

Criptologia: aspectos históricos e matemáticos

Autor: *Maythison Aparecido Manoel*

Orientador: *Prof. Dr. João Carlos Vieira Sampaio*

Disciplina: Trabalho de Conclusão do Curso

Curso: Licenciatura e Bacharelado em Matemática

Professores Responsáveis: João Carlos Vieira Sampaio
Alessandra Verri
Selma Helena de Jesus Nicola

São Carlos, 30 de março de 2017.

Criptologia: aspectos históricos e matemáticos

Autor: *Maythison Aparecido Manoel*

Orientador: *Prof. Dr. João Carlos Vieira Sampaio*

Disciplina: Trabalho de Conclusão do Curso

Curso: Licenciatura e Bacharelado em Matemática

Professores Responsáveis: João Carlos Vieira Sampaio
Alessandra Verri
Selma Helena de Jesus Nicola

Instituição: Universidade Federal de São Carlos
Centro de Ciências Exatas e de Tecnologia
Departamento de Matemática

São Carlos, 30 de março de 2017.

Autor (aluno)

Orientador (orientador)

Parte I

Trabalho de Conclusão de Curso A

Resumo

A necessidade de se comunicar com segurança, transmitindo informações importantes que decidem a vida de milhares de pessoas, sempre foi preocupação de reis e governantes ao longo da história. Com o passar do tempo, a evolução das sociedades e da tecnologia ampliou esta necessidade. Hoje vemos que esta preocupação não é mais restrita aos altos escalões do governo. Ao mesmo tempo que técnicas e códigos foram criados e aperfeiçoados para garantir a transmissão segura de informações, técnicas e métodos de decifragem também evoluíram. Sendo assim, a preocupação de se comunicar em segurança ronda todos aqueles que se utilizam das mais variadas formas de comunicação.

O intuito deste pequeno trabalho é acompanhar de forma superficial o desenvolvimento histórico da criptologia. São dados exemplos de como esta foi, ao longo do tempo, se constituindo uma área de interesse estimulando o desenvolvimento científico. Ao longo do texto são mostrados alguns métodos utilizados pelos mais diversos povos, assim como uma breve descrição matemática de tais métodos.

O foco deste trabalho é fornecer uma introdução ao estudo da criptologia, com alguns conceitos históricos e matemáticos desenvolvidos ao longo do tempo. Tal introdução é importante para a compreensão da cifra RSA, assunto do próximo Trabalho de Conclusão de Curso.

Sumário

I Trabalho de Conclusão de Curso A	iii
Elementos da Teoria dos Números	1
Divisibilidade e o algoritmo da divisão em \mathbb{Z}	1
Divisibilidade	1
Algoritmo da divisão em \mathbb{Z}	2
Máximo Divisor Comum e Mínimo Múltiplo Comum	2
Algoritmo euclidiano para o cálculo do mdc	3
Números Primos e Propriedades	4
Aritmética Modular	6
Relações de Equivalência	6
Congruência módulo n em \mathbb{Z} :	7
Pequeno Teorema de Fermat	7
Teorema de Euler	8
Aspectos Históricos da Criptologia	8
Introdução	9
Criptologia	9
A Criptologia ao longo da História	11
O surgimento da cifra RSA	19

II Trabalho de Conclusão de Curso B	23
A cifra RSA	25
Cifras simétricas e assimétricas	27
Implementação RSA	40
Testes de primalidade	42
Método da divisão	44
Pseudoprimidade	44
Teorema de Lucas e Pocklington	48
Números de Fermat e Mersenne	49
Métodos algorítmicos	50

Lista de Figuras

1	Modelo de Citale Espartano	12
2	Alfabeto Original	15
3	Alfabeto Cifrado	15
4	Alfabeto com a Cifra de César	16
5	Máquina Enigma com três rotores.	18

Elementos da Teoria dos Números

Divisibilidade e o algoritmo da divisão em \mathbb{Z}

Divisibilidade

Definição 1.1: Um inteiro a divide um inteiro b quando existe um número inteiro m , tal que $b = a \cdot m$. Quando $a \neq 0$, dizemos também que b é divisível por a . Neste caso, o inteiro m é chamado de quociente de b por a e é indicado por $m = \frac{b}{a}$.

Quando a divide b , denotamos $a|b$. No caso em que $a \neq 0$, dizemos ainda, que b é divisível por a . Quando a não divide b , escrevemos $a \nmid b$.

Propriedades Fundamentais:

- (1) $a|a$, para todo $a \in \mathbb{Z}$;
- (2) Se $a|b$ e $b|c$, então $a|c$;
- (3) Se $a|b$ e $c|d$, então $ac|bd$;
- (4) Se $a|b$ então $a|kb$ para qualquer inteiro k ;
- (5) Se $a|b$ e $a|c$, então $a|(mb + nc)$, $\forall m, n \in \mathbb{Z}$;
- (6) Se $a|b$ e $b|a$, então $a = \pm b$.

Demonstrações:

- (1): Como para qualquer inteiro a tem-se que $a = 1 \cdot a$, temos que $a|a$.
- (2): Como $a|b$ e $b|c$, existem inteiros m e n tais que $b = am$ e $c = bn$. Logo, $c = (am)n = a(mn)$ e, portanto, $a|c$.
- (3): Se $a|b$ e $c|d$, existem inteiros m e n , tais que $b = am$ e $d = cn$. Logo, $bd = (am)(cn) = (ac)(mn)$, ou seja, $ac|bd$.
- (4): Se $a|b$, então existe um inteiro m , tal que $b = am$. Logo, para qualquer inteiro k , teremos $kb = k(am) = a(km)$, ou seja, $a|kb$. Portanto, se $a|b$, então a divide qualquer múltiplo de b .
- (5): Como $a|b$ e $a|c$ existem inteiros e e f tais que $b = ae$ e $c = af$. Logo, $mb + nc = m(ae) + n(af) = (me + nf)a$. Portanto, $a|(mb + nc)$.

(6): Como $a|b$, existe m inteiro tal que $b = am$. Se $a = 0$, então $b = 0$ e temos $a = b = 0$. Suponhamos $a \neq 0$. Como $b|a$, existe n inteiro tal que $a = bn$. Logo, $a = amn$. Por cancelamento, temos $mn = 1$. Sendo m e n inteiros, então necessariamente $m = n = 1$ ou $m = n = -1$. Logo $a = b$ ou $a = -b$.

Propriedade de Arquimedes: Dados $a, b \in \mathbb{Z}$ com $b \neq 0$, então a é múltiplo de b ou se encontra entre dois múltiplos consecutivos de b , ou seja, para $b > 0$, temos $qb \leq a < (q+1)b$, e para $b < 0$, temos $qb \leq a < (q-1)b$, onde $q \in \mathbb{Z}$.

Algoritmo da divisão em \mathbb{Z}

Teorema 1.1: Se a e b são inteiros e $b \neq 0$, então existem inteiros q e r tais que $a = bq + r$ e $0 \leq r < |b|$. Os inteiros q e r , nas condições apresentadas, são únicos. Os inteiros q e r são chamados respectivamente de **quociente** e **resto** da **divisão euclidiana** de a por b .

Demonstração: Pela propriedade de Arquimedes, se $b > 0$, existe $q \in \mathbb{Z}$, satisfazendo a condição $qb \leq a < (q+1)b$. Isto implica que $0 \leq a - qb$, logo $a - qb < b$. Desta forma, se definirmos $r = a - qb$, teremos garantida a existência de q e r inteiros, com $0 \leq r < b$. Se $b < 0$ e como $|b| > 0$, temos a existência de q e r satisfazendo $a = |b|q + r$ e $0 \leq r < |b|$. Então $a = (-b)q + r$, ou $a = b(-q) + r$ e acertamos assim um quociente adequado.

Para provar que q e r são únicos, suponhamos $a = bq + r = bq' + r'$, sendo q, r, q', r' inteiros, $0 \leq r, r' < |b|$. Então $b(q - q') = r' - r$, daí $|b||q - q'| = |r - r'|$. Como $-|b| < r, r' < |b|$ temos $-|b| < r - r' < |b|$, e portanto $|r - r'| < |b|$. Assim sendo, $|b||q - q'| < |b|$, logo $|q - q'| < 1$ e sendo $|q - q'|$ um inteiro não negativo, temos necessariamente $|q - q'| = 0$. Portanto $q = q'$ e de $bq + r = bq + r'$ deduzimos $r = r'$.

Máximo Divisor Comum e Mínimo Múltiplo Comum

Definição 1.2 (mdc): Um inteiro não negativo d é o máximo divisor comum dos números inteiros a e b (denota-se por $d = \text{mdc}(a, b)$), se

- (i) $d|a$ e $d|b$;
- (ii) Se $c|a$ e $c|b$ então $c|d$;

Definição 1.3 (mmc): Um inteiro não negativo d , é o mínimo múltiplo comum dos números inteiros a e b (denota-se $d = \text{mmc}(a, b)$), se

- (i) $a|d$ e $b|d$;

(ii) Se $a|c$ e $b|c$ então $d|c$.

Definição 1.4 (primos relativos): Dois inteiros a e b , são ditos primos relativos ou co-primos se $\text{mdc}(a, b) = 1$

Algoritmo euclidiano para o cálculo do mdc

Lema 1.1: Sejam a e b dois inteiros, com $b \neq 0$, e seja r o resto da divisão Euclidiana de a por b . Então, $\text{mdc}(a, b) = \text{mdc}(b, r)$.

Demonstração: Para demonstrar o resultado enunciado no lema, é suficiente provar que todo divisor de a e b é também divisor de b e r , e reciprocamente. Dessa maneira, o maior divisor de a e b coincidirá com o maior divisor de b e r . Note que esse “maior divisor” existe, já que $b \neq 0$. Temos por hipótese, $a = bq + r$; logo, $r = a - bq$. Seja x um divisor inteiro de a e b . Então:

$$x|a \text{ e } x|b \Rightarrow x|(a - qb) \Rightarrow x|r$$

Portanto, $x|b$ e $x|r$. Sendo assim, $D(a, b) \subset D(b, r)$. (o conjunto dos divisores de a e b está contido no conjunto dos divisores de b e r). Agora, seja x um inteiro divisor de b e r . Então:

$$x|b \text{ e } x|r \Rightarrow x|(qb + r) \Rightarrow x|a$$

Logo, $x|b$ e $x|a$. Daí, $D(b, r) \subset D(a, b)$. Portanto, $D(a, b) = D(b, r)$ e assim sendo, $\text{mdc}(a, b) = \max D(a, b) = \max D(b, r) = \text{mdc}(b, r)$.

Lema 1.2: Sejam a e b inteiros ambos positivos com $a \geq b$, e definamos uma sequência de inteiros não negativos da seguinte forma:

(i) $r_1 = a$;

(ii) $r_2 = b$;

(iii) Para cada índice k , com $k \geq 2$, se $r_k \neq 0$, r_{k+1} é o resto da divisão euclidiana de r_{k-1} por r_k . E se $r_k = 0$, a sequência termina em r_k .

Então, a sequência r_1, r_2, \dots é finita e termina em zero, ou seja, existe um índice n tal que $r_1 \geq r_2 > \dots > r_n > 0$ e $r_{n+1} = 0$.

Demonstração: Por hipótese, $r_1 \geq r_2$ e pela definição de r_{k+1} , para $k \geq 2$ temos, $r_{k+1} < r_k$. Considere o conjunto de números naturais $S = r_1, r_2, \dots$. Como $S \subset \mathbb{N}$ e $S \neq \emptyset$, pelo princípio da boa ordenação dos números naturais, S possui um mínimo, o qual denotaremos por r_{n+1} . Pelo que foi observado, teremos $r_1 \geq r_2 > \dots > r_n > r_{n+1}$.

Afirmamos que $r_{n+1} = 0$. Para justificar isto, basta observar que se, $r_{n+1} \neq 0$, então

podemos definir $r_{n+2} \in S$ como o resto da divisão de r_n por r_{n+1} . Teremos então, $0 < r_{n+2} < r_{n+1}$, contrariando o fato de r_{n+1} ser o mínimo de S .

Teorema 1.2 (Algoritmo euclidiano para o cálculo do mdc): Sejam a e b inteiros, ambos positivos, com $a \geq b$, e seja

$$r_1, r_2, \dots, r_n, r_{n+1}$$

a sequência definida pelo **Lema 1.2**, sendo

$$r_1 \geq r_2 > \dots > r_n > r_{n+1} = 0$$

Então, $r_n = \text{mdc}(a, b)$.

Demonstração: Para cada $k \geq 3$, r_k é o resto da divisão de r_{k-2} por r_{k-1} . Pelo **Lema 1.1**,

$$\text{mdc}(r_k, r_{k-1}) = \text{mdc}(r_{k-1}, r_{k-2})$$

Logo,

$$r_n = \text{mdc}(0, r_n) = \text{mdc}(r_{n+1}, r_n) = \text{mdc}(r_n, r_{n-1}) = \dots = \text{mdc}(r_2, r_1) = \text{mdc}(a, b).$$

Números Primos e Propriedades

Definição 1.5: Dizemos que um número inteiro p é primo se $p \neq 0$, $p \neq 1$, $p \neq -1$, e os únicos divisores de p são 1 , p , -1 e $-p$. Dizemos que um inteiro m é composto se $m \neq 0$, $m \neq 1$, $m \neq -1$ e m não é primo.

Proposição 1.1: Se p é primo, então $\text{mdc}(p, (p-1)!) = 1$, ou seja, há exatamente $p-1$ números menores que p co-primos com p .

