇÕES NA CRIPTOGRAFIA RSA

MANAUS-AM
Fevereiro/2024

KAREN STEPHANE NOGUEIRA PACHECO

A FUNÇÃO ϕ DE EULER E APLICAÇÕES NA CRIPTOGRAFIA RSA

Trabalho de Conclusão de Curso elaborado junto ‘a disciplina TCC II, do Curso de Licenciatura em Matemática da Universidade do Estado do Amazonas, para a obtenção do grau de licenciatura em Matemática.

Orientador: Dr. Almir Cunha da Graça Neto

Manaus-AM
Fevereiro/2024

Agradecimentos

A Deus, por permitir que este trabalho fosse executado. A meus pais, por toda paciência e apoio. Ao meu orientador Dr. Almir Cunha da Graça Neto, que me apresentou o universo da Teoria dos Números e motivou o desenvolver dessa pesquisa e a professora Me. Helisângela Ramos da Costa, por todos os ensinamentos que me proporcionou.

Resumo

Essa pesquisa aborda a relação entre Teoria dos Números e Criptografia, limitando-se, especificamente, ao estudo da Função ϕ de Euler e sua aplicação na Criptografia RSA. Serão apresentados aspectos históricos e preliminares da Criptografia RSA, algumas definições e teoremas que são necessários para a compreensão da Função de Euler e, por fim, as propriedades, o cálculo da função e alguns exemplos de cálculo seguidos de algumas amostras da aplicação da função na criptografia RSA.

TERMO DE APROVAÇÃO DE TRABALHO DE CONCLUSÃO DO CURSO DE LICENCIATURA EM MATEMÁTICA DA UNIVERSIDADE DO ESTADO DO AMAZONAS

Ata de Defesa do Trabalho de Conclusão de Curso em Licenciatura em Matemática da Escola Normal Superior-UEA de KAREN STEPHANE NOGUEIRA PACHECO.

Em 06 de fevereiro de 2024, às 18h, na Sala Profª Maria Clara Dantas da Escola Normal Superior da UEA na presença da Banca Avaliadora composta pelos professores: Dr. Almir Cunha da Graça Neto, Dr. Edson Lopes de Souza e Dra. Nadime Mustafa Moraes a aluna KAREN STEPHANE NOGUEIRA PACHECO apresentou o Trabalho de Conclusão do Curso intitulado: "A FUNÇÃO DE EULER E APLICAÇÕES NA CRIPTOGRAFIA RSA". A Banca Examinadora deliberou e decidiu pela APROVAÇÃO do referido trabalho, com o conceito 9,76 divulgando o resultado a aluna e demais presentes.

Manaus, 06 de fevereiro de 2024.

Presidente da Banca Avaliadora

Orientador

Avaliador 1

Avaliador 2

Aluna

Sumário

Introdução

Importantes conceitos relativos à Teoria dos Números, propriedades, relações com os números primos, a função de Euler e a operação congruência módulo m, geralmente são desprovidos de praticidade no ensino básico. Mas, os números inteiros prestam um papel importante na criptografia de chave pública RSA devido, entre outros, o fluxo de importantes transações efetuadas por meio eletrônico passíveis de interceptação de terceiros. A criptografia estuda métodos que permitem escrever mensagens em cifras de modo que apenas os legítimos destinatários sejam capazes de decifrar e ler as mensagens. Assim, o problema da pesquisa é: Como a função ϕ de Euler pode ser aplicada na criptografia de mensagens?

Esse trabalho justifica-se a partir do interesse da autora, que além da constante apreciação pela Matemática, teve contato com linguagens de programação durante o ensino médio, o que ocasionou interesse por história da computação e assuntos relacionados. A partir desses dois interesses surgiu o tema escolhido para o trabalho de conclusão de curso, que aborda uma aplicação da Matemática na Criptografia, mais especificamente, a aplicação da função de Euler na criptografia RSA.

A criptografia é essencial para a comunicação entre duas partes que procuram manter o sigilo de informações. Nesse sentido, a Função ϕ de Euler é utilizada para que esse sigilo seja mantido somente entre as partes. A partir do estudo dessa função multiplicativa, a criptografia RSA é desenvolvida e em 1978 passa a ser a criptografia mais segura. Essa pesquisa consistirá em explorar o estudo da função de Euler destacando sua importância principalmente na ciência da computação através da criptografia.

O objetivo geral que esse trabalho apresenta é o de compreender a relação entre a função ϕ e a criptografia RSA. Para que essa finalidade seja alcançada, os objetivos específicos serão divididos em três etapas, sendo a primeira o estudo do cálculo e das propriedades da função de Euler, seguida pela compreensão de como essa função auxilia

na criptografia RSA, e, por último, explorar as aplicações que a função ϕ desempenha na criptografia RSA.

Quanto a abordagem metodológica utilizada, a pesquisa se concentra em demonstrar como o uso da função ϕ é essencial para a criptografia RSA, ou seja, é de natureza quantitativa, que consiste em mostrar determinado fenômeno a partir da linguagem matemática. Ademais, do ponto de vista dos objetivos, como o trabalho visa identificar como a função de Euler contribui para a criptografia em estudo, a pesquisa se classifica como explicativa. Finalmente, do ponto de vista do procedimento técnico, o trabalho preocupa-se em apresentar um estudo específico da aplicação da função ϕ, assim revisando conteúdos de Teoria dos Números e apresentando uma breve introdução ao universo da criptografia, por esse motivo, a pesquisa se classifica como bibliográfica.

A pesquisa está estruturada em 4 capítulos: No capítulo 1, destaca sobre a Revisão da Literatura, na qual aborda-se os aspectos históricos e preliminares bem como uma breve apresentação do matemático Leonhard Euler e alguns nomes importantes da criptografia RSA. O capítulo 2, refere-se a metodologia da pesquisa que particulariza os parâmetros metodológicos tais como: abordagem, estratégia e procedimento para a construção da pesquisa.

No capítulo 3, expõe-se o estudo da Função ϕ, seu cálculo e todas as suas propriedades bem como exemplos e demonstrações.

Por fim, o capítulo 4 apresenta como a Função ϕ auxilia na criptografia RSA e explora as aplicações através de exercícios criados pela autora e exemplos retirados de outros trabalhos de conclusão de curso disponíveis em repositórios de universidades.

Capítulo 1

Revisão de Literatura

1.1 Aspectos Históricos

1.1.1 Leonhard Paul Euler

O matemático suiço Leonhard Paul Euler (1707-1783) foi um dos mais importantes de sua época. Suas contribuições nas diversas áreas da Matemática mostram que ele se destacava pela sua versatilidade. Carvalho (2020) aponta que com seus cerca de 700 trabalhos, Euler talvez tenha sido o matemático mais produtivo de todos os tempos. Entre seus trabalhos, pode-se destacar a famosa identidade de Euler, dada por $e^{i\pi} + 1 = 0$, considerada por muitos como a mais bela identidade matemática por relacionar a Trigonometria à função exponencial. Outra importante contribuição que pode ser destacada, de acordo com Boyer, é o desenvolvimento do conceito de função, que contou com muitos matemáticos importantes como Nicole Oresme (1323-1382), G. W. Leibniz (1646-1716) e P. G. Lejeune Dirichlet (1805-1859), mas foi Euler quem atribuiu pela primeira vez, em 1734, a notação f(x) para indicar função de x.

Segundo Silva e Clemente (apud Hefez, 2016), além dos trabalhos já citados, ele escreveu sobre vários temas como números complexos, cálculo diferencial e integral, música e teoria das partições e mecânica, mas o foco deste trabalho está nas suas contribuições para a Teoria dos Números, mais especificamente na função multiplicativa nomeada por "Função ϕ de Euler" ou "Função totiente", usada por ele para provar o Pequeno Teorema de Fermat. Uma das aplicações dessa função está na criptografia RSA, criada em 1977 por Ronald Rivest, Adi Shamir e Leonard Adleman, que serão melhor apresentados em

tópicos posteriores.

