UNIVERSIDADE FEDERAL DO RECÔNCAVO DA BAHIA
CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS
MESTRADO EM MATEMÁTICA

CRIPTOGRAFIA RSA: UMA APLICAÇÃO DE TEORIA DOS NÚMEROS

LUCIANO DE SOUZA CERQUEIRA JUNIOR

CRUZ DAS ALMAS
2015

CRIPTOGRAFIA RSA: UMA APLICAÇÃO DE TEORIA DOS NÚMEROS

LUCIANO DE SOUZA CERQUEIRA JUNIOR

Trabalho de conclusão de curso apresentado ao curso de Mestrado Profissional em Matemática do Centro de Ciências Exatas e Tecnológicas da Universidade Federal do Recôncavo da Bahia e a Sociedade Brasileira de Matemática, como parte dos requisitos para a obtenção do título de mestre.

Orientador: Profº Dr. Eleazar Madriz Lozada

CRUZ DAS ALMAS
2015

FICHA CATALOGRÁFICA

C416c

Cerqueira Junior, Luciano de Souza.

Criptografia RSA: uma aplicação de teoria dos números / Luciano de Souza Cerqueira Junior._ Cruz das Almas, BA, 2015.

56f.; il.

Orientador: Eleazar Gerardo Madriz Lozada.

Dissertação (Mestrado) – Universidade Federal do Recôncavo da Bahia, Centro de Ciências Exatas e Tecnológicas.

1.Matemática – Criptografia. 2.Matemática – Teoria dos números. I.Universidade Federal do Recôncavo da Bahia, Centro de Ciências Exatas e Tecnológicas. II.Título.

CDD: 512.7

Ficha elaborada pela Biblioteca Universitária de Cruz das Almas - UFRB.

CRIPTOGRAFIA RSA: UMA APLICAÇÃO DE TEORIA DOS NÚMEROS

LUCIANO DE SOUZA CERQUEIRA JUNIOR

Trabalho de conclusão de curso apresentado ao curso de Mestrado Profissional em Matemática do Centro de Ciências Exatas e Tecnológicas da Universidade Federal do Recôncavo da Bahia e a Sociedade Brasileira de Matemática, como parte dos requisitos para a obtenção do título de mestre.

Banca Examinadora:

Orientador: Eleazar

Profº Dr. Eleazar Gerardo Madriz Lozada - UFRB

Membro: Adson Mota Rocha

Profº MSc. Adson Mota Rocha - UFRB

Membro:

Profº Dr.Pedro José Di Novella Cordero - UFBA

Cruz das Almas, 26 de Novembro de 2015.

Aos meus pais,
às minha irmãs e minha amada esposa
com muito amor.

"Se as pessoas não acham a Matemática simples é só por que ainda não perceberam o quanto a vida é complicada"

John von Neumann

AGRADECIMENTOS

Agradeço, essencialmente a Deus pelo Seu amor incondicional, pelo Seu amparo diante aos obstáculos que a vida me impôs e por ter permitido o cumprimento desta importante etapa da minha vida.

Agradeço ao meus pais, que sempre me incentivou nos estudos, as minhas irmãs, a minha família, a minha irmã Luciana, por estarmos juntos nesta jornada vivendo as mesmas dificuldades e felicidades.

Agradeço a minha esposa Maíra, pelo amor, confiança, incentivo, dedicação, e por todo o sacrificio que fez para que este momento pudesse se concretizar.

A Instituição e a todos que a compõem.

Ao professor e orientador Profº Dr. Eleazar Madriz, pelas contribuições, pela orientação, que me levaram a execução e conclusão deste trabalho.

A todos os colegas do mestrado, que contribuíram diretamente nesta etapa de novos conhecimentos. Por terem sido companheiros em todos os momentos.

A todos aqueles que direta ou indiretamente contribuíram para a realização deste trabalho de alguma forma, a todos que passaram pela minha vida e colaboraram para a construção de quem sou hoje. Os meus sinceros agradecimentos.

Agradeço ao professor Gilberto Pina, pelo o bom curso ministrado de MA14 o que influenciou na escolha do meu tema.

Enfim, a todos os que, de alguma maneira, contribuíram para a conclusão de mais esta fase da minha vida, os meus sinceros agradecimentos.

Luciano de Souza Cerqueira Junior

RESUMO

No âmbito da tecnologia de informação, a Criptografia é importante para que se possa garantir a segurança em todo o ambiente computacional que necessite de sigilo em relação às informações como: transações bancárias no internet banking, compras via internet, entre outras operações. Este tema tem bastante relevância na Matemática, pois o método RSA é uma aplicação da Teoria dos Números, que mostra aos alunos a importância do estudo da ciência matemática. Este trabalho consiste na apresentação de conteúdos matemáticos relacionados com a Criptografia, para isso são descritos todos os conteúdos pertinentes ao estudo, tais como elementos básicos da teoria dos números: conjunto dos naturais, indução, números inteiros, divisibilidade, divisão euclidiana, máximo divisor comum, números primos e congruência, além dos processos de pré-codificação, codificação e decodificação. Ao final, ver uma aplicação da criptografia RSA e propomos umas atividades envolvendo codificação e decodificação para serem desenvolvidas em sala de aula.

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

ABSTRACT

Inside of the information technology environment, the encryption is important to keep the safety of the whole computer environment that needs confidentiality in relation to information such as banking transactions, online buys, etc. This point is very relevant in mathematics because the RSA method is an application of the theory of numbers, showing the students the importance of the mathematics study as a science. This project brings an introduction of mathematics contents related to the RSA encryption, and for this, all the contents related to this study are described, such as basic elements of the theory of numbers, the natural group, induction, integer numbers, divisibility, Euclidian division, greatest common divisor, prime numbers and congruency. We present the processes of pre-coding, coding and enconding so that we can show in which case the RSA algorithm works and if it is possible to be broken, it means somebody to figure it out an information without being the sender or receiver of the message. At the end, we bring an application of the RSA encryption and propose some activities related to coding and decoding.

Keywords: Theory of numbers, encryption, RSA encryption.

SUMÁRIO

INTRODUÇÃO

O homem sentiu desde muito cedo, a necessidade de guardar informações em segredo; ela ampliou com a diplomacia e com as transações militares ao decorrer dos séculos. Generais, reis e rainhas, durante milênios, buscavam formas eficientes de comunicação para comandar os seus exércitos e governar seus países. A importância de não revelar segredos e estratégias as forças inimigas, motivou o desenvolvimento de códigos, cifras e técnicas para codificar uma mensagem, possibilitando apenas ao destinatário ler o conteúdo.

Tendo em vista a necessidade de se criar ferramentas capazes de proteger a informação e de prover a segurança aos documentos armazenados e transmitidos pelas organizações através do mundo, tem-se a motivação para o estudo da **Criptografia** que decorre de duas palavras gregas: *kriptos* que siginifica esconder, ocultar, secreto e *graphein*(grafria) que significa escrever.

Na época atual, entretanto, com o advento da comunicação eletrônica, a Criptografia deixou de ser unicamente segredo de estado ou de um Rei para o seu general, pois muitas atividades essenciais dependem do sigilo na troca de mensagens, principalmente aquelas que envolvem transações financeiras e o uso seguro da internet. Alguns exemplos onde ocorre aplicação da Criptografia atual: sigilo em bancos de dados, censos, investigações governamentais, dossiês de pessoas sob investigação, dados hospitalares, informações de crédito pessoal, comandos militares, mensagens diplomáticas, operações bancárias, comércio eletrônico.

De acordo com Staling em [6], atualmente a criptografia vai além da função de gerar priva-

cidade na troca de informações.Ela também tem a função de:

- **Autentificar**: confirmar que certa informação é verdadeira;
- **Irretratabilidade**: função que impossibilita ao emissor negar a autoria da mensagem;
- **Integridade:** garantir que a mensagem não foi modificada durante seu envio.

A criptografia utiliza diversos ramos da matemática, dentre os quais podemos citar: a cifra de César que neste trabalho apenas fazemos um comentário breve. Está relacionada a aritmética modular e pode ser entendido como uma lei algébrica ou uma função de acordo o público alvo; o RSA com o problema da fatoração de números inteiros e a utilização de congruência.

Por causa dessa intensa relação entre matemática e criptografia, e seu imprescindível uso nos temas atuais, propomos apresentar a relação existente entre o tema Criptografia RSA e conteúdos de Teoria do números, para os alunos do ensino básico e professores que busquem desenvolver novas atividades didáticas.

Afim de apresentar uma visão geral do trabalho, fornecemos uma breve descrição dos temas abordados em cada capítulo. No primeiro capítulo chamamos de preliminares, pois tem todo conteúdo matemático necessários para aplicação do método RSA. No segundo descrevemos do que se trata a criptografia e sua divisão em assimétrica e simétrica. No terceiro descrevemos o algoritmo RSA, desde a pré-codificação, codificação e por fim decodificação. Ainda nesse capítulo mostramos que de fato o algoritmo é útil, falamos as dificuldades em "quebrar"e sua aplicação que é a assinatura digital muito utilizada em operações bancárias. No último capítulo apresentamos algumas propostas de atividades envolvendo o tema, como aplicação.

CAPÍTULO 1

PRELIMINARES

NESTE trabalho o conjunto dos números inteiros é de muita importância, assim como o conjunto dos inteiros não negativos $(\mathbb{Z}_+)$ e conjunto dos naturais $(\mathbb{N})$. Neste capítulo, apresentaremos alguns pontos da teoria dos números importantes para compreender o método RSA. Ao final utilizaremos os resultados para codificar e decifrar de maneira mais rápida. Pautamos este capítulo nas referências: [1], [2], [3], [4] e [5].

1.1 Números naturais

Os números naturais é construído com um conjunto de axiomas que foi apresentado pelo italiano Giuseppe Peano no século XIX, onde ele se fundamenta em três conceitos básicos: o zero, o números natural e a relação de sucessor, para caracterizá-los formulou os seguintes axiomas descritos abaixo.