Demonstração: Seja p primo. Temos que $(p-1)! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)$, veja que p não divide nenhum dos termos da multiplicação e, portanto, não divide $(p-1)!$. Do fato de que p é primo, segue que nenhum fator positivo de $(p-1)!$ é divisor de p , ou seja, o maior número que divide os dois simultaneamente é 1 . Da definição de máximo divisor comum, chegamos em $\text{mdc}(p, (p-1)!) = 1$.

Teorema 1.3 (Teorema Fundamental da Aritmética): Todo inteiro m , $m \geq 2$, é um número primo ou tem a forma $m = p_1 \cdot p_2 \cdot \dots \cdot p_n$, para certos inteiros primos positivos p_1, p_2, \dots, p_n , com $n \geq 2$. Ou seja, cada inteiro, a partir do 2 , é um primo ou um produto de

fatores primos positivos.

Demonstração (indução sobre n): Se $m = 2$, então m é primo. Seja $k \geq 2$ e suponha que todo inteiro m , com $2 \leq m \leq k$, seja primo ou se decompõe em fatores primos. Trataremos de demonstrar que então $k+1$ também é primo ou se escreve como produto de primos. Consideremos o inteiro $k+1$. Se $k+1$ é primo, então não há mais o que demonstrar. Se $k+1$ não é primo, como $k+1 \geq 3$, temos que $k+1$ é composto. Então existem inteiros positivos a e b , com $1 < a < k+1$ e $1 < b < k+1$, tais que $k+1$ se fatora na forma $k+1 = a \cdot b$. Agora, como $2 \leq a \leq k$ e $2 \leq b \leq k$, pela hipótese de indução cada um dos inteiros a e b é um primo ou se decompõe como produto de fatores primos positivos. Logo, como $k+1 = ab$, $k+1$ se decompõe como um produto de fatores primos positivos. Portanto, cada inteiro $m \geq 2$ é primo ou se escreve como um produto de primos.

Teorema 1.4: Existem infinitos números primos.

Demonstração: Seja p_1, p_2, \dots, p_n um conjunto de n primos positivos, $n \geq 1$. Considere o inteiro positivo

$$a = 1 + p_1 \cdot \dots \cdot p_n$$

Mostraremos que a possui um fator primo diferente dos primos p_1, \dots, p_n . Obviamente, a é um inteiro positivo maior que cada um dos primos p_1, \dots, p_n . Seja a primo, ele mesmo é o primo procurado, fora do conjunto p_1, p_2, \dots, p_n . Se a não é primo, pelo **Teorema 1.3**, ele possui um fator primo positivo q . Temos então $q \notin \{p_1, p_2, \dots, p_n\}$, se $q = p_i$ para algum $i \in \{1, 2, \dots, n\}$, então $q | (p_1 \cdot p_2 \cdot \dots \cdot p_n)$; como $q | (a - p_1 \cdot \dots \cdot p_n)$ e portanto, $q | 1$, o que contradiz o fato de q ser primo.

Proposição 1.2: Sejam os números inteiros

$$a = p_1^{e_1} \cdot \dots \cdot p_k^{e_k} \text{ e } b = p_1^{f_1} \cdot \dots \cdot p_k^{f_k}$$

onde $e_i \geq 0$ e $f_i \geq 0$, para $i = 1, 2, \dots, k$. Então,

$$\text{mdc}(a, b) = p_1^{\min(e_1, f_1)} \dots p_k^{\min(e_k, f_k)}$$

$$\text{mmc}(a, b) = p_1^{\max(e_1, f_1)} \dots p_k^{\max(e_k, f_k)}$$

Definição 1.6 (Função φ de Euler): Para $n \neq 1$, a função $\varphi(n)$ denota o número de inteiros no intervalo $[1, n]$, que são co-primos com n . Esta função φ é chamada de **função totiente de Euler**.

Propriedades:

- (1) Se p é primo, então $\varphi(p) = p - 1$
- (2) $\varphi(p) = p^\alpha - p^{\alpha-1}$, para α inteiro positivo e p primo;
- (3) A função φ é multiplicativa, isto é, se $\text{mdc}(m, n) = 1$ então

$$\varphi(m, n) = \varphi(m)\varphi(n).$$

- (4) Se $n = p_1^{e_1} \dots p_k^{e_k}$, com p_i primos e $e_i \geq 0$, para todo i , então

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

Assim, se n é um número composto que pode ser fatorado como o produto de dois números primos p e q então, $\varphi(n) = (p - 1)(q - 1)$.

A função totiente de Euler e suas propriedades serão abordadas mais a frente.

Aritmética Modular

Relações de Equivalência

Uma relação binária \sim sobre um conjunto X não vazio é chamada de relação de equivalência sobre X , quando satisfaz as três seguintes propriedades:

- (1) $x \sim x$ para cada $x \in X$; (reflexiva)
- (2) Se $x \sim y$, então $y \sim x$; (simétrica)
- (3) Se $x \sim y$ e $y \sim z$, então, $x \sim z$ (transitiva)

Uma relação binária permite compararmos dois elementos de um conjunto segundo uma dada regra. As relações de equivalência são usadas para classificar os elementos de um conjunto em subconjuntos com propriedades semelhantes denominadas classes de equivalência. A classe de equivalência de um elemento $x \in X$ é denotada por

$$\bar{x} = \{y \in X : y \sim x\}$$

Temos ainda que qualquer elemento de uma classe de equivalência é um representante de toda a classe.

Destacamos ainda dois resultados muito importantes relacionados ao conjunto X com a relação de equivalência \sim :

- (1) X é a união de todas as classes de equivalência da relação \sim .

(2) A intersecção de duas classes de equivalência distintas é vazia.

Congruência módulo m em \mathbb{Z} :

Uma relação de equivalência no conjunto dos números inteiros pode ser construída do seguinte modo: dados dois inteiros a e b , cuja diferença é um múltiplo de um $m \in \mathbb{Z}^*$, são ditos congruentes módulo m se $a - b$ é múltiplo de m sendo essa relação denotada por $a \equiv b \pmod{m}$. Mostremos que a congruência módulo m é uma relação de equivalência:

Sejam $a, b, c \in \mathbb{Z}$ então:

(i) $a \equiv a \pmod{m}$. De fato, $a - a = 0 \cdot m$

(ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$. De fato, $a - b = km$ e $a - b = -(b - a) = -km \Rightarrow b \equiv a \pmod{m}$; $k \in \mathbb{Z}$

(iii) $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$. De fato, $a - b = k_1m$ e $b - c = k_2m$. Como $(a - b) + (b - c) = a - c$, temos $(k_1m) + (k_2m) = a - c \Rightarrow a - c = (k_1 + k_2)m$, ou seja, $a \equiv c \pmod{m}$; $k_1, k_2 \in \mathbb{Z}$

Propriedades: Sejam $a, b, c, d \in \mathbb{Z}$, então:

(1) $a \equiv b \pmod{m}, b \equiv a \pmod{m}$ e $a - b \equiv 0 \pmod{m}$ são proposições equivalentes;

(2) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$;

(3) Se $a \equiv b \pmod{m}$, então $ac \equiv bc \pmod{m}$;

(4) Se $ac \equiv bc \pmod{m}$, então $a \equiv b \pmod{\frac{m}{\text{mdc}(c, m)}}$, onde $d = \text{mdc}(c, m)$. Essa propriedade é conhecida com Lei do Cancelamento. Veja que basta termos satisfeita a condição de que $\text{mdc}(c, m) = 1$, teremos $ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{m}$.

Pequeno Teorema de Fermat

Teorema 1.5: Seja p um número primo. Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$.

Demonstração: Seja o conjunto de valores $a, 2a, 3a, \dots, (p-1)a$. Sabemos que pelo fato de que p não dividir a , $\text{mdc}(a, p) = 1$ e, portanto, nenhum dos números deste conjunto é divisível por p . Além disso, temos que, se $aj \equiv ak \pmod{p}$, então $j \equiv k \pmod{p}$, ou seja, todos os elementos são, dois a dois, não congruentes módulo p e portanto, podemos estabelecer uma relação biunívoca entre os $aj, j = 1, 2, \dots, p-1$ e o conjunto $1, 2, \dots, (p-1)$, em termos de congruência, isto é, a correspondência $\bar{a} \leftrightarrow \overline{aj}, j = 1, 2, \dots, p-1$, é bijetora.

Deste argumento, e da propriedade (3) da relação de congruência, segue a seguinte igualdade:

$$a(2a)(3a)\dots(p-1)a \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \pmod{p}$$

ou seja,

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

Da lei do cancelamento, e do fato de que $\text{mdc}((p-1)!, p) = 1$, segue que

$$a^{p-1} \equiv 1 \pmod{p}$$

Corolário 1.1: Se p é um primo e a é um inteiro positivo, então $a^p \equiv a \pmod{p}$

Demonstração: Se p não divide a , do **Pequeno Teorema de Fermat** temos que $p | (a^{p-1} - 1)$ ou seja $p | a(a^{p-1} - 1)$. Se p divide a , então $p | a(a^{p-1} - 1)$

Teorema de Euler

Teorema 1.6: Se m é um inteiro positivo e a é um inteiro com $\text{mdc}(a, m) = 1$, então $a^{\varphi(m)} \equiv 1 \pmod{m}$.

O teorema de Euler visa generalizar o Pequeno Teorema de Fermat para quaisquer números inteiros, utilizando, para isso a função φ de Euler. É interessante notar que para um número primo, o Teorema de Euler é exatamente o Pequeno Teorema de Fermat. Uma demonstração será reproduzida na segunda parte deste trabalho.

Aspectos Históricos da Criptologia

Introdução

Com o avanço da ciência e o desenvolvimento da tecnologia, vemos o crescimento da troca de informações pelo mundo, seja através do rádio, TV, telefone, internet, entre outros. Com essas mudanças, tornou-se imprescindível proteger o conteúdo de determinadas informações para que não caiam em mãos erradas. Apesar da existência de toda uma teoria especializada e dos métodos utilizados hoje serem muito elaborados, a preocupação em se proteger determinadas mensagens não é nova e possivelmente remonta desde a criação da escrita pelo homem.

Tal preocupação teve maior terreno na área militar, principalmente em épocas de guerras. Com tudo, novamente devido às inovações tecnológicas, principalmente o surgimento do computador e da internet, muitas atividades que eram realizadas pessoalmente e por trocas de objetos, hoje podem ser realizadas sem sairmos de casa, por meio de cartões magnéticos. Com isso, a necessidade de sigilo em transações e conversas deixou a exclusividade da área militar e se expandiu por toda a sociedade. Com o passar do tempo, tal preocupação ganhou corpo e métodos de proteção de mensagens se aperfeiçoaram dando força a uma teoria ampla, que abarca várias áreas do conhecimento humano.

Criptologia

De maneira geral, entende-se como Criptologia o conjunto dos conhecimentos, das mais diversas áreas do saber humano, necessários para o desenvolvimento da Criptografia e da Criptoanálise. Sendo que a primeira se ocupa com a cifragem das informações sigilosas para uma transmissão segura e a segunda, pelo contrário, procura, uma vez interceptada a informação, decifrá-la. No geral, os diferentes métodos utilizados na Criptografia são identificados como cifras.

À grosso modo, existindo um emissor, um receptor e uma mensagem de conteúdo secreto,

ambos tentarão se comunicar sem que um terceiro intercepte a mensagem. Para isso, lançarão mão da Criptografia, sobretudo o emissor, a fim de alterar a mensagem para que esta se torne ilegível, fazendo uso de um algoritmo de encriptação e de uma "chave de encriptação", geralmente um valor numérico necessário para a aplicação do algoritmo (processo de cifragem). Por sua vez, o receptor, ao receber a referida mensagem estará previamente de posse do algoritmo e da chave de deciptação (processo de decifragem), sendo esta o segredo que torna a mensagem novamente legível. Enquanto isso, um terceiro personagem pode procurar interceptar a mensagem e torná-la legível, porém, este não possui o algoritmo e chave de deciptação, logo, deve ele lançar mão da Criptoanálise, que consiste justamente no estudo das técnicas de se decifrar a mensagem. É importante mencionar que para algoritmos mais sofisticados, mesmo que o interceptador conheça tal algoritmo ainda se torna muito difícil que ele traduza a mensagem sem a chave de deciptação. Deste ponto de vista, a chave é o grande segredo que deve ser guardado.

Atualmente existem dois tipos de chaves criptográficas, a simétrica e a assimétrica. Sendo que o primeiro método consiste basicamente em se obter um algoritmo de encriptação e uma chave de encriptação/decriptação, neste caso, tal chave é única e deve estar em posse dos interlocutores. Por sua vez, no método da chave assimétrica, existe também o algoritmo de encriptação e duas chaves. Sendo uma para encriptar e a outra para deciptar a mensagem. A primeira cifra assimétrica foi criada na década de 1970, chamada DH, que possuía duas chaves, uma para cifrar e outra para decifrar, sendo ambas privadas, uma para cada interlocutor. Porém em 1977, fazendo uso desta cifra e de conhecimentos matemáticos referentes a Teoria dos Números, criou-se a cifra RSA, inaugurando o conceito de chave privada e chave pública, que será abordada mais à frente.

