INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA
CAMPUS CAJAZEIRAS

VALDIGLEY FERREIRA CAMPOS

CRIPTOGRAFIA RSA: UMA PROPOSTA DE INTERDISCIPLINARIDADE

CAJAZEIRAS
2020

Valdigley Ferreira Campos

CRIPTOGRAFIA RSA: UMA PROPOSTA DE INTERDISCIPLINARIDADE

Trabalho de Conclusão de Curso submetido à Coordenação do Curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, como parte dos requisitos para a obtenção do grau de Licenciado em Matemática.

Orientador(a): Prof.ª M.ª Kissia Carvalho

CAJAZEIRAS
2020

Campus Cajazeiras
Coordenação de Biblioteca
Biblioteca Prof. Ribamar da Silva
Catalogação na fonte: Daniel Andrade CRB-15/593

C198c

Campos, Valdigley Ferreira

Criptografia RSA: uma proposta de interdisciplinaridade / Valdigley Ferreira Campos; orientadora Kissia Carvalho.- Cajazeiras, 2020.
67 f.: il.

Orientador: Kissia Carvalho.
TCC (Licenciatura em Matemática) – Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Cajazeiras, 2020.

1. Teoria dos Números 2. Criptografia RSA. 3. Interdisciplinaridade. I. Título.

511(0.067)

Valdigley Ferreira Campos

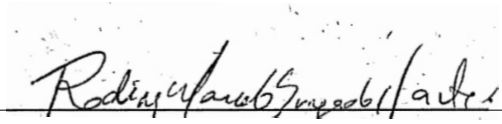
CRIPTOGRAFIA RSA: UMA PROPOSTA DE INTERDISCIPLINARIDADE

Trabalho de Conclusão de Curso submetido à Coordenação do Curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, como parte dos requisitos para a obtenção do grau de Licenciado em Matemática.

Aprovado em: **20** / **03** / **2020**

BANCA EXAMINADORA

Prof.ª M.ª Kissia Carvalho – IFPB
(Orientadora)



Prof. Dr. Rodiney Marcelo Braga dos Santos – IFPB

Prof. Dr. Vinicius Martins Teodosio Rocha – IFPB

Dedico este trabalho aos meus familiares, a minha esposa, a minha orientadora e a todas as pessoas que me ajudaram durante essa graduação.

AGRADECIMENTOS

Neste trabalho quero agradecer a Deus pela minha vida e por me conceder a oportunidade de estar concluindo essa etapa tão especial para mim, que é o curso de licenciatura em matemática. Deus é grandioso e tremendo e não pouparei agradecimentos a sua magnifica presença em tudo que eu fizer, pois tudo aqui na terra é no tempo dele e nesse momento estou aqui por ele.

Apresento aqui também, profunda gratidão a minha orientadora a Prof.ª M.ª Kissia Carvalho que sempre foi paciente e compreensiva, ao passo que me forneceu conhecimentos e ideias extraordinárias para as diversas etapas deste trabalho.

Agradeço a minha Esposa Vânia, aos meus familiares e ao amigo Weliton Íris de Sousa, que me ajudaram em vários momentos cruciais deste curso. “Meu muito obrigado a todos vocês”.

"Bem-aventurados os que trilham caminhos retos e andam na lei do SENHOR"

(BÍBLIA, Salmos, 119, 1)

RESUMO

A Teoria dos Números é um domínio científico, tanto de conhecimentos, quanto de pesquisas, com extrema importância dentro da Matemática. Atualmente ela se apresenta em forma de disciplinas a serem desenvolvidas nos cursos de graduação, e, para tanto, exige uma transformação em saber a ensinar, de modo a haver uma apropriação deste saber pelas novas gerações. Entretanto, por ser uma disciplina com grau de abstração elevado, ela ainda é vista pelos alunos, na maioria das vezes, como uma disciplina sem utilidades práticas. Assim surge este trabalho que tem como objetivo apontar o modelo de Criptografia RSA como uma estratégia interdisciplinar para potencializar o ensino da Teoria dos Números nos cursos de graduação. Esse propósito, surge com base no seguinte questionamento: É possível utilizar a criptografia RSA como proposta interdisciplinar para potencializar o ensino da Teoria dos Números nos cursos de graduação? Com base nisso, realizamos uma pesquisa predominantemente qualitativa do tipo exploratória e propomos a nossa intervenção por meio de um projeto interdisciplinar, de maneira que os alunos necessitem entrar em contato com cada parte do RSA, que por sua vez exigem os conceitos de Teoria dos Números para a sua compreensão. Esperamos que esta contribuição possa auxiliar professores de Teoria dos Números a potencializar suas aulas, melhorando a apropriação do saber por parte dos alunos, bem como atribuindo uma finalidade a essa área da matemática enquanto disciplina nos cursos superiores.

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

ABSTRACT

Number Theory is a scientific domain, both of knowledge and research, with extreme importance within Mathematics. Currently, it is presented in the form of disciplines to be developed in undergraduate courses, and, for that, it requires a transformation into to know to be taught, so that there is an appropriation by the new generations. However, because it is a discipline with a high degree of abstraction, it is still seen by students, most of the time, as a discipline with no practical uses. Thus, this work aims to point out the RSA cryptography model as an interdisciplinary strategy to potentialize the teaching of Number Theory in undergraduate courses. This purpose arises based on the following question: Is it possible to use RSA cryptography as an interdisciplinary proposal to potentialize the teaching of Number Theory in undergraduate courses? Based on this, we conducted a predominantly qualitative research of the exploratory type and proposed our intervention through an interdisciplinary project, so that students need to get in touch with each part of the RSA, which in turn, require the concepts of Number Theory for your understanding. We hope that this contribution can help Number Theory teachers to potentialize their classes,improving students' appropriation of this knowledge, as well as assigning a purpose to this area of mathematics as a discipline in undergraduate courses.

Keywords: Number theory. RSA cryptography. Interdisciplinarity.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

A Teoria dos Números é um domínio científico, tanto de conhecimentos, quanto de pesquisas, com extrema importância dentro da Matemática (RESENDE; MACHADO, 2012). Seus primeiros registros históricos, com semelhança ao que encontramos hoje, remontam a Grécia na antiguidade, embora civilizações mais antigas já estudassem algumas de suas propriedades (COUTINHO, 2014). Atualmente ela se apresenta em forma de disciplinas a serem desenvolvidas nos cursos de graduação e, para tanto, exige uma transformação em saber a ensinar, de modo a haver uma apropriação deste saber pelas novas gerações (RESENDE; MACHADO, 2012).

Entretanto, a Teoria dos Números, semelhantemente a Álgebra, ainda é vista, na maioria dos casos, como uma disciplina muito sofisticada e abstrata, constituindo uma componente curricular restrita, o que gera uma limitação ou ainda uma omissão de suas aplicações, não havendo espaço para o uso da criatividade/inovação (LOPES; LOPES, 2018). Com base nisso, a Teoria dos Números enquanto disciplina, torna-se motivo de repulsa por parte dos alunos, ao passo que impulsiona a ideia de algo "sobrenatural" e sem utilidade (LOPES; LOPES, 2018).

No tocante a essas dificuldades e limitações, deve haver uma intervenção de modo a possibilitar uma melhoria na compreensão dessa disciplina em sala de aula e isso pode ser realizado buscando metodologias que possibilitem a apropriação do conhecimento por todos os discentes, em oposição ao paradigma de que só aprende quem possui maior facilidade (LOPES; LOPES, 2018).

Nessa perspectiva, a Interdisciplinaridade parece ser interessante, uma vez que promove articulação entre as partes e o todo, à medida que proporciona o direcionamento à pratica, estimulando a superação de currículos fragmentados (SEVERINO, 2008). Isso pode possibilitar uma interação positiva entre a Teoria dos Números e suas aplicações, com vistas a melhoria do aprendizado pelos estudantes.

Nessa ótica, a Criptografia RSA, se apresenta como uma possibilidade, pois apresenta seus fundamentos na Teoria dos Números e constitui uma de suas principais aplicações na segurança dos sistemas comerciais da atualidade (COUTINHO, 2014). Isso acontece porque o RSA é um modelo de Criptografia, que por sua vez se origina da ideia de ocultar mensagens de uma maneira que somente o destinatário legítimo seja capaz de ler (COUTINHO, 2014).

Tomando como base o que foi discutido, surge o questionamento, norteador da nossa pesquisa: É possível utilizar a criptografia RSA como proposta interdisciplinar para po-

tencializar o ensino da Teoria dos números nos cursos de graduação? Portanto, o objetivo dessa pesquisa consiste em apontar o modelo de Criptografia RSA, como uma estratégia interdisciplinar, para potencializar o ensino da Teoria dos Números nos cursos de graduação.

A ideia de relacionar Teoria dos Números e Criptografia RSA se caracteriza como uma possibilidade muito interessante para a transformação dessa disciplina em um saber a ensinar com uma finalidade prática e isso é explorado em diversos trabalhos que buscam contribuir para esse propósito. Logo abaixo, apresentamos ao leitor alguns trabalhos detentores de propostas muito interessantes que abordam essa relação, mas que não farão parte da nossa construção

- Galdino (2014) propõe a Criptografia, com ênfase ao RSA, como uma proposta de aplicação prática para o ensino médio, com o objetivo de corroborar para a motivação do processo de ensino e aprendizagem de conceitos ligados a Teoria dos Números no ensino básico. Para essa finalidade utiliza alguns recursos tecnológicos, tais como o software MAPLE.

- Molinari (2016) realiza um profundo e exaustivo estudo sobre a Criptografia RSA, ao passo que elabora várias atividades envolvendo a criptografia como fator motivador nos anos finais do ensino fundamental e iniciais do ensino médio. Dentre uma de suas propostas encontra-se a ideia de suprimir pequenas partes do algoritmo RSA de modo a facilitar o entendimento dos conceitos que fazem parte da Teoria dos Números para as turmas de 9º ano.

- Machado (2018) utiliza a relação Teoria dos Números e Criptografia RSA para alunos de 8º e 9º anos do ensino básico, medalhistas de olimpíadas de matemática, com o objetivo de aprimorar e/ou desenvolver habilidades de interesses desses estudantes, que apresentam gosto por novos desafios.

A pesquisa realizada nesse estudo é predominantemente qualitativa, pois parte da ideia de que os métodos utilizados, associados a bagagem teórica a ser transmitida, devem se adequar ao objeto de estudo melhorando a aprendizagem do mesmo (GIBBS, 2009). Ela é do tipo exploratória, uma vez que busca trazer novas possibilidades para o aprimoramento do fato estudado, ao passo que considera os mais variados aspectos, possibilitando uma maior flexibilidade durante todo o processo (GIL, 2002).

Essa pesquisa é também de natureza básica, a medida que procura contribuir para a melhoria do ensino, mas sem previsão de uma aplicação prática (PRODANOV; FREITAS, 2013). Todavia, ainda nesta pesquisa, uma proposição metodológica, por meio da Interdisciplinaridade, será apresentada, com vistas à sua aplicação.

Em relação aos procedimentos técnicos, consiste em uma pesquisa bibliográfica, de modo que se constitui por meio de materiais já elaborados, como livros e revistas cientificas (GIL, 2002). Outrossim, a pesquisa se classifica também como de fontes secundárias uma vez que se origina com base no resultado da discussão de fontes já tornadas públicas anteriormente (LAKATOS, 2003).

Na pesquisa qualitativa maior ênfase é dada ao entendimento e exploração da natureza do objeto de estudo (GIBBS, 2009). Sendo assim, em um primeiro momento, nosso estudo será direcionado à conhecer a criptografia geral, bem como à revisar os conceitos da Teoria dos Números, necessários para entender o RSA, que só em um segundo momento será apresentado, como explicado detalhadamente logo abaixo.

Essa pesquisa será constituída a partir da fundamentação teórica encontrada em Coutinho (2014), Paar (2010) e Stallings (2015), que correspondem, respectivamente, as referências [2], [20] e [26]. Ainda assim, de acordo com cada etapa deste trabalho, serão utilizados outros referenciais como apoio. A mesma será dividida em quatro capítulos e estruturada a partir da seguinte sequência

1. No primeiro capítulo faremos uma revisão sobre alguns tópicos da Teoria dos Números, que servirão como subsídio para a compreensão do RSA, que por sua vez constitui o foco desse trabalho;

2. No segundo, estudaremos a Criptografia, no intuito de familiarizar o leitor a esta ciência.

3. Neste momento, amparados no primeiro e segundo capítulos, vamos delimitar o nosso trabalho a Criptografia RSA. Aqui, serão apresentados os principais tópicos para uma boa compreensão do método ou Algoritmo RSA, bem como a sua confiabilidade e funcionamento.

4. Por fim, vamos propor a nossa intervenção em forma de projeto interdisciplinar, com a ideia de contribuir para uma aprendizagem melhor e mais "justa" entre todos.

Ademais, acreditamos que só por meio da compreensão e execução da estrutura apresentada acima é que poderemos atingir o nosso objetivo.

CAPÍTULO 1

REVISÃO DA TEORIA DOS NÚMEROS

O sistema de Criptografia RSA apresenta grande relação com o conjunto dos números inteiros ($\mathbb{Z}$), em particular com os subconjuntos ($\mathbb{Z}_+$), ($\mathbb{N}$), nessa perspectiva, iniciaremos nosso estudo com um capítulo de revisão, abordando alguns conceitos da Teoria dos Números que servirão como subsídio para a compreensão do RSA. No entanto, mesmo que o leitor não tenha conhecimento algum da Teoria dos Números, os tópicos apresentados neste capítulo serão suficientes para o entendimento do sistema de criptografia supracitado. Outrossim, a construção será realizada com base em Coutinho (2014), Domingues (1991), Filho Alencar (1981), Hefez (2013), Junior Cerqueira (2015) e Santos (1998) que correspondem, respectivamente, aos referenciais [2], [3], [5], [10], [11] e [23].

1.1 Os Números Inteiros

Definição 1.1. *Os números Inteiros* ($\mathbb{Z}$) *são um conjunto formado a partir dos seguintes elementos*

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

Como todo conjunto numérico, $\mathbb{Z}$ é representado entre chaves, com seus elementos separados por vírgula, conforme representado abaixo

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

É notável que nem todos os números do conjunto ($\mathbb{Z}$) podem ser representados, uma vez que são infinitos. Os subconjuntos dos números inteiros que apresentam maior destaque são:

1. Conjunto dos inteiros não nulos ($\neq 0$)

$$\mathbb{Z}^* = \{\ldots, -3, -2, -1, 1, 2, 3, \ldots\}$$

2. Conjunto dos inteiros não negativos (≥ 0)

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

3. Conjunto dos inteiros não positivos (≤ 0)

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

4. Conjunto dos inteiros naturais ($\mathbb{N}$)

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

Historicamente o conjunto $\mathbb{N}$ surgiu antes do conjunto $\mathbb{Z}$ e mesmo que a **Definição 1.1** seja suficiente para este trabalho existe uma construção lógico-formal do conjunto dos números inteiros com base nos 5 *Axiomas (ou Postulados) de Peano*, introduzidos pelo matemático italiano Giuseppe Peano, no século XIX, tomando como base os seguintes conceitos: o zero, o número natural e a relação de sucessor de um número. Essa construção pode ser vista em detalhes nas referências Domingues (1991) e Junior Cerqueira (2015).