1.1.2 História da Criptografia

De acordo com Castro (2014, p.21), "a criptografia é utilizada há muito tempo na comunicação". Do grego *kryptós* significa escondido, e *gráphein*, escrita, com isso pode-se concluir que criptografia significa uma escrita sigilosa. Durante a Segunda Guerra Mundial a criptografia foi um importante método para que os planos de guerra não fossem descobertos por exércitos inimigos em caso de captura da mensagem, pois dessa forma não poderiam decifrar o que estava escrito sem conhecer os métodos que foram utilizados para criptografar.

Uma mensagem cifrada pode também ser chamada de criptografada. Para Paiva (2004), a criptografia é a ciência que transforma uma mensagem que se encontra numa linguagem escrita para outra também escrita, mas cifrada, com o objetivo de manter um sigilo entre o remetente e o destinatário. Alguns métodos de criptografia, como a Cifra de César e o Quadrado de Polybius, são importantes quando o assunto é história da criptografia, visto que são bases na hora de compreendê-la.

Cifra de César

Castro (2014) aponta que a cifra de César, método esse utilizado pelo imperador Júlio César, 100 a.C a 44 a.C, foi muito eficiente para a comunicação entre ele e seus generais. Esse processo consistia na translação de letras do alfabeto, da seguinte forma: trocavam-se as letras do alfabeto por outras, no caso dessa cifra, transladavam-se as letras três posições à direita. A Tabela 1.1 apresenta as letras do alfabeto e seus correspondentes na criptografia do imperador César, em que o correspondente de cada letra é a que se encontra na segunda linha.

Tabela 1.1: Cifra de César

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

Fonte: Da Autora (2023)

No caso da frase "A matemática é linda", a criptografia seria, sem levar em conside-

ração os acentos e espaçamentos,“DPDWHPDWLFAHOLQGD”, que quando decifrada pelos leitores que conheciam o método, seria “AMATEMATICAELINDA”.

Quadrado de Polybius

Outro importante método foi o do historiador grego Políbio (200a.C a 118 a.C), que consistia na transformação do alfabeto em números. Castro (2014), afirma que essa transformação utilizava uma tabela 5x5, chamada de quadrado de Políbio.

Analisando a Tabela 1.2, pode-se observar que cada letra corresponde a sua posição na matriz, por exemplo a letra T corresponde ao número 44 e a letra V ao 51. Embora essa tabela possua 25 espaços e exista 26 letras, isso é corrigido associando-se duas letras a um mesmo número, nesse caso, I e J estão associados ao número 24. Nesse caso, a palavra “totiente”, seria criptografada da seguinte forma: “4434442415334415”.

Tabela 1.2: Quadrado de Polybius

.	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Fonte: Da Autora (2023)

É importante apontar que esses métodos, embora tenham sido úteis na época que foram utilizados, são fáceis de decifrar, por esse motivo houve a necessidade de novos processos de criptografia, pois com a evolução da humanidade e da informática, as chaves tornaram-se mais acessíveis a “quebras”, causando facilidade na descoberta de dados sigilosos. Dois tipos de chaves foram criadas para solucionar os problemas que por muito tempo estiveram sem solução na criptografia, como a necessidade de compartilhamento prévio da chave. Castro (2014), assegura que Diffie e Hellman (1976), criaram duas chaves distintas: a **chave pública**, que é disponibilizada a todos, e a **chave privada**, que fica em posse do proprietário.

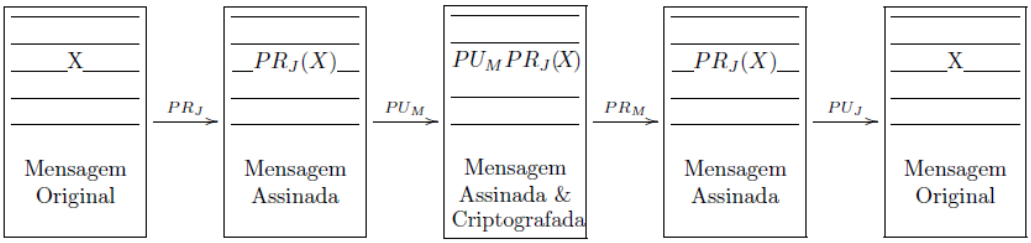
Criptografia Simétrica

Nesse tipo de criptografia, a única preocupação do remetente e destinatário é com a segurança da chave. Os processos abordados anteriormente (Quadrado de Políbio e Cifra de César), são exemplos desse tipo. O problema encontrado na criptografia simétrica está na insegurança do processo, pois qualquer pessoa que tenha acesso a chave, saberá o que é necessário para descriptografa-la.

Criptografia Assimétrica

A fim de resolver o problema da criptografia simétrica, a assimétrica tornou-se abundante em 1976, quando os já citados Diffie e Hellman, diferenciaram as chaves pública e privada. A criptografia assimétrica, também chamada de criptografia de chave pública, utiliza o par de chaves para descriptografar e criptografar as mensagens. O processo ocorre da seguinte maneira: primeiro utiliza-se a chave pública do remetente, que será codificada e enviada ao destinatário, e este consegue decifrar com sua chave privada.

Figura 1.1: Processo de criptografia assimétrica



Fonte: CASTRO (2014)

De acordo com a Figura 1.1, o método funciona da seguinte forma: Júlia e Melinda desejam trocar mensagens, para isto Júlia possui a sua chave privada (PR_J) e sua chave pública (PU_J) e Melinda também possui sua chave privada (PR_M) e pública (PU_M). Júlia deseja enviar uma mensagem "X" para Melinda, então ela assina a mensagem gerando $PR_J(X)$. Após isso ela utiliza a chave pública de Melinda, gerando a mensagem criptografada final $PU_M PR_J(X)$. Melinda ao receber a mensagem utiliza da sua chave privada, $PR_M(X)$, reobtendo a mensagem original a partir da mensagem assinada.

1.1.3 Criptografia RSA

O tema central desse trabalho está na criptografia assimétrica RSA, cujo nome está interligado às iniciais de seus criadores Ronald Rivest, Adi Shamir e Leonard Adleman. Os três estudantes do Massachusetts Institute Technology (MIT), procuravam uma criptografia que satisfizesse as ideias de Diffie e Hellman, elaborando assim um processo para alcançar esse objetivo. Dois deles - Ronald e Adi - preocupavam-se em criar formas de "esconder" a mensagem, enquanto Leonard tentava descobrir a técnica utilizada. Embora Leonard tenha ido bem desvendando os métodos, houve um algoritmo que ele não conseguiu "quebrar", dando início a criptografia RSA. (OKUMURA, 2014)

Esses criptologistas utilizaram a Teoria dos números para elaborar a criptografia RSA, por isso, nos próximos tópicos serão enfatizados conceitos prévios para a compreensão da Função de Euler e de como ela se aplica na criptografia.

1.2 Definições e teoremas preliminares

[1] Para um melhor entendimento da função de Euler e principalmente para a compreensão de sua aplicação na criptografia, são necessárias noções básicas da aritmética dos inteiros, que serão abordadas nas próximas subseções.

1.2.1 Divisibilidade em Z

Definição 1.2.1. *Sejam a e b dois inteiros, com $a \neq 0$. Diz-se que a divide b se e somente se existe um inteiro q tal que $b = aq$.*

Com a notação "$a|b$" indica-se que a $\neq 0$ divide b e, portanto, a notação $\nmid$ significa que a $\neq 0$ não divide b.

Algoritmo da divisão

A Definição 1.2.1 aborda o caso de divisões exatas, ou seja, divisões que não possuem resto. Por isso, o Algoritmo da divisão é apresentado como complemento para que haja uma compreensão completa de Divisibilidade em Z.

[1] As definições, teoremas e demonstrações desta seção estão de acordo com (FILHO, 1981).

