Tatiellen Souza Assis

Criptografia RSA: Teoria e Prática com Python

Rio Grande, Rio Grande do Sul, Brasil

Setembro, 2024

Tatiellen Souza Assis

Criptografia RSA: Teoria e Prática com Python

Trabalho de Conclusão de Curso, Matemática Aplicada Bacharelado, submetido por Tatiellen Souza Assis junto ao Instituto de Matemática, Estatística e Física da Universidade Federal do Rio Grande.

Universidade Federal do Rio Grande - FURG

Instituto de Matemática, Estatística e Física - IMEF

Curso de Matemática Aplicada Bacharelado

Orientador: Prof. Dr. Adilson da Silva Nunes

Rio Grande, Rio Grande do Sul, Brasil

Setembro, 2024

Este trabalho é dedicado à minha família, em especial, meu esposo, filho e aos meus pais por sempre estarem me apoiando mesmo nos momentos mais resistente durante minhas escolhas na vida. Seguidamente, ao meu professor, orientador Adilson da Silva Nunes por ter cedido seu tempo e ter tido toda paciência comigo.

Agradecimentos

Desde já, agradeço a Deus por ter permitido que eu tivesse saúde e determinação para não desanimar durante a realização deste trabalho.

Ao meu esposo Carlos Henrique Veiga e meu filho Kevin Veiga, que me incentivaram nos momentos difíceis e compreenderam a minha ausência.

Agradeço também aos meus pais, Sidney Assis e Rosimeri Souza e meus irmãos por todo ensinamento durante todos os dias desde meu nascimento.

Aos meus amigos, que sempre estiveram ao meu lado, pela amizade incondicional e pelo apoio demonstrado ao longo de todo o período de tempo do curso. Ao meu orientador Prof. Dr. Adilson da Silva Nunes, por ter desempenhado tal função dedicação e amizade, por todos os conselhos, pela ajuda e principalmente pela paciência com qual me guiou ao meu aprendizado. Por fim, mas não tão menos importante, à todos professores do IMEF que contribuíram de alguma forma, direta ou indiretamente ao longo desses anos de curso, certamente tiveram impactos na minha formação acadêmica.

"Faça as coisas o mais simples que puder, porém não as mais simples"

(Albert Einstein)

Resumo

O objetivo deste trabalho é explorar a aplicação da Criptografia RSA, analisando como é o funcionamento da codificação e decodificação de uma mensagem, utilizando a Chave Pública e a Chave Privada. São abordados conceitos importantes e para isso, se fez necessário apresentar noções básicas da Teoria dos Números, incluindo a teoria e resultado da Divisibilidade, Números Primos, Congruência e o Pequeno Teorema de Fermat. Ao longo do trabalho, foram realizadas implementações práticas utilizando a linguagem de programação Python.

Palavras-chaves: Criptografia RSA, Congruência, Álgebra, Números Primos.

Abstract

The objective of this work is to explore the application of RSA Cryptography, analyzing how the encoding and decoding of a message works, using the Public Key and the Private Key. Important concepts are covered and for this, it was necessary to present basic notions of Number Theory, including the theory and result of Divisibility, Prime Numbers, Congruence and Fermat's Little Theorem. Throughout the work, practical implementations were carried out using the Python programming language.

Key-words:RSA encryption, Congruence, Algebra, Prime Numbers.

Lista de ilustrações

Lista de tabelas

Sumário

Introdução

A criptografia é uma ferramenta fundamental para garantir a segurança da informação no mundo digital. Com o crescente volume de dados sendo transmitidos e armazenados eletronicamente, a proteção contra acessos não autorizados se tornou uma prioridade. Entre os diversos métodos de criptografia existentes, o RSA(Rivest-Shamir-Adleman) destaca-se por sua robustez e ampla aplicação em sistemas de comunicação segura.

Desenvolvido em 1977, o RSA é um algoritmo de criptografia assimétrica que utiliza um par de chaves, uma pública e uma privada, para codificar e decodificar mensagens. A segurança do RSA baseia-se em fatorar um número grande em seus componentes primos, um problema matemático que, até hoje, não possui uma solução eficiente.

Este trabalho tem como objetivo mostrar o algoritmo de criptografia RSA e demonstrar sua eficácia através de uma implementação prática utilizando a linguagem de programação Python.

A escolha do Python como ferramenta de implementação se dá pela sua simplicidade e poderosa capacidade de manipulação de dados, tornando-o ideal para esta simulação criptográfica. O estudo busca alcançar os seguintes objetivos específicos:

- (I) entender os fundamentos teóricos do algoritmo RSA;
- (II) implementar o algoritmo RSA em Python.

A metodologia adotada inclui o desenvolvimento de um programa em Python que simula o processo da criptografia e descriptografia RSA.

A estrutura deste trabalho está da seguinte forma: inicialmente será feita uma revisão da fundamentação matemática referente aos conceitos e noções básicas da Teoria dos Números. Na sequência, abordaremos a Criptografia, apresentando os tipos de cifras simétrica e assimétrica, além da utilização de matrizes na criptografia. Posteriormente, detalharemos a metodologia da Criptografia RSA e sua implementação na linguagem Python. No capítulo final, será apresentada a conclusão. Dessa forma, o objetivo deste estudo é contribuir para a compreensão da segurança que a Criptografia RSA proporciona.

1 Fundamentação Matemática

Este trabalho compila diversas fórmulas, teorias, teoremas e conceitos matemáticos, extraídos de fontes acadêmicas reconhecidas. O objetivo deste tópico é fornecer uma base teórica para compreensão dos temas abordados. Os tópicos incluem a divisibilidade dos números inteiros, números primos e congruências. As informações foram retiradas de livros, artigos de pesquisa e dissertações, para assegurar precisão e confiabilidade dos dados apresentados. Cada seção do trabalho está fundamentada em referências específicas que foram consultadas para a elaboração do conteúdo. Para isto, nos baseamos na seguintes literaturas (CERQUEIRA et al., (Ufal)), (COUTINHO, 1997), (HEFEZ,),(JORGE, 2012),(LOPES, 2011), (SANTOS, 1998).

1.1 Teoria dos Números

A Teoria dos Números é um tema em matemática cujo propósito é investigar a origem dos números, as inter-relações entre eles e suas propriedades intrínsecas. O principal objetivo deste campo de estudo é a análise das propriedades dos números inteiros positivos. Este estudo visa explorar os principais conceitos e teoremas dessa área, com foco na divisibilidade, números primos, congruências e suas aplicações, particularmente no sistema de criptografia RSA.

1.2 Números Inteiros

Para começarmos, o ponto de partida será admitir que o leitor esteja familiarizado com o conjunto dos números inteiros.

Definição 1.2.1. Os números inteiros, denotados pela letra $\mathbb{Z}$, é o conjunto formado por números naturais e ou, o oposto dos números naturais e o elemento neutro 0.

O conjunto dos números inteiros é infinito e pode ser expresso como:

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

1.2.1 Propriedades dos Números Inteiros

As operações de adição $(a, b) \to a + b$ e de multiplicação $(a, b) \to a.b$ em $\mathbb{Z}$, possuem as seguintes propriedades.

1. A adição e a multiplicação são bem definidas: Para todos $a, b, a', b' \in \mathbb{Z}$ se $a = a'$ e $b = b'$ então $a + b = a' + b'$ e $a.b = a'.b'$

2. A adição e a multiplicação são **associativas:** $\forall a, b, c \in \mathbb{Z}$ tem-se que:

$$a + (b + c) = (a + b) + c \ \ e \ \ a.(b.c) = (a.b).c$$

3. A adição e a multiplicação são **comutativas:** $\forall a, b \in \mathbb{Z}$ tem-se que:

$$a + b = b + a \ e \ \ a.b = b.a$$

4. A adição e a multiplicação possuem **elementos neutros:** $\forall a \in \mathbb{Z}$ tem-se que:

$$a + 0 = 0 + a = a \ e \ \ a.1 = 1.a = a$$

5. A adição possui **elemento simétrico:** $\forall a \in \mathbb{Z}$, existe um único elemento que será chamado oposto de a é indicado por $(b = -a)$ tem-se que:

$$a + b = 0$$

6. Na matemática, as operações de multiplicação e soma estão conectadas pelo axioma da **distributividade:** $\forall a, b, c \in \mathbb{Z}$, tem-se que:

$$a.(b + c) = a.b + a.c = (a.b) + (a.c)$$

Nem sempre se trabalha com esse conjunto munidos das operações de adição e multiplicação que possuem as propriedades acima. Neste caso esses elementos de tais conjuntos, juntamente com as suas operações, estão sujeitos às leis básicas da aritmética, que se chama de anel, como por exemplo, os números reais, números racionais e os números complexos, munidos das respectivas operações de adição e multiplicação, são anéis. Como existem de outros conjuntos sujeitos às leis básicas, os axiomas acima não caracterizam os inteiros, a seguir será mostrado os axiomas que faltam para diferenciar o conjunto dos inteiros desses conjuntos. O conjunto dos inteiros pode ser particionado em três subconjuntos $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-\mathbb{N}\}$, onde $\{-\mathbb{N}\}$ é o conjunto simétrico dos elementos de $\mathbb{N}$ vejamos uma consequência desses axiomas:

Proposição 1. $a.0 = 0 \ \forall a \in \mathbb{Z}$. Pois,

Demonstração.

$$a.0 = a(0 + 0) = a.0 + a.0$$

o que implica que

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

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

$$0 = a.0$$

□

Proposição 2. A adição é cancelativa com respeito à igualdade. $\forall a, b, c \in \mathbb{Z}$,

$$a = b \Leftrightarrow a + c = b + c$$

Demonstração. Como a adição está bem definida, segue que $a = b \Rightarrow a + c = b + c$ (propriedade 1). Suponha que

$$a + c = b + c$$

Somando $(-c)$ a ambos os lados:

$$a + c - c = b + c - c$$

$$a = b$$

Obtemos o desejado. □

Exemplo 1.2.1. Se $a + b = 0$, então $b = -a$ e $a = -b$. Começaremos com $b = -a$ para $a + b = 0$.

$$a + b = 0$$

$$a + b = a - a$$

$$b = -a$$

Agora para $a = -b$.

$$a + b = 0$$

$$a + b = b - b$$

$$a = -b$$

Portanto $a + b = 0$, então $b = -a$ e $a = -b$.