1.1.1 Propriedades dos números inteiros

O conjunto dos números inteiros é munido de duas operações fundamentais da matemática, a *adição* $(x, y) \mapsto x + y$ e a *multiplicação* $(x, y) \mapsto x \cdot y$, e com base nessa estrutura possui algumas propriedades importantes, quais sejam:

1. (*A adição e a multiplicação são bem definidas*). $\forall a, b, a', b' \in \mathbb{Z}$, se $a = a'$ e $b = b'$, temos então que

$$a + b = a' + b' \quad \text{e} \quad a \cdot b = a' \cdot b'$$

2. (*Associatividade*). $\forall a, b, c \in \mathbb{Z}$, temos que

$$a + (b + c) = (a + b) + c \quad \text{e} \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

3. (*Comutatividade*). $\forall a, b \in \mathbb{Z}$, temos que

$$a + b = b + a \quad \text{e} \quad a \cdot b = b \cdot a$$

4. (*Elementos neutros*). $\forall a \in \mathbb{Z}$, temos que

$$a + 0 = a \quad \text{e} \quad a \cdot 1 = a$$

5. (*Elementos simétricos*). $\forall a \in \mathbb{Z}$ existe $b = -a$, tal que

$$a + b = 0$$

6. (*Distributividade*). $\forall a, b, c \in \mathbb{Z}$, temos que

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

1.1.2 Módulo de um número inteiro

A noção de módulo de um número inteiro será de grande utilidade em algumas demonstrações deste trabalho, em particular do *algoritmo da divisão* que será muito importante nos processos de criptografar e descriptografar[1] uma mensagem pelo método RSA.

Definição 1.2. *Seja $a \in \mathbb{Z}$ denomina-se módulo de a, denotado por $|a|$, o inteiro que obedece a seguinte relação*

$$|a| = \begin{cases} a & se \quad a \geq 0 \\ -a & se \quad a < 0 \end{cases}$$

Além da definição acima, o módulo de um número inteiro a pode ser representado como

$$|a| = \sqrt{a^2}, \quad \text{ou} \quad |a| = \text{máx}(-a, a)$$

Destarte, $\forall\ a \in \mathbb{Z}$, temos que

1. $|a| \geq 0$
2. $|a|^2 = a^2$
3. $|-a| = |a|$
4. $a \leq |a|$

1.1.3 Indução

As propriedades vistas na subseção **1.1.1**, mesmo sendo muito importantes, não são características únicas dos números inteiros, existe uma propriedade que só pode ser encontrada no conjunto $\mathbb{Z}$, denominada *princípio da boa ordenação*, que será descrita abaixo. Para entendermos como funciona essa propriedade precisamos inicialmente entender a definição a seguir:

Definição 1.3. *Seja $S \subset \mathbb{Z}$ denomina-se por elemento mínimo de S, denotado por $min(S)$, o número $a \in \mathbb{Z}$ que possui as seguintes propriedades:*

i. $a \in S$,

[1] Tanto o termo criptografar, quanto o termo descriptografar serão apresentados no capítulo 2.

ii. $\forall n \in S, a \leq n$.

7. *(Princípio da Boa Ordenação).* Todo subconjunto não vazio de $\mathbb{Z}$, e limitado inferiormente, possui um elemento mínimo.

Como consequência do *Princípio da Boa Ordenação* surge o *Princípio da Indução Matemática*, muito importante na teoria dos números.

Teorema 1.1 (Princípio da Indução Matemática)**.** *Seja $S \subset \mathbb{Z}$ e seja $a \in \mathbb{Z}$ tais que*

i. $a \in S$.

ii. $\forall\ n,\ n \in S \Rightarrow n+1 \in S$.

Então, $\{x \in \mathbb{Z}; x \geq a\} \subset S$.

Demonstração. *Nomearemos por $S' = \{x \in \mathbb{Z}; x \geq a\}$ e suponhamos por absurdo que $S' \not\subset S$, assim $S' \setminus S \neq \emptyset$, em que $S' \setminus S$ corresponde a diferença entre S' e S. Como $S' \setminus S$ é limitado inferiormente por a então, pelo Princípio da Boa Ordenação, existe $c \in S' \setminus S$ tal que $c = min(S' \setminus S)$. Desse modo, como $c > a$, segue que $c \in S'$ e $c \notin S$. Daí $c-1 \in S'$ e $c - 1 \notin S$. Segue do item* **ii***, da nossa hipótese sobre S, que $c = (c-1)+1 \in S$, como $c \in S'$, obtemos uma contradição com o fato de $c \in S' \setminus S$.*

■

E com base no *Princípio da Indução Matemática* surge um importante método para a realização de demonstrações em vários tópicos deste capítulo.

Proposição 1.1 (Prova por Indução Matemática)**.** *Seja $a \in \mathbb{Z}$ e seja $p(n)$ uma proposição associada a n. tal que*

i. *$p(a)$ é verdade, e*

ii. *$\forall\ n \geq a,\ p(n) \Longrightarrow p(n+1)$ é verdade,*

então, $p(n)$ é verdade quando $n \geq a$.

Demonstração. *Seja $S \subset \mathbb{Z}$, tal que $S = \{n \in \mathbb{Z};\ p(n)$é verdadeira$\}$. Como* **i** *e* **ii** *são verdadeiras, então pelo Princípio da Indução Matemática podemos concluir que $S \subset \mathbb{Z}$.*

■

Além da *Prova por Indução Matemática* existe uma segunda forma de realizar demonstrações, e que também surge com base no *Princípio da Indução Matemática*, denominada *Prova por Indução Completa*. Essa variante será muito importante para a demonstração do *Teorema Fundamental da Aritmética* que é um dos principais fatores de segurança do sistema RSA.

Teorema 1.2 (Prova por Indução Completa)**.** *Seja $p(n)$ uma sentença aberta tal que*

i. *$p(a)$ é verdade, e que*

ii. *$\forall\ n, p(a)$ e $p(a+1)$ e $\ldots$ e $p(n) \Rightarrow p(n+1)$ é verdade, então, $p(n)$ é verdade para todo $n \geq a$.*

Demonstração. *Considere o conjunto*

$$\mathcal{T} = \{n \in a + \mathbb{N};\ p(n)\ \text{é verdadeira}\}$$

queremos provar que $\mathcal{D} = (a + \mathbb{N}) \setminus \mathcal{T} = \emptyset$. Suponha, por absurdo, que $\mathcal{D} \neq \emptyset$. Logo, pelo Princípio da Boa Ordenação, $\mathcal{D}$ deve possuir um elemento mínimo que, chamaremos de k. De **i** *sabemos que $a \in \mathcal{T}$, mas não pertence a $\mathcal{D}$, segue que existe n tal que $k = a + n > a$. Portanto, $a, a+1, \ldots, k-1 \notin \mathcal{D}$; logo $a, a+1, \ldots, k-1 \in \mathcal{T}$. Por* **ii** *conclui-se que $k = k - 1 + 1 \in \mathcal{T}$, o que contradiz o fato de que $k \in \mathcal{D}$.*

■

1.1.4 Potenciação nos inteiros

Como base na operação de multiplicação dos números inteiros vamos definir a potenciação no conjunto $\mathbb{Z}$, que servirá como subsídio durante todas as etapas do método RSA.

Definição 1.4. *Sejam $a, n \in \mathbb{Z}$, com $n \in \mathbb{Z}_+$, uma potência de base a e expoente n é o número a^n, onde*

i. $a^0 = 1, a \neq 0$

ii. $a^n = \underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{n\ \text{vezes}}, n \geq 1$

Decorre da definição, e do fato da multiplicação ser associativa, que $a^n = a^{(n-1)} \cdot a$. Definimos também, que $0^n = 0, n \neq 0$, por outro lado, fica indefinido que $0^0 = 0$. Por fim, a potenciação possui as seguintes propriedades, $\forall a, b, m, n \in \mathbb{Z}$, com $m, n \in \mathbb{Z}_+$:

1. $1^n = 1$

   Demonstração. *A demonstração é imediata pela condição* **ii** *da* **Definição 1.4**

   ■

2. $a^m \cdot a^n = a^{m+n}$

Demonstração. *Faremos a prova por indução sobre n, tomando a, m fixos.*

Para $n = 0$:

$$\begin{aligned} a^m \cdot a^0 &= a^m \cdot 1 \\ &= a^m \\ &= a^{m+0} \end{aligned}$$

Suponha agora que: $a^m \cdot a^n = a^{m+n}$

Então:

$$\begin{aligned} a^m \cdot a^{(n+1)} &= a^m \cdot (a^n \cdot a) \\ &= (a^m \cdot a^n) \cdot a \\ &= a^{(m+n)} \cdot a \\ &= a^{(m+n)+1} \\ &= a^{m+(n+1)} \end{aligned}$$

■

3. $(a^m)^n = a^{m \cdot n}$

Demonstração. *A prova será realizada por indução sobre n, tomando a, m fixos.*

Para $n = 0 : (a^m)^0 = 1 = a^{m \cdot 0}$

Suponha agora que: $(a^m)^n = a^{m \cdot n}$

Então:

$$\begin{aligned} (a^m)^{(n+1)} &= (a^m)^n \cdot a^m \\ &= a^{m \cdot n} \cdot a^m \\ &= a^{m \cdot n + m} \\ &= a^{m \cdot (n+1)} \end{aligned}$$

■

4. $a^n \cdot b^n = (a \cdot b)^n$

Demonstração. *A prova será realizada também por indução sobre n, tomando a, b fixos.*

Para $n = 0 : a^0 \cdot b^0 = 1 \cdot 1 = 1 = (a \cdot b)^0$

Suponha agora que: $a^n \cdot b^n = (a \cdot b)^n$

Então:

$$\begin{aligned} a^{(n+1)} \cdot b^{(n+1)} &= a^n \cdot a \cdot b^n \cdot b \\ &= a^n \cdot b^n \cdot a \cdot b \\ &= (a \cdot b)^n \cdot (a \cdot b) \\ &= (a \cdot b)^{(n+1)} \end{aligned}$$

■

1.1.5 Divisibilidade

Para o desenvolvimento deste trabalho precisamos da noção de divisibilidade com números inteiros, bem como de algumas de suas propriedades, sendo assim

Definição 1.5. *Sejam $a, b \in \mathbb{Z}$ dizemos que a divide b ou que a é um divisor de b ou ainda que b é múltiplo de a, e denotamos por $a|b$ se existir $c \in \mathbb{Z}$ tal que $b = ca$. Caso não exista c, dizemos que a não divide b, e escrevemos $a \nmid b$.*

Fica definido que $a \in \mathbb{Z} \Longrightarrow 0 \nmid a$.

É importante entender que a notação $a|b$ não representa nenhuma operação em $\mathbb{Z}$, tampouco uma fração. Trata-se de uma sentença que aponta como verdade a existência de c, com $c \in \mathbb{Z}$, tal que $b = ca$.

Decorre da **Definição 1.5** que, dados a, b, c e $d \in \mathbb{Z}$, são válidas as propriedades abaixo

i. $a|a$, com $a \neq 0$

ii. $a|b$ e $b|c \Longrightarrow a|c$

iii. $a|b$ e $c|d \Longrightarrow ac|bd$

Proposição 1.2. *Sejam $a, b, c \in \mathbb{Z}$ de modo que $a|b$ e $a|c$, então $\forall\ x, y \in \mathbb{Z}$*

$$a|(bx + cy)$$

Demonstração. *Se $a|b$ e $a|c$, então existem $m, n \in \mathbb{Z}$, onde $b = ma$ e $c = na$. Assim,*

$$\begin{aligned} bx + cy &= (ma)x + (na)y \\ &= m(ax) + n(ay) \\ &= m(xa) + n(ya) \\ &= (mx)a + (ny)a \\ &= (mx + ny)a \end{aligned}$$

■

Proposição 1.3. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, então $(a-b)|(a^n - b^n)$*

Demonstração. *A prova será realizada por indução sobre n, tomando a, b fixos.*
Para $n = 1 : a^1 - b^1 = a - b$ e $(a-b)|(a-b)$
Suponha agora que: $(a-b)|(a^n - b^n)$, ou seja $(a^n - b^n) = k(a-b)$. Então,

$$\begin{aligned} a^{(n+1)} - b^{(n+1)} &= a^n a - b^n b \\ &= a^n a - a^n b + a^n b - b^n b \\ &= a^n(a-b) + (a^n - b^n)b \\ &= a^n(a-b) + (a-b)kb \\ &= (a-b)[a^n + kb] \end{aligned} \tag{1.1}$$

Decorre de (1.1) que $(a-b)|(a^{n+1} - b^{n+1})$. Portanto, a proposição é válida para todo $n \in \mathbb{N}$.

■

Proposição 1.4. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup 0$, então $(a+b)|(a^{2n+1} + b^{2n+1})$*

Demonstração. *A prova será realizada também por indução sobre n, tomando a, b fixos.*
Para $n = 0 : a^{2\cdot 0+1} + b^{2\cdot 0+1} = a + b$ e $(a+b)|(a+b)$
Suponha agora que: $(a+b)|(a^{2n+1} + b^{2n+1})$, ou seja $(a^{2n+1} + b^{2n+1}) = k(a+b)$. Então,

$$\begin{aligned} a^{2(n+1)+1} + b^{2(n+1)+1} &= a^{(2n+2)+1} + b^{(2n+2)+1} \\ &= a^2 a^{2n+1} + b^2 b^{2n+1} \\ &= a^2 a^{2n+1} - b^2 a^{2n+1} + b^2 a^{2n+1} + b^2 b^{2n+1} \\ &= (a^2 - b^2)a^{2n+1} + b^2(a^{2n+1} + b^{2n+1}) \\ &= (a^2 - b^2)a^{2n+1} + b^2 k(a+b) \\ &= (a+b)(a-b)a^{2n+1} + b^2 k(a+b) \\ &= (a+b)[(a-b)a^{2n+1} + b^2 k] \end{aligned} \tag{1.2}$$

Decorre de (1.2) que $(a+b)|(a^{2(n+1)+1} + b^{2(n+1)+1})$. Portanto, a proposição é válida para todo $n \in \mathbb{N}$.