Teorema 1.2.1. *Se a e b são dois inteiros, com $b \neq 0$ e $r < |b|$, então existem e são únicos os inteiros q e r que satisfazem às condições:*

$$a = bq + r, \text{ com } 0 \leq r < |b|$$

1.2.2 Máximo divisor comum

Definição 1.2.2. *Sejam 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 ($d > 0$) que satisfaz às condições:*

1. *d/a e d/b*
2. *se c/a e se c/b, então c ≤d*

Observa-se que, 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).

Inteiros primos entre si

Definição 1.2.3. *Sejam a e b dois inteiros não conjuntamente nulos. Dis-ze que a e b são primos entre si se e somente se o mdc (a,b) = 1.*

Assim, por exemplo, são primos entre si os inteiros: 2 e 3, -7 e 16, -22 e -35, pois, temos:

$$\text{mdc } (2,3) = \text{mdc } (-7,16) = \text{mdc } (-22,-35) = 1$$

1.2.3 Números primos

Definição 1.2.4. *Diz-se que um inteiro positivo $p > 1$ é um número primo ou apenas um primo se e somente se 1 e p são os seus únicos divisores positivos. Um inteiro positivo maior que 1 e que não é primo diz-se composto.*

Exemplo 1.2.1. *Os números 5, 7, 11 e 13 são todos primos, pois só são divisíveis por eles mesmos e por 1.*

Teorema 1.2.2. *Se um primo p não divide a, então a e p são primos entre si.*

Demonstração. *Seja d = mdc(a,p). Então d|a e d|p. Da relação d|p, resulta que d = 1 ou d = p, porque p é primo, e como a segunda igualdade é impossível, porque p não divide a, segue-se que d = 1, isto é, o mdc (a,p) = 1. Logo, a e p são primos entre si.*

Teorema 1.2.3. (***Teorema fundamental da Aritmética***) *Todo inteiro positivo n > 1 é igual a um produto de fatores primos.*

Demonstração. *Com efeito, se n é primo, nada há acontecer, e se n é composto, então, pelo Teorema 1.2.3, possui um divisor primo p_1, e temos:*

$$n = p_1 n_1, \qquad 1 < n_1 < n$$

Se n_1 é primo, então esta igualdade representa n como produto de fatores primos, e se, ao invés, n_1 é composto, então, pelo Teorema 1.2.3, possui um divisor primo p_2, isto é, $n_1 = p_2 n_2$, e temos:

$$n = p_1 p_2 n_2, \qquad 1 < n_2 < n_1$$

Se n_2 é primo, então esta igualdade representa n como produto de fatores primos, e se, ao invés, n_2 é composto, então, pelo mesmo Teorema 1.2.3, possui um divisor primo p_3, isto é, $n_2 = p_3 n_3$, e temos:

$$n = p_1 p_2 p_3 n_3, \qquad 1 < n_3 < n_2$$

e assim por diante.
Assim sendo, temos a sequência decrescente:

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

e como só existe um número finito de inteiros positivos menores que n e maiores que 1, existe necessariamente um n_k que é um primo $p_k (n_k = p_k)$, e por conseguinte teremos:

$$n = p_1 p_2 p_3 ... p_k$$

igualdade que representa o inteiro positivo n > 1 como produto de fatores primos.
Obs. A decomposição de um inteiro positivo n > 1 como produto de fatores primos é única, a menos da ordem dos fatores.

Exemplo 1.2.2. *As decomposições em fatores primos dos inteiros positivos 285, 248 e 368 são:*

$$285 = 3.5.19, \qquad 248 = 2.2.2.31, \qquad 368 = 2.2.2.2.23$$

1.2.4 Congruências

Definição 1.2.5. *Sejam a e b dois inteiros quaisquer e seja m um inteiro positivo fixo. Diz-se que a é congruente a b módulo m se, e somente se, m divide a diferença a-b. Em outros termos, a é congruente a b módulo m se e somente se existe um inteiro k tal que a - b = km.*

Com a notação

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

indica-se que a é congruente a b módulo m. Portanto, simbolicamente:

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

ou seja:

$$\text{a} \equiv \text{b}(\text{mod m}) \Longleftrightarrow \exists\ \text{k} \in Z \mid a - b = km$$

Propriedades das congruências

Teorema 1.2.4. *Seja m um inteiro positivo fixo ($m > 0$) e sejam a, b e c inteiros quaisquer. Subsistem as seguintes propriedades:*

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

Demonstração. 1. *Com efeito:*

$$m|0 \text{ ou } m|(a - a) \Longrightarrow a \equiv a(mod\ m)$$

2. *Com efeito, se $a \equiv b(mod\ m)$, então a-b = km, com $k \in Z$. Portanto:*

$$b - a = -(km) = (-k)m \Longrightarrow b \equiv a(mod\ m)$$

3. *Com efeito, se $a \equiv b(mod\ m)$ e se $b \equiv c(mod\ m)$, então existem inteiros h e k tais que*

$$a - b = hm \text{ e } b - c = km$$

Portanto:

$$a - c = (a - b) + (b - c) = hm + km = (h + k)m$$

e isto significa que $a \equiv c(mod\ m)$.

Sistemas completos de restos

Definição 1.2.6. *Chama-se sistema completo de restos módulo m todo conjunto* $S = \{r_1, r_2, ..., r_m\}$ *de m inteiros tal que um inteiro qualquer* $\underline{a}$ *é congruente módulo m a um único elemento de S.*

Exemplo 1.2.3. *Os conjuntos* $\{1, 2, 3\}$, $\{0, 1, 2\}$, $\{1, 5, 9\}$ *são todos sistemas completos de restos módulo 3, pois todos quando divididos por 3 deixam restos de 0 a 2, não necessariamente nessa ordem.*

Teorema 1.2.5. *O conjunto* $S = \{0, 1, 2, ..., m - 1\}$ *é um sistema de restos completo módulo m.*

Demonstração. *Seja a um inteiro qualquer e sejam* $\underline{q}$ *e* $\underline{r}$ *o quociente e o resto da divisão de* $\underline{a}$ *pelo inteiro positivo m, isto é:*

$$a = mq + r, \qquad \text{onde } 0 \leq r < m$$

Então, pela definição de inteiros congruentes módulo m, temos:

$$a \equiv r(mod\ m)$$

e como $\underline{r}$ *só pode assumir os valores 0,1,2,...,m-1, segue-se que o inteiro* $\underline{a}$ *é congruente módulo* $\underline{m}$ *a um único elemento do conjunto S, e por conseguinte este conjunto é um sistema completo de restos módulo m.*

1.2.5 Congruências lineares

Definição 1.2.7. *Chama-se congruência linear toda equação da forma*

$$ax \equiv b(mod\ m) \tag{1.1}$$

onde a e b são dois inteiros quaisquer e m um inteiro positivo.
Todo inteiro x_0 tal que

$$ax_0 \equiv b(mod\ m)$$

diz-se uma solução da congruência linear (1.1).
Temos $ax_0 \equiv b(mod\ m)$ se, e somente se, $m|(ax_0 - b)$, isto é, se existe um inteiro y_0 tal que $ax_0 - b = my_0$.
É importante notar que, se x_0 é uma solução da congruência linear (1.1), então todos os inteiros $x_0 + km$, onde k é um inteiro arbitrário, isto é, os inteiros:

$$...,x_0 - 3m,\ x_0 - m,\ x_0 + m,\ x_0 + 3m,...$$

também são soluções da congruência linear (1.1), pois, temos:

$$a(x_0 + km) \equiv ax_0 \equiv b(mod\ m)$$

Exemplo 1.2.4. *Consideremos a congruência linear:*

$$8x \equiv 16(mod\ 12) \tag{1.2}$$

Como $8 \cdot 2 \equiv 16(mod\ 12)$, segue-se que $x_0 = 2$ é uma solução desta congruência linear, e por conseguinte todos os inteiros 2 + 12k, isto é, os inteiros: ..., -34, -22, -10, 14, 26, 38, ... também são soluções da congruência linear (1.2).