1.2.2 Divisibilidade dos números inteiros

A divisibilidade é um conceito fundamental na Teoria dos Números. Formalmente, podemos defini-lá da seguinte maneira:

Definição 1.2.2. Dados $a, b \in \mathbb{Z}$. Dizemos que a divide b quando existir algum inteiro $c \in \mathbb{Z}$ tal que

$$b = a.c$$

Neste caso, diremos também que a é um divisor ou um fator de b, ou ainda, b de dividendo ou que b é divisível por a e c o quociente.

A notação para indicar que a divide b é $a \mid b$ enquanto que, a não divide b a notação é $a \nmid b$, a negação dessa sentença, indica que não existe nenhum número inteiro c tal que $b = c.a$.

Vejamos alguns exemplos para ilustrar a definição.

Exemplo 1.2.2. Sejam os números inteiros 4 e 12. Observe que $4 \mid 12$, pois tomando $c = 3$, temos que $12 = 4.3$.

Exemplo 1.2.3. Sejam os números inteiros 7 e 42. Note que $7 \mid 42$, pois 42 é múltiplo de 7, porque existe $c \in \mathbb{Z}$, a saber c=6, tal que $42 = 7.6$.

Exemplo 1.2.4. Sejam os números inteiros -25 e 2325.Observe que 2325 é múltiplo de -25, pois $-25 \mid 2325$, logo então existe $c \in \mathbb{Z}$, tal que $2325 = (-25)(-93)$ neste caso $c = -93$.

Exemplo 1.2.5. Sejam os números inteiros 54 e 1524. Neste caso não há existência de $c \in \mathbb{Z}$, pois para c=28 e c=29, temos $28.(54) = 1512$ e $29.(54) = 1566$, pois entre dois números inteiros consecutivos não há existência de algum número inteiro. Portanto $54 \nmid 1524$.

Proposição 3. Sejam a, b, $c \in \mathbb{Z}$. Então:

- (i) $1 \mid a$, $a \mid a$ e $a \mid 0$.
- (ii) $a \mid b \Leftrightarrow |a|$ divide $|b|$.
- (iii) Se $a \mid b$ e $b \mid c$, então $a \mid c$.
- (iv) Se a divide $|b|$, então $a \mid b$.
- (v) $a \mid b$ e $b \neq 0 \Rightarrow |a| \leq |b|$.

A seguir, apresento a prova de cada um dos itens.

Demonstração.

(i) Basta observar que: $0 = 0.a$, $a = a.1$ e $a = 1.a$

□

Demonstração.

(ii) Se $a \mid b$ então existe $c \in \mathbb{Z}$ tal que $b = a.c$. Tomando $|b|$, dá-se

$$|b| = |c.a| = |c|\,|a|$$

logo $|a|\,||b|$, ou seja, $|a|$ divide $|b|$. Agora se $|a|$ divide $|b|$, então existe $c \in \mathbb{Z}$ de forma que $|b| = |a|\,.c$ Além do mais se $b \geq 0$, sabemos que

$$|b| = b$$

ou se $b < 0$, sabemos que

$$|b| = -b$$

Do mesmo modo, se $a \geq 0$, sabemos que

$$|a| = a$$

ou se $a < 0$, então

$$|a| = -a$$

Analogamente para os casos ($a \geq 0$ *e* $b < 0$) e ($a < 0$ *e* $b < 0$). □

Demonstração.

(iii) Se $a \mid b$ e $b \mid c$ então $a \mid c$. Assim existe k_1 e k_2 inteiros tais que:

$$b = a.k_1$$

$$c = a.k_2$$

Substituindo a primeira pela segunda igualdade, obtemos

$$c = (ak_1)k_2 \Rightarrow c = a(k_1k_2)$$

Como k_1 e k_2 é um número inteiro pois o produto de dois inteiros, podemos definir $k = k_1k_2$. Assim temos

$$c = ak$$

Ou seja,

$$a \mid c$$

□

Demonstração.

(iv) Por hipótese, existe $c \in \mathbb{Z}$ tal que $|b| = a.c$, se $b \geq 0$ sabemos que

$$|b| = b$$

ou se $b < 0$ então

$$|b| = -b$$

Agora se $b \geq 0$, temos que

$$b = a.c$$

isto é a divide b. Por outro lado no caso em que $b < 0$ temos

$$-b = c.a \Leftrightarrow b = (-c).a$$

ou seja, $a|b$. □

Demonstração.

(v) De fato como $a|b$ então existe um $c \in \mathbb{Z}$ com $(c \neq 0)$ tal que

$$b = a.c$$

Tomando o módulo de b, temos

$$|b| = |a.c| = |a|.|c|$$

Com $b \neq 0$ e $c \neq 0$ e por isso

$$|c| \neq 0 \Rightarrow |c| \geq 1$$

De fato de $|c| \geq 1$, vai existir $q \in \mathbb{Z}_+$ tal que

$$|c| = 1 + q$$

segue

$$|b| = (1 + q)|a| = |a| + |a|q$$

com outras palavras $|a| \leq |b|$. □

Proposição 4. Se a, b, c, $d \in \mathbb{Z}$ com $a \neq 0$ e $c \neq 0$, então

$$a \mid b \;\; e \;\; c \mid d \Rightarrow ac \mid bd$$

.

Demonstração. Se

$$a \mid b \;\; e \;\; c \mid d$$

então existem $m, n \in \mathbb{Z}$ tais que:

$$b = am \;\; e \;\; d = cn$$

então

$$bd = (am)(cn) = (ac)(mn)$$

Portanto,

$$ac \mid bd.$$

□

Proposição 5. Sejam a, b, c, $d \in \mathbb{Z}$, tais que:

$$a \mid (b \pm c) \;\; \textit{então}, \;\; a \mid b \Leftrightarrow a \mid c$$

Demonstração. Suponha que

$$a \mid (b + c)$$

assim existe $m \in \mathbb{Z}$ tal que

$$b + c = am$$

se por outro lado $a \mid b$, então existe $n \in \mathbb{Z}$ tal que pode ser representado como

$$b = an$$

unificando a igualdade, chegando à conclusão de que

$$an + c = am \Rightarrow c = am - an = a(m - n)$$

Portanto $a \mid c$. Agora, se

$$a \mid (b - c) \; e \; a \mid b$$

assim existem $m, n \in \mathbb{Z}$ tais que

$$b - c = am \;\; e \;\; b = an$$

$$c = b - am = an - am = a(n - m)$$

unificando a igualdade, $c = a(n - m)$, portanto $a \mid c$.

Analogamente, mostra-se que $a \mid c \Rightarrow a \mid b$ □

Proposição 6. Sejam a, b, c, $d \in \mathbb{Z}$, tais que:

$$a \mid b \ \ e \ \ a \mid c$$

então, para todo $x, y \in \mathbb{Z}$,

$$a \mid (bx + cy)$$

Demonstração. Do fato que

$$a \mid b \ \ e \ \ a \mid c$$

existem dois números $m, n \in \mathbb{Z}$ tais que

$$b = am \ \ e \ \ c = an$$

agora, realizaremos a operação de multiplicação nas duas igualdades, multiplicando os números inteiros x e y, respectivamente, resultando em $bx = (am)x$ e $cy = (an)y$. Por fim temos,

$$bx + cy = (am)x + (an)y$$

ao ordenar os termos, chegamos à conclusão de que,

$$bx + cy = (mx + ny)a$$

donde conclui-se $a \mid (bx + cy)$. □

Com os resultados expressados nessa subseção e dada as definições, conseguimos entender e falar da Divisão Euclidiana.

1.2.3 Divisão Euclidiana

É sempre possível efetuar a divisão de a por b, com resto, mesmo quando $b \neq 0$ não divide o número inteiro por a, esse fato já era conhecido por Euclides, porém sem demonstração, em "Os Elementos".

Teorema 1.2.1 (Princípio da Boa Ordem)**.** Todo subconjunto não vazio do conjunto dos naturais possui um menor elemento.

Proposição 7. Dados dois números inteiros a e b quaisquer, com $b \neq 0$ existe $n \in \mathbb{Z}$ tal que $nb > a$.

Teorema 1.2.2 (Algoritmo da Divisão)**.** Sejam a, b, dois números inteiros, com $b \neq 0$. Existem únicos números inteiros q, r tais que:

$$a = bq + r, \ 0 \leq r < |b|$$

Demonstração. A demonstração será dividida em duas etapas: a existência e a unicidade.

Existência: Considere o conjunto $X = \{a - bk; k \in \mathbb{Z}\}$, pela Proposição 7 existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$ e assim $a - bn > 0$. Este conjunto contém todos os valores que podem ser subtraindo múltiplos de b de a. O conjunto X é não vazio, pois quando $k = 0$ contém a e pelo Teorema 1.2.1 existe um menor elemento em X, que chamamos de r. Assim temos,

$$r = a - bq$$

para algum $q \in \mathbb{Z}$.

Precisamos mostrar que $0 \leq r < |b|$. Se $r < 0$, podemos escrever,

$$r = a - bq < 0$$

implica que

$$a < bq$$

Assim podemos escolher $k = q + 1$, e obter $b(k) = b(q + 1) = bq + b$ o que proporciona o próximo múltiplo de b. Reescrevendo a:

$$a < b(q + 1)$$

escrevendo a como a soma do próximo múltiplo de b e a diferença que leva até a:

$$a = b(q + 1) + (r + b)$$

onde $r + b > 0$ e $r + b < |b|$ se $|b| > 0$. Isso contradiz a escolha de r como o menor elemento, portanto r deve ser não negativo.
Agora, se $r \geq |b|$, podemos novamente escolher k de forma que:

$$r - |b| = a - bq - |b| \geq 0$$

levando a uma nova escolha de q, contradizendo, pois o fato de r ser o menor elemento. Portanto, $r < |b|$

Unicidade: Suponhamos que existem dois pares (q_1, r_1) e (q_2, r_2) que satisfazem a relação: $a = bq_1 + r_1$ e $a = bq_2 + r_2$ então temos:

$$bq_1 + r_1 = bq_2 + r_2$$

rearranjando, obtemos,

$$bq_1 - bq_2 = r_2 - r_1$$

$$b(q_1 - q_2) = r_2 - r_1$$

Como $0 \leq r_1 < |b|$ e $0 \leq r_2 < |b|$, temos $|r_2 - r_1| < |b|$. Assim, $b(q_1 - q_2)$, é um múltiplo de b e está restrito ao intervalo $(-|b|, |b|)$. Portanto $q_1 - q_2 = 0$, ou seja, $q_1 = q_2$ e consequentemente $r_1 = r_2$.