1.1.1 Axiomas de Peano

$(P_1)\ 0 \in \mathbb{N}$.

$(P_2)\ a \in \mathbb{N} \Rightarrow a+1 \in \mathbb{N}$.

$(P_3)\ (\forall a)\ (a \in \mathbb{N} \Rightarrow a+1 \neq 0)$.

$(P_4)\ a+1 = b+1 \Rightarrow a = b$.

(P_5) Se $S \subset \mathbb{N}$ e

i) $0 \in S$

ii) $a \in S \Rightarrow a+1 \in S$,

então $S = \mathbb{N}$.

1.2 Princípio da Indução Finita

O último dos axiomas de Peano é conhecido como o *axioma da indução* e gera o que é conhecido como o primeiro princípio de indução, o qual enunciamos a continuação.

Proposição 1.1. *(Primeiro Princípio de Indução) Suponhamos que a todo natural n esteja associada uma afirmação $P(n)$ tal que:*

i) $P(0)$ é verdadeira;

ii) $P(n+1)$ é verdadeira,sempre que P(n) é verdadeira.

Então $P(n)$ é válida qualquer que seja o número natural n.

Demonstração: A demonstração decorre do último axioma de Peano, maiores detalhes em [1].

■

Além do primeiro princípio de indução, existe outro tipo de princípio que envolve k hipóteses, isto é, formalmente o seguinte teorema.

Teorema 1.1. *(Segundo Princípio de Indução) Seja $P(n)$ uma sentença sobre $\mathbb{N}$, com $n \geq a$ para alguma $a \in \mathbb{N}$. Admitamos ainda que seja possível provar as condições seguintes.*

i) $P(a)$ é verdade;

ii) Seja $r > a$, se $P(k)$ é verdadeira sempre que $a \leq k < r$, então $P(r)$ também é válida.

Então $P(n)$ é válida para todo $n \geq a$..

Demosntração:
Seja o conjunto

$$D = \{n \in \mathbb{N} | \ m \geq a \ e \ P(m) \ falsa\}.$$

Iremos mostrar que $D = \emptyset$. Vamos supor por absurdo, que vale o contrário. Seja t o menor elemento do conjunto D. Como $P(a)$ é verdadeira, devido a hipótese $i)$, então $t > a$. Logo, para todo $k \in \mathbb{N}$, $a \leq k < t$, $P(k)$ é verdadeira, devido à t ser o mínimo dos $m \geq a$ para os quais $P(m)$ não é válida. Agora, pela hipótese $ii)$, $P(t)$ também é verdadeira, o que é uma contradição.
Portanto, $D = \emptyset$ e $P(m)$ é verdadeira para todo $m \geq a$.

■

1.3 Adição e Multiplicação

Sobre os números naturais consideraremos as operações de adição e multiplicação definidas axiomaticamente.

ADIÇÃO: Sejam $(x, y) \ \rightarrow \ x + y$ em $\mathbb{N}$ é definida mediante as seguintes condições:

- $m + 0 = m$
- $m + (n + 1) = [(m + n) + 1]$

Dizemos que

$$m + n = p,$$

onde m e n são as parcelas e p a soma.

MULTIPLICAÇÃO: Dados $(x, y) \ \rightarrow \ x \cdot y \ (ou \ xy)$ de números naturais é definida pelas condições seguintes:

- $m \cdot 0 = 0$
- $m \cdot (n + 1) = mn + m$

Em uma multiplicação

$$mn = p,$$

onde m e n são os fatores e p o produto.

A adição e multiplicação verificam as seguintes propriedades enunciadas abaixo:

1. A adição e a multiplicação são comutativas:

$$\forall\, a, b \ \in \mathbb{N},$$
$$a + b = b + a \ e$$
$$a \cdot b = b \cdot a$$

2. A adição e a multiplicação são associativas:

$$\forall a, b, c \ \in \mathbb{N},$$
$$(a + b) + c = a + (b + c) \ e$$
$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

.

3. A adição e a multiplicação possuem elementos neutros:

$$\forall a \ \in \mathbb{N}, \ a + 0 = a \ e$$
$$a \cdot 1 = a$$

4. A multiplicação é distributiva com relação à adição:

$$\forall\, a, b, c \ \in \mathbb{N},$$
$$a \cdot (b + c) = a \cdot b + a \cdot c$$

.

1.4 Potência de um número natural

A partir das multiplicação sobre os números naturais podemos definir recursivamente a potência dos números naturais, definição que enunciamos a seguir.

Definição 1.1. *Seja a um número natural e n um número natural. Potência de base a e expoente n é o número a^n tal que:*

(i) $a^0 = 1$

(ii) $a^i = a^{i-1} \cdot a$, $1 \leq i \leq n$.

A partir da definição 1.1 o do fato da multiplicação ser associativa decorre que:

$$a^1 = a^0 \cdot a = 1 \cdot a$$

$$a^2 = a^1 \cdot a = a \cdot a$$

$$a^3 = a^2 \cdot a = a \cdot a \cdot a$$

$$\cdots$$

$$a^i = a^{i-1} \cdot a = a \cdots a$$

e, desta forma, para k natural maior ou igual a 2, temos que a^k é um produto de k fatores iguais a a.

1.5 Princípio da Boa Ordem

O princípio fundamental para a prova do Teorema de Bachet-Bézout é o princípio da boa ordem, o qual estabelece que qualquer subconjunto não vazio dos naturais tem um menor elemento.

Definição 1.2. *Seja $S \subset \mathbb{N}$. Chama-se elemento mínimo de S um elemento a de S tal que $a \leq x$ para todo $x \in S$*

O menor elemento de S, quando existe, é denotado por ***min*** *S.*

Teorema 1.2. *(Principio da Boa Ordem) Todo subconjunto não vazio do conjunto dos naturais possui um menor elemento.*

Demonstração: Seja S um subconjunto não vazio de $\mathbb{N}$. Suponhamos, por absurdo, que S não possua um menor elemento. Mostraremos que S é $\emptyset$, conduzindo a um absurdo.
Considere o conjunto K, complementar de S em $\mathbb{N}$, ou seja, o conjunto dos números naturais que não estão em S. Queremos mostrar então que $K = \mathbb{N}$, ou seja, que $S = \emptyset$. Define-se o conjunto

$$I_n = \{k \in \mathbb{N} | \ k \leq n\},$$

e considere a sentença aberta

$$P(n) : I_n \subset K$$

Como $1 \leq n$, para todo $n \in \mathbb{N}$ segue-se que $1 \in K$, pois, caso contrário, 1 seria um menor elemento de S. Logo, $P(1)$ é verdadeira.
Suponha que $P(n)$ seja verdadeira, para algum n. Se $n+1 \in S$, como nenhum elemento de I_n está em S, teríamos que $n+1$ é um menor elemento de S, o que não é permitido. Logo, $n+1 \in K$, seguindo daí que

$$I_{n+1} = I_n \cup \{n+1\} \subset K,$$

o que prova que, para todo n, temos que $I_n \subset K$; portanto, $\mathbb{N} \subset K \subset \mathbb{N}$ e , consequentemente, $K = \mathbb{N}$.

■

1.6 Números Inteiros

No conjunto dos números naturais a diferença entre dois elementos nem sempre está bem definida, somente no caso em que um seja maior que o outro. Está observação motiva a construção dos números inteiros. Assim, neste trabalho assumiremos que o conjunto dos números inteiros está definido como o conjunto quociente gerado pela a seguinte relação sobre $\mathbb{N} \times \mathbb{N}$, definida por

$$(m,n) \sim (r,s) \Leftrightarrow m+s = n+r.$$

Além disso, admitiremos que o conjunto dos números inteiros possui uma estrutura de Anel comutativo com identidade em relação a adição e a multiplicação definida na continuação.

Definição 1.3. *(Adição) Sejam $m, n \in \mathbb{Z}$ tal que, $m = \overline{(x,y)}$ e $n = \overline{(z,w)}$. Chama-se soma de m com n, e se indica por $m + n$ o elemento de $\mathbb{Z}$ definido por:*

$$m + n = \overline{(x + z, y + w)}.$$

Definição 1.4. *(Subtração) Sejam $m, n \in \mathbb{Z}$ tal que, $m = \overline{(x,y)}$ e $n = \overline{(z,w)}$. Chama-se diferença de m com n, e se indica por*

$$m - n = m + (-n)$$

o elemento de $\mathbb{Z}$ definido por:

$$m - n = \overline{(x + (-z), y + (-w)}$$
$$m - n = \overline{(x - z, y - w)}.$$

Definição 1.5. *(Multiplicação) Sejam $m = \overline{(x,y)}$ e $n = \overline{(z,w)}$ genéricos de $\mathbb{Z}$. Chama-se produto de m por n e indica por $m \cdot n$ $(ou\ mn)$ o elemento de $\mathbb{Z}$ definido por:*

$$m \cdot n = \overline{(xz + yw, xw + yz)}$$

Decorrente da construção dos números inteiros podemos observar que se $m \in \mathbb{Z}$ e para qualquer $a \in \mathbb{N}$, então

$$m = \overline{(a,0)}\ ou\ m = \overline{(0,a)}.$$

Assim se fizermos

$$\begin{array}{ll} \overline{(0,0)} = 0 & \overline{(0,1)} = -1 \\ \overline{(1,0)} = 1 & \overline{(0,2)} = -2 \\ \overline{(2,0)} = 2 & \overline{(0,3)} = -3 \\ \overline{(0,0)} = 0 & \overline{(0,1)} = -1 \\ \vdots & \vdots \end{array}$$

torna-se verdadeiro escrever

$$\mathbb{Z} = \{\cdots, -2, -1, 0, +1, +2, \cdots\}$$

Definição 1.6. *Chamam-se inteiros positivos e inteiros negativos os subconjuntos dos inteiros representado por* $\mathbb{Z}_+ = \{0, +1, +2, +3, \cdots\}$ *e* $\mathbb{Z}_- = \{\cdots, -3, -2, -1, 0\}$. *Todo elemento* $a \in \mathbb{Z}_+^* = \{+1, +2, +3, \cdots\}$ *é chamado inteiro estritamente positivo; e todo* $a \in \mathbb{Z}_-^* = \{\cdots - 3, -2, -1\}$ *é um inteiro estritamente negativo.*

No que segue apresentaremos sobre o conjunto dos números inteiros a definição e resultados de divisibilidade, divisão euclidiana, máximo divisor comum que são de muita importância para o desenvolvimento desse trabalho.