Como se vê, obtida uma solução particular x_0 de uma congruência linear $ax \equiv b(mod\ m)$, pode-se construir uma infinidade de outras soluções, todas mutuamente congruentes módulo $\underline{m}$.
Duas soluções quaisquer da congruência linear (1.1), x_0 e x_1, que são congruentes módulo $\underline{m}$, isto é, tais que $x_0 \equiv x_1(mod\ m)$, não são consideradas soluções distintas, isto é, o número de soluções da congruência linear (1.1) é dado pelo número de soluções mutuamente incongruentes módulo $\underline{m}$ que a satisfazem.

Condição de existência de solução

Teorema 1.2.6. *A congruência linear $ax \equiv b(mod\ m)$ tem solução se, e somente se, $\underline{d}$ divide $\underline{b}$ $(d|b)$, sendo $d = mdc(a,m)$.*

Demonstração. *($\Longrightarrow$) Suponhamos que a congruência linear $ax \equiv b(mod\ m)$ tem como solução o inteiro x_0, isto é, que $ax_0 \equiv b(mod\ m)$. Então, existe um inteiro y_0 tal que*

$$ax_0 - b = my_0 \qquad ou \qquad ax_0 - my_0 = b$$

e como d|a e d|m, porque d = mdc(a,m), segue-se que $d|(ax_0 - my_0)$ e, portanto, d|b. ($\Longleftarrow$) Reciprocamente, suponhamos que d|b, isto é, que b = dk, onde $\underline{k}$ é um inteiro. Como o mdc(a,m) = d, existem inteiros x_0 e y_0 tais que

$$ax_0 + my_0 = d$$

ou, multiplicando ambos os membros desta igualdade por k:

$$a(kx_0) + m(ky_0) = dk = b$$

ou

$$a(kx_0) - b = m(-ky_0)$$

o que implica:

$$a(kx_0) \equiv b(mod\ m)$$

Portanto, o inteiro kx_0 é uma solução da congruência linear

$$ax \equiv b(mod\ m)$$

Teorema 1.2.7. *Se $\underline{d}$ divide $\underline{b}$ (d|b), sendo d = mdc(a,m), então a congruência linear*

$$ax \equiv b(mod\ m)$$

tem precisamente $\underline{d}$ soluções mutuamente incongruentes módulo $\underline{m}$.

Demonstração. *Foi mostrado no Teorema 1.2.6 que a congruência $ax \equiv b(mod\ m)$ tem solução se, e somente se, d = mdc(a,m) divide $\underline{b}$ (d|b). Além disso, sabe-se que se d|b e se o par de inteiros x_0, y_0 é uma solução particular da equação ax - my = b e seja x, y uma outra solução qualquer desta equação. Então, temos:*

$$ax - my = b = ax_0 - my_0$$

e, portanto:

$$a(x - x_0) = m(y - y_0)$$

Por ser o mdc(a,m) = d, existem inteiros $\underline{r}$ e $\underline{s}$ tais que $a = dr$ e $b = ds$, com $\underline{r}$ e $\underline{s}$ primos entre si. Substituindo estes valores de $\underline{a}$ e $\underline{b}$ na igualdade anterior e cancelando o fator com $\underline{d}$, obtemos:

$$r(x - x_0) = s(y - y_0)$$

Assim sendo, $r|s(y - y_0)$, e como o mdc(r,s) = 1, segue-se que $r|(y - y_0)$, isto é:

$$y - y_0 = rt \qquad e \qquad x - x_0 = st$$

onde $\underline{t}$ é um inteiro arbitrário. Portanto, temos as fórmulas:

$$x = x_0 + st = x_0 + (m/d)t$$
$$y = y_0 + rt = y_0 + (a/d)t$$

Entre o número infinito de inteiros dados pela primeira dessas fórmulas consideremos somente aqueles que resultam de atribuir a $\underline{t}$ os valores: 0, 1, 2,..., d-1, isto é, os $\underline{d}$ inteiros:

$$x_0, x_0 + m/d, x_0 + 2(m/d), ..., x_0 + (d - 1)(m/d)$$

Posto isto, vamos mostrar que estes $\underline{d}$ inteiros são mutuamente incongruentes módulo $\underline{m}$ e que todos os outros inteiros dados pela fórmula $x = x_0 + (m/d)t$ são congruentes módulo $\underline{m}$ a algum desses $\underline{d}$ inteiros. Com efeito, se fosse

$$x_0 + (m/d)t_1 \equiv x_0 + (m/d)t_2 \ (mod\ m)$$

onde $0 \leq t_1 < t_2 \leq d - 1$, então, teríamos:

$$(m/d)t_1 \equiv (m/d)t_2 \ (mod\ m)$$

E como o mdc(m/d,m) = m/d, podemos cancelar o fator comum m/d, o que dá a congruência:

$$t_1 \equiv t_2 \ (mod\ m)$$

e isto significa que $d\,|(t_2 - t_1)$, o que é impossível, visto que $0 < t_2 - t_1 < d$.
Além disso, qualquer outro inteiro $x_0 + (m/d)t$ é congruente módulo $\underline{m}$ a algum dos $\underline{d}$ inteiros acima enumerados. Com efeito, pelo algoritmo da divisão, temos:

$$t = dq + r, \text{ onde } 0 \leq r \leq d - 1$$

e, portanto:

$$x_0 + (m/d)t = x_0 + (m/d)(dq + r) = x_0 + mq + (m/d)r$$

isto é:

$$x_0 + (m/d)t \equiv x_0 + (m/d)r \ (mod\ m)$$

onde x_0 + (m/d)r é um dos $\underline{d}$ inteiros que foram selecionados.

Obs. Se o mdc(a,m) = 1, então a congruência linear $ax \equiv b(mod\ m)$ tem uma única solução módulo m.

Exemplo 1.2.5. *Resolver a congruência linear*

$$3x \equiv 6\ (mod\ 18).$$

O mdc(3,18) = 3 e como 3 |6, a congruência dada tem exatamente 3 soluções mutuamente incongruentes módulo 18.
Como $3 \cdot 8 \equiv 6(mod\ 18)$, uma solução da congruência dada é $x_0 = 8$, e por conseguinte as suas 3 soluções mutuamente incongruentes módulo 18 são dadas pela fórmula:

$$x = 8 + (18/3)t = 8 + 6t, \qquad onde\ t = 0,1,2$$

isto é, são os inteiros:

$$x = 8,\ 14,\ 20$$

Inverso de um inteiro

Definição 1.2.8. *Seja $\underline{a}$ um inteiro. Chama-se inverso de $\underline{a}$ módulo $\underline{m}$ um inteiro a* tal que $aa^* \equiv 1\ (mod\ m)$.*

Teorema 1.2.8. *Se o mdc(a,m) = 1, então $\underline{a}$ tem um único inverso módulo $\underline{m}$.*

Demonstração. *Com efeito, se o mdc(a,m) = 1, então a congruência linear*

$$ax \equiv 1\ (mod\ m)$$

tem uma única solução $x_0(mod\ m)$, isto é:

$$ax_0 \equiv 1(mod\ m)$$

de modo que o inteiro $\underline{a}$ tem um único inverso módulo $\underline{m}$:

$$a^* = x_0$$

Capítulo 2

Metodologia da pesquisa

2.1 Abordagem metodológica

A metodologia da pesquisa consiste em direcionar o pesquisador para a realização de seus objetivos. Em concordância com Cervo e Bervian (2007), a pesquisa se formula a partir de uma dúvida ou problema e, com o uso do método científico, buscam-se as soluções e respostas para essa questão.

Uma vez que a função de Euler aplicada na criptografia é essencial para sua segurança, a abordagem da pesquisa utilizada foi de caráter quantitativo, pois essa abordagem "recorre à linguagem matemática para descrever as causas de um fenômeno, as relações entre variáveis, etc." (FONSECA, 2002 apud GERHARDT e SILVEIRA, 2009, p.35).