□

Vejamos alguns exemplos.

Exemplo 1.2.6. Sejam os números inteiros 263 e 12. Existem e são únicos os inteiros, sendo o quociente 21 e o resto 11 isto é,

$$263 = 12(21) + 11.$$

Exemplo 1.2.7. A divisão euclidiana de 5.021 por 20 resulta em um quociente de 251 e um resto 1. Ou seja, ao dividir 5.021 por 20, obtemos:

$$5.021 = 20(251) + 1$$

Comentário: A validade do Teorema é crucial do fato de que $b \neq 0$, pois $r = a$ e q seriam qualquer inteiro se $b = 0$, isso torna inconstante a existência de $0 \leq r < |b|$ e a singularidade do próprio q.

1.2.4 Máximo Divisor Comum - MDC

Nesta subseção queremos saber se existe um número inteiro positivo que pertença ao conjunto dos divisores de dois números inteiros distintos, ambos não nulos, como o nome sugere que seja o maior divisor possível e capaz de dividir simultaneamente ambos os números, existindo esse elemento, vamos chamar de máximo divisor comum entre dois números inteiros.

Definição 1.2.3. Sejam $a, b \in \mathbb{Z}$, não simultaneamente nulos, o máximo divisor comum entre os números inteiros a e b é o maior inteiro positivo d que satisfaz as seguintes condições:

- (i) d é um divisor comum de a e b.
- (ii) Se d' é um divisor comum de a e b, então $d'|d$.

Vejamos alguns exemplos:

Exemplo 1.2.8. Repare os números inteiros 30 e 24. Enumerando o conjunto desses números, no qual é denotado por $D(30)$ e $D(24)$. Sendo assim o

$$D(30) = \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15\, e\, \pm 30\}$$

e

$$D(24) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12\, e\, \pm 24\}$$

Mas os divisores em comum entre o 30 e 24 vão ser $\pm 1, \pm 2, \pm 3\ e\ \pm 6$ e o máximo divisor comum é o 6, isto é, o mdc(30,24)=6.

Um teorema importante e eficiente para descobrir o máximo divisor comum, será enunciado e provaremos, esse teorema é chamado de Bézout, por conta do matemático Étienne de Bézout, nasceu no ano de 1730 na cidade de Nemours e morreu em 1783 na França em comuna da Avon.

Teorema 1.2.3 (Teorema de Bézout)**.** Dados a e b números inteiros, existe x,$y \in \mathbb{Z}$ tais que:

$$ax + by = mdc(a, b)$$

Demonstração. Seja $B = \{ax + by; x, y \in \mathbb{Z}\}$. Sabemos que existem elementos negativos em B. Seja $c = ax + by$ o menor número positivo em B, suponha por contradição que $c \nmid a$ e $c \nmid b$, se c não divide a, pelo teorema da divisão existem q,$r \in \mathbb{Z}$ tais que

$$a = qc + r\ \ em\ \ 0 < r < c$$

assim temos que $r = a - qc = a - q(ax + by) = a - qax - qby = a(1 - qx) + (-qy)b$, ou seja, r é combinação linear de a e b e $0 < r < c$ contradição! Pois c é o elemento mínimo de B. Logo $c|a$.
Analogamente nos mostra que $c|b$. Portanto $c|a$ e $c|b$.
Como $d = mdc(a, b)$ e c é um divisor comum, então $c \leq d$. Sabemos que existem q_1,$q_2 \in \mathbb{Z}$ tais que

$$a = q_1 d\ \ e\ \ b = q_2 d$$

logo

$$c = ax + by = xq_1 d + yq_2 d \tag{1.1}$$

$$= d(q_1 x + q_2 y) \tag{1.2}$$

logo $d \leq c$. Portanto $c \leq d$ e $d \leq c$, assim só podendo ser $d = c$. □

Vejamos alguns exemplos abaixo:

Exemplo 1.2.9. Sejam o mdc(17,153), sabemos que 153 é múltiplo de 17, logo o resto é zero, pois 153=17.9+0, agora substituindo na forma do Teorema 1.2.3 temos que:

$$d = ax + by$$

$$d = 153.x + 17.y$$

$$17 = 153x + 17y$$

$$17 = 153.0 + 17.1$$

logo $x = 0$ e $y = 1$.

Exemplo 1.2.10. Sejam o mdc(117,104)=13 pois,

$$117 = 104 + 13$$

subtraindo (104) ambos os lados da igualdade temos,

$$117 - 104 = 13 + 104 - 104$$

$$13 = 117 - 104$$

$$13 = 117.1 - 104.1$$

logo $x = 1$ e $y = 1$.

1.3 Números Primos

Um número primo é um número natural maior que 1 que não pode ser dividido por nenhum outro número natural além de 1 e ele mesmo, em outras palavras possui exatamente dois divisores positivos distintos: 1 e ele próprio.

Definição 1.3.1. Um número natural maior que 1 que só possui como divisores positivos 1 e ele próprio é chamado de número primo.

Observação: O único número par primo é o número 2. Pois de fato 2, satisfaz a Definição 1.3.1. Sendo seus únicos divisores $\pm 1, \pm 2$, os outros números pares como por exemplo o 6 não satisfaz, pois terá mais que quatro divisores como $\pm 1, \pm 2, \pm 3$ contrariando a definição.

Veja o exemplo a seguir:

Exemplo 1.3.1. O número 7 é primo, pois os únicos divisores são ± 1 *e* ± 7. Agora por outro lado, o número 20 é composto uma vez que seus divisores são $\pm 1, \pm 2, \pm 4, \pm 5, \pm 10$ *e* $\pm$ 20.

Decorrente da Definição 1.3.1. Dados dois números primos p e q, seguem os seguintes fatos:

- (i) Se $p|q$, então $p = q$
  De fato, q sendo primo e $p \mid q$, temos que $p = 1$ ou $p = q$. E p primo, isto é $p > 1$, o que acarreta $p = q$.

- (ii) Se $p \nmid a$, então $mdc(p, a) = 1$
  De fato, se $mdc(p, a) = d$, então d divide p e divide a. Do fato, $d|p$ temos $d = p$ ou $d = 1$, por hipótese $p \nmid a$ temos que $d = \pm 1$ e como $d > 0$, consequentemente $d = 1$.

  Proposição 8 (Lema Euclides)**.** Sejam $a, b, p \in \mathbb{Z}$ com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

  Demonstração. Suponha que $p \nmid a$, isso significa que a e p são coprimos, ou seja, o $mdc\,(p, a) = 1$ pelo Teorema 1.2.3, existe uma combinação linear a e p que resulta em 1, ou seja, existem inteiros x e y tais que,

  $$ax + py = 1$$

  multiplicando ambos os lados da equação por b, obtemos

  $$bax + bpy = b$$

  Sabemos que $p \mid ab$, existe algum inteiro k tal que $ab = kp$. Substituindo ab na equação anterior,

  $$kpx + bpy = b$$

  e reescrevendo a equação

  $$p(kx + by) = b$$

  isso mostra que b é uma combinação de p, esta equação implica que $p \mid b$. Pois se $p \nmid a$, então deve dividir b.

  □

  Corolário 1. Se $p, p_1, ..., p_n$ são números primos e, se $p \mid p_1, ...p_n$, então $p = p_i$ para algum $i \in \{1, 2, ..., n\}$.

Teorema 1.3.1 (Teorema Fundamental da Aritmética)**.** Todo número natural maior que 1 pode ser representado de modo único como produto de fatores primos (a menos a ordem de fatores).

Demonstração. Existência: Seja $n > 1$, se n é primo, não há nada a ser feito.

Suponha que n é composto. Seja $p_1 < n$ e maior que 1 e afirmamos que p_1 é primo.

Afirmação: p_1 é primo.

Se não for primo, caso contrário, teríamos que $p_1 = p_1^{'}.p_1^{''}$. Logo $p_1 = p_1^{'} < p_1$ e $p_1 = p_1^{'} \mid n$, contradição! Pois $p_1^{'}$ é divisor de n, logo $p_1^{'}$ de fato é número primo.

Agora temos $n = p_1.n_1$ se n_1 for primo, paramos por aqui, mas suponha que n_1 é composto. Seja p_2 o menor divisor de n_1 que é maior que 1 note que analogamente p_2 é primo, assim, $n = p_1.p_2.n_2$. Repetindo esse procedimento, obtemos uma sequência decrescente de inteiros positivos $n_1, n_2, n_3, ..., n_r$, como são inteiros maiores que 1, este processo deve terminar e como os primos na sequência $p_1, p_2, ..., p_k$ necessariamente não são distintos, obtemos em geral n na forma $n = p_1^{a_1}.p_2^{a_2}...p_k^{a_k}$

Pela Unicidade: Usamos a Indução Forte em n. Para $n = 2$, a afirmação é verdadeira, pois há nada a ser feito, porque 2 é um número primo.

Assumimos, então que ela se verifica para todos os inteiros maiores que 1 e menores que n. Se n for primo, então há nada ser feito. Agora supondo que n seja composto e que tenha duas fatorações, isto é, sejam $n = p_1p_2...p_s$ e $n = q_1q_2...q_r$, vamos provar $s = r$ e que $p_i = q_j$, assim temos que $p_1 \mid q_1q_2...q_r$, ele divide pelo menos um dos fatores q_j. Sem perda de generalidade, podemos supor que $p_1 \mid q_1$, como ambos são primos isto implica $p_1 = q_1$. Então temos $n = p_1p_2...p_s$ e $n = q_1q_2...q_r$ porém $p_1 = q_1$ logo $n = p_1q_2...q_r$. Como $\frac{n}{p_1} < n$, segue da hipótese de indução que a fatoração é única, isto é, $s = r$, logo a fatoração $p_2...p_s$ e $q_2...q_r$ são iguais (a menos de ordem). □

Exemplo 1.3.2. O número 252 pode ser decomposto em fatores primos, pois $252 = 2.2.3.3.7$, já que na fatoração pode houver primos iguais, podemos agrupar de modo que $252 = 2^2.3^2.7$.

Teorema 1.3.2 (Teorema de Euclides)**.** A sequência dos números primos é infinita.