1.6.1 Divisibilidade

Definição 1.7. *Dados dois números inteiro a e b com* $a \neq 0$. *Se existir c inteiro tal que* $b = ac$, *então dizemos que a divide b, e escrevemos por* $a|b$. *Podemos dizer ainda que a é divisor ou um fator de b ou ainda, que b é múltiplo de a. Caso não exista c, dizemos que a não divide b, e escrevemos* $a \nmid b$.

Proposição 1.2. *Para todo a, b, c e d em* $\mathbb{Z}$, *verifica-se:*

(i) $a|a$

(ii) $a|b$ *e* $b|c \Rightarrow a|c$.

(iii) $a|b$ *e* $c|d \Rightarrow ac|bd$.

(iv) $a|b$ *e* $a|c \Rightarrow a|(b + c)$.

(v) $a|b \Rightarrow a|mb$, *para todo* $m \in \mathbb{Z}$.

(vi) $a|b$ *e* $a|c \Rightarrow a|(bm + cn)$, *para todo* m *e* $n \in \mathbb{Z}$.

Proposição 1.3. *Sejam* $a, b \in \mathbb{Z}, n \in \mathbb{N}$, *com* $a \neq b$.*Temos que* $(a - b)|(a^n - b^n)$.

Demonstração: Usando o fato que $a^n - b^n = (a - b).(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1})$ (verifica-se esta igualdade por indução), e pela definição de divisibilidade a proposição fica demonstrada.

■

Proposição 1.4. *Sejam* $a, b \in \mathbb{Z}, n \in \mathbb{N}$, *com* $a \neq b$.*Temos que* $(a + b)|(a^{2n+1} + b^{2n+1})$.

Demonstração: Como $2n+1$ é ímpar, para todo n verifica-se que $(-b)^n = -b^n$, podemos afirmar que

$$a^n + b^n = a^n - (-b)^n,$$

e pela proposição anterior temos que,

$$a^n + b^n = (a-(-b)).(a^{n-1} + a^{n-2}(-b) + ... + a(-b)^{n-2} + (-b)^{n-1}),$$

e assim,

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + ... - ab^{n-2} + b^{n-1})$$

e pela definição, a proposição é verdadeira.

■

1.6.2 Divisão Euclidiana

Teorema 1.3. *(Divisão Euclidiana) Sejam m e n dois números inteiros com $n > 1$. Existem dois únicos números inteiros q e r tais que*

$$m = nq + r \;\; e \;\; 0 \leq r < n.$$

Demonstração: Por hipótese temos que $n \in \mathbb{Z}$, com $n > 1$. Dado um número $m \in \mathbb{Z}$ temos dois casos a analisar:

i) Como $m|n$, podemos afirmar que $\exists q \in \mathbb{Z}$, tal que $m = nq$, o que implica $r = 0$.

ii) A partir da propriedade arquimediana disponível em [4] podemos afirmar que m está entre dois múltiplos dele, $nq < m < n(q+1)$. Assim, subtraindo nq na desigualdade anterior, temos:

$$nq - nq < m - nq < nq + n - nq$$

$$0 < m - nq < n\ .$$

Seja $r \in \mathbb{Z}$, tal que $r = m - nq$ e

$$0 < r < n,$$

é claro que se $r = 0$, então $m = nq$.

Para isso vamos supor que r e q são únicos e que $m = nq + r$ e $m = nq_1 + r_1$ com $0 \leq r$, $r_1 < n$, e consideremos que $r \neq r_1$. Assim

$$nq + r = nq_1 + r_1$$

$$n(q_1 - q) = r - r_1,$$

concluindo-se assim que $q_1 > q$ e $r = r_1 + n(q_1 - q)$, como temos $r_1 > 0$ e $q_1 - q > 1$, pela última igualdade que $r > n$, o que é um absurdo, portanto $r = r_1$ e $q = q_1$, completando assim a demonstração do teorema.

■

Os números q e r dizem-se, respectivamente, quociente e resto da divisão de m por n, enquanto que m é o dividendo e n é o divisor.

1.6.3 Máximo Divisor Comum

Definição 1.8. *Sejam $a, b \in \mathbb{Z}$. Um número inteiro positivo d se diz máximo divisor comum de a e b (denota-se d=mdc(a,b)) se, e só se verifica:*

i) $d|a$ *e* $d|b$*;*

ii) Se $c|a$ *e* $c|b$*, então* $c|d$*.*

Por i) temos que d é divisor tanto de a quanto de b e por ii) temos que d é maior divisor com a característica i).
A partir desse resultado podemos enunciar o seguinte resultado.

Proposição 1.5. *Sejam a e b inteiros,*

$$a|b \Rightarrow mdc(a, b) = a.$$

Demonstração: De fato, $a|a$ e $a|b$. E se $c|a$ e $c|b$, é verdade que $c|a$

■

Proposição 1.6. *Sejam a,b números inteiros, se $a = bq + r$ (q e r gerados pelo algoritmo da divisão) e $d = mdc(a, b)$, então $d = mdc(b, r)$.*

Demonstração: Como $d = mdc(a, b)$, então $d|a$ e $d|b$. E a partir da propriedade (v) da Proposição 1.2 temos que, $d|bq$. Logo $d|(a - bq)$, ou seja, $d|r$. Por outro lado, se $c|b$ e $c|r$, então $c|(bq + r)$ devido a Proposição 1.3 ; como $bq + r = a$, então $c|a$ e $c|b$, o que implica $c|d$, já que $d = mdc(a, b)$.

■

A continuação enunciaremos e provaremos o Teorema de Bachet-Bézout que é de muita importância no estudo da congruência que são utilizados no algoritmo de criptografia.

Teorema 1.4. *(Teorema de Bachet-Bézout) Dados inteiros a e b únicos, não ambos nulos e $d = mdc(a, b)$, existem inteiros x e y tais que $d = ax + by$.*

Demonstração: Seja o conjunto de todas as combinações lineares de a e b possíveis

$$A = \{ax + by \mid x, y \in \mathbb{Z}\}.$$

Observamos que a e $-a \in A$, pois $a = 1 \cdot a + 0 \cdot b$ e $-a = (-1) \cdot a + 0 \cdot b$.
Tomemos

$$A_+ = \{w | w \in A \; e \; w > 0\}$$

pelo que vimos acima, A_+ não é vazio. Agora, pelo Princípio da Boa Ordem, A_+ tem um mínimo elemento, onde denotaremos por m. Como $m \in A_+$, temos que $m > 0$ e $m = ax_o + by_o$. Pelo algoritmo da divisão, existem $q \; e \; r$, tais que $a = mq + r$ com $0 \leq r < m$. Daí

$$a = (ax_o + by_o)q + r,$$

$$a = ax_oq + by_oq + r$$

$$r = a(1 - x_oq) + b(-y_oq).$$

Portanto $r \in A$.
Como $m = minA_+$, temos que $r = 0$, dai $m|a$ e analogamente $m|b$.
Seja n tal que $n|a$ e $n|b$, logo $n|ax_o + by_o$, dai $n|m$, então $n \leq |m| = m$. Portanto, $m = d$.

■

Proposição 1.7. *Sejam a e b números inteiros. Se* $mdc(a,b) = 1$ *se, e somente se, existem números inteiros s e t tais que* $sa + tb = 1$.

Demonstração: Suponha que $mdc(a,b) = 1$. Logo pelo Teorema 1.6, temos que existem números s e t tais que, $sa + tb = 1$. Reciprocamente, suponha que existam s e t tais que $sa + tb = 1$. Agora, se $d = mdc(a,b)$, temos que $d|(sa + tb)$, o que mostra que $d|1$, e, portanto, $d = 1$.

■

Proposição 1.8. *Sejam a, b inteiros positivos , tais que* $mdc(a,b) = 1$. *Para todo* $c \in \mathbb{Z}$ *verifica-se que*

i) *Se* $a|b \cdot c$, *então* $a|c$;

ii) *Se* $a|c$ *e* $b|c$, *então o produto* $ab|c$.

Demonstração: i) Se $a|b \cdot c$, então existe $f \in \mathbb{Z}$ tal que $bc = af$.
Se $mdc(a,b) = 1$, então, pela Proposição 1.7 , temos que existem $s, t \in \mathbb{Z}$ tais que

$$as + bt = 1.$$

Multiplicando por c ambos os lados da igualdade acima, temos que

$$c = asc + btc :$$

Substituindo bc por af nesta última igualdade, temos que

$$c = asc + btc = a(sc + tf)$$

com isso, $a|c$.

ii) Se $a|c$, podemos escrever $c = ak$, para algum k inteiro. Mas b também divide c. Como $mdc(a,b) = 1$, segue da afirmação i) que b tem que dividir k.Assim teremos $k = sb$, para algum inteiro s.Portanto

$$c = ak = a(sb) = s(ab)$$

é divisível por ab, o que completa a demonstração da proposição.

■

1.7 Números Primos

Um dos conceitos mais importantes na teoria do números é o conceito de número primo, o qual é fundamental no estudo da criptografia RSA ,que abordaremos neste trabalho, onde se utiliza no processo de criação do par de chaves.

Definição 1.9. *Um número inteiro p diferente de* 0 *e de* 1 *é chamado de número primo se é divisível apenas por* 1 *e por* $|p|$.

A partir da definição anterior, temos a seguinte proposição e seus respectivos corolários.