A Criptografia se divide em dois ramos, a de transposição e a de substituição. A primeira consiste basicamente em se construir anagramas das palavras de uma mensagem secreta. Este método possui alguma limitação se considerarmos mensagens com palavras curtas, porém em mensagens longas, o número de anagramas possíveis cresce consideravelmente, dificultando a decifragem. Já o segundo método, o de substituição, consiste essencialmente em se substituir os caracteres da palavra original por outros, afim de impossibilitar a leitura da mensagem.

Outra forma de se comunicar de maneira segura é fazendo uso da Esteganografia, cujo nome vem de um termo grego que significa "escrita escondida". A grande diferença entre Criptografia e Esteganografia, é que a primeira altera o conteúdo da mensagem, já a segunda procura transmitir a mensagem inalterada de maneira oculta. É possível combinar ambas as técnicas a fim de se aumentar a segurança da transmissão. Existem vários métodos de se ocultar uma mensagem, alguns elaborados, como o microponto ou tintas invisíveis por

exemplo.

A Criptologia ao longo da História

O desenvolvimento da Criptologia se dá paralelamente ao da Criptoanálise. Até hoje, o primeiro registro de Criptografia encontrado vem dos egípcios, no ano de 1900 a. C. Ao que parece, um escriba ao escrever uma mensagem, utilizou hieróglifos fora do padrão usual de escrita da época para se comunicar. Porém, vários estudiosos não reconhecem este texto como um exemplo de criptografia, mas uma espécie de brincadeira entre pessoas que sabiam ler e escrever e que teriam contato com a mensagem. Pelo conteúdo, o texto não tratava de uma informação importante a ser transmitida e não é garantido que havia um método sistemático para a encifração da mensagem. Além dos egípcios, vários povos utilizaram diversos métodos para proteger uma informação, sendo no início, em sua maioria métodos de esteganografia.

Têm-se relatos mais específicos de criptografia em tabuletas de argila encontradas na Mesopotâmia, de épocas posteriores, com algumas contendo mensagens de transações e acordos econômicos. Tempos depois, os hebreus utilizaram também métodos de criptografia rudimentares para protegerem informações. Em sua maioria eram métodos de substituição simples, onde os caracteres são substituídos um a um por outros. Atbash, Albam e Atbah são as três Cifras Hebraicas mais conhecidas, datando-se de 600-500 a.C. Com este método, por exemplo, foram capazes de encriptar alguns trechos bíblicos do livro de Jeremias. Estas cifras são totalmente reversíveis, pois ao aplicar o algoritmo de substituição utilizando-se de uma chave específica obtêm-se o texto cifrado e aplicando o mesmo algoritmo ao texto cifrado e utilizando-se o valor correspondente ao oposto do valor da chave anterior, obtêm-se novamente o texto original. Para ser mais preciso, ao se cifrar um texto é necessário um algoritmo e uma chave de cifragem. Tal chave é representada por um número, que neste tipo de cifra deve ser mantido em sigilo. Para se realizar a decifragem do texto é necessário um algoritmo de decifragem e de uma chave de decifragem. O algoritmo de decifragem pode ser obtido do algoritmo de cifragem, porém agora deve-se manipulá-lo com vistas a encontrar o texto original e fazendo uso da chave de decifragem, que também pode ser obtida da anterior. Por ser uma cifra relativamente simples, a diferença básica entre os processos de cifrar e decifrar é que se somamos o valor da chave para cifrar, iremos agora subtraí-lo e vice-versa.

Tais cifras são classificadas como Monoalfabéticas e Monográficas, isso indica que respectivamente, utiliza-se apenas um alfabeto para a substituição e cada letra é substituída por um único caracter. Hoje em dia, com métodos de criptoanálise avançados, sua segurança é considerada baixa, porém para a época era suficiente para qualquer conversação.

A cifra Atbash consiste em se trocar a primeira letra do alfabeto hebreu, Aleph, pela última, Taw, a segunda letra Beth é trocada pela penúltima, Shin, e assim por diante. Desta combinação de letras, resulta a palavra Atbash(**A**leph **T**aw **B**eth **S**Hin).

A cifra Albam, por sua vez, consiste em se trocar a primeira letra do alfabeto pela décima terceira subsequente. Temos assim que a primeira letra do alfabeto, Aleph, é trocada por Lamed, a segunda, Beth, é trocada por Mem. Daí a origem do nome da cifra: **A**leph **L**amed **B**eth **M**em, que resulta em ALBAM.

A cifra Atbah segue uma sequência de substituição especial. A letra Aleph, é trocada por Teth, a segunda, Beth, é trocada por Heth. Por consequência, Atbah vêm de **A**leph **T**eth **B**eth **H**eth.

Os Gregos antigos também utilizaram métodos para proteger suas mensagens, como o *skytálē*(citale ou cítalá), que significa bastão, muito utilizado pelos espartanos. Este aparelho para cifra de transposição consistia em se enrolar uma longa tira de couro ou pergaminho em torno de um bastão de dimensões conhecidas. O escriba então, escrevia a mensagem em torno do bastão. Após escrita, o pergaminho era desenrolado, sendo que assim as letras das palavras eram trocadas de lugar. Ao receber a mensagem, o receptor, de posse de um bastão de mesma medida, tornava a enrolar o pergaminho e lia a mensagem facilmente.



Figura 1: Modelo de Citale Espartano

Um episódio famoso onde se utiliza da esteganografia entre os gregos é narrado por Heródoto em “As Histórias”, século V a.C., que trata da frustrada batalha do exército de Xerxes, rei dos persas, contra os gregos. Aparentemente, por não receber tributos dos espartanos e atenienses para a construção de Persépolis, Xerxes resolve se vingar reunindo um grande exército para um ataque surpresa. Porém seu plano é entregue aos gregos por uma mensagem secreta:

"O perigo de ser descoberto era grande; havia apenas um modo pelo qual a mensagem poderia passar: isso foi feito raspando-se a cera de um par de tabuletas de

madeira, e escrevendo embaixo o que Xerxes pretendia fazer, depois a mensagem foi coberta novamente com cera. Deste modo, as tabuletas pareceriam estar em branco e não causariam problemas com os guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz de perceber o segredo, até que, pelo que entendi, a filha de Cleomenes Gorgo, que era casada com Leônidas, adivinhou e contou aos outros que se eles raspassem a cera encontrariam alguma coisa escrita na madeira. Isto foi feito, revelando a mensagem, então transmitida para os outros gregos."

Através desta artimanha de esteganografia, os gregos puderam vencer a batalha se preparando com antecedência.

Os chineses também utilizaram métodos de esteganografia, como por exemplo, escrever a mensagem em pequenas tiras de seda que eram enroladas e cobertas por cera, formando pequenas bolinhas. O mensageiro engolia tais bolinhas e as levava consigo até seu destino. Ou ao se utilizar certas tintas retiradas de plantas específicas que revelavam o conteúdo escrito ao se aquecer as páginas da mensagem.

Percebe-se a fraqueza da esteganografia em comparação com a criptografia, pois na primeira corre-se o risco de a mensagem ser interceptada e descoberta, porém na criptografia, mesmo que a mensagem seja interceptada, se o leitor não possuir a chave de decifração, não poderá lê-la.

Outra cifra famosa é a "Cifra de César", utilizada pelo imperador romano por volta de 50 a. C. Consiste em se substituir cada letra do alfabeto pela terceira letra subsequente. Tem grande semelhança com as cifras hebraicas citadas anteriormente. É também uma cifra de substituição simples, monoalfabética e monogâmica. Atualmente, cifras que seguem o mesmo método, por vezes são chamadas de "cifras de César". Suetônio, escritor romano, do início da era cristã, 69 d. C., narra em seu livro, "A vida dos Césares", detalhes das vidas dos imperadores, de Júlio César a Domiciano. Neste livro é narrado outro exemplo de uma cifra parecida utilizada pelos imperadores, a de Augusto, o qual trocava cada letra do alfabeto pela posterior. Sobre isso, Suetônio afirma em seu livro:

Sobre César:

"Se ele tinha qualquer coisa confidencial a dizer, ele escrevia cifrado, isto é, mudando a ordem das letras do alfabeto, para que nenhuma palavra pudesse ser compreendida. Se alguém deseja decifrar a mensagem e entender seu significado,

deve substituir a quarta letra do alfabeto, a saber 'D', por 'A', e assim por diante com as outras."

Sobre Augusto:

"Sempre que ele escrevia cifrado, escrevia B para A, C para B, e o resto das letras sob o mesmo princípio, usando AA para X."

Ao que parece, a cifra de César era suficientemente segura. Não existe relatos sobre tentativas de decifragem. Pelo que se sabe, as primeiras tentativas sistemáticas de criptoanálise surgem no século IX com Al-Kindi, desenvolvendo o que ficou conhecido como Análise de Frequência.

Podemos abordar o método de substituição através da Aritmética Modular. Ao identificarmos cada letra do alfabeto com um número inteiro específico, obteremos um conjunto numérico finito. Ao utilizarmos o algoritmo de substituição, cada letra é substituída por outra, sendo assim, cada número será substituído por outro. Porém, existe um número finito de letras em nosso alfabeto, o que acarreta um número finito de valores em nosso conjunto numérico. Desta forma, as últimas letras não poderiam ser substituídas. Por exemplo, a cifra de Augusto substitui cada letra pela letra imediatamente posterior. Desta forma, em nosso alfabeto de 26 letras, a letra z não poderia ser substituída, pois não existe letra posterior a esta em nosso alfabeto. Este empecilho ocorreria em qualquer alfabeto, tendo em vista que são finitos.

A solução é evidente. Aplicando a cifra de Augusto em nosso alfabeto e identificando cada letra com um número de 0 a 25, sendo $a = 00$, $b = 01$ e assim por diante até obtermos $z = 25$, podemos perceber que ao aplicar a cifra, a letra A não substitui nenhuma letra e por sua vez, a letra z não é substituída por nenhuma letra também. Logo, espera-se que a letra z deva ser substituída pela letra A, ou seja, o número 25 é substituído pelo número 00. Podemos perceber que desta forma obtemos um ciclo de substituição. Em cifras onde o valor para substituição é maior, como por exemplo na cifra de César, este aspecto é mais evidente. Note que podemos escolher $26!$, ou seja, 403.291.461.126.605.635.584.000.000 modos distintos de reescrevermos um alfabeto de 26 letras utilizando uma substituição simples monoalfabética e monográfica. Ao tratarmos de conjuntos numéricos em que os valores se alternam de forma cíclica, utilizamos a aritmética modular. Este processo é muito comum em nossa vida diária, basta perceber o modo de contagem das horas, dias, semanas e até meses do ano. Utilizando o mesmo raciocínio abaixo e em uma linguagem mais formal, poderemos visualizar a cifra de Augusto e a Cifra de César:

Primeiro identificar cada letra com um número correspondente:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	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

Figura 2: Alfabeto Original

$$A \rightarrow 00 \quad B \rightarrow 01 \quad C \rightarrow 02 \quad \dots \quad Z \rightarrow 25$$

Utilizando a cifra de Augusto, cada letra deve ser substituída pela subsequente:

$$\begin{aligned} a &\rightarrow B \Rightarrow 00 \rightarrow 01 \\ b &\rightarrow C \Rightarrow 01 \rightarrow 02 \\ &\vdots \\ z &\rightarrow A \Rightarrow 25 \rightarrow 00 \end{aligned}$$

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	00

Figura 3: Alfabeto Cifrado

De maneira mais ampla, sendo O o valor da letra na posição original e C o valor na posição cifrada, obtemos

$$C \equiv O + 1 \pmod{26} \text{ para } 0 \leq C \leq 25$$

Como C é um valor que deve representar a posição de uma letra no alfabeto, justifica-se que seja maior do que ou igual à 0 (a primeira posição) e menor do que ou igual à 25 (última posição). Note que ao analisarmos a cifragem da letra Z , obtemos o seguinte: $O = 25$ (posição original da letra Z), então, $C \equiv O + 1 \pmod{26}$, ou seja, $C \equiv 25 + 1 \pmod{26}$. Logo, $C \equiv 26 \equiv 0 \pmod{26}$, como $0 \leq C \leq 25$ implica $C = 0$, já que o único número positivo menor do que 26 que deixa resto zero quando dividido por 26 é o próprio zero.

Para cifra de César teremos procedimento análogo: $C \equiv O + 3 \pmod{26}$. Pois cada letra é substituída pela terceira letra subsequente. Desta forma, analisando novamente a letra Z obteremos, $O = 25$, daí, $C \equiv 25 + 3 \equiv 28 \equiv 2 \pmod{26}$. Como $0 \leq C \leq 25$, implica $C = 2$ já que $26 | C - (O + 3)$, ou seja, $26 | C - 2$, pela limitação de C temos que $C - 2 = 0$, ou seja, $C = 2$.