Demonstração. Suponha que a sequência dos números primos seja finita, ou seja, $p_1, p_2, ..., p_n$. Sem perda de generalidade, $p_1 < p_2 < ... < p_n$. Consideramos o número $b = p_1.p_2...p_{n+1}$ que não é divisível por nenhum dos p_i desta lista e $b > p_i$. Mas pelo Teorema 1.3.1, ou b é primo ou possui algum fator primo, implica que existe algum primo que não pertence à lista. Portanto a sequência dos números primos é infinito. □

Lema 1 (Lema de Erastótenes)**.** Se um número inteiro $n > 1$ não é divisível por nenhum primo p tal que $p^2 \leq n$, então ele é primo.

Demonstração. Por absurdo, suponhamos que n não seja divisível por nenhum número primo p tal que $p^2 \leq n$ e que não seja primo. Se n for composto, segue que existe algum

primo q, o menor número primo que divide n, isto é, $n = qn_1$ para algum $n_1 \in \mathbb{Z}$ com $q \leq n_1$. Ao multiplicar a desigualdade por q, segue daí que $q^2 \leq qn_1 = n$. Logo, n é divisível por um número primo q tal que $q^2 \leq n$ absurdo! □

Note que o Lema 1 também nos fornece um teste de primalidade e consiste em listar os números inteiros de 2 até n em uma tabela, conhecido por o Crivo de Erastótones, começaremos com o primeiro número primo o 2, todos os múltiplos de 2 serão retirados exceto o 2. Assim em seguida para o próximo número que é o 3, como é primo, retiramos todos os múltiplos de 3 exceto ele. Assim sucessivamente para os demais números, utilizaremos dessa estratégia até encontrar o número primo p cujo o valor ao quadrado não supere o n, pois o primeiro valor não "eliminado"será o p^2.

Exemplo 1.3.3. Vamos encontrar os primos entre 2 e 120, utilizando o Crivo de Erastótones, usando o processo de "retirar"os múltiplos de 2, até o primo "p", cujo o valor ao quadrado não supere n, neste caso iremos até o primo 7 pois o próximo número primo é o 11, mas $11^2 = 121$ neste caso ultrapassará o valor do nosso $n = 120$. Portanto os números primos serão os números não riscados na tabela a seguir:

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~
13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~
~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~
37	~~38~~	~~39~~	~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~
~~49~~	~~50~~	~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~	71	~~72~~
73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~	~~81~~	~~82~~	83	~~84~~
~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~	~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~
97	~~98~~	~~99~~	~~100~~	101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~
109	~~110~~	~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~

Comentário: Foram verificados todos os múltiplos dos números primos para retirar da tabela.

Solução: Após serem feitos os cálculos para encontrar os primos entre o 2 e 120, obtemos esses números primos descritos: 2,3,5,7,11,13,17,19,23,29,31, 37,41,43,47,53,59,61,67, 71,73,79,83,89,97,101, 103,107,109 e 113.

2 Aritmética Modular

Neste capítulo iremos abordar a congruência, sua definição e algumas propriedades, para o estudo da Criptografia RSA. Este capítulo será de grande utilidade.

2.1 Congruências

Congruência é um conceito central na teoria dos números e na criptografia.

Definição 2.1.1. Dizemos que dois números inteiros a e b são congruentes *módulo* n se os restos de sua divisão euclidiana de a e b por n são iguais. Matematicamente, escrevemos isso como:

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

lê-se: a côngruo à b módulo n, ou simplesmente a e b são congruentes *módulo* n.

Exemplo 2.1.1. Sejam $n = 5$, $a = 53$ e $b = 93$, observe que $53 \equiv 93\,(mod\ 5)$, aplicando a divisão euclidiana de 53 e 93 por 5, obtemos $53 = 5.10 + 3$ e $93 = 5.18 + 3$, conclui-se que os restos são iguais.

Observação: Se a relação $a \equiv b\,(mod\ 5)$ for falsa, denotamos como $a \not\equiv b\,(mod\ n)$, ou seja, a e b não são congruentes *módulo* n.

Exemplo 2.1.2. Ainda usando o Exemplo2.1.1 e apenas trocando o valor de b que antes era $b = 93$ neste exemplo será $b = 109$ temos que $109 = 5.21 + 4$, logo $53 \not\equiv 109\,(mod\ 5)$, pois observa que os restos são diferentes, no caso $a = 53$ deixa resto 3 e $b = 109$ deixa resto 4.

Definição 2.1.2. Sejam a, b e n números inteiros com $n > 1$, temos que $a \equiv b\,(mod\ n)$ se, e somente se, $n|b - a$.

2.1.1 Propriedades das Congruências

1. **Reflexiva:** $a \equiv a(mod\ n)$;

   Exemplo 2.1.3. Seja $a = 8$ e $n = 5$, então:

   $$8 \equiv 8\,(mod\ 5)$$

   pois $8 - 8 = 0$, e 0 é divisível por qualquer número incluindo o 5.

2. **Simétrica:** Se $a \equiv b(mod\ n)$, então $b \equiv a(mod\ n)$;

Exemplo 2.1.4. Se $a = 8$, $b = 3$ e $n = 5$, então:

$$8 \equiv 3\,(mod\ 5)$$

pois $8 - 3 = 5$, que é divisível pelo número 5 ou também

$$3 \equiv 8\,(mod\ 5)$$

pois $3 - 8 = -5$, também é divisível por 5

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

   Exemplo 2.1.5. Se $a = 12$, $b = 7$, $c = 2$ e $n = 5$, então:

   $$12 \equiv 7\,(mod\ 5)$$

   pois $12 - 7 = 5$ e

   $$7 \equiv 2\,(mod\ 5)$$

   pois $7 - 2 = 5$ e pela Transitividade:

   $$12 \equiv 2\,(mod\ 5)$$

   pois $12 - 2 = 10$, também é divisível por 5

4. **Compatibilidade com Operações:** Se $a \equiv b(mod\ n)$ e $c \equiv d(mod\ n)$, então $a + c \equiv b + d\,(mod\ n)$ e $a.c \equiv b.d\,(mod\ n)$.

   Exemplo 2.1.6. Se $a = 14$, $b = 9$, $c = 7$, $d = 2$ e $n = 5$, então:

   $$14 \equiv 9\,(mod\ 5)$$

   pois $14 - 9 = 5$ e

   $$7 \equiv 2\,(mod\ 5)$$

   pois $7 - 2 = 5$. Então:

   $$a + c \equiv b + d\,(mod\ n)$$
   $$14 + 7 \equiv 9 + 2\,(mod\ 5)$$

   ou seja,

   $$21 \equiv 11\,(mod\ 5)$$

   pois 21 e 11 quando divisível por 5 deixam resto 1.
   Agora para a multiplicação:
   Se $a = 14$, $b = 9$, $c = 7$, $d = 2$ e $n = 5$, então:

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

$$14.7 \equiv 9.2\,(mod\ 5)$$

ou seja,

$$98 \equiv 18\,(mod\ 5)$$

pois 98 e 18 quando divisível por 5 deixam resto 3.

Em outras palavras, dizer que a divide b significa dizer que a divisão de b por a é exata, ou que o resto dessa divisão é zero.

2.2 Teoremas da Aritmética

Nesta seção iremos apresentar alguns teoremas clássicos da aritmética.

Proposição 9. Seja $r_1, \cdots, r_{\phi(m)}$ um sistema reduzido de resíduos *módulo* m e seja $a \in \mathbb{Z}$ tal que $mcd\,(a, m) = 1$. Então $ar_1, \cdots, ar_{\phi(m)}$ é um sistema reduzido de resíduos *módulo* m

Teorema 2.2.1 (Teorema de Euler)**.** Sejam $m, a \in \mathbb{Z}$ com $m > 1$ e $mdc\,(a, m) = 1$. Então,

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

Demonstração. Seja $r_1, \cdots, r_{\phi(m)}$ um sistema reduzido de resíduos *módulo* m. Logo pela Proposição 9, $ar_1, \cdots, ar_{\phi(m)}$ formam um sistema reduzido de resíduos *módulo* m e, portanto,

$$ar_1 ar_2 \cdots ar_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)}\ mod\ m$$

consequentemente,

$$a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} = ar_1 ar_2 \cdots ar_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)}\ mod\ m$$

Como $(r_1 r_2 \cdots r_{\phi(m)})$=1, segue que:

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

□

Teorema 2.2.2 (Pequeno Teorema de Fermat)**.** Sejam $a \in \mathbb{Z}$ e p um número primo tais que $mdc(a, p) = 1$ se $p \nmid a$ então:

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

Demonstração. Basta notar que, sendo p primo $\phi(p) = p - 1$. □

Exemplo 2.2.1. Considerando 55 e encontrando o $\phi(55)$, sabemos que 55=11.5 e o mdc(5,11)=1. Observe que 11 e 5 são números primos, sabemos que $\phi(5) = 4$ e $\phi(11) = 10$. Logo, $\phi(55) = 4.10 = 40$

Teorema 2.2.3 (Teorema do Resto Chinês)**.** Sejam $m_1, m_2, \cdots, m_k$, inteiros positivos, dois a dois coprimos (ou seja, $mdc(m_i, m_j) = 1$ para $i \neq j$). Para cada $i = 1, 2, \cdots, k$, sejam dados inteiros a_i, o teorema afirma que existe um único inteiro x tal que:

$$x \equiv a_i \ (mod\ m_i)$$

para $i = 1, 2, \cdots, k$ e a solução é única *módulo* M, onde $M = m_1.m_2.\cdots.m_k$

Demonstração. Existência: Usando o método de construção para construir a solução x. Defina:

$$M = m_1.m_2.\cdots.m_k$$

para cada i, defina $M_i = \frac{M}{m_i}$, como m_i e M_i são coprimos, podemos aplicar o Teorema de Bezout que garante que existem inteiros b_i tais que:

$$M_i b_i \equiv 1 \ (mod\ m_i)$$

Agora construindo x como:

$$x = \sum_{i=1}^{k} a_i M_i b_i$$

temos por construção:

$$x \equiv a_i M_i b_i \ (mod\ m_i)$$

Como M_i é um múltiplo de m_i, o $M_i \equiv 0 \ (mod\ m_i)$. Portanto satisfaz todas as congruências dadas.

Unicidade: Mostraremos que x é único *módulo* M. Se x_1 e x_2 são duas soluções para o sistema de congruências temos:

$x_1 \equiv \ a_i \ (mod\ m_i)$ e $x_2 \equiv \ a_i \ (mod\ m_i)$ para todo i, então:

$d = x_1 - x_2$ é divisível por cada m_i, logo $d \equiv 0 \ (mod\ m_i)$.