■

Proposição 1.5. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, então $(a+b)|(a^{2n} - b^{2n})$*

Demonstração. *Novamente vamos realizar a prova por indução sobre n, tomando a, b fixos.*
Para $n = 1 : a^{2\cdot 1} - b^{2\cdot 1} = a^2 - b^2$ e $a + b$ divide $(a^2 - b^2) = (a+b)(a-b)$

Suponha agora que: $(a+b)|(a^{2n}-b^{2n})$*, ou seja* $(a^{2n}-b^{2n})=k(a+b)$*. Então,*

$$\begin{aligned} a^{2(n+1)}-b^{2(n+1)} &= a^{2n+2}-b^{2n+2} \\ &= a^2a^{2n}-b^2b^{2n} \\ &= a^2a^{2n}-b^2a^{2n}+b^2a^{2n}-b^2b^{2n} \\ &= (a^2-b^2)a^{2n}+b^2(a^{2n}-b^{2n}) \\ &= (a+b)(a-b)a^{2n}+b^2k(a+b) \\ &= (a+b)[(a-b)a^{2n}+b^2k] \end{aligned} \tag{1.3}$$

Decorre de (1.3)*, que* $(a+b)|(a^{2(n+1)}-b^{2(n+1)})$*. Portanto, a proposição é válida para todo* $n\in\mathbb{N}$*.*

■

1.1.6 Divisão Euclidiana

Nem sempre é possível efetuar uma divisão entre dois números inteiros, contudo podemos realizar uma divisão que deixa um resto pequeno denominada divisão euclidiana. Isso só é possível tomando como base o teorema conhecido como *Algoritmo da Divisão* e para realizar a sua demonstração vamos precisar de uma propriedade importante dos números inteiros, denominada *Propriedade Arquimediana*, que pode ser provada com base na seguinte proposição:

Proposição 1.6. $\nexists\, n\in\mathbb{Z}$ *tal que* $0<n<1$*.*

Demonstração. *Suponha, por absurdo, que existe* $n\in\mathbb{Z}$ *entre* 0 *e* 1*. Então o conjunto* $S=\{x\in\mathbb{Z};0<x<1\}$ *não é vazio, e, pelo Princípio da Boa Ordenação, possui um elemento mínimo* a*, assim:*

$$\begin{aligned} 0<a<1 &= 0\cdot a<a\cdot a<1\cdot a \\ &= 0<a^2<a \\ &= 0<a^2<a<1 \end{aligned}$$

Logo $a^2\in S$ *e* $a^2<a$*, mas isso é uma contradição. Portanto,* $S=\emptyset$*.*

■

Corolário 1.1 (Propriedade Arquimediana)**.** *Sejam* $a,b\in\mathbb{Z}$*, com* $b\neq 0$*. Então existe* $n\in\mathbb{Z}$ *tal que* $nb>a$*.*

Demonstração. *Como* $b\neq 0$ *decorre, da* **Proposição 1.6***, que* $|b|\geq 1$ *, desse modo:*

$$a\leq|a|<|a|+1\leq|b|(|a|+1)$$

Logo o resultado segue se, para $b > 0$, tomarmos $n = (|a|+1)$, ou então se, para $b < 0$, tomarmos $n = -(|a|+1)$.

■

Teorema 1.3 (Algoritmo da divisão)**.** *Sejam a e $b \in \mathbb{Z}$, com $b \neq 0$. Existem dois únicos q e $r \in \mathbb{Z}$ tais que*

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

Demonstração. *Considerando o conjunto $S = \{x = a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$, temos que:*

i. *(Existência). Segue, da Propriedade Arquimediana, que existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, assim $a - nb > 0$, o que implica em $S \neq \emptyset$. Então, pelo Princípio da Boa Ordenação, o conjunto S possui um elemento mínimo r e $r = a - bq$, com $q \in \mathbb{Z}$. Sabemos que $r \geq 0$, resta provar que $r < |b|$. Desse modo, vamos supor, por absurdo, que $r \geq |b|$. Portanto existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, assim*

$$\begin{aligned} 0 \leq s &= r - |b| \\ &= a - bq - |b| \\ &= a - b(q \pm 1) < r \end{aligned}$$

$0 \leq s < r$, logo $s \in \mathbb{S}$, mas isso contradiz o fato de r ser o menor elemento de S. Logo, fica provado que existem dois números q e $r \in \mathbb{Z}$ tais que

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

ii. *(Unicidade). Suponha que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}, 0 \leq r < |b|$ e $0 \leq r' < |b|$. Assim, temos que $-|b| < -r \leq r' - r \leq r' < |b|$. Logo, $|r' - r| < |b|$. Por outro lado, $b(q - q') = r' - r$, o que implica que*

$$|b||q - q'| = |r' - r| < |b|,$$

o que só é possível se $q = q'$, e consequentemente $r = r'$.

■

Os números q e r são denominados, respectivamente, *quociente* e *resto*, ao passo que a é o *dividendo* e b o *divisor*.

1.1.7 Máximo Divisor Comum

A ideia de máximo divisor comum de um número surge com base na divisibilidade e também é de grande relevância neste trabalho, com enfoque no teorema de *Bachet-Bézout* que por sua vez é essencial para o estudo da congruência, apresentada ainda neste capítulo.

Definição 1.6. *Sejam $a, b \in \mathbb{Z}$ diremos que $d \in \mathbb{Z}$, $d \geq 0$, é um máximo divisor comum de a e b, ou simplesmente $d = mdc(a, b)$, se satisfaz as seguintes condições:*

i. *$d|a$ e $d|b$, e também*

ii. *Se $c|a$ e $c|b$, então $c|d$.*

Proposição 1.7. *Se a, b, q e $r \in \mathbb{Z}$ e $a = bq + r$ e $d = mdc(a, b)$, então $d = mdc(b, r)$.*

Demonstração. *Como $d = mdc(a, b)$, então, pela* **Proposição 1.2**, *$d|(a - bq)$, o que implica que $d|r$. Por outro lado, se g é um divisor comum de b e r, da* **Proposição 1.2**, *$g|(bq + r)$, o que implica que $g|a$, e como $g|b$, segue que $g|d$. Portanto, $d = mdc(b, r)$.* ■

Teorema 1.4 (Bachet-Bézout)**.** *Sejam $a, b \in \mathbb{Z}$, então existem $x, y \in \mathbb{Z}$ tais que*

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

Demonstração. *Seja $C = \{ax + by \mid x, y \in \mathbb{Z}\}$ o conjunto de todas as combinações lineares de a e b. Claramente $0, a, -a \in C$, uma vez que $0 = a \cdot 0 + b \cdot 0$, $a = a \cdot 1 + b \cdot 0$ e $-a = a \cdot (-1) + b \cdot 0$, e portanto não é vazio. Desse modo, considere $C_+ = \{c \mid c \in C \text{ e } c > 0\}$. De acordo com o que foi dito acima C_+ também não é vazio, e assim, pelo Princípio da Boa Ordenação, possui um elemento mínimo, denotado por m, assim, $m > 0$ e $m = ax_0 + by_0$. Pelo Algoritmo da Divisão, existem q e r, de modo que $a = mq + r$, onde $0 \leq r < c$. Então*

$$\begin{aligned} a &= mq + r \\ &= (ax_0 + by_0)q + r \\ &= ax_0q + by_0q + r \end{aligned}$$

assim:

$$r = a(\underbrace{1 - x_0q}_{\in\mathbb{Z}}) + b(\underbrace{-y_0q}_{\in\mathbb{Z}})$$

Portanto, $r \in C$. Como $m = minC_+$, então $r = 0$, o que implica que $m|a$, e, de modo inteiramente análogo, $m|b$. Agora considere n, em que $n|a$ e $n|b$, logo $n|ax_0 + by_0$, ou seja $n|m$, então $n \leq m$ e portanto $m = d$.

■

Proposição 1.8. *Sejam $a, b \in \mathbb{Z}$ e $(a \neq 0$ ou $b \neq 0)$. Então $mdc(a, b) = 1$ se, e somente se, existem $l, s \in \mathbb{Z}$ tais que $al + bs = 1$.*

Demonstração.

($\Rightarrow$) *Se $mdc(a, b) = 1$, então pelo* **Teorema 1.4**, *existem $l, s \in \mathbb{Z}$ tais que $al + bs = 1$.*

($\Leftarrow$) *Se existem $l, s \in \mathbb{Z}$ tais que $al + bs = 1$ e $d = mdc(a, b)$, temos que $d|a$ e $d|b$, o que implica que $d|(al + bs)$, ou seja $d|1$. Logo $d = 1$, o que conclui a prova.*

■

Teorema 1.5 (Lema de Gauss)**.** *Sejam $a, b \in \mathbb{Z}$. Se $a|bc$ e $mdc(a, b) = 1$, então $a|c$.*

Demonstração. *Se $a|bc$, então existe $g \in \mathbb{Z}$, de modo que $bc = ag$. Como $mdc(a, b) = 1$, então pela* **Proposição1.8**, *temos que existem $l, s \in \mathbb{Z}$ tais que*

$$\begin{aligned} 1 &= la + sb \\ c &= lac + sbc \\ &= lac + sag \\ &= a(lc + sg) \end{aligned}$$

e, portanto, $a|c$.

■

Proposição 1.9. *Sejam $a, b, c \in \mathbb{Z}$. Se $mdc(a, b) = 1$, $a|c$ e $b|c$, então $ab|c$.*

Demonstração. *Se $a|c$, então existe $g, \in \mathbb{Z}$ tal que $c = ag$. Como o $mdc(a, b) = 1$ e também $b|c$, segue, pelo* **Teorema 1.5**, *que $b|g$. Desse modo, existe $k, \in \mathbb{Z}$ tal que $g = bk$. Assim:*

$$\begin{aligned} c &= ag \\ &= a(bk) \\ &= (ab)k \end{aligned}$$

e, portanto, $ab|c$.

■

1.1.8 Números Primos

A ideia de números primos é fundamental neste trabalho, pois o sistema de criptografia RSA surge com base na escolha de dois números primos. Nessa perspectiva, apresentaremos a sua definição, bem como várias de suas propriedades.

Definição 1.7. *Seja $a \in \mathbb{Z}$ e $a > 1$. Diz-se que a é um número primo se, e somente se, 1 e a são seus únicos divisores.*

A partir da definição acima, considerando dois números primos p e q e a um número inteiro, decorre que:

i. Se $p|q$, então $p = q$.

Demonstração. *Se $p|q$, sendo q um número primo, então $p = 1$ ou $p = q$. Como p também é primo, segue que $p > 1$. Logo $p = q$.*

■

ii. Se $p \nmid a$, então $mdc(p, a) = 1$.

Demonstração. *Considere $mdc(p, a) = d$, com $d \in \mathbb{Z}$, então $d|p$ e $d|a$ e portanto, $d = 1$ ou $d = p$. Como por hipótese $p \nmid a$, segue que $d \neq p$. Logo $d = 1$.*

■

Proposição 1.10 (Lema de Euclides)**.** *Sejam $a, b, p \in \mathbb{Z}$ e p um número primo. Se $p|ab$, então $p|a$ ou $p|b$.*

Demonstração. *Se $p|a$ então a tese é verídica. Por outro lado, se $p \nmid a$, temos que $mdc(p, a) = 1$ e como $p|ab$, segue que $p|b$.*

■

Corolário 1.2. *Seja p um número primo e sejam $a_1, \ldots, a_n \in \mathbb{Z}$. Se $p|a_1 \cdot a_2 \cdot \ldots \cdot a_n$, então $p|a_k$ para algum k, $1 \leq k \leq n$.*

Demonstração. *A prova será realizada por indução sobre n.*
Para $n = 1$: (Imediato)
Para $n = 2 : p|a_1a_2$, segue, do Lema de Euclides, que $p|a_1$ ou $p|a_2$.
Suponha agora que: $p|a_k$, com $1 \leq k \leq n - 1$.
Assim, pelo Lema de Euclides, se $p|a_1 \cdot a_2 \cdot \ldots \cdot, a_n$, então $p|a_n$ ou $p|a_k$, onde $1 \leq k \leq n-1$. Se $p|a_n$ é verdadeira a tese, por outro lado, se $p \nmid a_n$, então $p|a_k$. Em ambos os casos p divide um dos inteiros $a_1, \ldots, a_n$.

■

Corolário 1.3. *Sejam $p, p_1, \ldots, p_n$ números primos. Se $p|p_1 \cdot p_2 \cdot \ldots \cdot p_n$, então $p = p_k$ para algum k, $1 \leq k \leq n$.*

Demonstração. *Com efeito, pelo* **Corolário 1.2***, existe um índice k, de modo que $p|p_k$, como p_k é primo, então $p = 1$ ou $p = p_k$, e, como p também é primo, segue que $p > 1$. Logo $p = p_k$.*

■

Logo abaixo, apresentamos um teorema muito importante que garante a decomposição de um número inteiro, de maneira única e dentro de certas condições, em um produto de números primos. Como já mencionado nesse capítulo, esse teorema é um dos principais fatores de segurança do sistema RSA.

Teorema 1.6 (Teorema Fundamental da Aritmética)**.** *Seja $n \in \mathbb{Z}$ e $n > 1$. Podemos escrever n de maneira única como*

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$$

com $k \in \mathbb{Z}$ e $k \geq 1$, e, com $p_1 \leq \ldots \leq p_k$ números primos.

Demonstração.

i. *(Existência). A demonstração será realizada utilizando a Prova por Indução Completa sobre n.*

Para $n = 2$: É válido, pois o número 2 é primo.

Suponha agora que para $n > 2$ é válido que: $\forall i \in \mathbb{Z}, 1 < i < n$, tem-se $i = p_1 \cdot p_2 \cdot \ldots \cdot p_k$.

Assim, se n é primo, então a tese é verdadeira, por outro lado, se n não é primo, então $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Decorre, da nossa hipótese, que existem números primos $p_1, \ldots, p_r$ e $q_1, \ldots, q_s$. Portanto, $n = (p_1 \cdot p_2 \cdot \ldots \cdot p_r) \cdot (q_1 \cdot q_2 \cdot \ldots \cdot q_s)$.

ii. *(Unicidade). Suponha que $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r = p'_1 \cdot p'_2 \cdot \ldots \cdot p'_s$, de modo que os p_i e os p'_j são números primos. Como $p_1 | p'_1 \cdot p'_2 \cdot \ldots \cdot p'_s$, então pelo* **Corolário 1.3***, temos que $p_1 = p_j$, para algum j, que podemos supor que seja p'_1 a partir de um reordenamento de $p'_1, \ldots, p'_s$. Portanto,*

$$p_2 \cdot \ldots \cdot p_r = p'_2 \cdot \ldots \cdot p'_s.$$

Como $p_2 \cdot \ldots \cdot p_r < n$, então ocorre, por hipótese da indução, que $r = s$, e assim, $p_i = p'_j$ são iguais aos pares.

■

1.1.9 Congruências

As congruências constituem o ponto central da criptografia RSA, sendo assim vamos descrever a sua definição, bem como algumas de suas propriedades, logo abaixo. Outrossim, apresentaremos o Pequeno Teorema de Fermat que será de grande utilidade para a demonstração do funcionamento do RSA, realizada no capítulo 3 deste trabalho.