A	B	C	D	E	F	G	H	I	J	K	L	M
03	04	05	06	07	08	09	10	11	12	13	14	15
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
16	17	18	19	20	21	22	23	24	25	00	01	02

Figura 4: Alfabeto com a Cifra de César

$$a \rightarrow D \Rightarrow 00 \rightarrow 03$$

$$b \rightarrow E \Rightarrow 01 \rightarrow 04$$

$$\vdots$$

$$z \rightarrow C \Rightarrow 25 \rightarrow 02$$

A cifra de César, assim como as cifras que seguem um algoritmo de substituição simples semelhantes a esta, são classificadas como "transformações por substituição", onde temos:

$$C \equiv O + k \pmod{26}, 0 \leq C \leq 25$$

Sendo a congruência módulo 26 devido a quantidade de caracteres possíveis para substituição. O número K é um número inteiro maior do que ou igual a zero que representa a chave de encriptação. Como essa cifra é simétrica, a mesma chave é utilizada para a decifração, com a devida alteração no algoritmo. No caso da cifra de Augusto e de César, teremos respectivamente:

$$O \equiv C - 1 \pmod{26} \text{ e } O \equiv C - 3 \pmod{26}, 0 \leq O \leq 25$$

As cifras acima são casos particulares das chamadas "Transformações afins", dadas pela expressão mais geral:

$$C \equiv aO + b \pmod{m}, 0 \leq C \leq 25$$

para a e b inteiros, onde $\text{mdc}(a, m) = 1$. No caso das cifra anteriores temos $m = 26$, $a = 1$ e $b = 1$ no primeiro caso e $b = 3$ no segundo. Note que é necessário que $\text{mdc}(a, m) = 1$ para

que seja possível realizar a decifração da mensagem, em outras palavras, é necessário que a seja invertível módulo m , pois desta forma teremos:

$$\text{Se } C \equiv aO + b \pmod{m} \Rightarrow O \equiv a^{-1}(C - b) \pmod{m}$$

pois sendo a^{-1} o inverso de a módulo m e utilizando a Lei do cancelamento, obtemos:

$$C \equiv aO + b \pmod{m} \Rightarrow C - b \equiv aO \pmod{m} \Rightarrow a^{-1}(C - b) \equiv a^{-1}aO \equiv 1 \cdot O \equiv O \pmod{m}$$

Veja que sendo estas cifras simétricas, as chaves permanecem inalteradas, tanto para a encriptação quanto para decifração:

$$C \equiv O + 1 \pmod{26} \rightarrow O \equiv C - 1 \pmod{26} \text{ - chave: } 1$$

$$C \equiv O + 3 \pmod{26} \rightarrow O \equiv C - 3 \pmod{26} \text{ - chave: } 3$$

Note que b representa o número K nas transformações por substituição dadas anteriormente. Tal número, como já dito, representa a chave de encriptação/decifração. Veja que a quantidade de possíveis chaves depende diretamente da quantidade de caracteres de substituição que serão usados na mensagem. Para ser mais preciso, se tomarmos 0 como um valor a ser considerado, teremos $m - 1$ possíveis valores para b , ou seja, os possíveis restos da divisão euclidiana por m . Por outro lado, o número a , como já mencionado, deve ser invertível módulo m , ou seja, a deve ser relativamente primo com m , logo, temos $\varphi(m)$ possíveis valores para a . No caso de nosso alfabeto, com 26 letras, temos $\varphi(26) = 12$ valores para a e 26 valores para b , totalizando $12 \cdot 26 = 312$ transformações afins possíveis. Note que estas considerações aplicam-se também às cifras hebraicas consideradas anteriormente.

Já na Idade Média, existe um trabalho mais específico sobre Criptoanálise. Em seu livro, "*Risalah Istikhraj fi al-Mu'amma*" ("Manuscrito para decifrar mensagens criptográficas"), o matemático Al-Kindi em 800 d.C., descreve as primeiras técnicas de Criptoanálise, contendo também as primeiras descrições sobre a análise de frequência. De maneira grosseira, análise de frequência é o estudo que compara a frequência com que determinadas letras, palavras ou expressões, são usadas em um idioma com a frequência com que certos caracteres aparecem em um texto criptografado.

Como dito anteriormente, a criptografia sempre esteve atuante em guerras. Não foi diferente durante a primeira e segundas guerras mundiais. Na Primeira Guerra Mundial, a Sala 40 do Almirantado foi responsável por quebrar os códigos navais alemães desempenhando um papel importante em vários combates navais durante a guerra, particularmente na detecção de

grandes missões alemãs no Mar do Norte. Sua contribuição mais importante talvez tenha sido decodificar o Telegrama Zimmermann. O telegrama instruía o embaixador alemão no México a se aproximar do governo mexicano com a proposta de formar uma aliança militar contra os Estados Unidos. A proposta prometia ao México terras dos Estados Unidos caso o país aceitasse o acordo. O telegrama foi interceptado e decodificado por britânicos apressando a entrada dos Estados Unidos na guerra.

Já na Segunda Guerra Mundial o uso da Criptografia e da Criptoanálise foi mais intenso, sendo responsável por vitórias americanas contra o Japão, como por exemplo a batalha de Midway. Porém a atuação mais famosa seja talvez a quebra do Enigma, máquina eletro-mecânica de criptografia com rotores. Desenhada pelos alemães, utilizada tanto para criptografar como para decriptografar mensagens secretas, foi usada de várias formas na Europa a partir dos anos 1920. A sua fama vem de ter sido adaptada pela maior parte das forças militares alemãs a partir de 1930. A facilidade de uso e a suposta indecifrabilidade do código foram as principais razões para a sua popularidade. O código foi, no entanto, decifrado, e a informação contida nas mensagens que ele não protegeu é geralmente tida como responsável pelo fim da Segunda Guerra Mundial pelo menos um ano antes do que seria de se prever. Envolvendo matemáticos proeminentes da época, ambos os lados investiam na cifragem e decifragem de mensagens, sendo várias máquinas construídas e analisadas nessa época.



Figura 5: Máquina Enigma com três rotores.

Com o advento do computador na década de 60 e da internet, a criptografia emergiu da área militar para a sociedade, principalmente no que se refere a transações econômicas. Com o uso cada vez mais avançado da matemática e de computadores potentes, a criptologia deixou de ser apenas uma artimanha militar e passou a ser uma área profunda e fértil de estudo com vasta aplicação.

O surgimento da cifra RSA

A principal característica das cifras simétricas é que uma mesma chave é utilizada para cifrar e decifrar uma mensagem. Desta feita, é necessário que emissor e receptor tenham em mãos a chave para se comunicarem. Apesar da agilidade da encriptação e decríptação e razoável simplicidade dos métodos, percebe-se sua fragilidade, tendo em vista toda a logística necessária para que ambos tenham a chave e para que esta não caia em mãos erradas. Note que mais importante que se conhecer o algoritmo de encriptação/decriptação é ter em mãos a chave. Pode-se refletir o quão dificultoso seria a um banco manter seus clientes em posse das respectivas chaves de encriptação (que são as mesmas de decríptação) e ainda garantir a segurança e o sigilo das informações. Foram esta e outras dificuldades de mesma natureza que levaram matemáticos a procurar e desenvolver uma teoria que desse conta de produzir uma cifra que driblasse tais situações. Mais especificamente, era necessário que existisse um algoritmo no qual a chave que encriptasse não fosse a mesma que decríptasse e vice-versa. Esse é o princípio básico das cifras assimétricas. Ou seja, não se pensa em uma chave que "abre e fecha", mas uma chave que "só abre" e outra "que só fecha".

Essa ideia de uma cifra com duas chaves, como proposto acima, foi lançada em 1976 em um artigo escrito por Whitfield Diffie, Martin Hellman e Ralph Merkle. Além desta proposta de estudo, foi defendido também, ao longo do artigo, a desmilitarização da criptologia, ou seja, que se pudesse pesquisar e divulgar estudos científicos a respeito. Diffie, Hellman e Merkle, tiveram a ideia da cifra assimétrica, onde diferentemente dos códigos criados anteriormente, as chaves simétricas, saber codificar não implica em saber decodificar. Para desenvolver esta cifra, a ideia era encontrar uma função de mão única que, como o nome sugere, fosse irreversível. Diffie publicou um resumo de sua ideia em 1975, a partir daí, outros cientistas se uniram em busca de uma função de mão única que possibilitasse uma cifra assimétrica.

Porém, a ideia dos três não encontrou respaldo matemático por um bom tempo, já que não conseguiram obter tal função. Em 1977, Ronald Rivest, Adi Shamir e Leonard Adleman, professores do MIT, encontraram uma função capaz de colocar em prática a ideia do trio. A esperança de se obter tal função já estava quase esgotada quando Rivest direcionou suas

reflexões para os números primos. Ele lembrou-se que obter o produto de dois números primos é algo trivial, porém, se tivermos apenas o produto em mãos e quisermos obter os primos em questão, teremos um trabalho bem maior. Tal dificuldade aumenta a medida que o número inicial aumenta, pois fatorar números grandes é um trabalho que demanda muito processamento de dados. Desta forma, estava encontrado o caminho para a função proposta anos antes por Diffie, Helman e Markle. O trio de professores organizaram as idéias e trabalharam na formulação da cifra que inicialmente se chamaria ARS, o nome de cada integrante em ordem alfabética. Porém, Adleman, que a princípio não queria seu nome citado no trabalho, pediu para que seu nome fosse colocado em último lugar por julgar pequena sua participação no projeto. Até hoje, o RSA é o mais conhecido dos algoritmos de criptografia de chave pública, nome dado ao sistema de criptografia assimétrica, onde são usadas duas chaves distintas e uma delas é disponibilizada publicamente, uma vez que a chave utilizada para cifrar uma mensagem não é capaz de decifrar a mesma.

Rivest, Shamir e Adleman criaram um função especial que para utilidades práticas pode ser considerada unidirecional (ou de mão única). As funções unidirecionais autênticas produzem resultados que não podem ser revertidos para os valores iniciais. A função do RSA é tão complexa ou tão demorada de ser revertida que, para efeitos práticos, pode ser considerada como uma função de mão única. Isso se deve, principalmente, ao fato de que o algoritmo se apropria da dificuldade de se fatorar um número em fatores primos. Na prática ainda não existe um método eficiente e suficientemente rápido para se fazer isso.

Para se implementar o método é necessário que o destinatário escolha dois números primos p e q muito grandes, quanto maiores os números, maior será a segurança da cifra. A título de exemplo:

$$p = 19 \text{ e } q = 23$$

Agora toma-se o número n , tal que $n = pq$:

$$n = pq = 437$$

Agora tomamos o número e , de sorte que e não tenha fatores comuns com o produto $(p-1)(q-1)$, ou seja,

$$\text{mdc}(e, \varphi(n)) = \text{mdc}(e, [(p-1)(q-1)]) = 1, \text{ sendo } \varphi(n) = (p-1)(q-1)$$

Em nosso exemplo teremos,

$$(19-1)(23-1) = 18 \cdot 22 = 396$$

$$\text{mdc}(e, 396) = 1$$

basta escolher o número e de sorte que ele não tenha fatores primos em comum com $(p-1)(q-1)$, é claro que 13 satisfaz esta condição. Desta feita possuímos dois números, a saber, $n = 437$ e $e = 13$, ambos chamados de **chave pública**.

Como $\text{mdc}(e, \varphi(n)) = 1$, sabemos que e é invertível módulo n , seja d o inverso de e módulo n , necessariamente então $e \cdot d \equiv 1 \pmod{\varphi(n)}$. Em nosso exemplo temos,

$$e = 13 \text{ e } \varphi(n) = 396 \text{ com } \text{mdc}(13, 396) = 1$$

basta encontrarmos d , ou seja, o inverso de 13 módulo 396. Para isso é suficiente notar que a condição $e \cdot d \equiv 1 \pmod{396}$ e $\text{mdc}(13, 396) = 1$ nos dá que,

$$13 \cdot d \equiv 1 \pmod{396} \Rightarrow 13d = 396l + 1$$

para algum inteiro l . Logo,

$$d = \frac{396}{13}l + \frac{1}{13} = 30l + \frac{6}{13}l + \frac{1}{13} = \frac{6l+1}{13} + 30l$$

Lembre-se que $\frac{6l+1}{13}$ deve ser um número inteiro com $1 \leq d < 396$. Sendo assim $6l+1$ deve ser múltiplo de 13, podemos tomar $l = 2$, o que implica que

$$d = \frac{6 \cdot 2 + 1}{13} + 30 \cdot 2 = 1 + 60 = 61$$

O número d e o número n são chamados de **chave privada** que decifram a mensagem e que devem ser mantidas em segredo. De maneira geral:

p e q primos, sendo $n = p \cdot q \Rightarrow \varphi(n) = (p-1)(q-1)$;

escolhe-se e de tal sorte que $\text{mdc}(e, \varphi(n)) = 1$, n e e são as chaves públicas;

Encontra-se d , o inverso multiplicativo de e módulo n ; n e d são as chaves privadas.

Com este método é possível garantir o sigilo de uma mensagem enviada mantendo-se a chave privada em sigilo. Veja que o destinatário possui a chave privada que decifra a mensagem, por fim o remetente possui a chave pública que cifra a mensagem. Mesmo que esta venha a cair em mão erradas e que tais possuam a chave pública, esta não será de grande valia já que seu valor se relaciona com o valor da chave privada por meio da fatoração do número n nos primos p e q , que como já dito anteriormente, são difíceis de se obter. Veja que a escolha destes primos é de suma importância para o grau de confiabilidade do método. Note que ao inverter as chaves, ou seja, torna-se público o número d (que era a chave privada antes) e se mantém guardado o número e (a chave pública antes), a eficiência do método se mantém.

Por fim, é possível também utilizar este método como uma assinatura digital, ou seja, uma forma de garantir que a mensagem recebida é de fato da pessoa que se espera. Para isso é suficiente inverter as chaves, ou seja, passa-se para o remetente a chave privada e o destinatário permanece com a chave pública. Desta forma, o destinatário possui a chave que decifra a mensagem, que é pública, e o remetente a chave que cifra, que é privada. Sendo assim, caso o remetente envie uma mensagem cifrada para o destinatário, qualquer um que possua a chave pública, que decifra a mensagem, poderá lê-la, porém, o remetente não poderá negar que enviou a mensagem, pois só ele possui a chave de cifragem. Note que o importante aqui não é o sigilo da mensagem, mas sim a garantia de se saber quem é o remetente.