Ademais, a preocupação desse projeto estar em identificar a contribuição da função de Euler na eficiência da criptografia RSA, o que é caracterizado pela estratégia de investigação explicativa. Para Gil (2002, p.42), "essas pesquisas têm como preocupação central identificar os fatores que determinam ou que contribuem para a ocorrência dos fenômenos. Esse é o tipo de pesquisa que mais aprofunda o conhecimento da realidade".

Quanto ao procedimento técnico, de maneira a auxiliar nos estudos acerca de Criptografia, Teoria dos Números e da Função ϕ, buscou-se aprofundar o tema através de procedimento bibliográfico, usando alguns autores tais como: Filho (1981), Castro (2014), Filho (1988), Okumura (2014) e alguns outros autores que complementaram a compreensão e estão citados nas referências e no decorrer dessa monografia. Cervo e Bervian (2007) enfatizam que a pesquisa bibliográfica visa esclarecer um problema a partir de referências teóricas publicadas em trabalhos acadêmicos e livros e que este procedimento

analisa contribuições científicas sobre determinado problema.

2.2 Etapas da pesquisa

1ª etapa: Pesquisa bibliográfica sobre a Função ϕ a partir da obra de Filho (1988).

2ª etapa: Pesquisa bibliográfica sobre aplicações da Função ϕ na Criptografia RSA com a finalidade de compreender como ela auxilia nessa criptografia .As obras utilizadas para esse fim foram as de Okumura (2014) e Castro (2014).

3ª etapa: Exploração da aplicação da Função ϕ na criptografia RSA com maior aprofundamento. Nessa etapa, houve necessidade de revisão de alguns conceitos prévios como Divisibilidade, Máximo Divisor Comum, Números primos e Congruências.

4ª etapa: Revisão e organização da pesquisa.

Capítulo 3

Função de Euler

3.1 Função de Euler

[1]

Definição 3.1.1. *Chama-se função de Euler a função aritmética $\phi(n)$ assim definida para todo inteiro positivo n:*

$$\phi(n) = \text{número de inteiros positivos} \leq n \text{ e que são primos com } n.$$

Em particular, $\phi(1) = 1$, porque o único inteiro positivo ≤ 1 é o próprio 1 e o mdc(1,1) = 1.

Para todo $n \geq 2$, o mdc (n,n) = $n \neq 1$, de modo que

$$\phi(n) = \text{número de inteiros positivos} < n \text{ e que são primos com } n.$$

Logo, $\phi(n) < n$ para todo inteiro $n \geq 2$.

Exemplo 3.1.1. *Calcular $\phi(15)$.*

Resolução: Os inteiros positivos menores que 15 e que são primos com 15 são 1, 2, 4, 7, 8, 11, 13 e 14, de modo que $\phi(15) = 8$.

Exemplo 3.1.2. *Calcular $\phi(20)$.*

Resolução: Os inteiros positivos menores que 20 e que são primos com 20 são 1, 3, 7, 9, 11, 13, 17 e 19, de modo que $\phi(20) = 8$.

[1] As definições, teoremas e demonstrações deste capítulo estão de acordo com (FILHO, 1988).

3.2 Propriedade multiplicativa da Função de Euler

Lema 3.2.1. *Se m e n são inteiros positivos tais que o mdc(m,n) = 1 e se r é um inteiro qualquer, então os restos das divisões dos n inteiros:*

$$r, m + r, 2m + r, ..., (n - 1)m + r \tag{3.1}$$

por n são todos distintos e, dispostos em ordem crescente, são: 0, 1, 2, ..., n -1.

Demonstração. *Suponhamos, por absurdo, que dois inteiros da sequência (3.1):*

$$hm + r \qquad e \qquad km + r, \text{ onde } 0 \leq h < k < n$$

são congruentes módulo n. Então, a diferença entre esses dois inteiros: (k - h)m, é divisível por n, e como n é primo com m, segue-se que n|(k - h), o que é impossível, visto que 0 < k - h < n. Logo, os restos das divisões dos n inteiros da sequência (3.1) por n são todos distintos, e por conseguinte estes restos, dispostos em ordem crescente, são: 0, 1, 2, ..., n - 1.

Exemplo 3.2.1. *Com m = 4, n = 3 e r = -3, temos os 3 inteiros:*

-3, 1, 5

cujos restos quando divididos por 3 são, respectivamente, os inteiros distintos: 0, 1, 2.

Exemplo 3.2.2. *Seja m = 7, n = 13 e r = -11.*

Os números a serem divididos por r, então, serão:

-11, -4, 3, 10, 17, 24, 31, 38, 45, 52, 59, 66, 73

que deixam os restos, respectivamente:

2, 9, 3, 10, 4, 11, 5, 12, 6, 0, 7, 1, 8

que organizados em ordem crescente, são:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

Teorema 3.2.1. *A função ϕ de Euler é uma função aritmética multiplicativa.*

Demonstração. *Sejam m e n dois inteiros positivos tais que o mdc(m,n)=1. Cumpre demonstrar que $\phi(mn) = \phi(m)\phi(n)$.*

A proposição é verdadeira se m ou n é igual a 1, pois, temos:

$$\phi(1 \cdot n) = \phi(n) = 1 \cdot \phi(n) = \phi(m)\phi(n)$$

$$\phi(m \cdot 1) = \phi(m) = \phi(m) \cdot 1 = \phi(m)\phi(n)$$

Suponhamos, pois, $m > 1$ e $n > 1$. Neste caso, os inteiros positivos de 1 a mn podem ser dispostos em m colunas com n inteiros em cada uma delas, do seguinte modo:

1	2	...	r	...	m
m + 1	m + 2		m + r		2m
2m + 1	2m + 2		2m + r		3m
.	.		.		.
.	.		.		.
.	.		.		.
(n-1)m + 1	(n-1)m + 2		(n-1)m + r		nm

Como o mdc(qm + r, m) = mdc(r, m), os inteiros da r-ésima coluna são primos com m se e somente se r é primo com m. Mas,na primeira linha existem $\phi(m)$ inteiros que são primos com m e, portanto, existem precisamente $\phi(m)$ colunas formadas com inteiros que são todos primos com m. Por outro lado, supondo que que a r-ésima coluna é uma destas $\phi(m)$ colunas, então, pelo Lema 3.2.1, os restos das divisões dos n inteiros que a formam por n são 0, 1, 2,..., n-1, e por conseguinte, o número de inteiros da r-ésima coluna que são primos com n é $\phi(n)$. Assim sendo, em cada uma das $\phi(m)$ colunas existem exatamente $\phi(n)$ inteiros que são primos com n, de modo que o número total de inteiros que são primos com m e n, isto é, que são primos com mn, é dado pelo produto $\phi(m)\phi(n)$, e isto significa que $\phi(mn) = \phi(m)\phi(n)$.

Exemplo 3.2.3. *Dados $m = 7$ e $n = 8$, calcular $\phi(mn)$.*

Como 7 e 8 são primos entre si, $\phi(mn) = \phi(m) \cdot \phi(n)$, logo:

$\phi(7 \cdot 8) = \phi(7) \cdot \phi(8) \Longrightarrow \phi(7 \cdot 8) = 6 \cdot 4 = 24$

3.3 Cálculo de ϕ(n)

Teorema 3.3.1. *Se o inteiro n > 1, então $\phi(n) = n - 1$ se e somente se n é primo.*

Demonstração. *($\Longrightarrow$) Se o inteiro n > 1, então cada um dos inteiros positivos menores que n é primo com n e, portanto, $\phi(n) = n - 1$.*

($\Longleftarrow$) Reciprocamente, se $\phi(n) = n - 1$, com n > 1, então n é primo, pois, 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, d e n, e teríamos $\phi(n) \leq n - 2$. Logo, n é primo.