Proposição 1.9. *Sejam a, b inteiros e p um número primo. Se $p \mid a \cdot b$, então $p \mid a$ ou $p \mid b$.*

Demostração : Observe se $p \nmid a$, o único divisor comum positivo de a e p é 1, então $mdc(p, a) = 1$. Agora suponhamos que $p|ab$. Se $p|a$,então a tese é verdadeira, em caso contrário, $mdc(p, a) = 1$, e pela Proposição 1.8 podemos garantir que $p|b$.

■

Corolário 1.1. *Seja p um número primo e $p_1, p_2, \cdots, p_n$ números inteiros. Se $p|p_1p_2 \cdots p_n$, então p divide algum dos p_i, para algum i, $1 \leq i \leq n$.*

Demonstração: A demonstração segue diretamente da proposição 1.9, usando indução sobre $\mathbb{N}$.

■

Corolário 1.2. *Se $p_1p_2 \cdots p_n$ são números primos e se $p|p_1p_2 \cdots p_n$, então $p = p_i$ para algum $i \in \{1, \ldots, n\}$.*

Demonstração: Pelo corolário 1.1, existe um indice k, tal que $p|p_k$, como p_k é primo, segue-se que $p = 1$ ou $p = p_k$. Mas, $p > 1$, porque p é primo, logo, $p = p_k$.

■

1.7.1 Fatoração de números naturais

Fatorar um número natural significa escrevê-lo na forma de produto de fatores primos, disso é que trata um importante teorema, conhecido como **Teorema Fundamental da Aritmética**.

Teorema 1.5. *(Teorema Fundamental da Aritmética) Todo inteiro maior do que 1 é primo ou pode ser representado de maneira única (a menos da ordem dos fatores) como um produto de fatores primos.*

Demonstração: Demostraremos este teorema utilizando o Segundo Princípio de Indução.

Se $n = 2$, o resultado é óbvio pois 2 é primo. Suponhamos que o resultado seja válido para todo número natural menor do que n e vamos mostrar que vale para n.
Se o número n é primo, não há o que fazer. No caso de n não ser primo, existem números inteiros positivos n_1 e n_2, tais que $n = n_1 \cdot n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$.
Pela hipótese de indução, temos que existem primos $p_1, p_2, \ldots, p_r$ e $q_1, q_2, \ldots, q_s$ tais que $n_1 = p_1 \cdot p_2 \cdots p_r$ e $n_2 = q_1 \cdot q_2 \cdots, q_s$. Portanto,

$$n = n_1 \cdot n_2,$$

$$n = p_1 \cdot p_2 \cdots p_r \cdot q_1 \cdot q_2 \cdots, q_s \, .$$

Suponha, agora, que $n = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots, q_s$, onde os p_i e os q_j são números primos. Como $p | q_1 \cdot q_2 \cdots q_s$ pelo corolário 1.2, temos que $p_1 = q_j$ para algum $j \leq s$, que, ao reordenarmos os fatores $q_1, q_2, \ldots, q_s$ podemos chamar de q_1. Portanto,

$$p_2 \cdots p_r = q_2 \cdots q_s \, .$$

Como $p_2 \cdots p_r < n$, a hipótese de indução implica em $r = s$ e os p_i e q_j são iguais aos pares. Isso mostra a unicidade da fatoração de n.

■

1.8 Congruência

O centro do trabalho de codificar e decodificar está fundamentado com o conceito de congruência e desempenha um papel muito importante no algorítimo, que será abordado nesse

trabalho. Na continuação enunciamos a definição de congruência e as propriedades básicas. Além disso, enunciamos e provamos o Teorema de Fermat, que aplicaremos no Teorema 3.1, onde se mostra a funcionalidade do sistema RSA.

Definição 1.10. *Sejam a e b números inteiros. Dizemos que a e b são congruentes módulo m se* $m|a-b$.

No caso em que a seja congruente com b módulo m, usaremos a seguinte notação:

$$a \equiv b \; mod m.$$

Teorema 1.6. *Sejam* a, b, c, d, k *e* m *em* $\mathbb{Z}$. *Se* $a \equiv b \; mod m$ *e* $c \equiv d \; mod m$, *então:*

(i) $a + c \equiv b + d \; mod m$

(ii) $a - c \equiv b - d \; mod m$

(iii) $ka \equiv kb \; mod m$

(iv) $ac \equiv bd \; mod m$

(v) $a^k \equiv b^k \; mod m$

1.8.1 Teorema de Fermat

Teorema 1.7. *(Teorema de Fermat) Seja* p *um número primo e* $a \in \mathbb{Z}$, *tal que* $p \nmid a$. *Então*

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

Demonstração: Em geral quando fazemos a divisão de um número inteiro por p o resto é o número pertencente ao conjunto

$$\{1, 2, 3, \ldots, p-1\}$$

Multiplicando cada um destes restos por a, geramos a seguinte sequência

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

Para cada $i \in \{1, 2, 3, \ldots, p-1\}$, seja

$$r_i = a_i - q_i p,$$

onde r_i e q_i são gerados pelo algoritmo da divisão. Assim podemos escrever

$$\begin{aligned} r_1 &\equiv a \cdot 1 \ \ mod p \\ r_2 &\equiv a \cdot 2 \ \ mod p \\ \vdots &\quad \vdots \\ r_{p-1} &\equiv a \cdot (p-1) \ \ mod p \end{aligned}$$

Usando a propriedade (iv) do Teorema 1.6 podemos afirmar que

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

Agora como,

$$(a \cdot 1) \cdot (a \cdot 2) \cdot (a \cdot 3) \cdots (a \cdot (p-1)) = a^{p-1} \cdot (1 \cdot 2 \cdot 3 \cdots (p-1));$$

dessa forma

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

Portanto,

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

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

Como $p \nmid (p-1)!$ podemos afirmar que $mdc((p-1)!, p) = 1$. A partir da ultima congruência existe um $k \in \mathbb{Z}$, tal que

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

logo,

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

e como $p \nmid (p-1)!$, então $p | a^{p-1} - 1$ demonstrando assim o teorema.

■

Teorema 1.8. *(Teorema de Invertíveis) Sejam a m números inteiros para os quais existem $b \in \mathbb{Z}$ tal que $ab \equiv 1$ mod m. Então, $mdc(a, m) = 1$.*

Demonstração: Se

$$ab \equiv 1 \; mod \; n,$$

então existe um $k \in \mathbb{Z}$ tal que

$$ab = 1 + mk,$$

logo,

$$ab - mk = 1,$$

e pelo Teorema de Bachet-Bézout, $mdc(a, m) = 1$.

■

Com o Teorema de Invertíveis fechamos os fundamentos matemáticos necessários para a abordagem da Criptografia e algorismo RSA que será tratado neste trabalho.

CAPÍTULO 2

CRIPTOGRAFIA

NESTE capítulo descrevemos do que se trata a criptografia, após o significado de alguns termos utilizados no trabalho e , por fim, relatamos os dois tipos de criptografia: simétrica e assimétrica. Tomando como base [6]e [7].

2.0.2 Criptografia

Tendo em vista a necessidade de se criar ferramentas capazes de proteger a informação e de prover a segurança aos documentos armazenados e transmitidos pelas organizações através do mundo, tem-se a motivação para o estudo da **Criptografia** que decorre de duas palavras gregas: *kriptos* que quer dizer esconder, ocultar, secreto e *graphein*(grafia) que significa escrever.
Formalmente pode se entendeu que "Criptografia"é o estudo de técnicas matemáticas relacionadas para aspectos de segurança da informação, tais como confidencialidade, integridade, autentificação de entidades e verificação da origem.

2.1 Termos importantes

Vamos descrever o significado de alguns termos que vamos usar ao decorrer do nosso trabalho.

1) Criptografar: Significa transformar uma mensagem em outra, escondendo o verdadeiro sentido do texto. Utiliza-se funções matemáticas para que se torne impossível (ou quase)

que uma pessoa sem o conhecimento de como foi gerado consiga desvendar o texto original.

2) **Criptoanalista:** São pessoas que estudam mecanismos para comprometer ou desvendar um texto criptografado.

3) **Criptologia:** São os resultados estudados pelos os Criptoanalistas.

4) **Chave:** É um mecanismo matemático para criptografar e descriptografar um mensagem.

5) **Criptografar ou Cifrar:** É o ato de transformar uma mensagem em outra de tal forma que só o destinatário consiga ler, com a posse de sua chave.

6) **Descriptografar ou Decifrar:** É o ato de transformar o texto cifrado no texto original, com a posse de sua chave.

7) **Bloco:** Parte de uma mensagem a ser criptografada.

8) **Bit (Binary Digit):** É a menor unidade de informação de um sistema e pode assumir dois valores 0 ou 1.

2.2 Tipos de Criptografia

São dois tipos de criptografia onde cada uma possui características próprias com pontos positivos e negativos : a Criptografia **Simétrica** que utiliza apenas uma chave para cifrar e decifrar, e a Criptografia **Assimétrica** que utiliza duas chaves, uma para o ciframento e outra para o deciframento.

A Figura 2.1 exemplifica o modelo Simétrico e a utilização de uma chave.

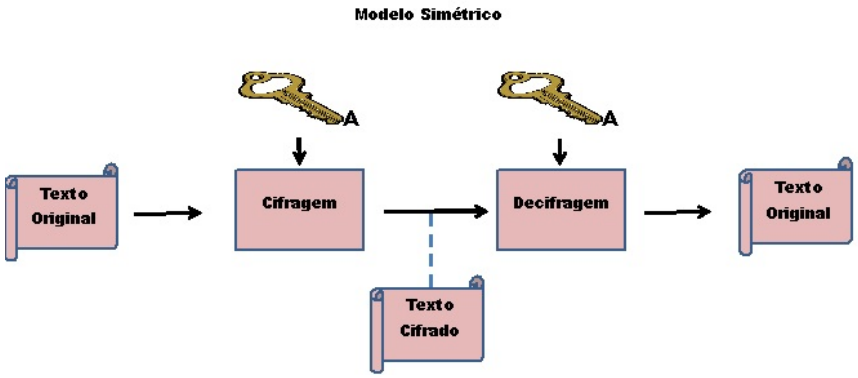

Figura 2.1: Modelo Simétrico

A Figura 2.2 exemplifica o modelo Assimétrico e a utilização de duas chaves.