Definição 1.8. *Sejam a, b e $m \in \mathbb{Z}$, e $m > 0$. Dizemos que a e b são congruentes módulo m se $m|a - b$. Denota-se*

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

Proposição 1.11. *Sejam a, b, c, d e $m \in \mathbb{Z}$, com $m > 1$.*

i. *Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então $a + c \equiv b + d \ (mod\ m)$.*

Demonstração. *Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então $m|a - b$ e $m|b - c$, desse modo, pela* **Proposição 1.2**, *temos que $m|(a - b) + (c - d)$ que é o mesmo que $m|(a + c) - (b + d)$ o que prova que $a + c \equiv b + d \ (mod\ m)$.*

■

ii. *Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então $ac \equiv bd \ (mod\ m)$.*

Demonstração. *Se $a \equiv b \ (mod\ m)$, então $m|a - b$, implica que $m|a$ e $m|b$, pela* **Proposição 1.2**, *temos que $m|ac$ e também que $m|bd$. Daí $m|(ac) - (bd)$ o que prova que $ac \equiv bd \ (mod\ m)$.*

■

Corolário 1.4. *$\forall\ a, b$ e $n \in \mathbb{Z}$, com $n \geq 1$ tem-se que se $a \equiv b \ (mod\ m)$, então $a^n \equiv b^n \ (mod\ m)$.*

Demonstração. *A prova será realizada por indução sobre n.*
Para $n = 1 : a^1 \equiv b^1 \ (mod\ m) = a \equiv b \ (mod\ m)$.
Suponha agora que: $a^n \equiv b^n \ (mod\ m)$.
Então, como $a \equiv b \ (mod\ m)$ e por hipótese $a^n \equiv b^n \ (mod\ m)$, segue, do item **ii** *da Proposição anterior, que $a \cdot a^n \equiv b \cdot b^n \ (mod\ m)$. Portanto, $a^{n+1} \equiv b^{n+1} \ (mod\ m)$*

■

Definição 1.9. *Sejam $a, m \in \mathbb{Z}$, com $m > 0$. Chamamos de inverso de a módulo m um inteiro b tal que $ab \equiv 1 \ (mod\ m)$.*

Proposição 1.12. *Sejam $a, m \in \mathbb{Z}$, com $m > 0$. Então existe $b \in \mathbb{Z}$ tal que $ab \equiv 1 \ (mod\ m)$ se, e somente se, $mdc(a, m) = 1$*

Demonstração.

($\Rightarrow$) *Se $ab \equiv 1 \ (mod\ m)$, então $m|ab - 1$. Desse modo, existe $n \in \mathbb{Z}$ tal que $ab - 1 = nm$ que é o mesmo que $ab - nm = 1$. E portanto, pelo Teorema de Bachet-Bézout, $mdc(a, m) = 1$.*

($\Leftarrow$) *Se* $mdc(a, m) = 1$, *e como* $a, m \in \mathbb{Z}$, *com* $m > 0$, *então, pelo Teorema de Bachet-Bézout, existem* $b, n \in \mathbb{Z}$ *tais que* $ab - nm = 1$. *o que conclui a prova.*

■

Teorema 1.7 (Pequeno Teorema de Fermat)**.** *Seja* p *um número primo. Se* $p \nmid a$, *então*

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

Demonstração. *Considere o conjunto* $D = \{1, 2, 3, \ldots, p-1\}$, *que corresponde ao conjunto dos restos da divisão de um número inteiro qualquer por* p. *Multiplicando cada um dos elementos deste conjunto por* a, *temos então*

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

Assim, seja $a_i = q_i p + r_i$ *para cada* $i \in \{1, 2, 3, \ldots, p-1\}$, *onde* a_i *corresponde a qualquer elemento da sequência acima e* q_i, r_i *são gerados pelo algoritmo da divisão, podemos escrever*

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

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

$$\vdots \qquad \vdots$$

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

segue, do item **ii** *da* **Proposição 1.11**, *que*

$$a \cdot 1 \cdot a \cdot 2 \cdot \ldots \cdot a \cdot (p-1) \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{p-1} \ (mod\ p)$$

Como no primeiro membro a ocorre $(p-1)$ *vezes, enquanto que no segundo cada* r_i *corresponde a um dos elementos do conjunto* D, *então*

$$a^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \ (mod\ p)$$

Portanto,

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

Da congruência acima tem-se que $\exists\ k \in \mathbb{Z}$ *tal que*

$$a^{p-1} \cdot (p-1)! - (p-1)! = kp$$

$$(a^{p-1} - 1) \cdot (p-1)! = kp$$

Como p é primo, então $p \nmid (p-1)!$. Logo, $p|(a^{p-1}-1)$ o que implica que

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

■

Apresentaremos agora um teorema que generaliza o Pequeno Teorema de Fermat. Esse teorema, bem como todas as suas consequências, é de extremo valor para o estudo de sistemas criptográficos. Trata-se do Teorema de Euler, que nesse trabalho será apenas enunciado. Designaremos por $\varphi(m)$ o número de elementos de um sistema reduzido de resíduos módulo $m > 1$, que corresponde à quantidade de números naturais entre 0 e $m-1$ que são primos com m, mais detalhes em Hefez (2013).

Teorema 1.8 (Teorema de Euler)**.** *Sejam $m, a \in \mathbb{Z}$, com $m > 1$ e $mdc(a, m) = 1$. Então,*

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

Demonstração. *A demonstração pode ser encontrada em* Hefez (2013).

■

Finalizamos os tópicos matemáticos necessários para o entendimento do RSA. No próximo capítulo, serão apresentados conhecimentos fundamentais sobre Criptografia. Veremos também em qual divisão da Criptografia o sistema RSA se encontra.

CAPÍTULO 2

CONHECENDO A CRIPTOGRAFIA

Este capítulo tem como finalidade apresentar a Criptografia ao leitor. Sendo assim, veremos, não só o conceito de Criptografia, mas também alguns de seus termos mais importantes, bem como suas principais divisões. Tudo isso será realizado com base em Azad e Pathan (2015), Kahn (1967), Mollin (2007), Paar e Pelzl (2010), Schneier (1996) e Stallings (2015), que correspondem, nessa ordem aos referenciais [1], [12], [19], [20], [24] e [26].

2.1 O que é criptografia?

Criptografia pode ser entendida como o estudo dos métodos e técnicas que tem como objetivo enviar mensagens de forma secreta (criptografadas), de modo que apenas o destinatário legítimo consiga *decifrar* e ler. A palavra Criptografia, de acordo com as regras da etimologia, é constituída por duas palavras gregas *kryptos*, secreto, e *graphein*, escrita, portanto seu significado literal é "escrita secreta".

Os primeiros registros históricos que se conhecem, em relação a Criptografia, surgiram a aproximadamente 4.000 anos atrás, em uma cidade chamada Menet Khufu na fronteira com o rio Nilo, quando um escriba mestre esboçou hieróglifos contando a história da vida de seu senhor. Não era um sistema secreto nem sofisticado como os sistemas de criptografia atuais. Sua inscrição, embora utilizasse alguns símbolos hieroglíficos incomuns no lugar dos mais comuns, não apresentava intenção em dificultar o entendimento do texto, apenas em conceder dignidade e autoridade a seu senhor.

Mesmo sem pretensão alguma o escriba mencionado acima fez uso do principal objetivo da Criptografia que consiste em esconder, não a existência, mas sim o significado da mensagem desejada. Este objetivo é considerado como um processo vantajoso que tem por finalidade assegurar proteção, em relação a comunicação, fazendo com que se torne "incompreensível" para quem não possuir os requisitos de decifração.

Para fazer com que uma mensagem se torne ininteligível devemos criptografá-la seguindo um protocolo específico, no qual existe um remetente e um destinatário com um acordo já estabelecido, uma espécie de "chave de segurança". Assim, o referido receptor pode reverter o protocolo do codificador e fazer a mensagem compreensível.

No que se refere a linguagem utilizada no processo de criptografia apresentaremos,

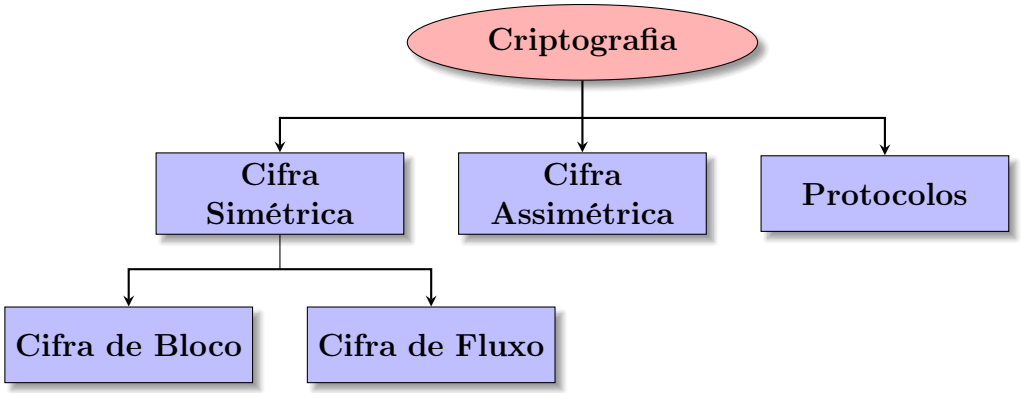
logo abaixo, alguns conceitos importantes, quais sejam:

- *Textos cifrados* são as mensagens criptografadas.
- *Textos comuns* são as mensagens não criptografadas.
- *Chaves de segurança* são recursos matemáticos utilizados, tanto para criptografar, quanto para descriptografar uma mensagem.
- *Criptografar (ou Cifrar)* é o processo de transformação do texto comum em um texto cifrado, de modo que apenas o destinatário, de posse de sua *chave de segurança*, consiga *decifrar*.
- *Descriptografar (ou Decifrar)* é o processo de transformação do texto cifrado no texto comum.
- *Criptoanálise* é a ciência que estuda formas de decifrar uma mensagem sem ter acesso a sua chave de segurança.
- *Bit (Dígito Binário)* é a menor unidade de informação utilizada na computação assumindo somente dois valores 0 ou 1.
- *Caractere* é um sinal gráfico não constituído por sinais menores, como por exemplo uma letra do alfabeto, um algarismo, entre outros.

2.2 Principais divisões da Criptografia

A Criptografia se divide em três dimensões independentes que são: *Cifra Simétrica*, que por sua vez se divide em *Cifra de Bloco* e de *Fluxo*, *Cifra Assimétrica* e os *Protocolos Criptográficos*. Vamos estudar um pouco sobre essas divisões, todavia, para este trabalho, omitiremos qualquer explicação sobre os *Protocolos*.

Figura 2.1: Divisões da Criptografia

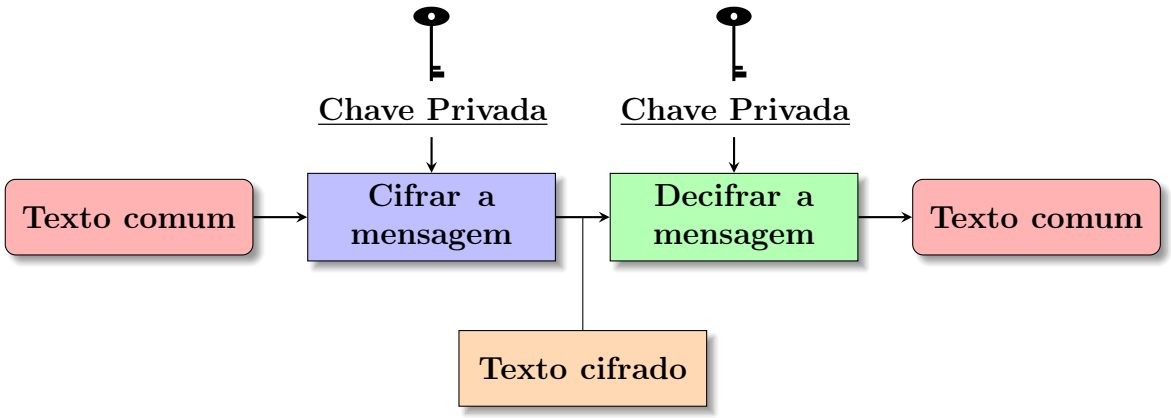


Fonte: Adaptada de Paar e Pelzl (2010).

2.3 Cifra Simétrica

A *Cifra Simétrica (ou Convencional)* é a forma de criptografar, onde se utiliza somente uma chave de segurança, tanto para a cifração, quanto para a decifração de uma mensagem. Esse método de criptografar era o único em uso até 1970, onde passou a dividir espaço com a revolucionária *Cifra Assimétrica*, e mesmo assim, continua sendo o mais utilizado até hoje. A Cifra Simétrica mais utilizada é a *Data Encription Standart (DES)* para mais informações consultar Stallings (2015).

Figura 2.2: Modelo de Cifra Simétrica



Fonte: Adaptada de Junior Cerqueira (2015).

2.3.1 Cifra de Substituição

Antes da criação dos computadores a Cifra Simétrica era constituída por duas técnicas, que não envolviam *bits*, mas sim *caracteres*, a *Cifra de Substituição* e a *Cifra de Transposição*. A *Cifra de Substituição* é uma técnica que consiste em trocar os caracteres de um texto comum por outras letras, números ou símbolos, sem que nenhuma informação se perca e todas as informações sejam reversíveis. Ela é uma das formas de criptografar que apresenta maior simplicidade e se divide em quatro categorias, mas neste trabalho apresentaremos somente duas delas, que são: *Cifra de Substituição Monoalfabética*, que utiliza apenas um alfabeto no processo de cifração e decifração, e *Cifra de Substituição Polialfabética*, que utiliza mais de um alfabeto para cifrar e decifrar uma mensagem.

Como exemplo de Cifra de Substituição Monoalfabética temos a *Cifra de César* que consiste em trocar cada letra por uma outra localizada três posições a sua frente. O nome Cifra de César surgiu a partir da ideia de que Júlio César (100 – 44 a.C.) foi o pioneiro ao utilizá-la. Essa técnica é considerada como o tipo de aplicação por substituição mais antigo que se conhece. Vejamos como ela funciona em um exemplo

Exemplo 2.1. *Criptografe a frase EUSOUALUNODOIFPB ("Eu sou Aluno do IFPB") utilizando a Cifra de César.*

Solução. *Para criptografar a frase pretendida, por meio da Cifra de César precisamos apenas substituir cada letra por outra três posições adiante, Logo*

Texto comum:	*E*	*U*	*S*	*O*	*U*	*A*	*L*	*U*	*N*	*O*	*D*	*O*	*I*	*F*	*P*	*B*
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Texto cifrado:	*h*	*x*	*v*	*r*	*x*	*d*	*o*	*x*	*q*	*r*	*g*	*r*	*l*	*i*	*s*	*e*

É possível Notar que, no **Exemplo 2.1**, 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 representação acima as letras que compõem os textos comuns são letras maiúsculas e as letras responsáveis pela composição dos textos cifrados são minúsculas, todavia, isso não é uma regra e os textos comuns podem ser representados conforme as regras da língua portuguesa ou de qualquer outra língua, sendo assim, o critério utilizado acima deve ser entendido apenas como uma forma de organização para este trabalho. Caso haja a necessidade de utilizarmos outra configuração as frases serão acompanhadas pelos termos *texto comum* e *texto cifrado*.

Na perspectiva de formalizar o processo de criptografar e descriptografar mensagens de modo geral, tomaremos como base uma ideia interessante, que consiste em atribuir a cada letra do alfabeto comum um correspondente numérico

Tabela 2.1: Equivalência entre os números e as letras do alfabeto comum

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

Fonte: Elaboração Própria

A partir da **Tabela 2.1**, podemos definir a Cifra de César da seguinte forma: Para cada letra em texto comum x, e sua equivalente em texto cifrado y, valem as relações $y = C(3, x) \equiv (x + 3) \mod 26$ e $x = D(3, y) \equiv (y - 3) \mod 26$, que correspondem, respectivamente, a cifração e decifração de uma mensagem.

Como um deslocamento, que nomearemos por k, pode ser de qualquer magnitude, ou seja a letra não precisa se deslocar necessariamente apenas 3 posições a sua frente, podemos generalizar a Cifra de César para o caso geral abaixo

Definição 2.3.1. *Para cada letra em texto comum x, e sua equivalente em texto cifrado y, valem as relações*

$$y = C(k, x) \equiv (x + k) \ mod \ 26 \tag{2.1}$$

$$x = D(k, y) \equiv (y - k) \ mod \ 26 \tag{2.2}$$

onde $0 \leq k \leq 25$.