Como $m_1, m_2, \cdots, m_k$ são coprimos, pelo Teorema da Divisão, d é divisível por M.

$$d \equiv 0 \ (mod\ M)$$

Portanto $x_1 \equiv x_2 \ (mod\ M)$, o que mostra que a solução é única *módulo* M.

□

Exemplo 2.2.2. Vamos abordar um desafio sugerido por um matemático chinês chamado Sun-Tsu.. Enunciamos o problema:

Um número deixa resto 2,3 e 2 quando dividido por 3,5 e 7, respectivamente. Qual é este número? Em linguagem matemática, envolvendo congruências lineares, temos:

$$x \equiv 2 \ (mod\ 3) \tag{2.1}$$

$$x \equiv 3 \ (mod\ 5) \tag{2.2}$$

$$x \equiv 2 \ (mod\ 7) \tag{2.3}$$

Primeiramente a identificação dos *módulos* e *resíduos*.

Módulos : $m_1 = 3,\ m_2 = 5\ e\ m_3 = 7$.

Resíduos : $a_1 = 2,\ a_2 = 3\ e\ a_3 = 2$.

O produto dos *módulos* será $M = m_1 m_2 m_3$, ou seja, $M = 2.5.7 = 105$.

O cálculo de M_i será:

$$M_1 = m_2 m_3 = 5.7 = \ 35$$

$$M_2 = m_1 m_3 = 3.7 = \ 21$$

$$M_3 = m_1 m_2 = 3.5 = \ 15$$

Agora precisamos encontrar b_i tais que $M_i b_i \equiv \ 1 \ (mod\ m_i)$ o cálculo será:

Para $i = \ 1$ (com $m_1 = 3$)

$$35b_1 \equiv \ 1 \ (mod\ 3) \ \Rightarrow 2b_1 \equiv \ 1 \ (mod\ 3)$$

Observe que testando $b_1 = 2$, temos:

$$2.2 = \ 4 \equiv \ 1 \ (mod\ 3)$$

Para $i = \ 2$ (com $m_2 = 5$)

$$21b_2 \equiv \ 1 \ (mod\ 5) \ \Rightarrow 1b_2 \equiv \ 1 \ (mod\ 5)$$

Observe que testando $b_2 = 1$, temos:

$$21.1 = \ 21 \equiv \ 1 \ (mod\ 5)$$

Para $i = \ 3$ (com $m_3 = 7$)

$$15b_3 \equiv \ 1 \ (mod\ 7) \ \Rightarrow 1b_3 \equiv \ 1 \ (mod\ 7)$$

Observe que testando $b_3 = 1$, temos:

$$15.1 = \ 15 \equiv \ 1 \ (mod\ 7)$$

Agora montando a solução:

$$x = a_1 M_1 b_1 + a_2 M_2 b_2 + a_3 M_3 b_3$$

$$x = 2.35.2 + 3.21.1 + 2.15.1$$

$$x = 140 + 63 + 30$$

$$x = 233$$

Como $233 \equiv 23$ (mod 105). Portanto o 23 é a solução *módulo* 105 do problema de Sun-Tsu, pois o número que deixa resto 2,3 e 2 quando dividido por 3,5 e 7 respectivamente, é: $x = \ 23 + 105k$ para qualquer $k \in \mathbb{Z}$.

3 Criptografia

A criptografia é a prática e o estudo de técnicas matemáticas para garantir que as comunicações sejam protegidas de observadores indesejados. Em outras palavras, a criptografia é a etapa de conversão dos dados em algo que só pode ser compreendido por quem tem acesso a eles. A palavra criptografia vem do grego: "kryptos", que significa secreto, e "graphein", que se traduz como escrita. Assim, seu significado é "escrita oculta". Deste modo, pode-se compreender a criptografia como um conjunto de métodos e técnicas que permitem cifrar dados legíveis utilizando um algoritmo, possibilitando, mediante um processo reverso, a recuperação das informações originais.

A compreensão da criptografia requer uma série de conceitos fundamentais, que são essenciais para compreender como ela funciona e como pode ser aplicada para proteger dados. Alguns conceitos importantes:

- Textos Comuns são as mensagens originais, não criptografadas.
- Textos Cifrados são as mensagens criptografadas, é o resultado do processo aplicado ao texto comum.
- Chaves de Segurança (chave criptográfica) transforma o texto comum em texto cifrado ou vice-versa.
- Criptografar (cifrar ou encryption) é a técnica utilizada para converter texto comum em texto cifrado, seu intuito é proteger informações, permitindo que somente o destinatário, munido da chave de segurança, possa decifrá-las.
- Descriptografar (decifrar ou decryption) consiste em reverter o processo de criptografar. Requer a utilização da chave de segurança, que possibilita a conversão do texto cifrado para o texto comum. Dessa forma, apenas as pessoas autorizadas conseguem acessar e compreender a informação.

3.1 Tipos de criptografia

3.1.1 Cifras Simétricas

Utiliza-se somente de uma chave, no qual é usada para tanto criptografar o texto comum quanto descriptografar o texto cifrado, neste caso o remetente e o destinatário possuem acesso a mesma chave secreta. A figura 1 representa a descrição da Cifra Simétrica.

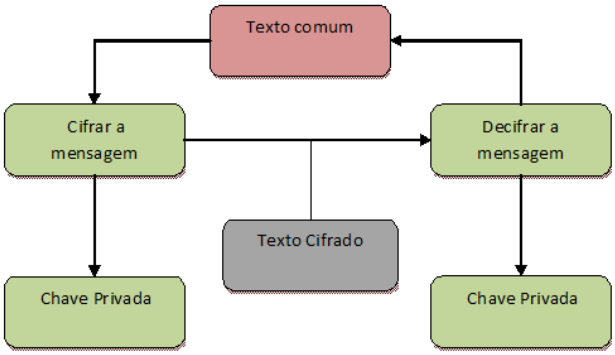

Figura 1 – Modelo de Cifra Simétrica

A cifra simétrica é constituída por duas técnicas, a Cifra de Transposição e de Substituição, porém será omitido neste trabalho qualquer explicação sobre a Cifra de Transposição.

A Cifra de Substituição utiliza-se da troca dos caracteres do texto comum por outras letras, neste caso temos como exemplo a Cifra de César, que é um código secreto simples no qual substitui cada letra do alfabeto por n posições a sua frente.

Exemplo 3.1.1. A frase a ser criptografada será $''ALUNODAFURG''$, ("Aluno da Furg"), utilizando a Cifra de César.

Solução : Por meio da Cifra de César, podemos criptografar a frase pretendida, simplesmente trocar cada letra por outra três posições à frente.

Texto comum:	A	L	U	N	O	D	A	F	U	R	G
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Texto cifrado:	d	o	x	q	r	g	d	i	x	u	j

Note que o Exemplo 3.1.1 o texto foi cifrado a partir da seguinte equivalência alfabética.

Alfabeto comum:	A	B	C	D	E	F	G	H	I	J	K	L	M
	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
Alfabeto cifrado:	d	e	f	g	h	i	j	k	l	m	n	o	p
Alfabeto comum:	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
Alfabeto cifrado:	q	r	s	t	u	v	w	x	y	z	a	b	c

Na ilustração acima, as letras que formam os textos comuns são maiúsculas, enquanto as que formam os textos cifrados são minúsculas, os textos comuns podem ser

representados conforme as regras de qualquer língua, este padrão adotado deve ser interpretado apenas como uma maneira de estruturar este trabalho. Se precisarmos usar outra configuração, as frases serão acompanhadas pelos termos texto comum e texto cifrado.

Com o objetivo de formalizar o processo de criptografar e descriptografar mensagens, de modo geral, adotamos uma ideia intrigante, que envolve a atribuição para cada letra do alfabeto comum um número correspondente.

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

Tabela 1 – Alfabeto comum e a sua equivalência

Conforme a Tabela 1, a cifra de César pode se definida da seguinte forma. Neste caso o texto comum definido como x, e sua equivalente em texto cifrado definido como y, pode atribuir a cada letra do alfabeto qualquer valor numérico valem as relações $y = C\ (3, x) \equiv (x + 3)\, mod\ 26$ e $x = D\ (3, y) \equiv (y - 3)\, mod\ 26$ que respectivamente, representam a cifração e decifração de uma mensagem. Como um deslocamento, que chamamos de k, pode ter qualquer dimensão, ou seja, necessariamente a letra não precisa se mover apenas três posições à frente, podemos generalizar a Cifra de César ao caso geral descrito a seguir:

Definição 3.1.1. Para cada letra em texto comum x, e sua equivalente em texto cifrado y, valem as relações:

$$y = C(k, x) \equiv (x + k)\, mod\, 26 \tag{3.1}$$

$$x = D(k, y) \equiv (y - k)\, mod\, 26 \tag{3.2}$$

onde $0 \leq k \leq 25$.
Caso o $k = 0$ não funcionará pois o texto cifrado será igual o texto comum, se conhecermos que uma mensagem foi criptografada através da cifra de César, portanto, uma análise criptográfica baseada em força bruta pode ser realizada de maneira simples. Apenas é necessário testar a condição $0 < k \leq 25$, ou seja, testar os 25 $k's$ restantes.

3.1.2 Cifras Assimétricas

Utiliza de par de chaves, combinação de uma Chave Privada que é utilizada para descriptografar, pois somente o destinatário pode ter acesso, e uma Chave Pública que

pode ser de conhecimento de qualquer pessoa, neste caso temos a Criptografia RSA que será o foco do trabalho. A figura 2 representa a descrição da Cifra Assimétrica.

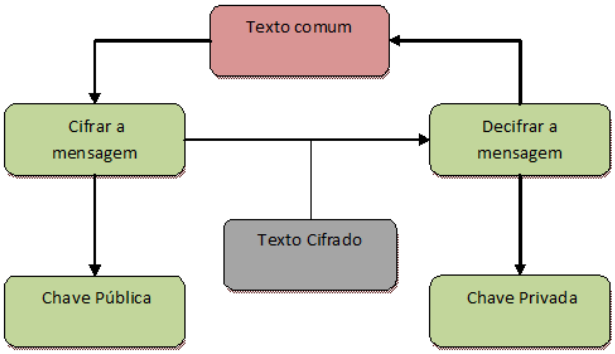

Figura 2 – Modelo de Cifra Assimétrica

Com essa base sólida, conseguimos avançar e se aprofundar no estudo da Criptografia RSA. Vamos estudar o funcionamento do RSA.