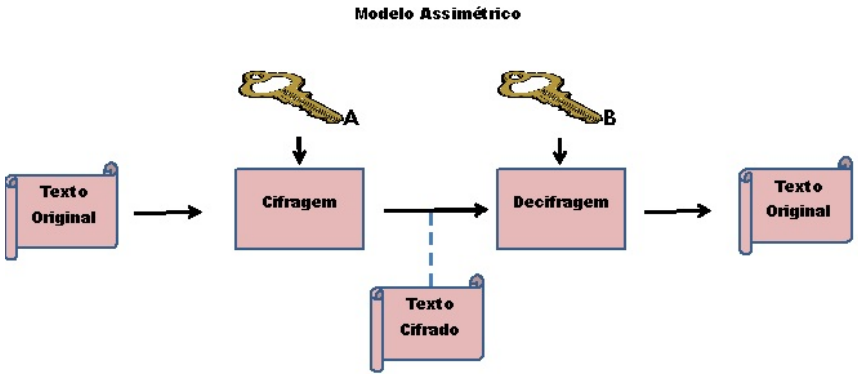

Figura 2.2: Modelo Assimétrico

2.3 Técnicas Simples de Criptografia

Antes da invenção dos computadores existiam duas técnicas de cifragem simétrica: a cifra de Substituição e a cifra de Transposição.

2.3.1 Cifras de Substituição

É uma das formas mais simples de cifrar e decifrar, pois consiste na substituição de uma letra do alfabeto por outra distinta até modificar a 26 letras do alfabeto. Vejamos um exemplo onde nós vamos trocar cada uma das 26 letras.

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

Este tipo de substituição é chamada de **monoalfabética**.

Exemplo 2.1. *Para exemplificar vamos cifrar a palavra "prova"com o processo de substituição:*

Texto original	*p*	*r*	*o*	*v*	*a*
Texto cifrado	*M*	*J*	*P*	*A*	*E*

Agora você pode está se perguntando quantas formas podemos fazer este método. Responderemos está pergunta com o comentário abaixo.

Se o a alfabeto tem 26 letras, então o número de combinações possíveis para a cifra de substituição é 26!, pois a primeira escolha temos 26 possibilidades, na segunda 25, na terceira 24 e assim por diante até chegar a última escolha que é 1. Aplicando o princípio multiplicativo teremos:

$$26 \cdot 25 \cdot 24 \cdot 23 \cdots 3 \cdot 2 \cdot 1 = 26!.$$

Cifra de César

O exemplo mais antigo e o mais simples é a cifra de César que consiste na substituição de um grupo de letras por outro grupo de letras. Essa técnica era utilizada pelo imperador Júlio César em mensagens para os seus generais em batalha. Para criptografar um mensagem, cada letra era substituída por outra que ficava três setores adiante, percorrendo o anel no sentido horário. Ao receber a mensagem, o general decodificava o texto, realizando a operação contrária, substituindo cada letrada mensagem cifrada pela que ficava a três setores dela percorrido no sentido anti-horário.

A correspondência feito pelos escribas de César entre as letras do texto original (letras minúsculas) e do texto criptografado (letras maiúsculas) é descrita pela tabela abaixo.

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

Letra	%	Letra	%	Letra	%	Letra	%
A	14,64	G	1,30	N	5,05	T	4,34
B	1,04	H	1,28	O	10,73	U	4,64
C	3,88	I	6,18	P	2,52	V	1,70
D	4,10	J	0,40	Q	1,20	X	0,21
E	12,57	K	2,78	R	6,53	Z	0,47
F	1,02	L	4,75	S	7,81		

Tabela 2.1: Frequência das letras no alfabeto português- disponível em [5].

Exemplo 2.2. *A mensagem "A vida é a soma de todas as suas escolhas"de Albert Camus seria escrito na cifra de César desprezando a pontuação como:*

D YLGD H D VRPD GH WRGDV DV VRGDV DV VXDV HVFROKDS

Como já foi dito anteriormente este método é fácil de ser descoberto, pois em qualquer língua, alguns sons são utilizados com mais frequência e por consequência, na linguagem escrita acontece o mesmo fenômeno, portanto para descobrir a chave basta computarmos a frequência de cada letra no texto cifrado e comparar com a tabela descrita abaixo .

2.3.2 Cifras de Transposição

A cifra de transposição usa como técnica a mudança da ordem das letras. Descreveremos o processo de codificação, em que consiste na transformação do texto original no formato de um retângulo, colocando as palavras linha por linha sem espaço entre elas e sem acentos ortográficos, após a mensagem será lida, coluna por coluna, mas permutando a ordem das colunas. A ordem das colunas será a chave para o algoritmo.
Para o melhor entendimento faremos um exemplo abaixo,que descreverá todo o processo de forma clara.

Exemplo 2.3. *Vamos cifrar a frase "Estamos sofrendo ataque". Para isso descreveremos as etapas:*

1) *Escolha de uma palavra para a chave. Escolheremos a palavra "Forte"como chave.*

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	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

2) *Transformaremos a chave em números de acordo a tabela descrita abaixo que corresponde a cada letra do alfabeto há um número.*

A chave será em números igual há

F	*O*	*R*	*T*	*E*
6	*15*	*18*	*20*	*5*

3) *Já descobrimos o valor numérico das letras que será responsável pela ordem da colunas na hora da cifragem, seguiremos uma ordem crescente, sendo o menores valores primeiro até chegar o de maior valor.*

Ordem Original	*1*	*2*	*3*	*4*	*5*
Chave	*F*	*O*	*R*	*T*	*E*
Valor Numérico das letras	*6*	*15*	*18*	*20*	*5*
Nova ordem	*2*	*3*	*4*	*5*	*1*

4) *Descrever a mensagem nas linhas da tabela e desprezando os espaços entre as palavras e os acentos gráficos.*

F	*O*	*R*	*T*	*E*
2	*3*	*4*	*5*	*1*
e	*s*	*t*	*a*	*m*
o	*s*	*s*	*o*	*f*
r	*e*	*n*	*d*	*o*
a	*t*	*a*	*q*	*u*
e				

5) *Escrever a mensagem cifrada obedecendo a ordem da chave.*

mfou eorae sset tsna aodq

A decodificação da mensagem será o processo reverso utilizando a chave.

2.3.3 Algoritmos Modernos de Criptografia Simétrica

Temos vários algorítimos computacionais, mais só vamos descrever dois: o primeiro da era moderna o DES e o mais utilizado atualmente AES.

Algoritmo DES

O DES (Data Encription Standart) foi o primeiro modelo de criptografia simétrica utilizado na época moderna, foi criado na década de 70 e consiste no processamento de bloco de textos de 64 bits cada vez, usando uma chave de 56 bits, produzindo um texto cifrado de 64 bits, entretanto esse algoritmo se tornou inseguro, devido ao avanço tecnológico e já foi quebrado por força bruta (é um ataque feito testando todas as chaves possíveis) em 1977 por um desafio feito pela internet.
Após o ataque sofrido foi feita uma versão mais fortalecida composta de três chaves de 56 bits e por isso chamada de 3-DES.

Algoritmo AES

O AES(ADdvanced Encryption Standart) é o algoritmo simétrico vitorioso a uma disputa feita pelo instituto americano de padrões e tecnologia dos Estados Unidos o NIST(U.S National Institute of Standards and Technology), foi desenvolvido para a proteção das informações do governo federal Americano e é um dos algoritmos mais populares desde 2006. O algorítimo pode usar chaves de 128, 192 ou 256 bits com bloco de dados de 128 bits.

2.3.4 Criptografia Assimétrica

A criptografia Assimétrica foi uma verdadeira revolução para a criptografia moderna pois utiliza-se o principio de duas chaves, uma pública que todos tem acesso e utiliza-se para o ciframento e uma privada em que apenas o destinatário tem a posse da chave e utiliza-se para o deciframento.

Em termos de segurança não podemos afirmar que a criptografia Assimétrica é mais segura que a Simétrica, pois o que torna seguro um algorítimo é o tamanho de sua chave, ou seja, quanto maior for a chave mais difícil será o trabalho do Criptoanalista e o sistema mais seguro.

A grande vantagem deste método é que qualquer pessoa pode codificar uma mensagem enquanto a Simétrica não, agora a grande desvantagem é o processamento que é muito lento. A simétrica é mais rápida e por isso ainda se utiliza a criptografia Simétrica.

2.3.5 Funcionamento das Chaves Públicas e Privadas

Como já foi dito a chave pública todos tem acesso e é utilizada para codificação, enquanto a chave privada só o destinatário tem acesso e é utilizada para a decodificação da mensagem. Vamos exemplificar uma situação onde, Maria que mandar uma mensagem para João através de um canal inseguro qualquer, por exemplo a internet, e requisitará a chave pública de João. Maria em posse da **chave pública A** irá codificar à mensagem **X** transformando em **Y**, utilizando um algoritmo conhecido de todos. João irá utilizar sua **chave privada B** para a decodificação de **Y** e a obtenção de **X**. Descreveremos este processo com a figura abaixo.