Note que, se $k = 0$, então temos o texto comum igual ao texto cifrado, o que não é interessante se queremos esconder a mensagem a ser transmitida. Nessa perspectiva, se conhecemos que uma mensagem foi criptografada através da Cifra de César, então uma análise criptográfica por força bruta pode ser facilmente executada. Basta testar a condição $0 < k \leq 25$ em outras palavras basta testar os 25 k's restantes.

Para exemplificar utilizaremos o exemplo apresentado por Stallings (2015, p.26), onde houve uma transformação do texto comum ***meet me after the toga party***[2], em cifrado ***PHHW PH DIWHU WKH WRJD SDUWB***, observe:

Figura 2.3: Criptoanálise por força bruta da Cifra de César.

CHAVE	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Fonte: Stallings (2015, p.26)

[2]que quer dizer ***me encontre depois da festa de toga***, um tipo de festa a fantasia com tema greco-romano.

A criptoanálise por força bruta só foi eficaz para esse problema por consequência de três características muito importantes. Em primeiro lugar, as fórmulas do caso geral da Cifra de César são conhecidas, tanto a de cifração, quanto a de decifração, em segundo lugar só precisamos testar os k's, onde $0 < k \leq 25$, e por último a linguagem do texto comum é facilmente reconhecida. Logo, é fácil perceber que a Cifra de César não era tão eficaz no que se refere a segurança de mensagens por ela criptografadas.

Veremos agora um exemplo de *Cifra por Substituição Polialfabética*, sendo uma das mais conhecidas e de fácil compreensão desse grupo, que é a *Cifra de Vigenère*, uma versão aprimorada da ideia inicial de Leon Battista Alberti, Importante Arquiteto do período renascentista, que foi surgindo entre 1460 e 1470. Ela é uma forma de criptografar baseada nas 26 possibilidades dos alfabetos para a Cifra de César, à guisa de ilustração representaremos essa ideia por meio de uma tabela, adaptada de Azad e Pathan (2015), que será intitulada como Grade de Viginère

Figura 2.4: Grade de Vigenère

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

Fonte: Adaptada de Azad e Pathan (2015).

Basicamente essa cifra se resume a cifrar cada letra do texto comum por meio de um dos alfabetos da Grade de Viginère, desse modo para a orientação do receptor da mensagem, uma chave de segurança é fornecida. Por exemplo, suponha que a mensagem abaixo será criptografada

Texto comum: EUSOUALUNODOIFPB (“Eu sou Aluno do IFPB”)

vamos escolher uma chave de segurança com base em dois critérios:

1. A chave pode ter no máximo o mesmo número de caracteres que a mensagem
2. Se a chave de segurança tem menos caracteres que a mensagem, então vamos repetir em sequência os caracteres da chave até que fique com a mesma quantidade de caracteres da mensagem.

desse modo, escolhendo a chave 123, temos:

Texto comum:	E	U	S	O	U	A	L	U	N	O	D	O	I	F	P	B
Chave:	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1

Cada número da chave indica a linha em que se localiza um alfabeto da Grade de Vigenère. Assim, a primeira letra do texto, que é a letra E, é codificada por meio do alfabeto da linha 1, a segunda letra é codificada por meio do alfabeto da linha 2, a terceira letra; por meio do alfabeto da linha 3 e assim sucessivamente até obter

Texto comum:	E	U	S	O	U	A	L	U	N	O	D	O	I	F	P	B
	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|	|
Alfabeto:	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Texto cifrado:	F	W	V	P	W	D	M	W	Q	P	F	R	J	H	S	C

Podemos encontrar uma definição formal para a Cifra de Vigenère, para isso, vamos considerar tanto uma sequência de letras em texto comum $x = x_0, x_1, \ldots, x_{n-1}$, quanto uma chave dada por $k = x_0, x_1, \ldots, x_{m-1}$, em que geralmente $m < n$, consequentemente o texto cifrado $y = y_0, y_1, \ldots, y_{n-1}$ será calculado como:

$$\begin{aligned} y &= E(k, x) \\ y_0, y_1, \ldots, y_{n-1} &= E[(k = k_0, k_1, \ldots, k_{m-1}), (x = x_0, x_1, \ldots, x_{n-1})] \\ &= (x_0 + k_0) \bmod 26, (x_1 + k_1) \bmod 26, \ldots, (x_{m-1} + k_{m-1}) \bmod 26, (x_m + \\ &\quad k_0) \bmod 26, (x_{m+1} + k_1) \bmod 26, \ldots, (x_{2m-1} + k_{m-1}) \bmod 26, \ldots \end{aligned}$$

A partir da ideia acima surge a seguinte definição, que é a generalização da Cifra de Vigenère, onde (2.3) e (2.4) representam, respectivamente, a cifração e a decifração de uma mensagem.

Definição 2.3.1. *Para cada letra em texto comum x_i, e sua equivalente em texto cifrado y_i, valem as relações*

$$y_i \equiv (x_i + k_{i \ mod \ m}) \ mod \ 26 \tag{2.3}$$

$$x_i \equiv (y_i - k_{i \ mod \ m}) \ mod \ 26 \tag{2.4}$$

onde $i = 0, 1, 2, \ldots, n-1$.

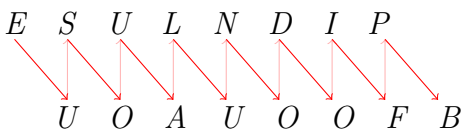
Para uma pessoa comum, esse método de criptografar pode parecer bastante seguro, pois o mesmo apresenta um grande avanço, no que se refere a segurança de uma mensagem. Todavia para um criptoanalista não é tão difícil quebrá-lo utilizando como subsidio formas de distribuição de frequência, para mais detalhes consultar Stallings (2015).

2.3.2 Cifra de Transposição

Enquanto a Cifra de Substituição realiza uma troca de caracteres, a *Cifra de Transposição* realiza apenas uma permutação entre os caracteres do *texto comum*. Um exemplo simples de codificação utilizando a transposição seria a técnica da *Cerca de Trilho*, em que a mensagem é escrita como uma sequência de diagonais e, logo após, é lida como uma linha única obedecendo a ordem da esquerda para a direita. As diagonais desse tipo de cifra apresentam uma ideia de profundidade, sendo assim, se por hipótese temos uma *Cerca de Trilho de profundidade 3*, significa dizer que em cada uma das diagonais da mensagem haverão três caracteres. Logo abaixo apresentamos um exemplo de Cerca de Trilho de profundidade 2.

Exemplo 2.2. *Criptografe a frase EUSOUALUNODOIFPB utilizando o método da Cerca de Trilho com profundidade 2.*

Solução. *Em primeiro lugar vamos escrever a mensagem em diagonais de dois caracteres*



Agora basta escrever como uma linha única respeitando a ordem da esquerda para a direita

Texto cifrado: ESULNDIPUOAUOOFB

É notável que esse tipo de procedimento seria facilmente criptoanalisado. Desse modo, descreveremos abaixo, uma maneira mais complexa de criptografar utilizando a mesma frase do **Exemplo 2.2**.

1. Escolher uma palavra como chave de segurança. Vamos escolher a palavra "ESTUDO".

2. Transformar cada letra em seu equivalente numérico, de acordo com a tabela padrão, que em nosso caso, é a **Tabela 2.1**.

E	S	T	U	D	O
↕	↕	↕	↕	↕	↕
4	18	19	20	3	14

   Essa chave numérica será responsável pela ordenação das colunas, nesse método de criptografar, como mostra o quadro abaixo

Ordem original das colunas:	1	2	3	4	5	6
	|	|	|	|	|	|
Chave de segurança:	4	18	19	20	3	14
	↓	↓	↓	↓	↓	↓
Nova ordem das colunas:	2	4	5	6	1	3

3. Escrever a mensagem no quadro abaixo desprezando qualquer espaço ou acento. Observe que os números acima do quadro, correspondem a nova ordem das colunas geradas pela chave de segurança.

2	4	5	6	1	3
E	U	S	O	U	A
L	U	N	O	D	O
I	F	P	B		

4. Escrever os caracteres de cada coluna do quadro, obedecendo a numeração de cada uma, em somente uma linha.

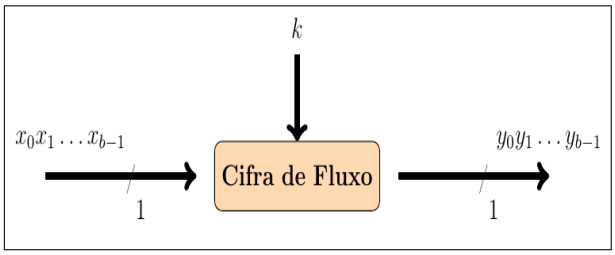
Texto cifrado: UDELIAOUUFSNPOOB

Para descriptografar a mensagem, de posse da chave de segurança, basta realizar o processo inverso.

2.3.3 Cifra de fluxo e Cifra de bloco

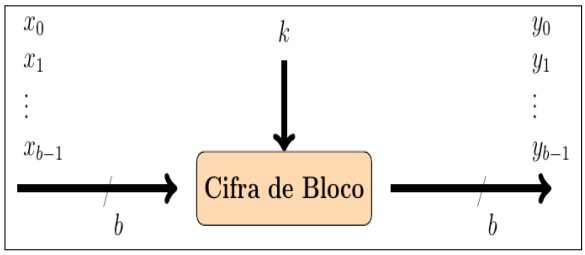
Com a criação dos computadores, e a utilização dos *bits* na Criptografia, a Cifra Simétrica passou a se dividir em duas formas, quais sejam: *Cifra de Fluxo* e *Cifra de Bloco*. A *Cifra de Fluxo* é uma maneira de criptografar *bits* de forma contínua, com saída de um elemento por vez, em contrapartida, a *Cifra de Bloco* sempre processa blocos (conjunto de *bits*) de cada vez, onde todos os blocos tem o mesmo tamanho. Nas figuras abaixo é possível perceber claramente a diferença entre as duas.

Figura 2.5: Modelo de Cifra de Fluxo



Fonte: Adaptada de Paar e Pelzl (2010).

Figura 2.6: Modelo de Cifra de Bloco

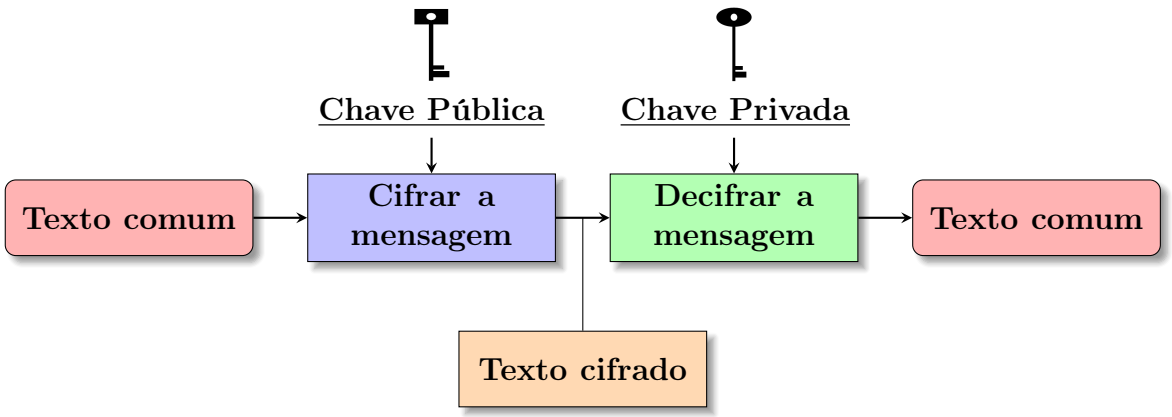


Fonte: Adaptada de Paar e Pelzl (2010).

2.4 Cifra Assimétrica

Ao contrário do modelo de *Cifra Convencional* a *Cifra Assimétrica (ou de Chave Pública)* é a forma de criptografar, onde são utilizadas duas chaves de segurança uma para criptografar, *Chave Pública*, e outra para descriptografar, *Chave Privada*. É importante entender que a Chave Pública é de conhecimento de qualquer pessoa, enquanto que a Chave Privada somente o destinatário tem acesso. Como exemplo temos a *Criptografia RSA*, que é o enfoque deste trabalho.

Figura 2.7: Modelo de Cifra Assimétrica



Fonte: Adaptada de Junior Cerqueira (2015).

Em termos de segurança não é certo pensar que a *Criptografia de Chave Pública* leva

vantagem em relação a *Criptografia Simétrica*, pois o que determina essa segurança é o tamanho da chave, bem como o trabalho computacional realizado para quebrá-la.

Concluímos este capítulo com o modelo de Cifra Assimétrica. A partir dos tópicos estudados, até este momento, adquirimos o conhecimento necessário para entender o Sistema de Criptografia RSA. No próximo capítulo, descobriremos o porquê do nome RSA, estudaremos sua organização, seu funcionamento e discutiremos um pouco sobre a sua segurança.

CAPÍTULO 3

A CRIPTOGRAFIA RSA

Chegamos ao ponto central deste trabalho. É neste capítulo que vamos utilizar todo o conhecimento adquirido anteriormente. Não obstante, faremos essa construção com base em Coutinho (2014), bem como em Freitas, Sousa e Agustini (2004), além de Junior Cerqueira (2015) que são [2], [6] e [11], respectivamente. Vale ressaltar que todas as etapas, vistas aqui, serão necessárias para o bom entendimento da nossa proposta interdisciplinar no capítulo 4.

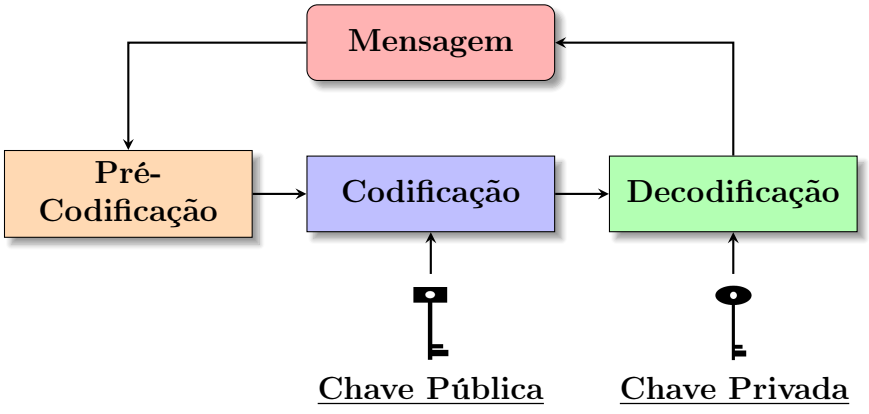
3.1 Algoritmo RSA

O objetivo desta seção é descrever detalhadamente o sistema de Criptografia RSA (ou Algoritmo RSA), que entre todos os métodos de Criptografia de Chave Pública é o mais difundido, ao passo que é o mais utilizado em aplicações comerciais. A sigla RSA corresponde às letras iniciais dos nomes daqueles que inventaram o código, R. L. Rivest, A. Shamir e L. Adleman, em 1977. Levando em consideração o objetivo mencionado acima iniciaremos com a seguinte definição

Definição 3.1 (Algoritmo)**.** *É uma sequência finita e ordenada de passos que têm por finalidade estabelecer a solução para um problema.*

Com base na **Definição 3.1** apresentamos o Algoritmo RSA que é composto por três etapas, quais sejam: Pré-Codificação, Codificação e Decodificação que serão estudadas ao longo deste capítulo.