Parte II

Trabalho de Conclusão de Curso B

Resumo

Esta parte do trabalho visa contribuir para um maior aprofundamento nas teorias matemáticas necessárias para o desenvolvimento da criptografia RSA. Abordaremos mais detidamente e conceitualmente os elementos mais básicos subjacentes a esta cifra. Procuraremos abordar também, ainda que superficialmente, as implicações da aplicação desta cifra. Bem como possíveis métodos de criptoanálise.

A cifra RSA

Cifras simétricas e assimétricas

Com o aumento da troca de informações, cresce a necessidade de se garantir o sigilo no envio das mensagens. Geralmente informações importantes, tais como senhas de contas de bancos, informações pessoais, ou qualquer tipo de mensagens que as pessoas não gostariam de divulgar publicamente. Porém, tais mensagens são trocadas por canais públicos, ou seja, são ambientes onde outras pessoas não autorizadas podem ter contato com tais informações.

As cifras que vimos anteriormente são formas antigas de se proteger informações, historicamente ligadas a guerras ou conflitos de interesses entre nações. Com a modernização dos meios de comunicação e do desenvolvimento da ciência, tornou-se necessária uma sofisticação e modernização nos mecanismos de proteção de mensagens, ou seja, na criptografia como um todo. Vimos que um grande marco neste desenvolvimento foi a publicação do artigo de W. Diffie e M. Hellman de 1976, onde foi apresentado um sistema de criptografia de chave pública, ou seja, um tipo de cifra assimétrica.

Como já dito anteriormente, existe uma importante divisão no conceito de cifras em Criptografia. Existem as cifras simétricas e as assimétricas. A principal característica das cifras simétricas é que ambos os interlocutores podem decifrar as mensagens um do outro. Ou seja, as chaves de cifragem e decifragem são compartilhadas, sendo idênticas. Já no caso da cifra assimétrica, cada fonte de comunicação possui sua chave privada de decifração e encriptação. No caso de uma cifra assimétrica pública, que é o caso da cifra RSA, não é necessário o compartilhamento seguro de chaves, pois cada fonte possui uma chave específica para decifrar a mensagem recebida e distribui publicamente (daí o nome) uma chave para encriptar a mensagem. A chave de encriptação é enviada a outra fonte, com quem se deseja comunicar. Não é necessário garantir a segurança desta chave, nem mesmo do algoritmo pois todo o segredo se mantém na chave privada, uma vez que é quase impossível obter-se a chave privada a partir da pública. Vale lembrar que este método foi realmente revolucionário para a segurança nas trocas de informações.

A cifra RSA, sendo a mais famosa cifra de chave pública (assimétrica), se desenvolve sobre relações matemáticas razoavelmente simples. O interessante deste método é que não é necessário se proteger o algoritmo nem a chave de encriptação, por isso mesmo é chamado de "sistema de chave pública". Mas a beleza desta cifra é que o ponto principal de toda a sua construção reside exatamente naquilo que ainda não conseguimos fazer. Em outras palavras, o ponto central da cifra RSA está em se fatorar um número qualquer em seus fatores primos, algo que, a depender deste número, ainda não existe um método razoavelmente prático de se fazer.

Apesar de ser um método muito sofisticado e de se apoiar em conceitos matemáticos relativamente simples, este processo ainda é extremamente trabalhoso e demorado, exigindo um alto custo computacional. Por isso, é mais comum que se utilizem métodos mais simples, ou seja, cifras simétricas, para a proteção das mensagens e se utilize a cifra assimétrica para a proteção das chaves que serão compartilhadas. Levando em conta que estas chaves são números com poucos algarismos, o processo de se criptografar estes números é mais rápido do que se utilizar a cifra para toda a mensagem.

Precisamos agora entender mais formalmente as relações construídas dentro da Criptografia. Imagine que uma fonte A queira enviar uma mensagem x para uma fonte B . Para isso A usa um método de encifração E e uma chave de encifração e encifra a mensagem x , obtendo a mensagem encifrada y . Ou seja, $E(x) = y$, E funciona como uma função que associa x (mensagem original) a sua imagem y (mensagem encifrada). A envia y para B que utiliza um método de decifração D e uma chave de decifração, conhecida por ambos. Daí temos $D(y) = x$, podemos dizer então que D é a função inversa de E , pois essa associa y (mensagem encifrada) a x (mensagem original). Note que a função E deve ser bijetora, afim de que possamos obter sua inversa D . Podemos reunir todo o processo na seguinte relação:

$$x := D(y) = D[E(x)] = x$$

Se recuperarmos o exemplo da cifra de César, teremos o seguinte:

$$E := C \equiv T + 3 \pmod{26}$$

Que representa o processo de encifração. Por outro lado, o processo de decifração D é exatamente o processo oposto ao anterior:

$$D := T \equiv C - 3 \pmod{26}$$

Vemos então que aplicando ao texto T o processo E obtemos o texto cifrado C . A fonte B ,

por sua vez, ao receber o texto C da fonte A , aplica o processo D em C e obtém novamente o texto original T . Desta forma, defini-se um **cripto** como a dupla (E, D) , ou seja, a função de encifração e sua inversa.

Definição 1.1: Um **sistema de cifras** ou um sistema de **criptos** é um conjunto (finito) de criptos.

Um sistema de criptos é um método de tornar a comunicação secreta entre um grupo de fontes em um meio público, reunindo as várias funções de encifração e suas respectivas inversas. Este meio público é um ambiente onde pessoas que não estão no grupo cripto, que é o grupo de fontes que utilizam os criptos, possam obter as informações trocadas. Exemplos de um meio público são os *e-mails*, as transmissões de rádio ou o correio. Nestes ambientes, cada fonte utiliza um cripto para se comunicar com outra fonte. Note que é necessário que cada fonte utilize determinado cripto para se comunicar com outra, uma vez que nem sempre todas as fontes se comunicarão entre si. Ou seja, uma fonte envia uma mensagem para outra específica e não deseja que as demais tenham acesso a esta mensagem. Como nas transações bancárias. Algumas informações são compartilhadas entre as fontes/clientes, como número de conta e nomes, porém algumas informações são sigilosas entre cada fonte/cliente e o Banco.

Passemos agora a abordar alguns conceitos da Teoria de Números como preparação para a explicitação do algoritmo da cifra RSA. Tais conceitos envolvem a Aritmética Modular e Números Primos. Muitos deles já foram abordados na primeira parte do trabalho e serão revisitados agora.

Uma vez que já enunciamos o Algoritmo da Divisão de Euclides e definimos Congruência Modular, vamos iniciar nossos estudos analisando como se constrói o conjunto de classes de equivalência módulo m , sendo m um inteiro positivo qualquer.

Primeiro considere um conjunto J , tal conjunto será formado por todos os múltiplos de m . Sendo assim,

$$J = m \cdot \mathbb{Z}, m \in \mathbb{Z}_+$$

Dessa forma, sendo a e b dois inteiros, podemos definir a congruência módulo m da seguinte maneira,

$$a \equiv b \pmod{m} \Leftrightarrow a - b \in J$$

Ora, veja que o conjunto J é formado por todos os múltiplos de m , assim se $a \equiv b \pmod{m}$ então $m|a - b$, ou seja, $a - b \in J$. Por outro lado, se $a - b \in J$ então $m|a - b$, logo $a \equiv b \pmod{m}$.

Usaremos o símbolo (\mathbb{Z}/J) ou $(\mathbb{Z}/m\mathbb{Z})$ para representar o conjunto das classes de equiva-

lência módulo m .

Considere o seguinte, dado um inteiro positivo m , tomamos todos os possíveis restos da divisão por m , ou seja, $0, 1, \dots, m-1$. Agora, dividimos o conjunto dos números inteiros em m subconjuntos, sendo cada um desses subconjuntos formado especificamente pelos inteiros que quando divididos por m dão resto $0, 1, \dots, m-1$. Por exemplo, seja $m = 4$, temos que os possíveis restos da divisão por 4 são $0, 1, 2, 3$. Sendo assim, dividindo o conjunto \mathbb{Z} como dito anteriormente, temos o seguinte,

$$\bar{0} = \{\dots, -4, 0, 4, 8, \dots\}$$

$$\bar{1} = \{\dots, -9, -5, 5, 9, \dots\}$$

$$\bar{2} = \{\dots, -6, -2, 2, 6, \dots\}$$

$$\bar{3} = \{\dots, -7, -3, 3, 7, \dots\}$$

Essa barra sobre os números representa que não estamos falando especificamente do número mas sim da classe de equivalência que ele representa, em outras palavras, o subconjunto dos inteiros formado pelos números que dão esse resto quando divididos por m . Resumindo,

$$(\mathbb{Z}/m\mathbb{Z}) = \{\bar{0}, \dots, \overline{m-1}\}$$

O próximo teorema garante que para qualquer inteiro a , sempre existe um "representante" x de a em $(\mathbb{Z}/m\mathbb{Z})$. Ou seja, todos os inteiros devem pertencer a uma classe de equivalência.

Teorema 1.1: Para um dado inteiro positivo a e um inteiro positivo m , existe um único inteiro x , com $0 \leq x < m$ tal que

$$a \equiv x \pmod{m}$$

Pelo teorema da divisão de Euclides é óbvio que x é o resto da divisão de a por m .

Com isso podemos ter certeza de que fixado um inteiro positivo m podemos trabalhar com todo o conjunto dos inteiros.

Uma vez que temos bem entendido o conjunto $(\mathbb{Z}/m\mathbb{Z})$, passamos agora a verificar como se dão as operações aritméticas nesse conjunto.

Sendo $a(\bmod m)$ e $b(\bmod m)$, ou simplesmente \bar{a} e \bar{b} duas classes de equivalência, definimos a soma e produto módulo m da seguinte maneira,

$$a(\bmod m) + b(\bmod m) := a + b(\bmod m)$$

$$a(\bmod m) \cdot b(\bmod m) := a \cdot b(\bmod m)$$

Onde o lado esquerdo representa a soma e o produto em \mathbb{Z} e o lado direito representa as classes de equivalência $a + b$ e $a \cdot b$. Por exemplo, se $a = 3$, $b = 5$ e $m = 9$, teremos o seguinte,

$$3(\bmod 9) + 5(\bmod 9) = 8(\bmod 9)$$

$$3(\bmod 9) \cdot 5(\bmod 9) = 6(\bmod 9)$$

Note que $3 \cdot 5 = 15$, sendo que 15 deixa resto 6 quando dividido por 9, ou seja, $15 \equiv 6 \pmod{9}$. Por isso, $6(\bmod 9)$ é a classe que representa o produto $3(\bmod 9) \cdot 5(\bmod 9)$. É fácil perceber que as classes $0(\bmod m)$ e $1(\bmod m)$ são respectivamente os elementos neutros da adição e da multiplicação em $(\mathbb{Z}/m\mathbb{Z})$.

Falta definirmos a divisão, para isso iremos utilizar a ideia da inversão. Lembre-se que para quaisquer inteiros a e b com $b \neq 0$ temos que, $a \div b = a \cdot \frac{1}{b}$. Da mesma forma, sendo $a(\bmod m)$ e $b(\bmod m)$ classes quaisquer. Se existir uma classe $d(\bmod m) \in (\mathbb{Z}/m\mathbb{Z})$ tal que

$$b(\bmod m) \cdot d(\bmod m) = 1(\bmod m)$$

dizemos que $b(\bmod m)$ é invertível e sua inversa é a classe $d(\bmod m)$. Dessa forma podemos dizer que,

$$a(\bmod m) \div b(\bmod m) = a(\bmod m) \cdot d(\bmod m)$$

Porém nem todas as classes são invertíveis, essa propriedade depende dos números a , b e m em questão. Para entendermos melhor como isso se dá, será oportuno lembrarmos o conceito de *mdc* e algumas relações importantes. Vimos anteriormente o que vem a ser o *máximo divisor comum* entre dois inteiros, e que esse divisor pode ser expresso por uma combinação linear entre os dois números iniciais. Com isso em mente podemos analisar a seguinte proposição.

Proposição 1.1: Sejam $a, b, c \in \mathbb{Z}$. Então existem inteiro x, y tal que

$$ax + by = c$$

se, e somente se $mdc(a, b) | c$.

Essa proposição, cuja demonstração pode ser encontrada no livro de Shokranian [8], nos será útil para o próximo resultado, que é exatamente o que procuramos para respondermos quais classes de equivalência terão inversas.

Proposição 1.2: Seja $b \neq 0$ um número inteiro. Então a classe de equivalência $b(\bmod m)$ tem inversa se e somente se $\text{mdc}(b, m) = 1$

Demonstração: Primeiro suponhamos que a classe $b(\bmod m)$ tenha inversa, e que sua inversa seja a classe $d(\bmod m)$. Então,

$$bd(\bmod m) = 1(\bmod m)$$

Daí resulta que,

$$bd - 1 \equiv 0(\bmod m)$$

Logo, $bd - 1 = ym$ para algum inteiro y . Portanto, $bd - ym = 1$. Isso pode ser escrito na forma $bd + (-y)m = 1$. Então, pela proposição anterior temos o $\text{mdc}(b, m) = 1$. Agora, suponhamos que o $\text{mdc}(b, m) = 1$, e dessa forma provaremos que a classe $b(\bmod m)$ tem inversa. Para fazer isso, novamente, usaremos a proposição anterior que garante, sob a condição $\text{mdc}(b, m) = 1$, que a equação $bx + my = 1$ tem solução. Portanto, existem números inteiros $x = x_0$ e $y = y_0$ tal que

$$bx_0 + my_0 = 1$$

Essa equação pode ser escrita assim,

$$bx_0 - 1 \equiv 0(\bmod m).$$

E essa congruência pode ser escrita dessa forma

$$bx_0 = 1(\bmod m).$$

Daí, a classe $x_0(\bmod m)$ é a inversa da classe $b(\bmod m)$ e a demonstração fica completa.