Exemplo 3.3.1. *Seja 103 um número primo, calcular $\phi(103)$.*

Utilizando o Teorema 3.3.1.

$$\phi(103) = 102.$$

Teorema 3.3.2. *Se p é um primo e se k é um inteiro positivo, então:*

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

Demonstração. *Obviamente, o mdc(n,p^k) = 1 se e somente se p não divide n($p \nmid n$), de modo que os únicos inteiros da sequência 1, 2, 3, ..., p^k que não são primos com p^k são aqueles divisíveis por p, isto é, os inteiros pt, onde t é um inteiro positivo tal que $pt < p^k$, ou seja, tal que $t \leq p^{k-1}$. Portanto, na sequência 1, 2, 3, ..., p^k existem precisamente p^{k-1} inteiros que não são primos com p^k - os inteiros:*

$$p,\ 2p,\ 3p,\ ...,\ p(k-1)p$$

isto é, a sequência 1, 2, 3, ..., p^k contém exatamente $p^k - p^{k-1}$ inteiros que são primos com p^k. Logo, pela definição da função ϕ, temos:

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

Exemplo 3.3.2. *Calcular $\phi(128)$.*

$\phi(128) = \phi(2^7) = 2^7 - 2^6 = 128 - 64 = 64$

Teorema 3.3.3. *Se $n = p_1^{a_1}p_2^{a_2}...p_r^{a_r}$ é a fatorização canônica do inteiro n > 1, então:*

$$\phi(n) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1})...(p_r^{a_r} - p_r^{a_r-1}) = n(1 - 1/p_1)(1 - 1/p_2)...(1 - 1/p_r)$$

Demonstração. *Como ϕ é uma função aritmética multiplicativa (Teorema 3.2.1) e os fatores $p_1^{a_1}p_2^{a_2}, ..., p_r^{a_r}$ são primos entre si dois a dois, temos:*

$$\phi(n) = \phi(p_1^{a_1})\phi(p_2^{a_2})...\phi(p_r^{a_r})$$

Mas, pelo teorema 3.3.2:

$$\phi(p_1^{a_1}) = p_1^{a_1} - p_1^{a_1-1}, \quad \phi(p_2^{a_2}) = p_2^{a_2} - p_2^{a_2-1}, ..., \quad \phi(p_r^{a_r}) = p_r^{a_r} - p_r^{a_r-1}$$

Portanto:

$$\phi(n) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1})...(p_r^{a_r} - p_r^{a_r-1}) = n(1 - 1/p_1)(1 - 1/p_2)...(1 - 1/p_r)$$

Exemplo 3.3.3. *Calcular $\phi(14400)$.*

Resolução:

Por ser $14400 = 3^2 \cdot 4^3 \cdot 5^2$, têm-se:

$$\phi(14400) = 14400 \cdot \tfrac{2}{3} \cdot \tfrac{3}{4} \cdot \tfrac{4}{5} = 14400 \cdot \tfrac{2}{5} = 5760.$$

Capítulo 4

Função de Euler e Criptografia RSA

A Teoria dos Números tem um importante papel na criptografia RSA, uma vez que através da função de Euler e do conhecimento das Congruências lineares, é acessível ao leitor que entenda como esse algoritmo funciona. Respaldada pelo primeiro capítulo deste trabalho, essa etapa da pesquisa respondeu como a função é aplicada nessa criptografia.

A criptografia RSA utiliza congruências para sua funcionalidade. É necessário decodificar um bloco codificado e deve voltar ao bloco que corresponde a mensagem original. Em outras palavras, considera-se, por exemplo, b. Ou seja, um bloco que ainda não foi codificado. Assim, quando codificado torna-se C(b). Agora, quando decodificado torna-se D(C(b)), que deve ser o próprio b.

Assim, precisa-se provar que se b é um inteiro maior ou igual a 1 e menor igual a n - 1, então D(C(b)) $\equiv$ b(mod n). Como D(C(b)) $<$ n, pois os blocos codificados precisavam ser menores que n, basta mostrar que D(C(b)) = b.

Assim, por definição D(a) $\equiv a^d$(mod n) e C(b) $\equiv b^e$(mod n). Elevando ambos os lados da segunda congruência por d, então:

$$\text{C(b)} \equiv b^e(mod\ n) \Longrightarrow [C(b)]^d \equiv (b^e)^d(mod\ n) \Longrightarrow D(C(b)) \equiv b^{ed}(mod\ n).$$

Porém d é o inverso multiplicativo de e (mod $\phi(n)$), logo

$$\text{e}\cdot d = 1 + k \cdot \phi(n) \quad (4.1)$$

para algum inteiro k. Como e e d são inteiros maiores que 2 e $\phi(n)$ é obrigatoriamente maior que 0, então k também será maior que zero. Então, substituindo $e \cdot t$ em (4.1). Assim, resulta em:

$$b^{ed} \equiv b^{1+k\cdot\phi(n)} \equiv b \cdot (b^{\phi(n)})^k (mod\ n)$$

Sabe-se que $n = p \cdot q$, onde p e q são primos distintos. Agora, é necessário encontrar a forma reduzida de $b^{ed}(mod\ p)$ e $b^{ed}(mod\ q)$. Viu-se anteriormente que $\phi(n) = (p-1)\cdot(q-1)$, substituindo isso em (4.1) ficamos com:

$$e \cdot d = 1 + k \cdot (p-1) \cdot (q-1)$$

Substituindo a nova forma de $e \cdot d$

$$b^{ed} \equiv b^{1+k\cdot\phi(n)} \equiv b \cdot (b^{\phi(n)})^k \equiv b \cdot (b^{p-1})^{k\cdot(q-1)}$$

Isso tudo, côngruo módulo p.

Para prosseguir com a prova, supõe-se que b e p são primos entre si, assim, pelo pequeno Teorema de Fermat têm-se que $b^{p-1} \equiv 1(mod\ p)$ e, daí

$$b^{ed} \equiv b \cdot (b^{p-1})^{k\cdot(q-1)} \equiv b \cdot 1^{k\cdot(q-1)} \equiv b$$

Portanto, $b^{ed} \equiv b(mod\ p)$.

Agora, se p divide b, e p é obrigatoriamente primo, então $b \equiv 0(mod\ p)$. Para qualquer valor de b, eleva-se ambos os lados da equivalência a ed, e têm-se, então:

$$(b)^{ed} \equiv (0)^{ed} \Longrightarrow (b)^{ed} \equiv 0(mod\ p)$$

De maneira muito análoga, consegue-se demonstrar que para qualquer valor de q, $b^{ed} \equiv b(mod\ q)$. Em outras palavras, $b^{ed} - b$ é divisível por p e por q, como p e q são primos distintos. Ou seja, mdc(p,q) = 1. Temos que $pq|(b^{ed} - b)$. Portanto, como n = pq, temos

$$\mathrm{D(C(b))} = b^{ed} \equiv b(mod\ n)$$

o que mostra que D(C(b)) = b.

Portanto, a criptografia RSA é desenvolvida a partir de três passos: pré-codificação, que é feita utilizando, por exemplo, o Quadrado de Polybius (Tabela 1.2), codificação,

que envolve as congruências lineares e a função ϕ, e a decodificação, que consiste em fazer o processo inverso da codificação para retornar a mensagem original (etapa de pré-codificação).

PRÉ-CODIFICAÇÃO

Nesse primeiro momento, a preocupação está em transformar as letras em números. Para isso utilizou-se o Quadrado de Polybius. Para demonstrar o processo, pré-codificou-se a frase ´´AMATEMATICAELINDA". Utilizando a Tabela 1.2 chegou-se ao número ´´1132114415321144241311153124331411". O último passo da pré-codificação consiste em separar esse número em blocos que devem ser números menores que n. Nesse caso, apenas para fins de exemplificação, utilizou-se n = 35, então:

1 - 13 - 21- 14 - 4 - 15 - 32 - 11 - 4 - 4 - 24 - 1 - 31 - 11 - 5 - 3 - 12 - 4 - 3 - 31 - 4 - 11

É importante ressaltar que alguns cuidados devem ser tomados na hora de separar os blocos. Junior (2015, p. 40) afirma que o bloco não pode iniciar com o 0 porque isso traria problemas no momento da decodificação, pois seria difícil distinguir, por exemplo, o bloco 012 do bloco 12, além disso, é necessário que para fins de dificultar que um estranho desvende a palavra, que não haja frequência e que o bloco não corresponda a uma palavra ou letra.