Figura 3.1: Descrição do Algoritmo RSA.



Fonte: Elaboração Própria

3.1.1 Obtenção das chaves do RSA

Como o RSA é um modelo de *Cifra Assimétrica* existe a necessidade de uma Chave Pública $\{e, n\}$ e de uma Privada $\{d, \Phi(n)\}$, nessa perspectiva essa subseção visa realizar os processos necessários para a obtenção dessas "Chaves". Embora esse tópico possa ser realizado de forma gradativa, a partir de cada etapa do RSA, vamos tratá-lo, neste trabalho, como o passo inicial do Algoritmo RSA que será descrito abaixo:

1. Escolha os parâmetros RSA que basicamente são dois números primos, que vamos representar neste trabalho por p e q com $p \neq q$.
2. Calcule n, que é definido como $n = p \cdot q$.
3. Calcule $\Phi(n) = (p-1)(q-1)$.
4. Escolha $e \in \mathbb{Z}$, com $1 < e < \Phi(n)$, ao passo que $mdc(e, \Phi(n)) = 1$.
5. Encontre $d \in \mathbb{Z}_+$, tal que $de \equiv 1 \ (mod\ \Phi(n))$. Em outras palavras, devemos encontrar d, que é o inverso de e módulo $\Phi(n)$.

Portanto, seguindo essa sequência de passos obtemos $\{e, n\}$ e $\{d, \Phi(n)\}$. Outrossim, no intuito de melhorar a nossa compreensão em relação à obtenção das chaves, veremos como isso funciona em um exemplo.

Exemplo 3.1. *Utilize os passos, de 1 a 5, para obter as chaves, pública e privada, que serão utilizadas no decorrer deste trabalho.*

Solução.

1. *Vamos escolher* $p = 11$ *e* $q = 29$.
2. *Sendo* $p = 11$ *e* $q = 29$, *então* $n = 11 \cdot 29 = 319$.
3. *Utilizando as informações anteriores, temos que* $\Phi(319) = (11-1)(29-1) = 280$.
4. *Nossa escolha será* $e = 3$, *pois* $1 < 3 < 280$ *e* $mdc(3, 280) = 1$.
5. *Como* $e = 3$, *e* $\Phi(n) = 280$, *então:*

$$3 \cdot d \equiv 1 \ (mod\ 280)$$

que equivale a dizer que

$$280 | 3 \cdot d - 1$$

assim, existe um inteiro positivo k, de modo que

$$3 \cdot d - 1 = 280k \text{ ou } 3 \cdot d = 280k + 1 \tag{3.1}$$

note que,

$$3 \cdot 187 = 280 \cdot 2 + 1 \tag{3.2}$$

comparando (3.1) *com* (3.2)*, temos então que* $d = 187$*. Logo a Chave Pública é* $\{3, 319\}$*, enquanto que a Chave Privada é* $\{187, 280\}$*.*

3.1.2 Pré-Codificação

Pré-Codificação é a etapa em que criamos a correspondência entre as letras e os números **Tabela 3.1**. Os números serão escolhidos começando do 10 para evitar que ocorra ambiguidades, pois se escolhêssemos A=1, B=2 ... então o número 12 seria o L, mas devido a representação escolhida o AB, juntos, também seriam 12 o que não pode acontecer. Outrossim, vamos desconsiderar os acentos (ˆ), (´), (`) e o til (∼). Por fim, para esse estudo, vamos considerar que a mensagem seja constituída apenas por letras, e também que o número 99 será um espaço(*space*) entre as palavras de cada frase.

Definição 3.2. *Dados dois conjuntos A e B, uma correspondência biunívoca é a equivalência entre os elementos de A e B, onde cada elemento de A corresponde a um único elemento de B e vice-versa.*

O conjunto das letras, e o espaço em branco, será representado por

$$L = \{\text{A,B,C, } \ldots\text{,J, } \ldots\text{,X,Y,Z, space}\}$$

já o conjunto dos números será

$$S = \{10,11,12, \ldots,19, \ldots,33,34,35,99\}$$

Tabela 3.1: Correspondência biunívoca entre os conjuntos L e S

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	space
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
23	24	25	26	27	28	29	30	31	32	33	34	35	99

Fonte: Elaboração Própria

Exemplo 3.2. *Escreva a frase EU SOU ALUNO DO IFPB de acordo com a* **Tabela 3.1**

Solução. *Precisamos apenas fazer a correspondência entre as letras e os números utilizando a tabela solicitada, desse modo:*

E	U	space	S	O	U	space	A	L	U
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
14	30	99	28	24	30	99	10	21	30
N	O	space	D	O	space	I	F	P	B
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
23	24	99	13	24	99	18	15	25	11

Portanto, a frase EU SOU ALUNO DO IFPB corresponde a:

14309928243099102130232499132499181525 11

Ainda na Pré-codificação dividimos a frase convertida em blocos numéricos, mas para isso precisamos escolher os parâmetros RSA que basicamente são dois números primos, que vamos representar neste trabalho por $p = 11$ e $q = 29$, utilizados no **Exemplo 3.1**. Os números constituintes de cada bloco devem ser menores do que n, onde $n = 11 \cdot 29$, ou seja, $n = 319$. Adotaremos a definição abaixo para prosseguir em nosso trabalho.

Definição 3.3. *Denomina-se bloco, denotado por b, a toda e qualquer parte de um texto convertido em número(s), onde* $0 < b < n$.

Assim, o **Exemplo 3.2**, que foi convertido numericamente pode ser desmembrado como segue abaixo

BLOCOS																			
1	4	309	9	282	4	309	9	102	130	232	49	9	132	49	9	181	5	251	1

Não existe uma única maneira de representar os blocos o que deixa claro que a escolha do seu tamanho é variável e bastante pessoal, ainda que seja interessante quebrarmos a mensagem de modo a não haver unidade linguística, mas é necessário tomar certos cuidados para não comprometer o significado da mensagem original no momento da *Decodificação*. Sendo assim, não é viável escolher um bloco que inicie por 0, pois não teríamos como saber a diferença, por exemplo, entre o bloco 023 e o bloco 23.

3.1.3 Codificação

Para codificar uma mensagem utilizando o método RSA precisamos definir uma fórmula que transforme cada um dos blocos, originados na Pré-Codificação de uma mensagem, em trechos encriptados da mensagem original, que nomearemos por *Codificador*, e que será formalmente apresentada a seguir.

Definição 3.4 (Codificador)**.** *Dados n e e chama-se Codificador de um bloco b, denotado por $C(b)$, o resto da divisão de b^e por n, isto é*

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

com $0 \leq C(b) < n$.

No exemplo abaixo veremos o que vai acontecer com a mensagem pré-codificada do **Exemplo 3.2**, onde utilizaremos a Chave Pública encontrada anteriormente $\{3, 319\}$.

Exemplo 3.3. *De posse da Chave Pública* $\{3, 319\}$*, codifique a frase EU SOU ALUNO DO IFPB, que se encontra pré-codificada, logo abaixo.*

BLOCOS																			
1	4	309	9	282	4	309	9	102	130	232	49	9	132	49	9	181	5	251	1

Solução. *Faremos os cálculos necessários para codificar todos os blocos da mensagem começando do primeiro até chegar ao último com exceção dos blocos que tiverem seus valores numéricos repetidos. Desse modo, temos que:*

$$\begin{aligned} C(1) &\equiv 1^3 \ (mod\ 319) \\ &\equiv 1 \ (mod\ 319) \end{aligned}$$

$$\begin{aligned} C(4) &\equiv 4^3 \ (mod\ 319) \\ &\equiv 4^2 \cdot 4 \ (mod\ 319) \\ &\equiv (-315)^2 \cdot 4 \ (mod\ 319) \\ &\equiv 99225 \cdot 4 \ (mod\ 319) \\ &\equiv 64 \ (mod\ 319) \end{aligned}$$

$$\begin{aligned} C(309) &\equiv 309^3 \ (mod\ 319) \\ &\equiv 309^2 \cdot 309 \ (mod\ 319) \\ &\equiv (-10)^2 \cdot 309 \ (mod\ 319) \\ &\equiv 30900 \ (mod\ 319) \\ &\equiv (-43) \ (mod\ 319) \\ &\equiv 276 \ (mod\ 319) \end{aligned}$$

$$C(9) \equiv 9^3 \ (mod\ 319)$$

$$\begin{aligned}
&\equiv 9^2 \cdot 9 \ (mod\ 319)\\
&\equiv (-310)^2 \cdot 9 \ (mod\ 319)\\
&\equiv 96100 \cdot 9 \ (mod\ 319)\\
&\equiv 400 \cdot 9 \ (mod\ 319)\\
&\equiv 91 \ (mod\ 319)
\end{aligned}$$

$$\begin{aligned}
C(282) &\equiv 282^3 \ (mod\ 319)\\
&\equiv 282^2 \cdot 282 \ (mod\ 319)\\
&\equiv (-37)^2 \cdot 282 \ (mod\ 319)\\
&\equiv 1369 \cdot 282 \ (mod\ 319)\\
&\equiv 93 \cdot 282 \ (mod\ 319)\\
&\equiv (-251) \ (mod\ 319)\\
&\equiv 68 \ (mod\ 319)
\end{aligned}$$

$$\begin{aligned}
C(102) &\equiv 102^3 \ (mod\ 319)\\
&\equiv 102^2 \cdot 102 \ (mod\ 319)\\
&\equiv (-217)^2 \cdot 102 \ (mod\ 319)\\
&\equiv 515 \cdot 102 \ (mod\ 319)\\
&\equiv 52530 \equiv 214 \ (mod\ 319)
\end{aligned}$$

$$\begin{aligned}
C(130) &\equiv 130^3 \ (mod\ 319)\\
&\equiv 130^2 \cdot 130 \ (mod\ 319)\\
&\equiv (-189)^2 \cdot 130 \ (mod\ 319)\\
&\equiv (312) \cdot 130 \ (mod\ 319)\\
&\equiv 40560 \ (mod\ 319)\\
&\equiv 47 \ (mod\ 319)
\end{aligned}$$

$$\begin{aligned}
C(232) &\equiv 232^3 \ (mod\ 319)\\
&\equiv 232^2 \cdot 232 \ (mod\ 319)\\
&\equiv (-87)^2 \cdot 232 \ (mod\ 319)\\
&\equiv 232 \cdot 232 \ (mod\ 319)\\
&\equiv (-87)^2 \ (mod\ 319)
\end{aligned}$$

$$\equiv \quad 232 \ (mod\ 319)$$

$$\begin{aligned} C(49) &\equiv 49^3 \ (mod\ 319) \\ &\equiv 49^2 \cdot 49 \ (mod\ 319) \\ &\equiv 168 \cdot 49 \ (mod\ 319) \\ &\equiv 8232 \ (mod\ 319) \\ &\equiv 257 \ (mod\ 319) \end{aligned}$$

$$\begin{aligned} C(132) &\equiv 132^3 \ (mod\ 319) \\ &\equiv 132^2 \cdot 132 \ (mod\ 319) \\ &\equiv 198 \cdot 132 \ (mod\ 319) \\ &\equiv 26136 \ (mod\ 319) \\ &\equiv 297 \ (mod\ 319) \end{aligned}$$

$$\begin{aligned} C(181) &\equiv 181^3 \ (mod\ 319) \\ &\equiv 181^2 \cdot 181 \ (mod\ 319) \\ &\equiv (-138)^2 \cdot 181 \ (mod\ 319) \\ &\equiv 223 \cdot 181 \ (mod\ 319) \\ &\equiv 40363 \ (mod\ 319) \\ &\equiv 169 \ (mod\ 319) \end{aligned}$$

$$\begin{aligned} C(5) &\equiv 5^3 \ (mod\ 319) \\ &\equiv 5^2 \cdot 5 \ (mod\ 319) \\ &\equiv (-314)^2 \cdot 5 \ (mod\ 319) \\ &\equiv 25 \cdot 5 \ (mod\ 319) \\ &\equiv 125 \ (mod\ 319) \end{aligned}$$

$$\begin{aligned} C(251) &\equiv 251^3 \ (mod\ 319) \\ &\equiv 251^2 \cdot 251 \ (mod\ 319) \\ &\equiv (-68)^2 \cdot 251 \ (mod\ 319) \\ &\equiv 158 \cdot 251 \ (mod\ 319) \\ &\equiv 39658 \ (mod\ 319) \end{aligned}$$

$$\equiv \quad 102 \ (mod\ 319)$$

Portanto, a mensagem codificada é:

BLOCOS																		
1	64	276	91	68	64	276	91	214	47	232	257	91	297	257	91	169	125	102	1

Vale ressaltar que a mensagem, após codificada, jamais pode ser escrita juntando-se seus blocos, pois se isso acontecer será impossível decodificar a mensagem novamente ocasionando um total desperdício de todo o processo feito até aqui.

3.1.4 Decodificação

Para decodificar uma mensagem, criptografada em RSA, vamos precisar de uma fórmula capaz de reverter o processo de Codificação, ou seja, que retorne aos números correspondentes, em nossa tabela de correspondência entre os conjuntos, às letras que compõem a nossa mensagem original. Tal fórmula será denominada nesse estudo por *Decodificador*.

Definição 3.5 (Decodificador)**.** *Dados $C(b)$, n e d chama-se Decodificador de um bloco b, denotado por $D(C(b))$, o resto da divisão de $(C(b))^d$ por n, isto é*

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

com $0 \leq D(C(b)) < n$.