Existe um resultado que garante que uma vez que o mdc entre dois números, como b e m , pode ser expresso como uma combinação linear, ou seja, $bx + my = d$, com $x, y \in \mathbb{Z}$ e $d = \text{mdc}(b, m)$ têm-se que qualquer outra combinação linear de inteiros que se possa formar com b e m terá como resultado um múltiplo de d . Dessa forma, sendo $\text{mdc}(b, m) = d = 1$ temos a liberdade de escrever qualquer inteiro como combinação de b e m . Como estamos interessados na aritmética modular, qualquer múltiplo de m será congruente a 0 . Podemos assim proceder como na última parte da demonstração, tomando uma combinação linear que seja igual a 1 , obtendo assim o inverso multiplicativo de b , ou seja, a classe inversa da classe \bar{b} . Para clarear as ideias, vejamos um exemplo.

Seja $m = 9$, dessa forma,

$$(\mathbb{Z}/m\mathbb{Z}) = (\mathbb{Z}/9\mathbb{Z}) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}\}.$$

Vejam agora o mdc desses números com 9 para descobrirmos quais dessas classes são invertíveis. Dando $\text{mdc}(a, b) = (a, b)$ temos o seguinte,

$(0, 9) = 9$, $(1, 9) = 1$, $(2, 9) = 1$, $(3, 9) = 3$, $(4, 9) = 1$, $(5, 9) = 1$, $(6, 9) = 3$, $(7, 9) = 1$ e $(8, 9) = 1$.

Podemos concluir, pelo resultado anterior, que as únicas classes que não possuem inversa são $\bar{0}$, $\bar{3}$ e $\bar{6}$. sendo assim,

CLASSE	0	1	2	3	4	5	6	7	8
INVERSA	-	1	5	-	7	2	-	4	8

Esses resultados aparentemente desconexos do nosso propósito, nos serão muito úteis mais a frente, quando oportunamente serão lembrados. Por ora, pode-se perceber a importância de se obter classes de equivalência invertíveis lembrando o que foi dito anteriormente sobre as cifras simétricas. Lembre-se de que mensagens encriptadas por cifras do tipo $C \equiv aT + b \pmod{m}$, ditas "Transformações afins", só podem ser decriptadas caso o número a seja invertível módulo m . O princípio aqui é exatamente o mesmo, a diferença é que ainda necessitamos de mais alguns resultados para podermos construir a cifra RSA.

Agora que já conhecemos o conjunto e as operações que podemos realizar com seus elementos, podemos passar a estudar como resolver equações.

Uma equação afim ou equação de congruência de grau 1 de uma variável é uma equação do tipo

$$ax \equiv b \pmod{m}$$

onde a , b e x são inteiros sendo x é a incógnita e a e b os coeficientes. A próxima proposição, estabelece um resultado muito semelhante a um que já vimos (Proposição 1.1). Na verdade, esse resultado é um caso particular do anterior.

Proposição 1.3: A equação afim $ax \equiv b \pmod{m}$ tem solução se e somente se o $\text{mdc}(a, m) | b$

Demonstração: Primeiro suponhamos que a equação tenha solução e provemos que $\text{mdc}(a, m) | b$. Então existe um inteiro x_0 tal que $ax_0 \equiv b \pmod{m}$. Essa congruência pode

ser escrita como,

$$ax_0 - b = -ym$$

$$ax_0 + ym = b.$$

Pela proposição 1.1 temos que $\text{mdc}(a, m) | b$. Agora suponhamos que $\text{mdc}(a, m) | b$. Vamos provar que a equação afim tem solução. Mas a congruência $ax \equiv b \pmod{m}$ pode ser escrita da seguinte forma

$$ax + (-y)m = b$$

Dado que $\text{mdc}(a, m) | b$, necessariamente a equação tem solução. Assim a demonstração está completa.

Observe que a proposição 1.1 garante que a combinação linear entre dois números a e b com resultado c tem solução se $\text{mdc}(a, b) | c$, ou seja,

$$ax + by = c, \quad x \text{ e } y \in \mathbb{Z}$$

Note que ao garantirmos que a equação afim tem solução, basta agora encontrarmos o inverso de a , ou seja, a^{-1} . Porém nem sempre esse inverso existe. Lembre-se que é necessário que $\text{mdc}(a, m) = 1$. No caso em que o inverso existe, temos,

$$ax \equiv b \pmod{m} \Rightarrow a^{-1}ax \equiv ba^{-1} \pmod{m}$$

$$x \equiv ba^{-1} \pmod{m}$$

Uma vez que $a^{-1}a = 1$.

Proposição 1.4: O número das soluções da equação afim $ax \equiv b \pmod{m}$ é igual a $\text{mdc}(a, m)$.

Estamos considerando que a equação afim $ax \equiv b \pmod{m}$ tenha solução. Dessa forma, sabemos que existe um inteiro $x_0 \in (\mathbb{Z}/m\mathbb{Z})$ que multiplicado por a dá resultado b . Como pela proposição 1.3 esse x_0 existe, podemos calculá-lo assim,

$$b \equiv ax \pmod{m} \Rightarrow b = qm + ax, \quad q \in \mathbb{Z}$$

Veja que ax é o resto da divisão de b por m , ou seja, procuramos os restos da divisão de b por m que sejam múltiplos de a . Sendo $\text{mdc}(b, m) > 1$ sabemos que existe mais de uma solução para a equação, dado que o mdc de dois inteiros é sempre um inteiro não negativo. Seja então x_0 a primeira solução, ou seja, o menor número cujo resto da divisão de b por m

é múltiplo de a . Dessa forma,

$$b \equiv ax_0 \pmod{m}$$

Uma vez que encontramos o primeiro múltiplo de a é resto de b quando este é dividido por m , passamos a procurar as demais soluções. Mas o processo é simples, uma vez que já sabemos por onde começar, ou seja por x_0 . As próximas soluções devem ser múltiplas de a e pertencerem a $(\mathbb{Z}/m\mathbb{Z})$. Em outras palavras, para $w \in \mathbb{Z}$,

$$x_1 = a + x_0$$

$$x_{i+1} = a + x_i, \quad i = 0, 1, \dots$$

É óbvio que por se tratar de um conjunto finito, ou seja, os possíveis restos da divisão de b por m , ao repetirmos o processo indefinidamente estaremos obtendo as mesmas soluções repetidas vezes.

Denotaremos por $(\mathbb{Z}/m\mathbb{Z})^*$ o conjunto das classes de equivalência representadas por números que são co-primos com m . Lembre-se que um número x é co-primo com m se $\text{mdc}(x, m) = 1$. Em outras palavras,

$$(\mathbb{Z}/m\mathbb{Z})^* = \{x \in (\mathbb{Z}/m\mathbb{Z}) \mid \text{mdc}(x, m) = 1\}$$

O teorema a seguir nos mostra qual é e como calcular o número de elementos do conjunto $(\mathbb{Z}/m\mathbb{Z})^*$

Teorema 1.2: O número de elementos do conjunto $(\mathbb{Z}/m\mathbb{Z})^*$ é dado pela função φ de Euler, e esse número é igual a

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right),$$

na qual os números p representam os divisores primos de m contados sem repetição.

Façamos um exemplo para termos uma melhor compreensão do funcionamento dessa função. Para isso tomemos $m = 26$, o que nos dá dois fatores primos, $p_1 = 2$ e $p_2 = 13$. Para

calcular, basta substituir os respectivos valores e multiplicá-los,

$$\begin{aligned}
 \varphi(26) &= 26 \prod_{p|26} \left(1 - \frac{1}{p}\right) \\
 &= 26 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{13}\right) \\
 &= 26 \cdot \frac{1}{2} \cdot \frac{12}{13} \\
 &= 12
 \end{aligned}$$

temos assim 12 números invertíveis módulo 26.

É importante não perdermos de vista nosso foco, qual seja, o de criarmos as condições necessárias para a obtenção da cifra RSA. Como tal, é importante sabermos decifrar a mensagem. Para isso, como já dito anteriormente, é necessário trabalharmos com números invertíveis. Desta feita, vimos também que o processo para a obtenção das soluções de uma equação afim é demasiado simples quando a e m são co-primos, pois assim garantimos que a possua inverso multiplicativo módulo m .

O próximo teorema, assim como a proposição 1.1, garante que todos os números possuem representantes em $(\mathbb{Z}/m\mathbb{Z})$. Porém, agora o teorema garante que esse representante será co-primo com m caso o número inicial também o seja. O que é muito útil, pois podemos tomar qualquer número com a condição de que seja co-primo com m que garantimos que essa propriedade não se perderá ao tomarmos o resto da divisão desse número por m .

Teorema 1.3: Para qualquer número inteiro positivo n com $n > m$ e co-primo com m , isso é $\text{mdc}(n, m) = 1$, existe um elemento $x \in (\mathbb{Z}/m\mathbb{Z})^*$ tal que $\text{mdc}(x, m) = 1$ e $n \equiv x \pmod{m}$.

Demonstração: Os possíveis restos da divisão de n por m são os elementos de $(\mathbb{Z}/m\mathbb{Z})$, logo, $n = mq + x$, em que $q \in \mathbb{Z}$ e $x \in (\mathbb{Z}/m\mathbb{Z})$. Se o $\text{mdc}(x, m) \neq 1$, temos o $\text{mdc}(n, m) \neq 1$, que é uma contradição, portanto o $\text{mdc}(x, m) = 1$ e $n \equiv x \pmod{m}$. Isso completa a demonstração.

Agora que já possuímos algum conhecimento sobre equações modulares de grau um, vamos direcionar nossos estudos para algumas relações que envolvem potências e congruências, particularmente entre números co-primos. Esse estudo será fundamental para a construção da cifra RSA. A título de recapitulação, vamos enunciar o Pequeno Teorema de Fermat, já enunciado e demonstrado na Parte 1 desse trabalho.

Teorema 1.4 (Teorema de Fermat): Seja p um número primo. Se p não divide a , então $a^{p-1} \equiv 1 \pmod{p}$.

Esse teorema é um caso particular do Teorema de Euler, que segue abaixo.

Teorema 1.5 (Teorema de Euler): Sejam a , m inteiros com $m > 0$ tal que $\text{mdc}(a, m) = 1$. Então

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

Para ver como o pequeno Teorema de Fermat (Teorema 1.4) é uma consequência do Teorema de Euler basta supor que $m = p$. Nesse caso as condições do Teorema 1.4 estão satisfeitas. Por outro lado, temos $\varphi(p) = p - 1$, portanto o Teorema de Euler nos fornece

$$a^{p-1} \equiv 1 \pmod{p}.$$

Que é exatamente a afirmação do teorema de Fermat. A seguir reproduzimos uma demonstração para o teorema de Euler.

Demonstração: Sejam $r_1, r_2, \dots, r_{\varphi(m)}$ os elementos de $(\mathbb{Z}/m\mathbb{Z})^*$. Nesse conjunto estão presentes os elementos 1 e $m - 1$, chamaremos $r_1 = 1$ e $r_{\varphi(m)} = m - 1$. Agora considere o conjunto $J = ar_1, ar_2, \dots, ar_{\varphi(m)}$.

É fácil mostrar que os elementos de J são incongruentes, módulo m dois a dois. Agora, de acordo com o Teorema 1.3 temos que

$$\begin{aligned} ar_1 &\equiv r_i \pmod{m} \\ ar_2 &\equiv r_j \pmod{m} \\ &\dots \equiv \dots \\ &\dots \equiv \dots \\ ar_{\varphi(m)} &\equiv r_k \pmod{m} \end{aligned}$$

em que r_i, r_j, \dots, r_k são elementos de $(\mathbb{Z}/m\mathbb{Z})^*$. Fazendo o produto dos dois lados dessas congruências, chegamos ao seguinte teorema:

$$a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}.$$

O fato de que todos os elementos $r_1, r_2, \dots, r_{\varphi(m)}$ são co-primos com m implica o produto $r_1 r_2 \cdots r_{\varphi(m)}$ que também é co-primo com m , logo, pela lei do cancelamento, após o cancelamento de $r_1 r_2 \cdots r_{\varphi(m)}$ dos dois lados dessa última congruência, ficamos com $a^{\varphi(m)} \equiv 1 \pmod{m}$. A demonstração está completa.

A principal razão de estudarmos esse teorema nesse contexto em que estamos é que por esse resultado podemos determinar se um número não é primo. Veja, tomemos $m = 51$. Vamos usar o teorema anterior para mostrar que m não é primo. Primeiro tomamos um

número que seja co-primo com 51, lembre-se de que essa é a primeira hipótese do teorema. Como 51 é ímpar, basta tomar $a = 2$. Se 51 for primo, então, pelo teorema tiramos que,

$$\varphi(m) = m - 1 \Rightarrow \varphi(51) = 51 - 1 = 50.$$

Assim,

$$a^{m-1} \equiv 1 \pmod{m} \Rightarrow 2^{50} \equiv 1 \pmod{m}$$

porém, $2^{50} = 1.125.899.906.842.624$, daí,

$$2^{50} - 1 = 1.125.899.906.842.623$$

que não é divisível por 51, logo $m = 51$ não pode ser primo.