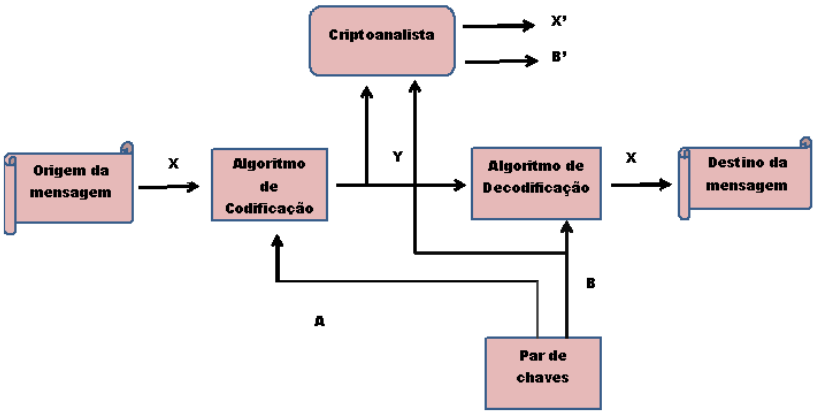

Figura 2.3: Modelo de Criptografia Assimétrica para garantir a confidencialidade

A partir dos conteúdos expostos neste capítulo contextualizamos os elementos básicos da criptografia, que necessitaremos para apresentar o método RSA e a proposta de atividade pedagógica desse trabalho.

CAPÍTULO 3

CRIPTOGRAFIA RSA

NESTA capítulo, apresentamos o algoritmo RSA, um dos métodos de criptografia considerados mais seguros nos dias atuais, que tem esse nome devido aos seus idealizadores Ronald Rivest, Adi Shamir e Leonard Adleman, matemáticos do Massachusetts Institute of Technology que, em 1977 desenvolveram este sistema de encriptação cujo princípio é construir chaves públicas utilizando números primos e congruências. Pautamos este capítulo nas referências [2], [3], [6] e [7].

3.1 Descrição do Algoritmo RSA

Para a construção do algoritmo RSA precisamos das chaves e para isso necessitamos de alguns elementos antes para a confecção das mesmas.Para a geração da chaves podemos seguir a seguinte metodologia.

1. Escolha dois primos p e q muito grandes(acima de 100 algarismos) que chamaremos de **parâmetros RSA** .
2. Denotemos n como o produto de p por q.
3. Dado $n = pq$, seja $\Psi(n) = (p-1) \cdot (q-1)$.
4. Encontre um inteiro e tal que $1 < e < \Psi(n)$, de forma que $mdc(e, \Psi(n)) = 1$ chamaremos de **expoente de enciframento**.

5. Encontre um inteiro positivo d, de forma que $de \equiv 1 \mod \Psi(n)$, ou seja, d, seja o inverso multiplicativo de e, em *mod* $\Psi(n)$.

Feito isso teremos nosso par de chaves onde, $\{e, n\}$ é a **chave pública**, enquanto $\{d, \Psi(n)\}$ será a **chave privada**.

A fim do entendimento do processo de obtenção das chaves escolheremos dois primos não muito grande para evitar uma complexidade nos cálculos no exemplo a seguir.

Exemplo 3.1. *Vamos encontrar as chaves com os números primos* $p = 19$ *e* $q = 31$ *os passos são descritos abaixo:*

1. $p = 19$ *e* $q = 31$
2. $n = 19 \cdot 31 = 589$.
3. $\Psi(n) = (19 - 1) \cdot (31 - 1) = 18 \cdot 30 = 540$.
4. *Escolhemos* $e = 7$, *pois* $mdc(7, 540) = 1$.
5. *Para encontrar o d utilizaremos a definição de congruência e conceitos de divisibilidade. Observe que,*

$$7d \equiv 1 \mod 540,$$

por definição temos que isto equivale a

$$540 | 7d - 1,$$

ou seja, precisamos encontrar um inteiro positivo k tal que,

$$1 = 7d - 540k \text{ } ou \text{ } 540k + 1 = 7d \tag{3.1}$$

Como $\Psi(589) = 540$ *e* $e = 7$, *note que*

$$540 = 77 \cdot 7 + 1 \text{ ,}$$

assim,

$$1 = 540 + (-77) \cdot 7. \tag{3.2}$$

Comparando as equações 3.1 e 3.2 temo que $d = -77$,mais d não pode ser negativo. Já que

$$7 \cdot (-77) \equiv 7 \cdots 463 \; mod \; 540$$

$$7 \cdot (-77) \equiv 1 \; mod \; 540$$

que é equivalente há

$$7 \cdot 463 \equiv 1 \; mod \; 540$$

com isso $d = -77$ equivale ao número positivo $d = 463$.

Portanto, a chave pública será o par $\{7, 589\}$ e a chave privada será $\{463, 540\}$.

Após encontrado as chaves o algoritmo RSA se divide em três etapas: pré- codificação (etapa onde o texto é convertido em números e logo após é dividido em blocos), codificação e a decodificação.

3.1.1 Pré-Codificação

Pré-codificação é a parta que convertemos o texto original em números. Note que se começarmos $A = 1$, $B = 2$, $C = 3$ e assim por diante, quando aparecer o número 13 ele pode representar AC ou M o que não é legal, por isso convencionalmente começaremos do 10 ,vamos desconsiderar o acentos ,ou seja, A, Ã,Á, À e Â todos são representado pelo número 10 e por fim considerar 99 como espaço entre duas palavras.

Assim usaremos a seguinte **tabela de conversão**.

Letras	A	B	C	D	E	F	G	H	I	J	K	L	M
Números	10	11	12	13	14	15	16	17	18	19	20	21	22

Letras	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Numeros	23	24	25	26	27	28	29	30	31	32	33	34	35

Exemplo 3.2. *Por exemplo a frase EU AMO MATEMÁTICA é convertida no número*

$$14309910222499221029142210291812 10.$$

Agora que já convertemos o texto em um número temos que dividi-lo em blocos e para isso precisamos entender o que é um bloco. Para definirmos os blocos precisamos escolher os parâmetros RSA p e q, para que possamos definir $n = pq$. Por fim devemos separar os algarismos em números menores do que n, veremos por que isso mais a frente.Por exemplo se escolhemos os números $p = 19$ e $p = 31$, então $n = 589$.
Agora vamos escrever uma definição necessária para continuação do processo.

Definição 3.1. *Um bloco é um parte do texto convertido em número, tal que esse número inteiro ele é maior que* 1 *e menor do que n.*

Consideremos algumas observações decorrentes da definição e alguns cuidados para a mensagem não ser facilmente decifrada pelo Criptoanalista.

- Quebrar o texto pré-codificado em números menores do que n e diferente de 0, depois veremos porque esse bloco tem que ser menor do que n.
- o bloco não pode ser iniciar com o 0 porque isso traria problemas na hora de decodificar, já que por exemplo, não temos como distinguir o bloco 014 do bloco 14.
- Não se tem uma forma única de escolher um bloco para uma codificação.
- O bloco não pode corresponder uma palavra ou letra, o que facilitaria o trabalho de decodificação por uma pessoa estranha.

Tomando as observações anteriores da frase do exemplo 3.2 podemos separar em blocos conforme segue abaixo.

$$14 - 309 - 9 - 102 - 22 - 499 - 22 - 102 - 91 - 422 - 102 - 91 - 81 - 210$$

3.1.2 Codificação

Agora vamos descrever o processo de codificação. Precisamos da seguinte definição.

Definição 3.2 (Fórmula de Codificação)**.** *Dados e, b e n a codificação do bloco b, denotada como* $C(b)$*, é o resto da divisão de* b^e *por n ou na notação de congruência, C(b) verifica*

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

onde $0 < C(b) < n$.

Vamos codificar cada bloco que obtivemos no passo anterior utilizando a formula de Codificação apresentada.

Exemplo 3.3. *Vamos utilizar os dados do exemplo 3.1, ou seja,* $n = 589$ *e* $e = 7$*. Assim, o bloco* 14 *da mensagem anterior é codificado como o resto da divisão de* 14^7 *por* 589*. Agora vamos fazer as contas:*

Como $14^7 = 14^6 \cdot 14$*, e* $14^6 \equiv 349$ *mod* 589 *temos que* $14^7 \equiv 349 \cdot 14$ *mod* 589 *e assim,* $14^7 \equiv 4886$ *mod* 589*, agora como* $4886 \equiv 174$ *mod* 589 *podemos concluir que* $14^7 \equiv 174$ *mod* 589*.*

$$(309^7 = (309^3)^2 \cdot 309 \wedge (309^3)^2 \equiv 30^2 mod\ 589 \wedge 30^2 \equiv 311\ mod\ 589) \Longrightarrow 309^7 \equiv 92\ mod\ 589$$

$$(9^7 = (9^6) \cdot 9 \wedge (9^6) \equiv 163\ mod\ 589) \Longrightarrow 9^7 \equiv 289\ mod\ 589$$

$$(102^7 = (102^3)^2 \cdot 102 \wedge (102^3)^2 \equiv 419^2 mod\ 589 \wedge 419^2 \equiv 39\ mod\ 589)$$
$$\Longrightarrow 102^7 \equiv 444\ mod\ 589$$

$$(22^7 = (22^6) \cdot 22 \wedge (22^6) \equiv 349\ mod\ 589) \Longrightarrow 22^7 \equiv 21\ mod\ 589$$

$$(499^7 = (4999^3)^2 \cdot 499 \wedge (499^3)^2 \equiv 182^2\ mod\ 589 \wedge 182^2 \equiv 140\ mod\ 589)$$
$$\Longrightarrow 499^7 \equiv 358\ mod\ 589$$

$$(91^7 = (91^3)^2 \cdot 91 \wedge (91^3)^2 \equiv 240^2\ mod\ 589 \wedge 240^2 \equiv 467\ mod\ 589)$$
$$\Longrightarrow 91^7 \equiv 89\ mod\ 589)$$

$$(422^7 = (422^3)^2 \cdot 422 \wedge (422^3)^2 \equiv 349^2\ mod\ 589 \wedge 349^2 \equiv 467\ mod\ 589)$$
$$\Longrightarrow 422^7 \equiv 348\ mod\ 589$$

$$(81^7 = (81^3)^2 \cdot 81 \wedge (81^3)^2 \equiv 163^2\ mod\ 589 \wedge 163^2 \equiv 64\ mod\ 589)$$
$$\Longrightarrow 81^7 \equiv 472\ mod\ 589$$

$$(210^7 = (210^3)^2 \cdot 210 \wedge (210^3)^2 \equiv 153^2\ mod\ 589 \wedge 153^2 \equiv 438\ mod\ 589)$$
$$\Longrightarrow 210^7 \equiv 96\ mod\ 589$$

Agora, vamos escrever a sequências de blocos já codificados:

$$174 - 92 - 289 - 444 - 21 - 358 - 21 - 444 - 89 - 348 - 444 - 89 - 472 - 96.$$

3.1.3 Decodificação

Vejamos como fazer a decodificação de uma mensagem codificada, para isto é necessário a chave privada e portanto isso precisamos de $\Psi(n)$ e de d,e também da definição que segue abaixo.