Exemplo 3.4. *De posse da Chave Privada $\{187, 280\}$, determine a mensagem original que se encontra codificada logo abaixo*

BLOCOS																		
1	64	276	91	68	64	276	91	214	47	232	257	91	297	257	91	169	125	102	1

Solução. *Para esse exemplo vamos realizar o procedimento apenas nos dois primeiros blocos, pois os demais podem ser encontrados de modo análogo*

$$\begin{aligned} D(1) &\equiv 1^{187} \ (mod\ 319) \\ &\equiv 1 \ (mod\ 319) \end{aligned}$$

$$\begin{aligned} D(64) &\equiv 64^{187} \ (mod\ 319) \\ &\equiv (64^{10})^{10} \cdot (64^{10})^8 \cdot 64^7 \ (mod\ 319) \\ &\equiv (45)^{10} \cdot (45)^8 \cdot 64^7 \ (mod\ 319) \\ &\equiv (45^2)^5 \cdot (45^2)^4 \cdot 64^7 \ (mod\ 319) \end{aligned}$$

$$
\begin{aligned}
&\equiv (111)^5 \cdot (111)^4 \cdot 64^7 \ (mod\ 319)\\
&\equiv (111)^4 \cdot 111 \cdot (111)^4 \cdot 64^7 \ (mod\ 319)\\
&\equiv 45 \cdot 111 \cdot 45 \cdot 64^7 \ (mod\ 319)\\
&\equiv 45^2 \cdot 111 \cdot 64^7 \ (mod\ 319)\\
&\equiv 111 \cdot 111 \cdot 64^7 \ (mod\ 319)\\
&\equiv 111^2 \cdot 64^7 \ (mod\ 319)\\
&\equiv 199 \cdot 64^7 \ (mod\ 319)\\
&\equiv 199 \cdot 202 \ (mod\ 319)\\
&\equiv 4 \ (mod\ 319)
\end{aligned}
$$

logo, a mensagem decodificada é:

BLOCOS																			
1	4	309	9	282	4	309	9	102	130	232	49	9	132	49	9	181	5	251	1

Portanto, após a organização em blocos de dois algarismos e observação de sua respectiva equivalência com as letras da **Tabela 3.1**, *a mensagem retorna ao seu estado original que é:*

EU SOU ALUNO DO IFPB

3.2 Confiabilidade

Neste tópico vamos discutir um pouco sobre o porquê do RSA ser tão confiável e seguro. Para isso, vamos supor a seguinte situação: *"imagine que o aplicativo Whatsapp utiliza a criptografia RSA para manter a privacidade dos seus usuários; um usuário anônimo que chamaremos de X, interessado em interceptar a conversa de outros que nomearemos por Y e Z, consegue ter acesso as mensagens codificadas de Y e Z".*

Sendo assim, além de estar de posse das conversas criptografadas, X ainda tem acesso a uma das chaves de segurança que é a Chave Pública $\{e, n\}$, onde n é igual ao produto de dois primos p e q escolhidos para a implementação do RSA. Aparentemente, não existe obstáculo algum para que X decodifique as mensagens de Y e Z, uma vez que conhecendo o valor de n ele só vai precisar fatorá-lo, descobrir os valores de p e q, e assim, utilizá-los para calcular d.

Na prática tudo o que foi mencionado acima, mesmo parecendo muito simples, é completamente inviável, pois não existem nem computadores, nem algoritmos com tamanha eficiência, que sejam capazes de nos permitir realizar a fatoração de um número inteiro muito grande que não tenha fatores relativamente pequenos. Para se ter uma noção mais

precisa do tamanho das Chaves Públicas atuais entenda que estamos falando de chaves com até 200 algarismos, sendo que em algumas implementações são admitidas Chaves Públicas com cerca de 2467 algarismos.

O **Teorema 1.6**, Teorema Fundamental da Aritmética, é um dos responsáveis por essa segurança, pois ele garante que só existem p e q, onde p e q são únicos, capazes de gerar n. Sem conhecer p ou q é impossível calcular $\Phi(n)$, por outro lado sem conhecer $\Phi(n)$ é impossível calcular d o que torna inviável qualquer tentativa de decodificar a mensagem sem a chave privada $\{d, \Phi(n)\}$.

Se por hipótese X conhecesse, ou houvesse inventado, um algoritmo capaz de encontrar $\Phi(n)$, onde $\Phi(n) = (p-1)\cdot(q-1)$, a partir de $\{e, n\}$, então ele poderia encontrar p e q observe:

$$\begin{aligned}\Phi(n) &= (p-1)\cdot(q-1)\\ &= pq - p - q + 1\\ &= n - (p+q) + 1\\ &= (n+1) - (p+q)\end{aligned}$$

sendo assim,

$$p + q = n + 1 - \Phi(n)$$

note que,

$$\begin{aligned}(p+q)^2 - 4n &= p^2 + 2pq + q^2 - 4n\\ &= p^2 + q^2 + 2pq - 4pq\\ &= p^2 - 2pq + q^2\\ &= (p-q)^2\end{aligned}$$

o que implica em,

$$p - q = \sqrt{(n + 1 - \Phi(n))^2 - 4n}$$

Portanto, conhecendo $p+q$ e $p-q$ podemos calcular p e q, ou seja fatorar n. Podemos imaginar a possibilidade de achar b, a partir de $C(b) \equiv b^e \ (mod\ n)$, sem tentar achar d, mas isso é inviável se n é muito grande. Ademais, acredita-se que quebrar o RSA seja um problema equivalente à fatorar n, ainda que isso não tenha sido demonstrado até agora.

Por fim, devemos ter cuidado na escolha dos primos p e q, pois se $|p-q|$ for encontrado facilmente, então o sistema estará totalmente comprometido, vale ressaltar ainda,

que a segurança do RSA, além da matemática, depende de outros fatores que não serão discutidos neste trabalho.

3.3 Funcionamento

Se o método RSA funciona, então ele deve cumprir um requisito básico que se resume a: *Se um bloco codificado for decodificado, então obtém-se novamente o bloco correspondente à mensagem original.* Isso não é trivial e surge com base no teorema abaixo que iremos demonstrar afim de deixar claro que o método RSA funciona com perfeição.

Teorema 3.1. *Sejam b, n e $C(b) \in \mathbb{Z}$ tal que $1 \leq b \leq n$, então é valido que $D(C(b)) = b$.*

Demonstração. *Como b e $D(C(b))$ estão entre 1 e $n-1$, então só precisamos provar que $D(C(b)) \equiv b \ (mod\ n)$. Por definição, tanto de D, quanto de C, temos que*

$$\begin{aligned} D(C(b)) &\equiv (C(b))^d \ (mod\ n) \\ &\equiv (b^e)^d \ (mod\ n) \\ &\equiv b^{e\cdot d} \ (mod\ n) \end{aligned}$$

Assim, precisamos mostrar que $b^{e\cdot d} \equiv b \ (mod\ n)$. Sabemos que

$$e \cdot d \equiv 1 \ (mod\ \gamma(n))$$

que implica em,

$$e \cdot d = 1 + \gamma(n) \cdot k$$

Como $n = pq$, onde $p \neq q$, vamos calcular $b^{e\cdot d} \ (mod\ p)$ e $b^{e\cdot d} \ (mod\ q)$, daí

$$\begin{aligned} D(C(b)) &\equiv b^{e\cdot d} \\ &\equiv b^{1+\gamma(n)\cdot k} \\ &\equiv b^{1+k(p-1)(q-1)} \ (mod\ p) \\ &\equiv b \cdot (b^{(p-1)})^{k(q-1)} \ (mod\ p) \end{aligned}$$

Agora precisamos analisar duas situações **i.** *$p|b$ e* **ii.** *$p \nmid b$. Dessa forma, se $p|b$, então*

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

o que implica em,

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

Por outro lado, se $p \nmid b$*, então pelo Teorema de Fermat, temos que*

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

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

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

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

Analogamente, obtemos que

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

Como $b^{e \cdot d} \equiv b \ (mod\ p)$ *e* $b^{e \cdot d} \equiv b \ (mod\ q)$*,então existem* l_1 *e* l_2 *tais que*

$$b^{e \cdot d} = b + l_1 p \ \textit{e também}\ b^{e \cdot d} = b + l_2 q$$

Sendo assim,

$$b^{e \cdot d} - b = l_1 p \ \textit{e}\ b^{e \cdot d} - b = l_2 q$$

Note que $b^{e \cdot d} - b$ *é divisível tanto por* p*, quanto por* q *e também que* $mdc(p, q) = 1$*. Desse modo, pela* **Proposição 1.9**, $pq | b^{e \cdot d} - b$ *e como* $n = pq$*, temos portanto que*

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

Logo, $D(C(b)) = b$

■

Fechamos este capítulo com o "Entendimento" do Algoritmo RSA. Reiteramos que o método RSA é o ponto central deste trabalho e somente entendendo esse sistema de Criptografia é que será possível obter um boa compreensão da nossa proposta interdisciplinar que será vista no capítulo seguinte.

CAPÍTULO 4

PROJETO INTERDISCIPLINAR

Amparados pelos capítulos anteriores podemos dizer que o RSA é um algoritmo de Cifra Assimétrica constituído por três etapas, mas que neste trabalho dividimos em quatro, e que têm forte relação com a Teoria dos Números; é um algoritmo que pode ser forte ou fraco, dependendo de alguns fatores matemáticos, computacionais, entre outros pontos. Neste capítulo vamos utilizar o sistema de Criptografia RSA como proposta interdisciplinar, mas antes de anunciarmos a nossa proposta, vamos discorrer um pouco sobre Interdisciplinaridade balizados em Fazenda (2011), Lenoir (2008), Lück (1995) e Severino (2008). Referenciais [4], [14], [16] e [25].

4.1 Interdisciplinaridade

No que se refere ao campo da ciência, a Interdisciplinaridade corresponde à necessidade de superação da ideia de que o conhecimento se constrói de maneira fracionada, não obstante, representa a concepção de que se faz necessária a articulação entre os múltiplos fragmentos que constituem o conjunto de conhecimentos adquiridos pela humanidade (LÜCK, 1995). Fazenda (2011) corrobora quando define o termo "Interdisciplinaridade" como a cooperação existente entre disciplinas ou setores heterogêneos constituintes de uma mesma ciência na perspectiva de um enriquecimento entre as partes.

Conforme Lenoir (2008) existe uma diferença entre a interdisciplinaridade cientifica e a escolar. Enquanto a interdisciplinaridade científica tem como finalidade as disciplinas cientificas, com vistas a ideia de pesquisa, a interdisciplinaridade escolar apresenta como propósito as disciplinas escolares, na perspectiva de formar e capacitar.

Embora este trabalho seja voltado ao ensino superior, é perceptível a sua proximidade com a ideia de interdisciplinaridade escolar. Isso acontece porque se ampara nas ideias de ensinar, e de formar, e tem como referencial o educando e sua relação com o conhecimento (LENOIR, 2008).

De acordo com Severino (2008) ao questionar o caráter prático da interdisciplinaridade entende-se que:

- Haverá sempre articulação entre as partes e o todo.
- Haverá sempre articulação entre os meios e os fins.

- Haverá sempre o direcionamento à pratica. O saber isolado não apresenta tanta eficácia.
- Precisará sempre ser conduzida de acordo com uma força interna de uma intencionalidade.

Um dos benefícios de utilizar a Interdisciplinaridade está em colaborar para a superação de currículos fragmentados. Possibilitando ao aluno uma visão mais ampla, em relação as disciplinas estudadas. Portanto, é com base nestas ideias sobre Interdisciplinaridade que propomos o projeto a seguir.

4.2 Descrição do projeto

Este projeto interdisciplinar pode ser realizado em vários cursos superiores, que apresentam em sua grade curricular disciplinas baseadas na Teoria dos Números, enquanto campo cientifico, citaremos apenas algumas, quais sejam: Bacharelado e Licenciatura em Computação, bem como a Engenharia da Computação e a Engenharia Elétrica, com a disciplina Matemática Discreta e o Bacharelado ou Licenciatura em Matemática com a disciplina Teoria dos Números.

O mesmo pode ser executado envolvendo um ou mais cursos que contenham pelo menos uma dessas disciplinas, funcionando como um trabalho cooperativo (intercursos) com atribuição de nota pelo professor, ou pelos professores, caso trabalhem em conjunto. Pode envolver ainda, outras disciplinas que contenham programação e se isso for acontecer sugerimos ao leitor consultar o item 2 da **Subseção 4.2.8**. Tudo isso será realizado levando em consideração a flexibilidade e o "bom senso" do professor.

4.2.1 Público-Alvo

Alunos de Bacharelado e/ou Licenciatura em:

- Computação
- Engenharia da Computação
- Engenharia Elétrica
- Matemática

4.2.2 Objetivo Geral

Apontar a Criptografia RSA, através da ideia de Interdisciplinaridade, como estratégia para potencializar o ensino das disciplinas, que surgem com base na Teoria dos Números, nos cursos de graduação supracitados.

4.2.3 Objetivos Específicos

- Reforçar os conceitos de Divisão, Potenciação, Números Primos e Congruências dentro do conjunto dos Números Inteiros presentes na Teoria dos Números.
- Apresentar uma das aplicações da Teoria dos Números com extrema importância para a nossa sociedade.

4.2.4 Conteúdo Programático, Competências, Habilidades e Atitudes/Valores

Conteúdo Programático

Apresentamos o conteúdo programático para a realização deste projeto, que corresponde a:

- Os Números Inteiros
- Propriedades dos números inteiros
- Módulo de um número inteiro
- Indução
- Potenciação nos inteiros
- Divisibilidade
- Divisão Euclidiana
- Máximo Divisor Comum
- Números Primos
- Congruências
- Noções básicas de Criptografia e do algoritmo RSA
- Obtenção das chaves do RSA
- Pré-Codificação
- Codificação
- Decodificação

Competências

As Competências (o saber agir) que devem ser desenvolvidas são:

- Capacidade Para entender cada etapa de uma das aplicações da Teoria dos Números que é o sistema de criptografia RSA.
- Capacidade para entender os conceitos de Teoria dos Números que são a base do Algoritmo RSA.
- Capacidade para identificar as principais características da Teoria dos Números, bem como a sua aplicabilidade no mundo moderno.

Habilidades

As Habilidades (o saber fazer) que devem ser desenvolvidas são:

- Reconhecer as relações da Teoria dos Números com outras áreas do saber e com a segurança da informação.
- Aplicar os conceitos da Teoria dos Números, de acordo com a sua necessidade, em cada etapa do Algoritmo RSA.
- Elaborar relatórios, trabalhos para publicação e seminários relacionados as disciplinas que envolvem Teoria dos Números.

Atitudes/Valores

As Atitudes/Valores que devem ser priorizadas são:

- Demonstrar relações de cooperação, intentando a consolidação de trabalhos em equipe.
- Demonstrar ética, honestidade e responsabilidade nas ações desenvolvidas em sala de aula.
- Demonstrar iniciativa na busca de novas possibilidades e/ou recursos para facilitar o entendimento dos fundamentos básicos da Teoria dos Números.

4.2.5 Protocolo de Execução

Esse projeto deve ser executado em dois momentos, quais sejam:

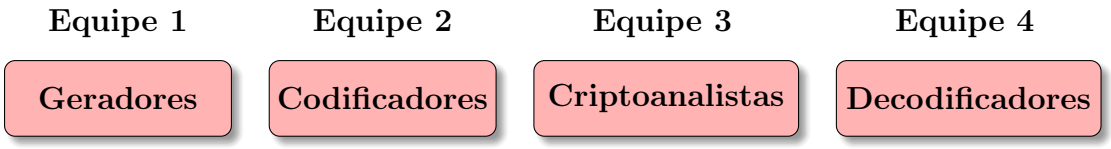
1º Momento

1. É Realizada uma breve revisão dos tópicos de Teoria dos Números, bem como é feita uma ambientação da Criptografia e do Algoritmo RSA. Esse passo deve ser executado de acordo com o conteúdo programático apresentado na subseção **4.2.4**.

2º Momento

1. Divide-se a sala em quatro grupos que serão nomeados respectivamente por: *Geradores*, *Codificadores*, *Criptoanalistas* e *Decodificadores*. Os grupos não precisam conter o mesmo número de integrantes.