CODIFICAÇÃO

Demonstrado o processo de pré-codificação, o algoritmo evoluiu, nesse momento, para a codificação. Como já foi feita a pré-codificação, restava determinar um valor e que devia ser inversível módulo $\phi(n)$, ou seja, com mdc(e, $\phi(n)$) = 1. Nessa etapa precisa-se de n, que é dado pelo produto de dois primos p e q. Como já mencionado anteriormente, n = 35, pois os primos escolhidos foram p = 5 e q = 7. Em concordância com os Teoremas 3.2.1 e 3.3.1, podemos afirmar que $\phi(n) = 24$. A chave de codificação, que é pública, é dada pelo par (n, e). Denota-se cada bloco codificado por C(b), em que b é o bloco que é um inteiro positivo menor que n. Para codificar foi utilizado que C(b) = resto da divisão de b^e por n, que em outras palavras significa que C(b) $\equiv b^e (mod\ n)$. Nesse exemplo, o menor valor para e é 5, pois é o menor inteiro primo que não divide $\phi(n) = 24$. Assim, tomando o primeiro bloco 1 para codificá-lo, precisa-se encontrar o resto da divisão de 1^5 por 35. Assim, C(1) = 1. Codificando-se todos os blocos da mensagem, obtêm-se:

Processo de codificação

b^e	C(b)
$1^5 = 1$	1
$13^5 = 371293$	13
$21^5 = 4084101$	21
$14^5 = 573824$	14
$4^5 = 1024$	9
$15^5 = 759375$	15
$32^5 = 33554432$	2
$11^5 = 161051$	16
$4^5 = 1024$	9
$4^5 = 1024$	9
$24^5 = 7962624$	19
$1^5 = 1$	1
$31^5 = 28629151$	26
$11^5 = 161051$	16
$5^5 = 3125$	10
$3^5 = 324$	33
$12^5 = 248832$	17
$4^5 = 1024$	9
$3^5 = 324$	33
$31^5 = 28629151$	26
$4^5 = 1024$	9
$11^5 = 161051$	16

Fonte: Da Autora (2024)

Logo, a mensagem codificada pela criptografia RSA fica da seguinte maneira:

1 - 13 - 21 - 14 - 9 - 15 - 2 - 16 - 9 - 9 - 19 - 1 - 26 - 16 - 10 - 33 - 17 - 9 - 33 - 26 - 9 - 16

DECODIFICAÇÃO

Para a decodificação precisa-se de n e o inverso de e módulo $\phi(n)$, que pode ser chamado de d. Dessa forma, a nossa chave de decodificação é dada pelo par (n, d). Os

blocos de decodificação serão chamados de D(a), em que a são os blocos codificados. Da mesma forma que foi feito na codificação, na decodificação, D(a) = resto da divisão de a^d por n, que em outras palavras pode ser entendido como D(a) $\equiv a^d(mod\ n)$. Se forem conhecidos o valor de e e de $\phi(n)$, fica fácil encontrar o valor de d.

No exemplo utilizado, o valor de d também é 5, pois como e = 5 e $\phi(n) = 24$, então:

$$5\text{d} \equiv 1(\text{mod } 24) \Longrightarrow d = 5.$$

Com isso, basta executar a decodificação de maneira análoga à codificação. Para isso eleva-se a 5 cada bloco a codificado, e encontra-se o resto da divisão por n = 35. A Tabela representa os resultados obtidos.

Processo de decodificação

b^e	C(b)
$1^5 = 1$	1
$13^5 = 371293$	13
$21^5 = 4084101$	21
$14^5 = 573824$	14
$9^5 = 59049$	4
$15^5 = 759375$	15
$2^5 = 32$	32
$16^5 = 1048576$	11
$9^5 = 59049$	4
$9^5 = 59049$	4
$19^5 = 2476099$	24
$1^5 = 1$	1
$26^5 = 11881376$	31
$16^5 = 1048576$	11
$10^5 = 100000$	5
$33^5 = 39135393$	3
$17^5 = 1419857$	12
$9^5 = 59049$	4
$33^5 = 39135393$	3

$26^5 = 11881376$	31
$9^5 = 59049$	4
$16^5 = 1048576$	11

Fonte: Da Autora (2024)

Portanto, a mensagem decodificada retorna aos blocos de pré-codificação separados no início.

1 - 13 - 21- 14 - 4 - 15 - 32 - 11 - 4 - 4 - 24 - 1 - 31 - 11 - 5 - 3 - 12 - 4 - 3 - 31 - 4 - 11

Para exemplificar melhor o algoritmo, foram utilizados mais dois exemplos de aplicação da criptografia RSA com outra tabela de conversão.

Tabela 4.3: Tabela de conversão

Letras	A	B	C	D	E	F	G	H	I	J	K	L	M
Números	10	11	12	13	14	15	16	17	18	19	20	21	22
Letras	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Números	23	24	25	26	27	28	29	30	31	32	33	34	35

Fonte: Da Autora (2024)

Exemplo 4.0.1. *Deseja-se criptografar e descriptografar a frase "OTEATROAMAZONASÉLINDO" utilizando a Tabela 4.3 para pré-codificação.*

Escolhendo $p = 17$ e $q = 23$, têm-se $n = 391$ e, consequentemente, $\phi(n) = 352$.

Pré-codificação:

$242-9-14-102-9-272-4-102-210-352-42-310-281-42-118-42-118-231-324$

Codificação

Nesse caso, $e = 3$, pois 3 é o menor inteiro primo que não divide $\phi(n) = 352$. Logo, os resultados da codificação foram:

Tabela 4.4: Codificação

b^e	$C(b)$
$243^3 = 14172488$	302
$9^3 = 729$	338
$14^3 = 2744$	7
$102^3 = 1061208$	34
$9^3 = 729$	338
$272^3 = 20123648$	51
$4^3 = 64$	64
$102^3 = 1061208$	34
$210^3 = 9261000$	165
$352^3 = 43614208$	113
$42^3 = 74088$	189
$310^5 = 29791000$	319
$281^3 = 22188041$	355
$42^3 = 74088$	189
$118^3 = 1643032$	50
$42^3 = 74088$	189
$118^3 = 1643032$	50
$231^3 = 12326391$	116
$324^3 = 34012224$	307

Fonte: Da Autora (2024)

Lembrando que C(b) é o resto da divisão de b^e por n.