Definição 3.3 (Fórmula para Decodificação)**.** *Dado $a = C(b)$, d e n a decodificação do bloco a, denotada como $D(a)$, é o resto da divisão de a^d por n ou na notação de congruência, $D(a)$ verifica*

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

onde $0 < D(a) < n$.

Exemplo 3.4. *Utilizaremos a chave $\{463, 540\}$, encontrada no exemplo 3.1 para decodificar o bloco 21 codificado no exemplo 3.3 . Assim para decodificar o bloco temos:*

$$D(21) \equiv 21^{463} = [(21^{10})^4]^{10} \cdot (21^{10})^6 \cdot 21^3$$

$$\equiv [36^4]^{10} \cdot 36^6 \cdot 21^3 \equiv [(377^2)]^5 \cdot 311 \cdot 21^3 \equiv 180^5 \cdot 550 \equiv 377 \cdot 550 \equiv 22 \ mod \ 589.$$

3.2 Funcionalidade do Sistema RSA

Como foi visto, o método descrito acima só será válido se, decodificando um bloco codificado, obtemos de volta o bloco corresponde a mensagem original. Para mostrar que os sistemas de codificação e decodificação apresentados na subseção anterior funcionam e são seguros, devemos mostrar que é válido o resultado que segue.

Teorema 3.1. *Sejam b, n e $C(b)$ inteiros e $1 \leq b \leq n$, então $D(C(b)) = b$.*

Demonstração: Teremos que mostrar que $D(C(b)) \equiv b \ mod \ n$, já que $D(C(b))$ e b pertencem ao intervalo de 1 a $n - 1$ e, eles seriam congruentes módulo n, no caso em que forem iguais. Pela definição de D e C, como $b \leq n$ e temos que,

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

e assim,

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

Sabemos também que n é o produto de p e q, então, vamos calcular b^{ed} módulo p e b^{ed} módulo q. Primeiro, vamos verificar o caso de b^{ed} módulo p. Temos que d é tal que $ed \equiv 1\ mod \Psi(n)$. Considerando a definição de $\Psi(n)$, isto é, $\Psi(n) = (p-1)(q-1)$, temos

$$ed \equiv\ 1 \mod\ \Psi(n) \Rightarrow\ ed = 1 + k\Psi(n) = 1 + k(p-1)(q-1),$$

observe que, como e e d são inteiros maiores que 2 e $\Psi(n) > 0$, então $k > 0$. Daí,

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

Vamos analisar os casos em que $p|b$ e os casos em que $p \nmid b$.

Queremos usar o Teorema 1.7 (Teorema de Fermat) e para isso vamos supor que p não divide b. Então, por Fermat temos

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

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

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

$$b^{ed} \equiv\ b\ mod\ p.$$

Agora, suponha que $p|b$. Se isso acontece temos $b \equiv\ 0\ mod\ p$. Logo, $b^{ed} \equiv b\ mod\ p$, para qualquer b inteiro.

Como $b^{ed} \equiv\ b\ mod\ p$, de modo inteiramente análogo, podemos mostrar que $b^{ed} \equiv\ b\ mod\ q$. Agora, como $b^{ed} \equiv\ b\ mod\ p$ e $b^{ed} \equiv\ b\ mod\ q$, temos que existem t e l tais que

$$b^{ed} = b + tp \text{ e } b^{ed} = b + lp,$$

o que implica que

$$b^e d - b = tp \text{ e } b^{ed} - b = lq,$$

o que quer dizer que $(b^{ed} - b)$ é divisível por p e q. Mas, como p e q são primos entre si, isto é, $mdc(p, q) = 1$, por ii) da proposição 1.8, temos que $pq|(b^{ed} - b)$. Portanto, como $n = pq$, temos

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

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

■

3.3 Por que o sistema RSA é seguro?

Sabemos que o RSA é um método de chave pública. Já foi dito que p e q são os parâmetros do sistema que estamos usando e n é igual ao produto de p e q. Portanto o par $(\{n, e\}$ é disponível a qualquer usuário. O RSA só será seguro se for difícil calcular d quando n e e são conhecidos.

Para calcularmos d precisamos de $\Psi(n)$ e e como já foi visto. Por outo lado, só sabemos calcular $\Psi(n)$ se soubermos fatorar n para obter p e q. Portanto, só podemos quebrar o código se conseguirmos fatorar n. Mas sabemos que, se n for muito grande, este é um problema muito difícil e demorado, já que não são conhecidos algoritmos rápidos de fatoração.
Veremos agora o que foi dito formalizado em um teorema.

Teorema 3.2. *Para decodificarmos uma mensagem apenas conhecendo e e n se, e só se fatorarmos o número n, onde* $n = p \cdot q$.

Demonstração: A condição suficiente é trivial visto que se conseguirmos fatorar n , conhecemos p e q, com isso conseguimos decodificar a mensagem utilizando os processos descritos no item anterior. Já a condição necessária não é trivial, vamos analisar alguns casos. Suponha que foi inventado um algoritmo eficiente para se calcular $\Psi(n)$ a partir de d e e, então temos:

$$\Psi(n) = (p-1) \cdot (q-1) = pq - p - q + 1 = n - (p+q) + 1 = (n+1) - (p+q)$$

e

$$p = n + 1 - q - \Psi(n) \ e \ q = n + 1 - p - \Psi(n)$$

com isso,

$$p + q = n + 1 - \Psi(n).$$

Observe que

$$(p+q)^2 - 4n = p^2 + 2pq + q^2 - 4n = p^2 + q^2 + 2pq - 4pq = p^2 - 2pq - q^2 = (p-q)^2$$

portanto,

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

Observe que

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

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

$$p = \frac{\sqrt{(n+1-\Psi(n))^2 - 4n} + n + 1 - \Psi(n)}{2}.$$

Analogamente se encontra q

$$q = \frac{\sqrt{(n+1-\Psi(n))^2 - 4n} + n + 1 - \Psi(n)}{2}.$$

Em resumo, o número n foi fatorado.

■

3.4 Assinaturas Digitais

3.4.1 O que é Assinatura Digital?

É uma aplicação da criptografia Assimétrica utilizada para a validação de operações online, ou seja, é a verificação que de fato aquela pessoa ou empresa tenha comprado ou firmado um compromisso com outra pessoa ou empresa.
O princípio da assinatura digital é ter segurança de quem está enviando a mensagem, e é muito utilizada principalmente nas relações comerciais online, visto que a empresas e Bancos precisam da certeza de que é as suas informações estão sendo transferidas sem que ninguém além deles tenham conhecimento.

3.4.2 Funcionamento da Assinatura Digital

Vamos supor que Antônio esteja em um internet banking de um banco qualquer e esteja realizando transações bancárias. Por segurança, tanto Antônio quanto o Banco desejam que a mensagem seja codificada. Entretanto, o RSA é um sistema de encriptação de chave pública e qualquer pessoa poderia realizar transações bancárias utilizando esse sistema. Por este motivo, necessita-se que a mensagem esteja assinada de forma digital. Vamos ver como assinar, de forma digital, uma mensagem pelo RSA.

Sejam C_a e D_a as funções de codificação e decodificação de Antônio, respectivamente, e C_b e D_b as funções de codificação e decodificação, respectivamente, do Banco. Considere x como um bloco de mensagem que vai ser enviada ao Banco por Antônio. Então, a codificação desse bloco vai ser $C_b(x)$. Para que a assinatura faça parte da mensagem ela deve ser $C_b(D_a(x))$. Inicialmente, usamos a função decodificação ao bloco x e, em seguida, usando a função codificação do Banco, codificamos o bloco. Ao receber a mensagem $C_b(D_a(x))$, o Banco utiliza a sua função de decodificação, e obtém $D_a(x)$. Logo em seguida, como a função codificação de Antônio é pública, o Banco a aplica no intuito de obter o bloco original x. A figura abaixo representará o que foi escrito.

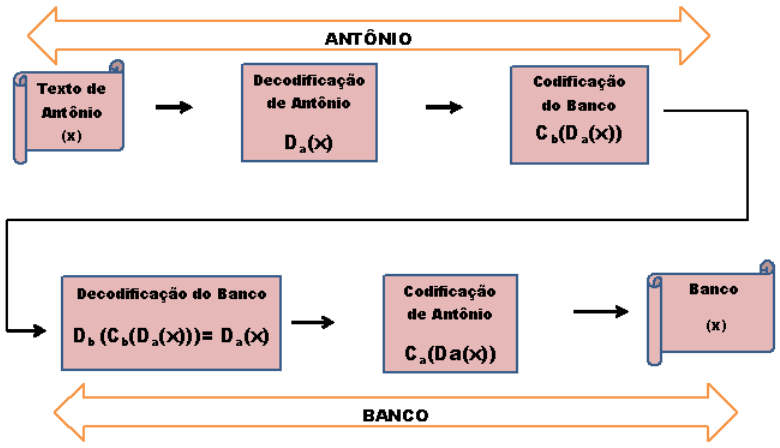

Figura 3.1: Esquema de Assinatura Digital

Como, apenas Antônio sabe qual é a função D_a, se a mensagem recebida tiver sentido, ela

teve origem dele próprio, pois a probabilidade de que uma mensagem enviada por uma pessoa que não conhece D_a, tenha sentido depois de ser decodificada pelo Banco, é quase zero. Dessa maneira, o Banco pode ter certeza de que a mensagem é segura.