3.1.3 Criptografia e matrizes

Agora falaremos um pouco do uso da criptografia envolvendo matrizes, para cifrar e decifrar mensagens sigilosas. Para isso utiliza-se dos conceitos de Álgebra Linear.

Seja A uma matriz com inversa B. O remetente da mensagem usará a matriz A para cifrar o texto comum e para decifrar o texto cifrado o destinatário usará a matriz B. Segue o exemplo abaixo:

$$A = \begin{bmatrix} 5 & 7 \\ 2 & 3 \end{bmatrix} \; e \; B = \begin{bmatrix} 3 & -7 \\ -2 & 5 \end{bmatrix}$$

Antes de realizar um exemplo será criada uma tabela de conversão, ou seja, para codificar a mensagem será usada uma tabela na forma de conversão alfabética para numérica. Segue abaixo a tabela de conversão:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P	Q	R	S	T	U	V	W	X	Y	Z	.	!	@	-
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Tabela 2 – Conversão alfabética para numérica.

O remetente e destinatário devem estar cientes dessa tabela.

Exemplo 3.1.2. O texto para exemplo será MATEMÁTICA APLICADA. Desconsidere os acentos e para cada espaço entre uma palavra e outra usaremos o símbolo @. Logo

M	A	T	E	M	A	T	I	C	A	@	A	P	L	I	C	A	D	A	.
13	1	20	5	13	1	20	9	3	1	29	1	16	12	9	3	1	4	1	27

Tabela 3 – Conversão das letras.

Solução: Começaremos montando a matriz M colocando a sequência de números em uma matriz de duas linhas.

$$M = \begin{bmatrix} 13 & 1 & 20 & 5 & 13 & 1 & 20 & 9 & 3 & 1 \\ 29 & 1 & 16 & 12 & 9 & 3 & 1 & 4 & 1 & 27 \end{bmatrix}$$

Após essa matriz começaremos a codificação, tal que $N = AM$

$$N = \begin{bmatrix} 5 & 7 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 13 & 1 & 20 & 5 & 13 & 1 & 20 & 9 & 3 & 1 \\ 29 & 1 & 16 & 12 & 9 & 3 & 1 & 4 & 1 & 27 \end{bmatrix}$$

$$N = \begin{bmatrix} 268 & 12 & 212 & 109 & 128 & 26 & 107 & 73 & 22 & 194 \\ 113 & 5 & 88 & 46 & 53 & 11 & 43 & 30 & 9 & 83 \end{bmatrix}$$

Mensagem codificada é apresentada pela matriz N, logo: 268, 12, 212, 109, 128, 26, 107, 73, 22, 194, 113, 5, 88, 46, 53, 11, 43, 30, 9, 83.

Assim que o destinatário receber essa mensagem usará a matriz B para conseguir fazer a decodificação e ler o texto.

Sabendo que $B.N = B.A.M = I.M = M$ obtemos $M = B.N$,tal que:

$$M = \begin{bmatrix} 3 & -7 \\ -2 & 5 \end{bmatrix} \cdot \begin{bmatrix} 268 & 12 & 212 & 109 & 128 & 26 & 107 & 73 & 22 & 194 \\ 113 & 5 & 88 & 46 & 53 & 11 & 43 & 30 & 9 & 83 \end{bmatrix}$$

$$M = \begin{bmatrix} 13 & 1 & 20 & 5 & 13 & 1 & 20 & 9 & 3 & 1 \\ 29 & 1 & 16 & 12 & 9 & 3 & 1 & 4 & 1 & 27 \end{bmatrix}$$

Assim o destinatário chega na mensagem do remetente, ou seja, retorna a mensagem original. Logo após achar os números: 13, 1, 20, 5, 13, 1, 20, 9, 3, 1, 29, 1, 16, 12, 9, 3, 1, 4, 1, 27.

Retornando a tabela de conversão das letras para os números descobrirá o texto original que neste exemplo é MATEMÁTICA@APLICADA.

4 Criptografia RSA

É um conjunto de regras e processos desenvolvidos e tem como objetivo proteger determinada informação, ou seja, contra vazamentos.

Atualmente é uma forma mais segura para o destinatário e o remetente, não deixando que outro consiga ler seu conteúdo.

4.1 Algoritmo RSA

A descrição do RSA inclui explicações sobre as fórmulas usadas para codificar e decodificar mensagens. Mas lembre-se de que descriptografar significa passar da mensagem criptografada para a mensagem original. Portanto, nossa tarefa neste capítulo não se limita a descrever fórmulas de codificação e decodificação. A sigla RSA corresponde às letras iniciais dos nomes daqueles que inventaram o código, R. L. Rivest, A. Shamir e L. Adleman, em 1977. Os algoritmos consistem em uma série limitada e organizada de etapas que buscam alcançar a resolução de uma questão específica. O Algoritmo RSA, também conhecido como Criptografia RSA e formado por três etapas: Pré-Codificação, Codificação e Decodificação serão abordados ao longo deste capítulo. A figura3 representa a descrição do Algoritmo RSA.

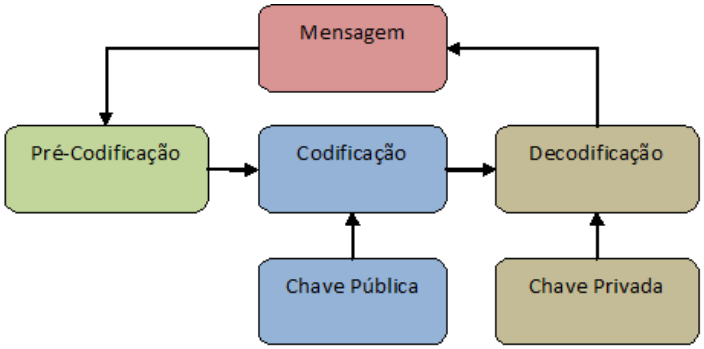

Figura 3 – Descrição para o Algoritmo RSA

4.1.1 Aquisição das chaves do Algoritmo RSA

O RSA configura-se como um exemplo de Criptografia Assimétrica, em outros termos, utilização de par de chaves, uma Chave Pública (e, n) e outra Chave Privada (d, n). Alguns pontos a serem considerados ao criar as chaves:

1. Escolher dois números primos, representados por este trabalho p e q sendo $p \neq q$.
2. Calcule o n que é definido como $n = pq$.
3. Calcule o $\Phi(n) = (p-1).(q-1)$.
4. Escolher $e \in \mathbb{Z}$ tal que $1 < e < \Phi(n)$, de forma para ter unicidade do inverso o $mdc = (e, \Phi(n)) = 1$.
5. Calcule o $d \in \ Z^*{}_+$ de forma que $ed \equiv 1(mod\Phi(n))$, isto é, encontrar o d, que é o inverso multiplicativo de e módulo $\Phi(n)$.
6. A chave Pública: o par (e, n).
7. A chave Privada: o par (d, n).

Exemplo 4.1.1. Para obter as chaves pública e privada, seguimos os passos 1 a 5, que serão empregadas ao longo deste trabalho.

1. Escolheremos o $p = 5$ e $q = 11$.
2. Como o $p = 5$ e $q = 11$, logo $n = 5.11 = 55$.
3. Conforme o $\Phi(n) = (p-1).(q-1)$, então $\Phi(n) = (5-1).(10-1) = 4.10 = 40$.
4. Escolhe-se $e = 3$, visto que $1 < 3 < 40$ e o $mdc = (3, 40) = 1$.
5. O $\Phi(n) = 40$ e $e = 3$,logo.

   $$3d \equiv 1(mod\ 40)$$

   equivale

   $$40|3d - 1$$

   sendo que existe um k que é um número inteiro positivo. Portanto

   $$3d = 40k + 1 \tag{4.1}$$

   repare que,

   $$3.27 = 40.2 + 1 \tag{4.2}$$

   Observe que a Equação 4.1 e a Equação 4.2, conseguimos então encontrar o $d = 27$. Portanto a Chave Pública $(3, 55)$ e a Chave Privada $(27, 55)$.

4.2 Pré-Codificação

Primeiramente converte-se a mensagem em sequências de números, para evitar ambiguidade os números são escolhidos a partir de dois algarismos, começando do 10, pois se fosse escolhido $A = 1$, $B = 2$, conforme for o número 12 seria a letra L e caso fosse escolhido AB juntos, também seriam 12 o que não pode acontecer. Além disso, desconsidera-se os acentos das palavras será constituída apenas por letras e o espaço entre uma palavra e outra será denotada pelo número 99. A Tabela 4.2 apresenta as letras convertidas em números.

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

Tabela 4 – Correspondência entre as letras e os números para a pré-codificação.

Exemplo 4.2.1. Para melhor entender a pré-codificação, vamos escrever a frase MATEMÁTICA APLICADA.

Solução : Como a frase é MATEMÁTICA APLICADA, lembrando que não usaremos os acentos e o espaço entre uma palavra e outra será preenchido com o número 99.

M	A	T	E	M	A	T	I	C	A		A	P	L	I	C	A	D	A
22	10	29	14	22	10	29	18	12	10	99	10	25	21	18	12	10	13	10

Tabela 5 – Conversão das letras para os números.

Assim a frase MATEMÁTICA APLICADA, observa-se que as letras foram convertida em números, fica:

22102914221029181210991025211812101310

Ainda na pré-codificação precisamos quebrar a frase que foi convertida em números em blocos, mas antes de tudo usamos dois números primos conforme o Exemplo 4.1.1 e esses blocos são obrigatoriamente menores que o produto dos dois primos, logo $b : b < n$. Continuando com o Exemplo 4.1.1, sabemos que nosso $p = 5$ e $q = 11$ nosso $n = 55$, logo nosso $b : b < 55$. Portanto quebrando os números em blocos, resultará em:

BLOCOS
22-10-29-14-22-10-29-18-12-10-9-9-10-25-21-18-12-10-13-10

O critério de formação dos blocos pode ser usado de várias maneiras como quebrar em dois algarismo, em três ou até mesmo em um algarismo mas nunca sendo maior que o n, entretanto precisa ter alguns cuidados como por exemplo quebrar o bloco começando pelo zero, pois ao decodificar não saberíamos a diferença.

4.3 Codificação

Começamos com os blocos transformados pela pré-codificação, e por fim a regra para a codificação.