Decodficação

Nesse exemplo percebeu-se que o processo de decodificação não seria possível utilizando apenas lápis e papel, tendo que recorrer ao uso do aplicativo Symbolab, que respondeu apenas algumas congruências, e, portanto, pôde decodificar poucos blocos. Porém, mesmo com a ocorrência dessas limitações foi possível analisar que esses blocos retornam para o que foi criado na etapa de pré-codificação. Resolvendo a congruência linear $3d \equiv 1 \pmod{352}$ obteve-se $d = 235$, pois $3 \cdot 235 = 1 + 352 \cdot 2$. Então:

Tabela 4.5: Decodificação

b^e	$C(b)$	a^d	$D(C(b))$
$243^3 = 14172488$	302	302^{235}	242
$9^3 = 729$	338	338^{235}	-
$14^3 = 2744$	7	7^{235}	14
$102^3 = 1061208$	34	34^{235}	-
$9^3 = 729$	338	338^{235}-	
$272^3 = 20123648$	51	51^{235}	-
$4^3 = 64$	64	64^{235}	-
$102^3 = 1061208$	34	34^{235}	-
$210^3 = 9261000$	165	165^{235}	-
$352^3 = 43614208$	113	113^{235}	-
$42^3 = 74088$	189	189^{235}	-
$310^3 = 29791000$	319	310^{235}	310
$281^3 = 22188041$	355	355^{235}	-
$42^3 = 74088$	189	189^{235}	-
$118^3 = 1643032$	50	50^{235}	-
$42^3 = 74088$	189	189^{235}	-
$118^3 = 1643032$	50	50^{235}	-
$231^3 = 12326391$	116	116^{235}	231
$324^3 = 34012224$	307	307^{235}	324

*Fonte: Da Autora (*2024*)*

Exemplo 4.0.2. *Dados $p = 7$, $q = 11$, $n = 77$, $\phi(n) = 60$, $e = 7$ e $d = 43$, têm-se a Pré-codificação realizada a partir da Tabela 4.3.*

$$14 - 30 - 10 - 2 - 22 - 42 - 9 - 1 - 42 - 42 - 71 - 8 - 10 - 13 - 2 - 42 - 8 - 23 - 30 - 2 - 21 - 4 - 27 - 2 - 42 - 8$$

Codifique e decodifique para verificar se retorna aos mesmos blocos da pré-codificação.

Tabela 4.6: Codificação/Decodificação

b^e	$C(b)$	a^d	$D(C(b))$
$14^7 = 105413504$	42	42^{43}	14
$30^7 = 21870000000$	2	2^{43}	30
$10^7 = 10000000$	10	10^{43}	10
$2^7 = 128$	51	51^{43}	2
$22^7 = 2494357888$	22	22^{43}	22
$42^7 = 230539333248$	70	70^{43}	42
$9^7 = 4782969$	37	37^{43}	9
$1^7 = 1$	1	1^{43}	1
$42^7 = 230539333248$	70	70^{43}	42
$42^7 = 230539333248$	70	70^{43}	42
$71^7 = 9095120158391$	36	36^{43}	71
$8^7 = 2097152$	57	57^{43}	8
$10^7 = 10000000$	10	10^{43}	10
$13^7 = 62748517$	63	63^{43}	13
$2^7 = 128$	51	51^{43}	2
$42^7 = 230539333248$	70	70^{43}	42
$8^7 = 2097152$	57	57^{43}	8
$23^7 = 3404825447$	23	23^{43}	23
$30^7 = 21870000000$	2	2^{43}	30
$2^7 = 128$	51	51^{43}	2
$21^7 = 1801088541$	21	21^{43}	21
$4^7 = 16384$	60	60^{43}	4
$27^7 = 10460353203$	69	69^{43}	27
$2^7 = 128$	51	51^{43}	2
$42^7 = 230539333248$	70	70^{43}	42
$8^7 = 2097152$	57	57^{43}	8

*Fonte: Da Autora (*2024*)*

Concluindo, todos os blocos retornaram para o bloco pré-codificado inicialmente. A

frase em questão é “EUAMOTEORIADOSNUMEROS”. Embora nos exemplos dados não tenham sido considerados os espaços para as frases, eles poderiam ser incluídos normalmente na pré-codificação com um número já determinado.

Como o RSA é uma criptografia de chave pública e o par (e,n) fica disponível a qualquer usuário, encontrando-se p e q, ou seja, fatorando n, torna-se fácil encontrar $\phi(n)$, que é o que deve ser sigiloso para que não seja encontrado d por meio da resolução da congruência linear $ed \equiv 1(mod\ \phi(n))$. Com base nos exemplos solucionados neste trabalho, seria fácil quebrar essa criptografia, mas o que a torna eficiente é a utilização de p e q muito grandes. Conforme observado nos exemplos, mesmo com números pequenos alguns aplicativos simples não suportaram calcular, por conta da limitação tecnológica. Ademais, imaginando p um número com mais de dez algarismos, por exemplo, e q um número com cinco ou mais algarismos que p, nota-se a relevância da Teoria dos Números, sobretudo, da Função de Euler para a eficiência do RSA.

Considerações finais

Este trabalho demonstrou a relevância da função de Euler e da Teoria dos Números para a criptografia RSA. O estudo sobre a função apresentou-se de forma completa, mostrando a definição, os Teoremas e suas demonstrações, além de exemplos de como executar cada cálculo. A aplicação da função na Criptografia alcançou os objetivos da pesquisa, revelando como funciona o algoritmo, como ele utiliza a Teoria dos Números e como o valor de $\phi(n)$ influencia para a sua segurança. Os exemplos criados pela autora satisfizeram a expectativa da pesquisa em relação à ligação da função e da Criptografia.

A criptografia RSA é utilizada até hoje por conta da sua alta segurança, e ressaltar como a Matemática está presente no cotidiano é importante para que mais pesquisas se desenvolvam em torno de aplicações pouco conhecidas. A Teoria dos Números estudada nas universidades em sua forma mais pura, por exemplo, é aplicada nas criptografias e muitos graduandos não possuem esse conhecimento. Portanto, este trabalho cumpriu seu principal objetivo: compartilhar o conhecimento de uma aplicação da Teoria dos Números na Criptografia.

Referências Bibliográficas

[1] BOYER, C. B. **História da Matemática**. Tradução: Helena Castro. 3ª ed. Editora: Edigar Blucher Ltda. São Paulo. 2012.

[2] CARVALHO, L. M. C. de. **Tópicos de Funções aritméticas e o Teorema de Euler**. Dissertação - Departamento de Matemática, Universidade Federal do Ceará, Fortaleza, 2020. Disponível em: <https://repositorio.ufc.br/handle/riufc/53470>. Acesso em: 20 jun. 2023.

[3] CASTRO, C. C. **Criptografia RSA**. Trabalho de Conclusão de Curso – Universidade Federal de Santa Catarina, Blumenau, 2019. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/203902/TCC_ Camila.pdf?sequence=1&isAllowed=y>. Acesso em: 11 jan. 2024.

[4] CASTRO, F. L. **Criptografia RSA: uma abordagem para professores do ensino básico**. Trabalho de Conclusão de Curso – Instituto de Matemática, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014. Disponível em: <https://lume.ufrgs.br/bitstream/handle/10183/110014/000951896.pdf>. Acesso em: 21 jun. 2023.

[5] CERVO, A. L.; BERVIAN, P. A.; SILVA, R. da. **Metodologia científica**. 6. ed. São Paulo: Pearson Prentice Hall, 2007.

[6] FILHO, E. de A. **Teoria elementar dos números**. São Paulo: Nobel, 1981.

[7] FILHO, E. de A. **Funções aritméticas**: Números notáveis. São Paulo: Nobel, 1988.

[8] GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2002.

[9] JUNIOR, L. de. S. C. **Criptografia RSA: uma aplicação de Teoria dos Números**. Trabalho de Conclusão de Curso – Centro de Ciências Exatas e Tecnológicas,

Universidade Federal do Recôncavo da Bahia, Cruz das Almas, 2015. Disponível em: <https://sca.profmat-sbm.org.br/profmat_tcc.php?id1=2370&id2=84555>. Acesso em: 10 jan. 2024.

[10] OKUMURA, M. K. **Números primos e criptografia RSA**. 2014. Dissertação – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Paulo, 2014. Disponível em: <https://www.teses.usp.br/teses/disponiveis/55/55136/tde-04042014-101744/publico/mirella_okumura_revisada.pdf>. Acesso em: 22 jun. 2023.

[11] PAIVA, M. **Matemática**. São Paulo: Moderna, 2004.

[12] SILVA, E. R. da; CLEMENTE, R. G. **Função ϕ de Euler e o princípio da inclusão e exclusão**. 2021. 277f. Coletânea de estudos de egressos do ProfMat - Universidade Federal Rural de Pernambuco, Recife, 2021.