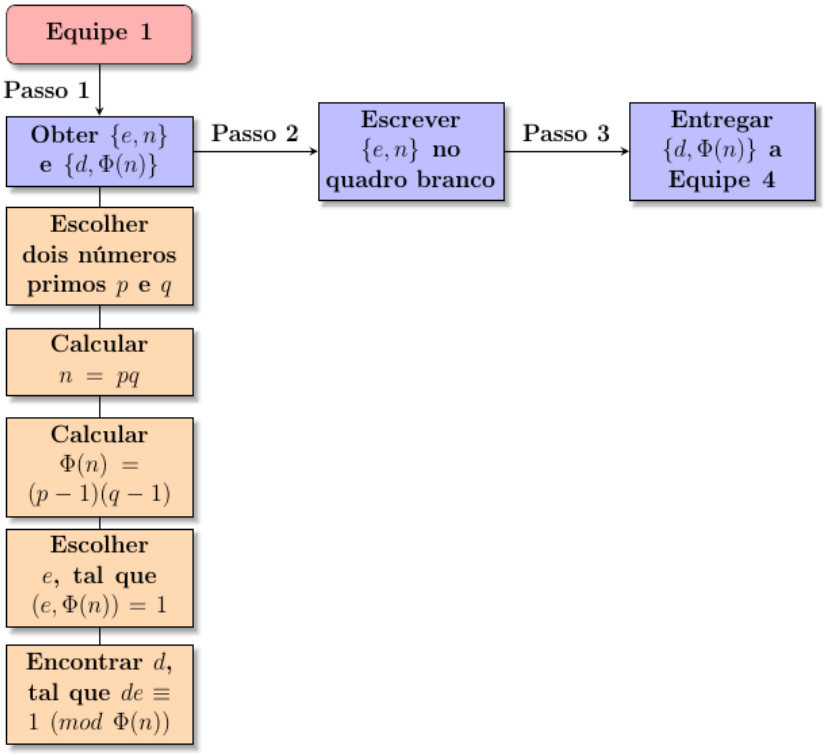
Figura 4.1: Divisão da sala em Equipes



Fonte: Elaboração Própria

2. Os *Geradores* criam as chaves utilizadas no Algoritmo RSA; a Chave Pública é colocada no quadro branco, enquanto que a Chave Privada é entregue aos *Decodificadores*.

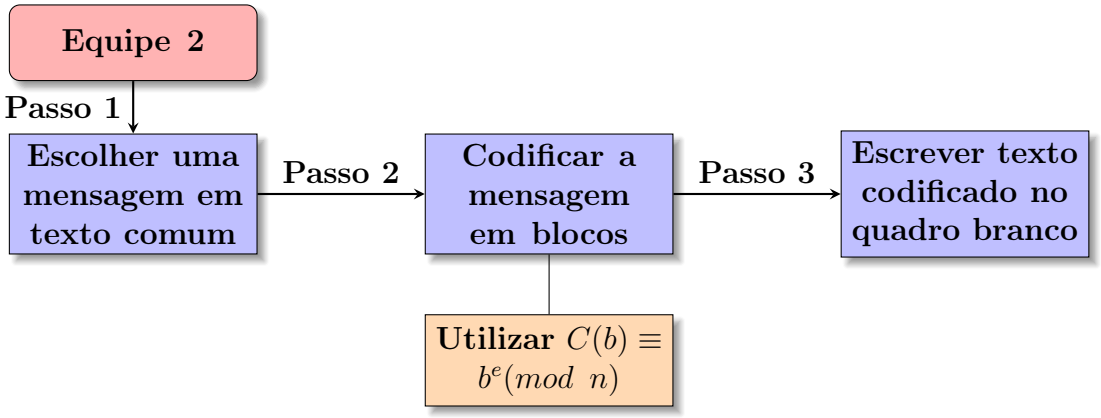
Figura 4.2: Fluxograma de execução da Equipe 1



Fonte: Elaboração Própria

3. De posse da Chave Pública, os *Codificadores* serão responsáveis por escolher uma mensagem em texto comum e em seguida realizar a sua Codificação. Por fim, cabe aos Codificadores, escrever o texto cifrado no quadro branco.

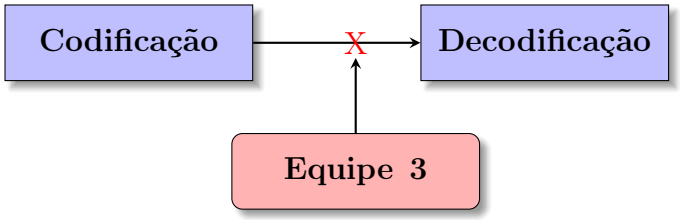
Figura 4.3: Fluxograma de execução da Equipe 2



Fonte: Elaboração Própria

4. Conhecendo a Chave Pública e a mensagem criptografada, ambas escritas no quadro branco, os *Criptoanalistas* serão responsáveis por tentar desenvolver formas de quebrar a criptografia da mensagem, que, para este trabalho, é o mesmo que obter a Chave Privada sem precisar decodificar a mensagem.

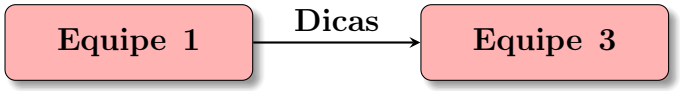
Figura 4.4: Fluxograma de execução da Equipe 3



Fonte: Elaboração Própria

5. Após os 10 primeiros minutos, do texto criptografado escrito no quadro branco, os *Geradores* serão responsáveis por fornecer uma dica, que tenha relação com o algoritmo de geração das chaves, aos *Criptoanalistas*. Depois disso, a cada 20 minutos deverá ser dada uma nova dica até completar o total de 5 dicas.

Figura 4.5: Fluxograma da relação entre as Equipes 1 e 3



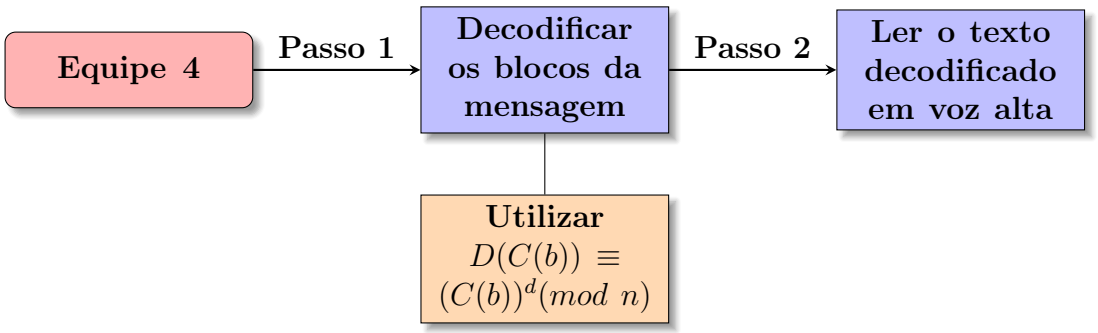
Fonte: Elaboração Própria

Atenção: Não serão aceitas dicas que entreguem alguma parte do algoritmo, sem que haja um pequeno esforço da **Equipe 3** para decifrá-las, por exemplo, supondo que a Chave Privada seja $\{5, 7\}$:

i. $d = 5$ (Invalida). **ii.** d é duas vezes o número e mais a metade de n. (Válida).

6. Os *Decodificadores* serão responsáveis por decodificar a mensagem, e, ao final da atividade, deverão ler o significado da mesma em voz alta.

Figura 4.6: Fluxograma de execução da Equipe 4



Fonte: Elaboração Própria

4.2.6 Materiais

Serão utilizados os seguintes Materiais:

- Lápis;
- Borracha;
- Calculadora;
- Folhas de papel em branco.

4.2.7 Avaliação da Aprendizagem

A avaliação será realizada com base nos seguintes critérios:

- Compreensão dos tópicos da Teoria dos Números e do Algoritmo RSA;
- Aplicação coerente dos conceitos da Teoria dos Números, conforme a sua necessidade, em cada uma das etapas do Algoritmo RSA.
- Honestidade na execução de cada passo;

4.2.8 Algumas sugestões

1. Sugerimos que fique a critério do professor aumentar ou diminuir, tanto o primeiro momento, quanto o segundo, com base em sua flexibilidade.

2. Caso o curso superior apresente em seu currículo disciplinas que envolvam programação, é interessante que algumas das etapas do segundo momento do projeto sejam solicitadas em linguagem de programação, que podem ser: C, Pyton, entre outras. Um modelo interessante misturando RSA e Pyton pode ser encontrado em https://github.com/Everton42/video-youtube-rsa/tree/master/rsa-em-python.

3. Ao professor interessado em aplicações mais práticas sugerimos alguns *softwares* para *Smartfones*, disponíveis no *Google Play Store*, que são destinados a realizar as etapas do algoritmo RSA. Basta digitar no campo de busca do mesmo o nome *Criptografia RSA* e selecionar o aplicativo que desejar utilizar. E com essas 3 sugestões fechamos o nosso trabalho.

CONSIDERAÇÕES

Finalizamos este trabalho enfatizando a notoriedade da criptografia na sociedade moderna, pois podemos encontra-lá em aplicativos como o *Whatsapp*, *Telegram*, em assinaturas digitais, entre outras funcionalidades que apresentam extrema importância para a sociedade atual. Enfatizamos, ainda o seu potencial para despertar a curiosidade e interesse dos alunos em todos os níveis de ensino.

Nossa intenção era apresentar a Criptografia como uma possibilidade para potencializar o ensino da Teoria dos Números nos cursos de graduação, e para tanto, recorremos aos conceitos de Interdisciplinaridade e Criptografia RSA, uma vez que este último constitui uma de suas principais aplicações. Com esse objetivo propomos a nossa intervenção através de um projeto interdisciplinar, de maneira que os alunos entrem em contato com cada parte do RSA, ao passo que necessitem dos conceitos de Teoria dos Números para concluir as etapas desse projeto.

A contribuição realizada nesse trabalho foi de extrema importância para a minha formação, a medida que passei a enxergar a Teoria dos Números como uma disciplina base para conhecimentos extracurriculares que envolvem a segurança e privacidade do mundo moderno.

Vale ressaltar que a pesquisa realizada nesse estudo não se esgota, bem como sinaliza algumas possibilidades interessantes que envolvem a Criptografia nos cursos superiores, tais como: a Cifra de Hill, como proposta interdisciplinar, nos cursos superiores que contenham a disciplina de Álgebra Linear, a Criptografia como proposta, para potencializar o estudo das funções e suas inversas, a relação Criptografia e Códigos de Barras, como recurso potencial, para o ensino da Teoria dos Números, entre outras.

Por fim, esperamos que esta contribuição possa auxiliar professores de Teoria dos Números a potencializar suas aulas, melhorando a apropriação do saber por parte dos alunos, bem como atribuindo uma finalidade a essa área da matemática enquanto disciplina nos cursos superiores, de modo a facilitar a sua aprendizagem para todos os discentes.

REFERÊNCIAS

[1] AZAD, Saiful; PATHAN Al-Sakib Khan. **Pratical Cryptography: Algorithms and Implementations Using C++**. CRC Press, 2015.

[2] COUTINHO, Severino Collier. **Números Inteiros e Criptografia RSA**. 2. ed. Rio de Janeiro: IMPA, 2014.

[3] DOMINGUES, Hyguino Hugueros. **Fundamentos de aritmética**. São Paulo: Atual, 1991.

[4] FAZENDA, Ivani Catarina Arantes. **Integração e interdisciplinaridade no ensino brasileiro: Efetividade ou ideologia**. São Paulo: Loyola, 2011.

[5] FILHO ALENCAR, Edgard de. **Teoria Elementar dos Números**. São Paulo: Nobel, 1981.

[6] FREITAS, Helén Cristina de; SOUSA, Angélica Silva de; AGUSTINI, Edson. **Um Enfoque Computacional da Criptografia RSA**. FAMAT em Revista, Minas Gerais, 2004.

[7] GALDINO, Uelder Alves. **Teoria dos Números e Criptografia com Aplicações Básicas**. 2014. Dissertação (Mestrado Profissional em Matemática) – Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia.

[8] GIBBS, Graham. **Análise de dados qualitativos**. Tradução de Roberto Cataldo Costa. Coleção Pesquisa Qualitativa. Porto Alegre: Artmed, 2009.

[9] GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

[10] HEFEZ, Abramo. **Aritmética**, Coleção PROFMAT. 1.ed. Rio de Janeiro: SBM, 2013.

[11] JUNIOR CERQUEIRA, Luciano de Souza. **Criptografia RSA: Uma aplicação de Teoria dos números**. 2015. 56f. Dissertação (Mestrado Profissional em Matemática) – Universidade Federal do Recôncavo da Bahia, Centro de Ciências Exatas e Tecnologias, Cruz das Almas, Bahia.

[12] KAHN, David. **The Codebreakers: The Story of Secret Writing**. New York: Macmillan, 1967.

[13] LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia cientifica**. 5. ed. São Paulo: Atlas, 2003.

[14] LENOIR, Yves. **Didática e Interdisciplinaridade: uma complementaridade necessária e incontornável**. In: FAZENDA, I. C. A. (Org). Didática e interdisciplinaridade. 13. ed. Campinas: Papirus, 2008.

[15] LOPES, Gabriela Lucheze de Oliveira; LOPES, Jaques Silveira. **Criptografia: A evolução histórica e seu potencial como ferramenta no ensino da Teoria dos Números nos cursos de Licenciatura em Matemática**. V Congresso Nacional de Educação, Olinda, 2018.

[16] LÜCK, Heloisa. **Pedagogia interdisciplinar: fundamentos teórico-metodológicos**. Petrópolis: Vozes, 1995.

[17] MACHADO, Anderson Pinheiro. **Teoria dos Números e Criptografia RSA: uma proposta de ensino para alunos de matemática olímpica**. 2018. Dissertação (Mestrado Profissional em Matemática) – Universidade Federal de Santa Maria, Centro de Ciências Naturais e Exatas, Rio Grande do Sul.

[18] MOLINARI, José Robyson Aggio. **Números primos e a criptografia RSA**. 2016. 54f. Dissertação (Mestrado Profissional em Matemática) – Universidade Estadual de Ponta Grossa, Ponta Grossa.

[19] MOLLIN, Richard A. **An Introduction to Cryptography**. 2. ed. Chapman & Hall/CRC, 2007.

[20] PAAR, Christof; PELZL, Jan. **Understanding Cryptography: A Textbook for Students and Practitioners**. Springer, 2010.

[21] PRODANOV, Cleber Cristiano.; FREITAS Ernani Cesar de. **Metodologia do trabalho cientifico: métodos e técnicas de pesquisa e do trabalho acadêmico**. 2. ed. Novo Hamburgo: Feevale, 2013.

[22] RESENDE, Marilene Ribeiro; MACHADO, Sílvia Dias Alcântara. **O ensino de matemática na licenciatura: a disciplina Teoria Elementar dos Números**. Revista educação matemática pesquisa, São Paulo, v. 14, n. 2, p. 257-278, 2012.

[23] SANTOS, José Plínio de Oliveira. **Introdução a Teoria dos Números**. Rio de Janeiro: IMPA, 1998.

[24] SCHNEIER Bruce. **Applied Cryptography**. 2. ed. John Wiley & Sons, 1996.

[25] SEVERINO, Antônio Joaquim. **O Conhecimento Pedagógico e a Interdisciplinaridade: o saber como intencionalização da prática**. In: FAZENDA, I. C. A. (Org). Didática e interdisciplinaridade. 13. ed. Campinas: Papirus, 2008.

[26] STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas**. 6. ed. Tradução de: Daniel Vieira. São Paulo: Pearson Education do Brasil, 2015.