Os próximos corolário e teorema serão os últimos que precisaremos para finalmente enunciarmos a cifra RSA..

Corolário 1.1: Sejam p e q dois números primos distintos. Seja $m = pq$. Suponhamos que exista um inteiro r tal que

$$r \equiv 1 \pmod{(p-1)} \text{ e } r \equiv 1 \pmod{(q-1)}$$

Então, para todo número inteiro a teremos

$$a^r \equiv a \pmod{m}.$$

Demonstração: Existem dois casos a considerar. Primeiro, p não divide a . Então

$$a^r = a^{k(p-1)+1} = (a^{p-1})^k(a) \equiv 1^k a \equiv a \pmod{p}.$$

Segundo, $p|a$. Nesse caso $a \equiv 0 \equiv a^r \pmod{p}$. Isso é exatamente $a^r \equiv a \pmod{p}$. Portanto, nos dois casos obtemos,

$$a^r \equiv a \pmod{p}$$

Similarmente podemos provar que

$$a^r \equiv a \pmod{q}$$

Daí

$$a^r \equiv a \pmod{m}$$

pois $p|(a^r - a)$ e $q|(a^r - a)$ então $m = pq|(a^r - a)$. Isso completa a demonstração.

O teorema a seguir foi enunciado na primeira parte desse trabalho, porém não foi demonstrado. O enunciaremos novamente e apresentaremos uma demonstração.

Teorema 1.6: Sejam p e q dois números primos distintos e $a \in \mathbb{Z}$ tal que

$$a \not\equiv 0 \pmod{p}, \quad a \not\equiv 0 \pmod{q}$$

Então,

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$

Demonstração: Pelo pequeno teorema de Fermat temos $a^{p-1} \equiv 1 \pmod{p}$. Então, tomando $(q-1)$ -ésima potência nos dois lados dessa congruência teremos

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

Isso implica

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

Da mesma forma, dessa vez usando o pequeno Teorema de Fermat, $a^{q-1} \equiv 1 \pmod{q}$ podemos ver que

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

Portanto, p e q dividem $a^{(p-1)(q-1)} - 1$, logo

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$

A demonstração está completa.

Mostraremos agora a cifra **RSA** formalmente. O seguinte teorema mostrará o que é o sistema **RSA**, como estão definidas as cifras e como podemos decifrá-las.

Teorema 1.7 (cifra RSA): Suponhamos que:

- 1) p e q são números primos distintos;
- 2) $e \in \mathbb{Z}$ é um número tal que $\text{mdc}(e, (p-1)(q-1)) = 1$;
- 3) $T \in \mathbb{Z}$ é um inteiro tal que $T \not\equiv 0 \pmod{p}$ e $T \not\equiv 0 \pmod{q}$;
- 4) $C \in \mathbb{Z}$ é um inteiro definido por $C \equiv T^e \pmod{pq}$;

5) $d \in \mathbb{Z}$ é um inteiro definido pelas duas condições

$$ed \equiv 1 \pmod{(p-1)(q-1)}, \quad 1 \leq d < (p-1)(q-1).$$

Então

$$T \equiv C^d \pmod{pq}.$$

Demonstração: Pela condição (4) temos que

$$C^d \equiv (T^e)^d \pmod{pq}.$$

Isso nos diz que

$$C^d \equiv T^{ed} \pmod{pq}.$$

Mas, $ed \equiv 1 \pmod{(p-1)(q-1)}$. Portanto,

$$ed \equiv l(p-1)(q-1) + 1,$$

para algum inteiro $l \in \mathbb{Z}$ (na verdade $l \in \mathbb{N}$, pois $e, d \in \mathbb{N}$). Então

$$C^d \equiv T^{ed} \equiv T^{l(p-1)(q-1)+1} \pmod{pq}.$$

Pelo Teorema 1.6 temos

$$T^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

Logo,

$$C^d \equiv T^{l(p-1)(q-1)+1} \equiv (T^{(p-1)(q-1)})^l \times T \equiv 1^l \times T \equiv T \pmod{pq}.$$

Pode ser representado também da seguinte forma

$$T \equiv C^d \pmod{pq}.$$

A demonstração está completa.

Veja que apesar de o sistema se apoiar sobre conceitos razoavelmente simples, ele necessita de certas relações que só podemos compreender tendo considerado os resultados anteriores.

Implementação RSA

A seguir mostraremos como usar o teorema precedente e implementar o sistema de criptografia **RSA**. Observe que nesse sistema a questão também é como escrever cifras e decifrá-las. Nas discussões a seguir T denota o texto da mensagem, está escrito em números (usando o que chamamos de alfabeto digital) e C as cifras, usadas para encriptar a mensagem.

Definição 1.3: Chamaremos o número $n = pq$ de **módulo**, o número e de **potência de encifração**, d de **potência de decifração** e a tripla (n, e, d) de **chave do sistema RSA**.

Definição 1.4: O par (n, e) é a **chave pública do sistema RSA** e o par (n, d) é a **chave privada do sistema RSA**.

A comunicação entre as fontes A e B está baseada no uso das chaves pública e privada. A chave pública (n, e) da fonte A deve ser conhecida por B e a chave pública (n', e') da fonte B deve ser conhecida por A . Neste caso, B e A podem trocar mensagens secretas no sistema RSA.

Para que B consiga enviar mensagens para A as etapas são:

- 1) B deve saber da chave pública (n, e) de A .
- 2) B traduz a mensagem x no alfabeto digital T (esse alfabeto deve ser conhecido pelas mesmas fontes).
- 3) B escreve T em blocos numéricos T_1, T_2, \dots, T_r . Os números T_1, T_2, \dots, T_r não devem ultrapassar o número $n = pq$.
- 4) B encripta os blocos T_1, T_2, \dots, T_r usando a condição (4) do Teorema 1.7 e assim estabelece as cifras C_1, C_2, \dots, C_r . Logo

$$C_1 \equiv T_1^e \pmod{n}, C_2 \equiv T_2^e \pmod{n}, \dots, C_r \equiv T_r^e \pmod{n}.$$

Relembre que os C_i devem ser escolhidos de tal forma que $C_i < n$ para todo $i = 1, \dots, r$.

- 5) B transmite as cifras C_1, C_2, \dots, C_r para A .
- 6) Ao receber a cifra, a fonte A decifra as cifras C_1, C_2, \dots, C_r usando o resultado do Teorema 1.7, que diz

$$T_i = C_i^d \pmod{n}, i = 1, 2, \dots, r,$$

usando a chave privada (n, d) , na verdade somente d é privada para A e somente A sabe esse número.

- 7) Uma vez que T_1, T_2, \dots, T_r são conhecidos por A , ele/ela podem usar o alfabeto digital e

transformar esses blocos numéricos na mensagem original x .

E o processo está completo.

Testes de primalidade

Você já deve ter percebido que o nível de confiabilidade na cifra depende diretamente de uma boa escolha dos números p e q que determinarão o número n . É essencial que tais números sejam grandes, com muitas e muitas casas decimais. Porém, isso não é suficiente, é também necessário que o número n seja de difícil fatoração, ou seja, que os números primos escolhidos não sejam fáceis de determinar.

Para responder se as escolhas de p e q são boas, devemos considerar as dificuldades envolvidas em se fatorar números inteiros. Existem vários algoritmos (métodos) para se fatorar números inteiros. Alguns mais simples ou mais eficientes do que outros, porém todos envolvem certa teoria e certo trabalho computacional. Aliás, é bom que se diga que toda nossa discussão insere no contexto da teoria computacional de números, que seria uma espécie de intersecção entre a teoria de números e a computação.

Como dizia, nosso primeiro problema é encontrar números primos grandes. Sabemos que o conjunto dos números primos é infinito, por isso temos a certeza de que dado um primo, sempre existe um primo maior. A distribuição dos números primos pode ser estimada por um famoso teorema, chamado de Teorema do número primo. Esse teorema faz uso da função $\pi(n)$, que calcula a quantidade de números primos menores que ou iguais a um inteiro positivo n .

Quando o número n é pequeno, a função $\pi(n)$ é fácil de se calcular. Veja,

$$\pi(2) = 1, \pi(3) = 2, \pi(7) = 4.$$

Porém, para valores de n muito grandes não sabemos como calcular o número exato de $\pi(n)$. O interessante é que para fins práticos, não precisamos desse valor exato, mas sim uma aproximação. Tal aproximação é dada pelo seguinte teorema.

Teorema 2.1 (Teorema do número primo): A seguinte igualdade é verdadeira

$$\lim_{n \rightarrow \infty} \left\{ \pi(n) / \frac{n}{\ln n} \right\} = 1$$

A demonstração desse Teorema pode ser encontrada no livro de Apostol [1], ou no livro de análise funcional de Rudin [4].

Esse teorema diz que para valores muito altos de n , ou seja, quando n tende ao infinito, a função $\pi(n)/\frac{n}{\ln n}$ tende a 1. A partir disso podemos estabelecer um limitante superior e inferior (cotas) para $\pi(n)$.

Teorema 2.2: Para todo $n \geq 2$ temos que

$$\frac{1}{6} \frac{n}{\ln n} < \pi(n) < 6 \frac{n}{\ln n},$$

em que $\ln n$ é o logaritmo de n na base e .

Note que a função $n/\ln n$ é mais fácil de se calcular do que a função $\pi(n)$. A demonstração desse resultado também pode ser encontrada em Apostol [1].

Método da divisão

O método da divisão é muito simples, na verdade baseia-se na definição de um número primo. Para saber se um inteiro n é primo basta dividi-lo pelos primos menores do que ele. Na verdade, percebe-se que é suficiente verificar se o inteiro n é divisível pelos primos menores que $\sqrt{n}-1$, uma vez que se a é um divisor de n , ou seja, $n = a \cdot b$, então b também é divisor de n , sendo assim, se a se aproxima de \sqrt{n} então b também o faz.

É óbvio que esse método é eficiente para números pequenos e muito ineficiente para números grandes. Veja por exemplo se quisermos saber se $n = 10^9$ é primo. Precisamos dividir n por pelo menos $\sqrt{\pi(10^9)} = \sqrt{\pi(50.847.478)} \approx 7.130$ divisões. Considere agora a dificuldade de se saber se um número com digamos 100 casas decimais é primo.

Vejamos agora outra abordagem para se dizer se um inteiro n é primo. Esse método é baseado no pequeno teorema de Fermat.

Pseudoprimidade

Pelo pequeno teorema de Fermat, sabemos que se $\text{mdc}(a, n) = 1$ e n é um número primo, então

$$a^{n-1} \equiv 1 \pmod{n}.$$

Agora, tomemos o conjunto

$$(\mathbb{Z}/n\mathbb{Z})^+ := \{1, 2, 3, \dots, n-1\}.$$

Com isso podemos escrever o pequeno teorema de Fermat de uma forma mais conveniente ao que pretendemos.

Teorema 2.3 (Pequeno teorema de Fermat adaptado): Se n é um número primo, então para todo $a \in (\mathbb{Z}/n\mathbb{Z})^+$ temos que

$$a^{n-1} \equiv 1 \pmod{n}$$

Ou seja, se n é primo, então $\text{mdc}(n, a) = 1$ para todo $a \in \mathbb{Z}$ que não seja múltiplo de n , em particular para $a \in (\mathbb{Z}/n\mathbb{Z})^+$. Assim podemos afirmar que n é co-primo com todos os possíveis restos da divisão de um inteiro qualquer por n . Dessa forma, qualquer dos restos da divisão por n , elevados a $n-1$, são congruentes a 1 módulo n .

Isso nos conduz ao mais importante que é o corolário a seguir.

Corolário 2.1: Se existir um número $a \in (\mathbb{Z}/n\mathbb{Z})^+$ tal que

$$a^{n-1} \not\equiv 1 \pmod{n}$$

então n não é primo, é composto.

Note que o corolário anterior é na verdade uma versão recíproca do teorema de Fermat. Veja também que tomando $a = 2$, temos que se para um inteiro n , $2^{n-1} \not\equiv 1 \pmod{n}$, então n é composto. Porém, a recíproca não é verdadeira, ou seja, se $2^{n-1} \equiv 1 \pmod{n}$, não podemos afirmar que n é primo. Desse modo, esse resultado é útil para se verificar se um inteiro n não é primo. Se por esse método não pudermos afirmar que n é composto, não podemos afirmar mais nada.

A justificativa para tomarmos $a = 2$ mais acima é que nossa intenção é determinar se um inteiro $n \geq 2$ é primo. Como estamos considerando números inteiros maiores que ou iguais a 2 podemos concluir que $2 \in (\mathbb{Z}/n\mathbb{Z})^+$ para qualquer n , além é claro de que 2 é o único inteiro com essa propriedade.

Quando utilizarmos o método anterior, baseado no teorema de Fermat e obtermos uma congruência, chamaremos o número n em questão de **pseudoprimo**.

Definição 2.1: Dizemos que um inteiro positivo n é **a-pseudoprimo** ou **pseudoprimo**

na base $a \in (\mathbb{Z}/n\mathbb{Z})^+$, se

$$a^{n-1} \equiv 1 \pmod{n}.$$

Quando $a = 2$, simplesmente dizemos que n é **pseudoprimo**. Nesse caso, n satisfaz $2^{n-1} \equiv 1 \pmod{n}$.