Definição 4.3.1. Seja o par de Chave Pública (e, n), e a é o resto da divisão de b^e por n, denotado por $C(b)$ isto significa

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

com $1 \leq C(b) < n$ logo,

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

Para compreender como codificamos continuaremos usando o Exemplo 4.2 usados para a pré-codificação.

Solução: Usaremos a regra $C(b) \equiv b^e (mod\, n)$, com os blocos: 22-10-29-14-22-10-29-18-12-10-9-9-10-25-21-18-12-10-13-10.

Para $C(22)$:

$$C(22) \equiv 22^3 (mod\, 55)$$
$$C(22) \equiv 10.648\, (mod\, 55)$$
$$C(22) \equiv 33\, (mod\, 55)$$

Observação: $C(22)$ é igual a 22^3 (ou seja, 22 elevado a 3) módulo 55. Calculando $22^3 = 22 * 22 * 22 = 10.648$. Isto é $C(22) \equiv 10.648\, (mod\ 55)$. Precisamos reduzir 10.648 módulo 55, ou seja, queremos determinar o resto da divisão de 10.648 por 55.

Dividindo $10.648 \div 55 = 193,6$ como o resultado é um valor não inteiro, podemos verificar que o quociente é 193 e o resto é 33, pois fazendo o cálculo conseguimos descobrir o resto, observe que $10.648 \div 55 = 193,6$ agora pega o valor inteiro e diminui, ou seja, $193,6 - 193 = 0,6$ após multiplica pelo 55 que neste caso é o módulo, assim $0,6 * 55 = 33$ encontramos o resto.

Portanto $C(22) \equiv 33\, (mod\, 55)$.Confere os demais blocos.

Para $C(10)$:

$$C(10) \equiv 10^3 (mod\, 55)$$
$$C(10) \equiv 1.000\, (mod\, 55)$$
$$C(10) \equiv 10\, (mod\, 55)$$

Observação: $C(10)$ é igual a 10^3 módulo 55. Calculando $10^3 = 1.000$. Isto é $C(10) \equiv 1.000\, (mod\ 55)$.

Dividindo $1.000 \div 55 = 18,1818$, calculando o resto $18,1818 - 18 = 0,1818$ após multiplica pelo 55 que neste caso é o módulo, assim $0,1818 * 55 = 10$ simples e fácil de encontrar o resto. Portanto $C(10) \equiv 10\, (mod\, 55)$

Para $C(29)$:

$$C(29) \equiv 29^3 (mod\, 55)$$
$$C(29) \equiv 29^2.29\, (mod\, 55)$$
$$C(29) \equiv 841.29\, (mod\, 55)$$
$$C(29) \equiv 16.29\, (mod\, 55)$$
$$C(29) \equiv 464\, (mod\, 55)$$
$$C(29) \equiv 24\, (mod\, 55)$$

Para $C(14)$:

$$C(14) \equiv 14^3 (mod\, 55)$$
$$C(14) \equiv 14^2.14 (mod\, 55)$$
$$C(14) \equiv 196.14\, (mod\, 55)$$
$$C(14) \equiv 31.14\, (mod\, 55)$$
$$C(14) \equiv 434\, (mod\, 55)$$
$$C(14) \equiv 49 (mod\, 55)$$

Observação: $C(14)$ é igual a 14^3 módulo 55. Calculando $14^2 = 196$, e como 196 módulo 55 deixa resto 31, logo posso substituir o 196 por 31, mas $31 * 14 = 434$ e o 434 modulo

55 deixa resto 49.Portanto $C(14) \equiv 49\,(mod\,55)$

Para $C(18)$:

$$\begin{aligned} C(18) &\equiv 18^3 (mod\,55) \\ C(18) &\equiv 18^2.18 (mod\,55) \\ C(18) &\equiv 324.18\,(mod\,55) \\ C(18) &\equiv 49.18\,(mod\,55) \\ C(18) &\equiv 2\,(mod\,55) \end{aligned}$$

Para $C(12)$:

$$\begin{aligned} C(12) &\equiv 12^3\,(mod\,55) \\ C(12) &\equiv 12^2.12\,(mod\,55) \\ C(12) &\equiv 144.12\,(mod\,55) \\ C(12) &\equiv 34.12\,(mod\,55) \\ C(12) &\equiv 408\,(mod\,55) \\ C(12) &\equiv 23\,(mod\,55) \end{aligned}$$

Para $C(9)$:

$$\begin{aligned} C(9) &\equiv 9^2.9\,(mod\,55) \\ C(9) &\equiv 81.9\,(mod\,55) \\ C(9) &\equiv 26.9\,(mod\,55) \\ C(9) &\equiv 234\,(mod\,55) \\ C(9) &\equiv 14\,(mod\,55) \end{aligned}$$

Para $C(25)$:

$$\begin{aligned} C(25) &\equiv 25^3 \,(mod\, 55) \\ C(25) &\equiv 25^2.25 \,(mod\, 55) \\ C(25) &\equiv 625.25 \,(mod\, 55) \\ C(25) &\equiv 20.25 \,(mod\, 55) \\ C(25) &\equiv 500 \,(mod\, 55) \\ C(25) &\equiv 5 \,(mod\, 55) \end{aligned}$$

Para $C(21)$:

$$\begin{aligned} C(21) &\equiv 21^3 \,(mod\, 55) \\ C(21) &\equiv 21^2.21 \,(mod\, 55) \\ C(21) &\equiv 441.21 \,(mod\, 55) \\ C(21) &\equiv 1.21 \,(mod\, 55) \\ C(21) &\equiv 21 \,(mod\, 55) \end{aligned}$$

Para $C(13)$:

$$\begin{aligned} C(13) &\equiv 13^3 \,(mod\, 55) \\ C(13) &\equiv 13^2.13 \,(mod\, 55) \\ C(13) &\equiv 169.13 \,(mod\, 55) \\ C(13) &\equiv 4.13 \,(mod\, 55) \\ C(13) &\equiv 52 \,(mod\, 55) \end{aligned}$$

Portanto após a codificação, foram transformados nos blocos:

BLOCOS
33-10-24-49-33-10-24-2-23-10-14-14-10-5-21-2-23-10-52-10

Observação: Conforme analisar nem todos os blocos foram feitos, após verificar que existem blocos repetidos uma vez feito não ha necessidade de refaze-lo para a demonstração.

4.4 Decodificação

Começamos com os blocos transformados pela codificação, e por fim a regra para a decodificação.

Definição 4.4.1. Seja o par de Chave Privada (d, n), e $D(a)$ é o resto da divisão de a^d por n, denotado por $D(C(b))$, isto significa

$$D(C(b)) \equiv (C(b))^d (mod\, n)$$

com $1 \leq D(C(b)) < n$ logo,

$$a^d \equiv b\,(mod\, n)$$

Para compreender como codificamos continuaremos usando o Exemplo 4.2 usados para a pré-codificação e codificação. Lembrando que o valor do $d = 27$ conforme foi feito os cálculos pelo Exemplo4.1.1

Solução: Usaremos a regra $D(C(b)) \equiv a^d (mod\, n)$, com os blocos: 33-10-24-49-33-10-24-2-23-10-14-14-10-5-21-2-23-10-52-10.

Para $D(33)$:

$$\begin{aligned} D(33) &\equiv 33^{27} (mod\, 55) \\ D(33) &\equiv (33^{10})^2 .33^7\, (mod\, 55) \\ D(33) &\equiv 44^2 .22\, (mod\, 55) \\ D(33) &\equiv 1936.22\, (mod\, 55) \\ D(33) &\equiv 11.22\, (mod\, 55) \\ D(33) &\equiv 242\, (mod\, 55) \\ D(33) &\equiv 22\, (mod\, 55) \end{aligned}$$

Observação: $D(33)$ é igual a 33^{27} módulo 55. Calculando $(33^{10})^2$, mas 33^{10} deixa resto 44 módulo 55 e $44^2 = 1.936$ módulo 55 deixando resto 11, podemos trocar o 1936 por 11, logo $11 * 22 = 242$ e módulo 55 deixa resto 22. Portanto $D(33) \equiv 22\,(mod\, 55)$

Para $D(10)$:

$$D(10) \equiv 10^{27} (mod\, 55)$$
$$D(10) \equiv (10^{10})^2.10^7 \, (mod\, 55)$$
$$D(10) \equiv 45^2.10 \, (mod\, 55)$$
$$D(10) \equiv 2025.10 \, (mod\, 55)$$
$$D(10) \equiv 45.10 \, (mod\, 55)$$
$$D(10) \equiv 450 \, (mod\, 55)$$
$$D(10) \equiv 10 \, (mod\, 55)$$

Observação: $D(10)$ é igual a 10^{27} módulo 55. Calculando $(10^{10})^2$, mas 10^{10} deixa resto 45 módulo 55 e $45^2 = 2.025$ módulo 55 deixando resto 45, podemos trocar o 2.025 por 45, logo $45 * 10 = 450$ e módulo 55 deixa resto 10. Portanto $D(10) \equiv 10 \, (mod\, 55)$

Para $D(24)$:

$$D(24) \equiv 24^{27} (mod\, 55)$$
$$D(24) \equiv (24^{10})^2.24^7 \, (mod\, 55)$$
$$D(24) \equiv 1^2.29 \, (mod\, 55)$$
$$D(24) \equiv 1.29 \, (mod\, 55)$$
$$D(24) \equiv 29 \, (mod\, 55)$$

Para $D(49)$:

$$D(49) \equiv 49^{27} (mod\, 55)$$
$$D(49) \equiv (49^{10})^2.49^7 (mod\, 55)$$
$$D(49) \equiv 1^2.14 \, (mod\, 55)$$
$$D(49) \equiv 1.14 \, (mod\, 55)$$
$$D(49) \equiv 14 (mod\, 55)$$

Para $D(2)$:

$$\begin{aligned} D(2) &\equiv 2^{27} (mod\, 55) \\ D(2) &\equiv (2^{10})^2.2^7 (mod\, 55) \\ D(2) &\equiv 34^2.18\, (mod\, 55) \\ D(2) &\equiv 1156.18\, (mod\, 55) \\ D(2) &\equiv 1.18\, (mod\, 55) \\ D(2) &\equiv 18\, (mod\, 55) \end{aligned}$$