Este sistema de assinatura digital não só permite que a mensagem entre destinatário e remetente seja transmitida de forma segura, como também garante que ela não será adulterada no processo, pois qualquer alteração da mensagem faz com que a assinatura não corresponda mais ao documento.

A credibilidade da assinatura digital possibilita uma maior segurança quando se navega na Internet e tem se tornado uma forma de precaução muito utilizada diante dos tão frequentes crimes digitais. Negócios online e transações bancárias, por exemplo, podem ser feitas com a garantia de que os dados e informações trocadas estão seguros.

CAPÍTULO 4

PROPOSTA DE ATIVIDADES PEDAGÓGICAS

4.1 Atividade 1- Criptografia RSA

Nesta atividade vamos utilizar o método de criptografia RSA, utilizada pela criptografia Assimétrica, o qual promoveram uma verdadeira mudança nos tradicionais meios de envio de mensagens secretas, diminuindo muito a fragilidade dos sistemas criptográficos, foi criado em 1977 e baseia-se no sistema de chaves duplas e na impossibilidade prática de se obter a chave secreta a partir da chave pública. Isto se deve ao fato de não se conhecer atualmente algoritmos para decompor números grandes em fatores primos em um tempo razoável - uma impossibilidade tecnológica.

4.1.1 Objetivo Geral

Mostrar a aplicação da Matemática em um ramo muito importante dos dias atuais, que é a Criptografia, onde o método RSA utiliza a teoria dos números como ferramenta para o seu algoritmo, fazendo com que seja compreendido o processo de codificação e decodificação .

4.1.2 Objetivos Específicos

- Fortalecer à aprendizagem sobre o algoritmo da Divisão.
- Calcular potências de números naturais.

- Mostrar uma aplicação dos números primos.
- Utilizar a calculadora como uma ferramenta para a resolução de problemas.

4.1.3 Público Alvo

Alunos do 6 ao 9 ano.

4.1.4 Pré-requisitos

Os alunos deverão conhecer o algoritmo de divisão e calculo de potências de números naturais.

4.1.5 Materiais

Os materiais utilizados nesta atividade são lápis, borracha e a folha contendo a atividade.

4.1.6 Dificuldades Previstas

Esta atividade no início irá requer uma atenção especial do professor, para que os alunos sigam passo a passo e não gere dificuldades, desmotivando os mesmos durante o processo.

4.2 Proposta de Atividade

Primeiramente temos que entender o que é criptografar, que consiste em transformar uma mensagem em outra, escondendo o verdadeiro texto.
Para tornar esta mensagem sem sentido é feito a codificação(cifra) e o processo inverso para obtenção do texto original é a decodificação(decifração).

Nesta atividade vamos usar o algoritmo RSA que tem um par de chaves onde, $\{e, n\}$ é a **chave pública** utilizada para a codificação, enquanto $\{d, \Psi(n)\}$ será a **chave privada** utilizada para a decodificação. Nesta atividade será dada as chaves porém precisamos saber como codificar e decodificar uma mensagem e por isso precisamos da duas fórmulas listadas abaixo:

- **Codificação:** É o resto da divisão de b^e por n,

- **Decodificação:** É o resto da divisão de a^d por n.

Sendo b o bloco da mensagem a codificar e a o bloco codificados e ambos compreendidos entre 1 e n.

Faremos agora um exemplo codificando e decodificando uma mensagem, só que vamos escolher números primos pequenos pois não estamos utilizando o computador.

Exemplo 4.1. *Sejam $p = 3$,$q = 11$, $e = 3$ e $d = 7$, vamos codificar e decodificar a frase sem espaço*

"BOATARDE"

e descrevermos os processos.

Codificação:

1° Passo Utilize a tabela de conversão e escreva a palavra em forma de número o espaço entre as palavras será desprezado.

Letras	A	B	C	D	E	F	G	H	I	J	K	L	M
Números	10	11	12	13	14	15	16	17	18	19	20	21	22

Letras	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Numeros	23	24	25	26	27	28	29	30	31	32	33	34	35

Que ficará da seguinte forma.

1124102910271314

2° Passo Separe a palavra convertida em blocos de forma que o número encontrado seja menor do que n é igual 33($n = 3 \cdot 11 = 33$).

$$11 - 24 - 10 - 29 - 10 - 27 - 13 - 14$$

3° Passo Agora vamos codificar a mensagem que será

o resto da divisão de b^e por n ,

onde b é bloco dividido anteriormente.

Por exemplo para o bloco 24 ,primeiramente elevaremos $24^3 = 24 \cdot 24 \cdot 24 = 13824$, após dividiremos por 33 e o resto corresponderá a parte criptografada. Vejamos

$$\begin{array}{r|l} 1\,3\,8\,2\,4 & 33 \\ \underline{-1\,3\,2} & 4\,1\,8 \\ \quad 6\,2 & \\ \quad \underline{-3\,3} & \\ \quad 2\,9\,4 & \\ \quad \underline{-2\,6\,4} & \\ \quad\quad 3\,0 & \end{array}$$

Portanto, o bloco **24** codificado será o bloco **30**.

Repetindo o mesmo processo, teremos todos o blocos codificados.

4° Passo Agora vamos escrever o Texto codificado.

$$11 - 30 - 10 - 2 - 10 - 15 - 19 - 5.$$

Feito isso vamos fazer o processo reverso.

Decodificação

5° Passo Para decodificarmos a mensagem, também utilizaremos o resto de uma divisão. Portanto, a função decodificação será

O resto da divisão de a^d por n,

onde a é o bloco codificado anteriormente e d já é um valor conhecido.

Por exemplo para o bloco 2 ,inicialmente, vamos elevar $2^7 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cot 2 \cdot 2 = 128$, após dividiremos por 33 e o resto corresponderá o bloco original. Vejamos

$$\begin{array}{r|l} 1\,2\,8 & 33 \\ \underline{-9\,9} & 3 \\ 2\,9 & \end{array}$$

Portanto, o bloco codificado 2 corresponderá ao bloco 29, o que verifica de fato o funcionamento do algoritmo. Repetindo o mesmo processo teremos os blocos:

$$11 - 24 - 10 - 29 - 10 - 27 - 13 - 14.$$

6° Passo Obter a mensagem original com a utilização da tabela de conversão com os resultados obtidos no **Passo 5** para ter o texto original.

BO-AT-AR-DE, ou seja, Boa tarde!

4.3 Atividades Recomendada

4.3.1 Atividade Recomendada 1

Como base nos dados fornecidos e aos passos 1,2,3,4,5 e 6 apresentados no exemplo 4.1 faça o seguinte:

a) Codifique à frase "Boa Noite";

b) Utilizando os dados da questão anterior decodifique a mensagem codificada no item a);

c) Descreva as dificuldades encontradas nos processos de codificação e decodificação.

4.3.2 Atividade Recomendada 2

A segunda atividade será explorado o trabalho em grupo, no qual a sala será dividida em dois grupos um para Cifrar e outro para Decifrar a mensagem "BOASORTE"utilizando a chaves dos exemplo 4.1. Agora descreveremos os passos para a execução da atividade:

1. Dividir a sala em dois grupos um para codificar a mensagem e outro grupo para decodificar;
2. Entregar a frase "BOASORTE"para o grupo de Codificação;
3. O grupo de codificação irá passar o texto numérico codificado para o grupo de Decodificação;
4. O grupo de Decodificação, após o processo de decifração irá ler em voz alta a mensagem.

CONCLUSÃO

Sem sombra de dúvida, a presença da matemática é notória em vários segmentos da tecnologia que surgiu ou ainda irá surgir. O surgimento da Criptografia foi de grande importância para a segurança de informações em trânsito, ou seja, o envio de uma mensagem do destinatário para um remetente. Além dessa função, a Criptografia permite que milhões de usuários da internet no mundo consigam realizar transações comerciais online de forma segura e rápida.

Como foi visto neste trabalho, a Criptografia tornou-se uma ferramenta indispensável durante aos séculos. Inicialmente com sua função de confidencialidade e atualmente com as funções de autenticidade, irretratabilidade e integridade que permitem transações comerciais online.

Ao abordar o tema Criptografia RSA, reiteramos conceitos matemáticos imprescindíveis para a realização do tema, sendo aplicados nos processos de codificação, decodificação, no estudo da funcionalidade e da segurança do sistema criptográfico citado.

Ao final, foram propostas duas atividades pedagógicas que possibilitam a aprendizagem do método RSA e o fortalecimento do algoritmo da divisão. Desta forma torna-se possível responder à pergunta usual dos alunos: "por que estudar isso?", mostrando aos mesmos a importância da matemática abstrata, que muitas vezes uma teoria criada não há uma aplicação atual, porém no futuro pode existir. Fala-se de algo que se possa ser aplicado além do desenvolvimento lógico dedutivo, que é tão importante nesta disciplina.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] DOMINGUES; H. Hygino.**Fundamentos de aritmética**; São Paulo, Atual, 1991.

[2] COUTINHO. **Números Inteiros e Criptrografia RSA**. 2ª ed. Rio de Janeiro: Impa, 2003.

[3] KOSHY, Thomas. **Elementary Number Theory with Applications**; 2ª ed, USA, AP, 2007.

[4] HEFEZ, Abramo. **Elementos de Aritmética**; 2ª ed, Rio de Janeiro, SBM, 2011.

[5] _____ **Iniciação a Aritmética** . Programa de Iniciação Científica, OBMEP, Ed. da SBM, Rio de Janeiro-RJ, 2012.

[6] STALINGS,William.**Criptografia e Segurança de redes** , 4ª ed., São Paulo, Pearson, 2008.

[7] FALEIROS, Antonio Cândido. **Criptografia**; São Carlos: SBMAC, 2011, 138 P,(Notas em Matemática Aplicada; v. 52). Disponível em < http:www.sbmac.org.br\arquivos\notas*livro*_52.pdf > acesso em 07.08.2015.