Observação: $D(2)$ é igual a 2^{27} módulo 55. Calculando $(2^{10})^2$, mas 2^{10} deixa resto 34 módulo 55 e $34^2 = 1.156$ módulo 55 deixando resto 1, podemos trocar o 1.156 por 1, logo $1 * 18 = 18$ e módulo 55 deixa resto 18. Portanto $D(2) \equiv 18\, (mod\, 55)$
Para $D(23)$:

$$\begin{aligned} D(23) &\equiv 23^{27}\, (mod\, 55) \\ D(23) &\equiv (23^{10})^2.23^7\, (mod\, 55) \\ D(23) &\equiv 34^2.12\, (mod\, 55) \\ D(23) &\equiv 1156.12\, (mod\, 55) \\ D(23) &\equiv 1.12\, (mod\, 55) \\ D(23) &\equiv 12\, (mod\, 55) \end{aligned}$$

Para $D(14)$:

$$\begin{aligned} D(14) &\equiv 14^{27}\, (mod\, 55) \\ D(14) &\equiv (14^{10})^2.14^7\, (mod\, 55) \\ D(14) &\equiv 1^2.9\, (mod\, 55) \\ D(14) &\equiv 9\, (mod\, 55) \end{aligned}$$

Observação: $D(14)$ é igual a 14^{27} módulo 55. Calculando $(14^{10})^2$, mas 14^{10} deixa resto 1 módulo 55 e $1^2 = 1$, logo $1*9 = 9$ e módulo 55 deixa resto 9. Portanto $D(14) \equiv 9\, (mod\, 55)$

Para $D(5)$:

$$\begin{aligned} D(5) &\equiv 5^{27} \,(mod\, 55) \\ D(5) &\equiv (5^{10})^2.5^7 \,(mod\, 55) \\ D(5) &\equiv 45^2.25 \,(mod\, 55) \\ D(5) &\equiv 2025.25 \,(mod\, 55) \\ D(5) &\equiv 45.25 \,(mod\, 55) \\ D(5) &\equiv 1125 \,(mod\, 55) \\ D(5) &\equiv 25 \,(mod\, 55) \end{aligned}$$

Para $D(21)$:

$$\begin{aligned} D(21) &\equiv 21^{27} \,(mod\, 55) \\ D(21) &\equiv (21^{10})^2.21^7 \,(mod\, 55) \\ D(21) &\equiv 1^2.21 \,(mod\, 55) \\ D(21) &\equiv 1.21 \,(mod\, 55) \\ D(21) &\equiv 21 \,(mod\, 55) \end{aligned}$$

Para $D(52)$:

$$\begin{aligned} D(52) &\equiv 52^{27} \,(mod\, 55) \\ D(52) &\equiv (57^{10})^2.57^7 \,(mod\, 55) \\ D(52) &\equiv 34^2.13 \,(mod\, 55) \\ D(52) &\equiv 1156.13 \,(mod\, 55) \\ D(52) &\equiv 1.13 \,(mod\, 55) \\ D(52) &\equiv 13 \,(mod\, 55) \end{aligned}$$

Portanto os blocos codificados após forem decodificados, retornou aos blocos iniciais: 22-10-29-14-22-10-29-18-12-10-9-9-10-25-21-18-12-10-13-10.
Logo 22102914221029181210991025211812101310, usando a Tabela 4.2 retornamos a mensagem original MATEMÁTICA APLICADA.

5 O Python

Nos anos noventa, surge a linguagem Python graças ao esforço de Guido van Rossum, pesquisador holandês do CWI (Centrum Wiskunde & Informática) em Amsterdã. Sua missão inicial era criar um sistema operacional distribuído chamado Amoeba, substituindo a linguagem ABC por uma nova, que viria a ser o Python, capaz de superar as restrições enfrentadas em projetos anteriores. Essa motivação foi fundamental para o nascimento e desenvolvimento do Python.

O Python será utilizado para praticar a criptografia RSA. Começaremos com um exemplo de mensagem sendo codificada pelo programa e em seguida veremos essa mesma mensagem sendo descodificada.

Aqui estão dois códigos QR code abaixo: o primeiro é para o programa online, caso não o tenha instalado em seu computador, e o segundo QR code contém o programa com a mensagem criptografada e descriptografada. Lembrando que sempre que abrir o programa e começar a executá-lo, os blocos da mensagem criptografada serão diferentes, já que ele escolhe aleatoriamente os dois números primos.

Python | On-line

LaTeX | Código em Python no Overleaf

```python
import math
import random


msg = "Matematica Aplicada Furg"
msgCifrada = []
msgCifradaTemp = []
msgDecifrada = []
msgDecifradaTemp = []
```

```
n,d,e,m = None,None,None,None

def sort_prime(num):
    prime_num1 = []
    prime_num2 = [True] * (num + 1)
    for i in range(2, num + 1):
        if prime_num2[i]:
            prime_num1.append(i)
            for j in range(2, int(num / i) + 1):
                prime_num2[i * j] = False
    return prime_num1

def get_random_int(min, max):
    min = math.ceil(min)
    max = math.floor(max)
    return math.floor(random.random() * (max - min + 1)) + min

def mdc(x,y):
    while(y) :
        t=y
        y=x%y
        x=t
    return x

def modInverse(a, m):
    for x in range(1, m):
        if ((a % m) * (x % m)) % m == 1:
            return x

# Aumentar muito esse valor vai deixar a conta muito mas MUITO LENTA
primos = sort_prime(300)

p = primos[get_random_int(len(primos)-60,len(primos))]
q = primos[get_random_int(len(primos)-60,len(primos))]

n = p*q
m = (p-1)*(q-1)

tempE = 0
temp=(get_random_int(1,m))
e=0
while(e==0) :
  tempE = mdc(temp,m)
  if tempE==1 : e = temp
  else : temp=(get_random_int(1,m))

d = modInverse(e,m)
```

```
57
58 print("p:",p)
59 print("q:",q)
60 print("n:",n)
61 print("m:",m)
62 print("e:",e)
63 print("d:",d)
64
65
66 strBytes = bytes(msg, 'utf-8')
67 # actual bytes in the the string
68 for byte in strBytes:
69     msgCifradaTemp.append(byte)
70
71 print('mensagem convertida para bytes: ')
72 print(msgCifradaTemp)
73
74 for index in range(len(msgCifradaTemp)):
75   temp = pow(msgCifradaTemp[index],e)
76   temp2 = temp % n
77   msgCifrada.append(temp2)
78
79 print('\n')
80 print('mensagem criptografada: ')
81 print(msgCifrada)
82 ---------------------------------------------
83 p: 89
84 q: 197
85 n: 17533
86 m: 17248
87 e: 13779
88 d: 10491
89 mensagem convertida para bytes:
90 [77, 97, 116, 101, 109, 97, 116, 105, 99, 97, 32, 65, 112, 108, 105, 99,
       97, 100, 97, 32, 70, 117, 114, 103]
91
92
93 mensagem criptografada:
94 [675, 6275, 11796, 15612, 8497, 6275, 11796, 3090, 13755, 6275, 983,
     11195, 3765, 15247, 3090, 13755, 6275, 15395, 6275, 983, 12076, 2462,
       15864, 14205]
```

Listing 5.1 – Exemplo de Codificação

Depois de executar o programa mencionado anteriormente, o programa seleciona aleatoriamente os valores p e q, e após essa seleção, automaticamente fornece os demais resultados, incluindo a chave pública e a chave privada.

Neste momento, o programa está decodificando a mensagem mencionada anteriormente.

```
1
2 for index in range(len(msgCifrada)):
3   temp = pow(msgCifrada[index],e)
4   temp2 = temp % n
5   msgDecifradaTemp.append(pow(msgCifrada[index],d) % n)
6
7
8 print('\n')
9 print('mensagem decriptografada: ')
10 print(msgDecifradaTemp)
11
12 msgDecifrada = bytes(msgDecifradaTemp)
13
14 # for i in range(len(msgDecifradaTemp)):
15 #     msgDecifrada.append(str(msgDecifradaTemp[i],'utf-8'))
16
17
18 print('\n')
19 print('mensagem traduzida: ')
20 print(msgDecifrada)
21 ----------------------------------------
22 mensagem decriptografada:
23 [77, 97, 116, 101, 109, 97, 116, 105, 99, 97, 32, 65, 112, 108, 105, 99,
    97, 100, 97, 32, 70, 117, 114, 103]
24
25
26 mensagem traduzida:
27 b'Matematica Aplicada Furg'
```

Listing 5.2 – Exemplo de Decodificação

6 Conclusões

Acredita-se que este trabalho, a Criptografia RSA (Rivest-Shamir-Adleman) é um dos métodos de criptografia assimétrica, amplamente utilizados para assegurar a proteção das comunicações digitais. Sua importância se faz presente em diversas aplicações, como assinatura digital, autenticação, compras online. Entender e aprimorar a criptografia RSA é vital para proteger dados sensíveis contra ameaças e ataques, devido a medida do crescimento de troca de informações pela internet.

O algoritmo RSA por trás do método, à aplicação que utilizam o estudo de Teoria dos Números, no qual o crucial é os números primos, pois ao fatorarem primos muito grande, levará muito tempo (zilhões de anos) mesmo se usar o mais poderoso computador existente atualmente. Ao decorrer do trabalho foi implantado a linguagem Python, confirmando a validade dos cálculos que envolvem esse método.

Enfim, acreditamos que esse trabalho será de muito proveitoso. Ademais, tem o potencial para motivação, inspiração e até incentivar os envolvidos a procurar aprimoramento em programas de pós-graduação, elevando assim sua própria atuação.

Referências

CERQUEIRA, M. C. et al. O estudo da criptografia rsa no ensino básico com auxílio de softwares computacionais. Universidade Federal de Alagoas, (Ufal). Citado na página 11.

COUTINHO, S. C. *Números inteiros e criptografia RSA*. [S.l.]: IMPA, 1997. Citado na página 11.

HEFEZ, A. *Aritmética*. 2. ed. [S.l.]: SBM. (Coleção PROFMAT; 08). Citado na página 11.

JORGE, F. R. Introdução à linguagem python. FLISOL 2012, 2012. Citado na página 11.

LOPES, M. A. Introdução à teoria dos números e dos números primos. *Universidade Estadual da Paraíba, Centro de Ciências Humanas e Exatas*, 2011. Citado na página 11.

SANTOS, J. P. de O. *Introdução à Teoria dos Números*. [S.l.]: IMPA, 1998. (Coleção matemática universitária). Citado na página 11.