É importante ressaltar que todo primo p com $p \neq 2$ é pseudoprimo. A palavra pseudoprimo não deve ser interpretada como "falso primo", mas sim como "semelhante a um primo". Perceba que os números n que não são primos se assemelham a números primos pois, assim como eles, satisfazem a congruência $2^{n-1} \equiv 1 \pmod{n}$. Sendo assim, todo número primo é também um pseudoprimo.

Definição 2.2: Se um número n é pseudoprimo para toda base $a \in (\mathbb{Z}/n\mathbb{Z})^+$ dizemos que esse número é um **número de Carmichael**.

Veja que o corolário 2.1 diz: "se existir um inteiro $a \in (\mathbb{Z}/n\mathbb{Z})^+$ ". Sendo assim, vemos que nem todo a goza dessa propriedade. Os números n para os quais qualquer um dos possíveis restos de sua divisão têm a propriedade anterior (é pseudoprimo para toda base a), são chamados de números de Carmichael.

Vejamos alguns exemplos de pseudoprimos e de números de Carmichael. Os quatro números a seguir são os primeiros pseudoprimos.

$$341, 561, 645, 1.105.$$

Que são fatorados da seguinte forma,

$$341 = 11 \times 31$$

$$561 = 3 \times 11 \times 17$$

$$645 = 3 \times 5 \times 43$$

$$1.105 = 5 \times 13 \times 17$$

Por sua vez, temos os primeiros cinco números de Carmichael e suas respectivas fatorações em primos.

$$561, 1.105, 1.725, 2.465, 2.821.$$

$$\begin{aligned}
561 &= 3 \times 11 \times 17 \\
1.105 &= 5 \times 13 \times 17 \\
1.725 &= 7 \times 13 \times 19 \\
2.465 &= 5 \times 17 \times 29 \\
2.821 &= 7 \times 13 \times 31
\end{aligned}$$

É interessante notar que os números acima têm 3 fatores primos. Porém isso não corre sempre. Veja abaixo outros exemplos.

$$41.041 = 7 \times 11 \times 13 \times 41$$

e

$$825.265 = 5 \times 7 \times 17 \times 19 \times 73.$$

Os números acima são respectivamente o primeiro a ter quatro fatores primos e o primeiro a ter cinco fatores primos. Você deve ter percebido que os valores dos números cresceram rapidamente. Por isso se diz que os números de Carmichael são raros. Na verdade, Carmichael escreveu em seu artigo de 1912 que existem infinitos números com essa propriedade, ou seja, existem infinitos números de Carmichael. Hoje, essa afirmação é considerada um teorema, que foi demonstrado em 1994 por Alford, Granville e Pomerance.

A importância dos números de Carmichael está no fato de que eles satisfazem diversas condições. Veja os próximos resultados.

Teorema 2.4 (Korselt 1899): Um inteiro $n = p_1 p_2 \cdots p_k$ representado pelo produto de seus divisores primos p_i é um número de Carmichael se, e somente se os divisores p_i para todo $i = 1, 2, 3, \dots, k$ são distintos e o mínimo múltiplo comum

$$\text{mmc}(p_1 - 1, p_2 - 1, \dots, p_k - 1) \text{ divide } n - 1.$$

Demonstração: Se n é um número de Carmichael, então $a^{n-1} \equiv 1 \pmod{n}$ para todo $a \in (\mathbb{Z}/n\mathbb{Z})^+$. Logo, n satisfaz o sistema

$$a^{n-1} \equiv 1 \pmod{p_i} \quad i = 1, 2, \dots, k.$$

Pelo Teorema de Resto Chinês, o sistema tem solução se, e somente se o mínimo múltiplo

comum mmc $(p_1 - 1, p_2 - 1, \dots, p_k - 1)$ divide $n - 1$. A demonstração está assim completa.

Veja que pelo teorema não encontraremos potências na fatoraçoão de um número de Carmichael.

Corolário 2.2: n é um número de Carmichael se, e somente se ele é livre de quadrados e $(p - 1) | (n - 1)$ para todo divisor primo p de n .

Corolário 2.3: Números de Carmichael são ímpares e têm pelo menos três divisores primos.

Teorema de Lucas e Pocklington

Os teoremas de Lucas de 1876 e Pockington de 1914 nos fornecem mais condições para determinar se um inteiro n é primo.

Teorema 1.5 (Lucas 1876): Seja $n \geq 3$ um inteiro e $a \in \mathbb{Z}$ tal que $a^{n-1} \equiv 1 \pmod{n}$ e $a^x \not\equiv 1 \pmod{n}$ para todo x com $1 \leq x < n - 1$, então n é primo.

Demonstração: A congruência $a^{n-1} \equiv 1 \pmod{n}$ implica que o mdc $(a, n) = 1$. Por outro lado, os inteiros a^i e a^j para todo número i e j tal que $1 \leq i < j \leq n - 1$ são incongruentes módulo n , pois caso contrário teremos $a^i \equiv a^j \pmod{n}$. Isso implica que $a^i(a^{j-i} - 1) \equiv 0 \pmod{n}$. Mas, o mdc $(a, n) = 1$, e então

$$a^{j-i} \equiv 1 \pmod{n}.$$

Isso é impossível pela segunda condição do teorema, logo, os números a, a^2, \dots, a^{n-1} são congruentes a $1, 2, \dots, n - 1$ módulo n . Isso implica que se p é o menor número primo que divide n , então existe um inteiro positivo r tal que $a^r \equiv p \pmod{n}$. Mas isso é impossível, pois mdc $(a, n) = 1$, assim não existem primos que dividem n . Portanto, n é primo. Com isso a demonstração está completa.

Teorema 2.6 (Pocklington 1914): Seja $n > 1$ inteiro e $s > 0$ um divisor de $n - 1$. Suponha que exista um inteiro a satisfazendo

$$a^{n-1} \equiv 1 \pmod{n},$$

e

$$\text{mdc}(a^{(n-1)/q} - 1, n) = 1$$

para todo divisor q de s . Então, todo divisor primo p de n satisfaz a congruência $p \equiv$

$1 \pmod{s}$ e, se $s > \sqrt{n} - 1$, então n é primo.

Demonstração: Seja p um divisor primo de n , e b o resto da divisão de $a^{(n-1)/s}$ por n . Então, temos que $a^{n-1}/s \equiv b \pmod{n}$. Portanto, também, $a^{n-1} \equiv b^s \pmod{n}$. Por outro lado, a congruência $a^{n-1} \equiv 1 \pmod{n}$ implica que $b^s \equiv 1 \pmod{p}$, logo, o expoente de $b \pmod{p}$ ou a ordem de $b \pmod{p}$ no grupo $(\mathbb{Z}/p\mathbb{Z})^*$ divide s . Por outro lado, se q é um divisor primo de s , $b^{s/q} \not\equiv 1 \pmod{p}$, pois pela hipótese $a^{(n-1)/q} - 1$ não é divisível por p . Portanto, a ordem de $b \pmod{p}$ não é um divisor de s/q , qualquer que seja o divisor primo q de s , então essa ordem é igual a s . Porém o expoente, ou ordem, divide $p-1$ e portanto,

$$p \equiv 1 \pmod{s}.$$

Isso completa a primeira parte do teorema. Para provar a segunda afirmação, primeiro observe que de $p \equiv 1 \pmod{s}$ segue-se que $p-1 = ks \geq s$, para certo inteiro positivo k . Logo, $p \geq s+1 > \sqrt{n}$. Mas, $s > \sqrt{n} - 1$, então $p > \sqrt{n}$. E isso só pode ser verdadeiro para todo divisor primo p de n uma vez que n é primo. Sendo assim, a demonstração está completa.

Veremos agora como utilizar o Teorema de Pocklington no contexto de nossa discussão.

Números de Fermat e Mersenne

Um uso interessante para o teorema de Pocklington é verificar se certos números especiais são primos. Um conjunto desses números é o conjunto dos números de Fermat e Mersenne.

Definição 2.3 (número de Fermat): O número $F_n = 2^{2^n} + 1$ é chamado **n -ésimo número de Fermat**.

Nem todos os números de Fermat são primos. Na verdade, não se sabe se a quantidade de números de Fermat que são primos é infinita. Veja alguns exemplos de números de Fermat que são primos ou compostos.

$$F_1 = 5$$

$$F_2 = 17$$

$$F_3 = 257$$

$$F_4 = 65537$$

$$F_5 = 4.294.967.297 = 641 \times 6.700.417$$

$$F_6 = 18.446.744.073.709.551.617 \\ = 274.177 \times 67.280.421.310.721$$

Os próximos dois teoremas estabelecem propriedades interessantes sobre os números de Fermat. Maiores considerações e demonstrações destes resultados podem ser encontradas no livro de Shokranian [07].

Teorema 2.7: Quaisquer dois números distintos de Fermat são primos entre si. Em outras palavras, se $F_m \neq F_n$ são números de Fermat, então $\text{mdc}(F_n, F_m) = 1$.

Teorema 2.8: Um número de Fermat ou é primo ou é pseudoprimo.

Outro conjunto de números utilizado nos problemas de primalidade é o conjunto dos números de Mersenne.

Definição 2.4 (número de Mersenne): O n -ésimo número de Mersenne é o número da forma $M_n = 2^n - 1$

Teorema 2.9: Se n é um número composto, então M_n é composto.

Veja que é necessário que n seja primo para termos M_n primo, mas essa condição não é dita suficiente. Em outras palavras, se n é primo, não necessariamente M_n será primo.

Métodos algorítmicos

O princípio básico que torna o Teorema de Pocklington útil à nossa discussão é que ele nos fornece meios alternativos de investigar a primalidade de números, tanto os de Fermat quanto os de Mersenne.

Primeiro tomamos o número n como o número a ser investigado. Tomando n de tal sorte que n não seja um pseudoprimo e que s seja o maior divisor de $n - 1$, e que conheçamos sua fatoração. Tomemos agora um terceiro número, o número $a \pmod{s}$, escolhido arbitrariamente, com a única condição de que ele satisfaça ambas as condições do Teorema

de Pocklington. A princípio, podemos realizar os testes necessários sobre a , uma vez que conhecemos os fatores primos de s . Satisfazendo todas essas condições, teremos obtido em n um divisor primo, apoiados no Teorema anterior.

Tomando $n = 2^{2^k} + 1$ como um número de Fermat, teremos $n - 1 = 2^{2^k}$, que nos fornece os divisores de $n - 1$, possibilitando o uso do Teorema de Pocklington para descobrir de n é primo.

Porém, se n é um número de Mersenne, do tipo $n = 2^k - 1$, teremos $n - 1 = 2^k - 2 = 2(2^k - 1)$, cujos divisores são 2 e os divisores de $2^k - 1$, que não são facilmente obtidos. Teremos então de interpretar o Teorema de uma maneira mais conveniente neste caso. Chamaremos esta nova interpretação de **Teorema Torcido de Pocklington**.

Teorema 2.10 (Teorema Torcido de Pocklington): Seja $n > 1$ um inteiro e $s > 0$ um divisor de $n + 1$. Suponhamos que exista um inteiro a satisfazendo

$$a^{n+1} \equiv 1 \pmod{n},$$

e

$$\text{mdc}(a^{(n+1)/q} - 1, n) = 1$$

para todo divisor primo q do número s , que por sua vez é o maior divisor de $n - 1$. Sendo assim, todos os divisores primos p de n satisfazem a relação $p \equiv -1 \pmod{s}$, e tendo $s > \sqrt{n} + 1$, então $p > \sqrt{n}$ e n então é primo.

Se n é um número de Mersenne, pelo resultado anterior, encontramos os divisores de $n + 1$,

$$n + 1 = 2^k - 1 + 1 = 2^k$$

ou seja, os divisores de n são potências de 2.

Note que com estes resultados e algum esforço, podemos testar a primalidade de números de Fermat e Mersenne.

Pelas observações feitas, fica claro que tomar candidatos para p e q na cifra RSA entre os pseudoprimos, números de Carmichael, números de Fermat e Mersenne não é uma boa ideia, tendo em vista o amplo estudo sobre esses números. Vale dizer que esses estudos possibilitam uma maior compreensão das relações entre os números e a obtenção de possíveis soluções para os problemas de primalidade. Apesar de talvez esses números não terem implicação direta na cifra RSA, com certeza estão inseridos na teoria em que a cifra se apoia. Desse ponto de vista, quanto maior a expansão da teoria, maiores serão as possibilidades de aperfeiçoamento das cifras em geral.

Referências Bibliográficas

- [1] APOSTOL, T. M. **Introduction to analytic number theory**. Berlim: Springer-Verlag, 1980.
- [2] CAMPELLO, A. C.; LEAL, I. **Teoria Aritmética dos Números e Criptografia RSA**. Disponível em: http://www.ime.unicamp.br/~ftorres/ENSINO/MONOGRAFIAS/antonio_RSA.pdf Acesso em Nov. de 2015.
- [3] FREITAS, H. C. de; SOUSA, A. S. de; AGUSTINI, E. **Um Enfoque Computacional da Criptografia RSA**. FAMAT em Revista.Uberlândia, n. 3, p. 121-136, set. 2004.
- [4] RUDIN, W. **Functional Analysis**. New York: McGraw-Hill Book Company, 1973.
- [5] SHOKRANIAN, S. **Criptografia para iniciantes**. Brasília-DF: Editora Universidade de Brasília, 2005.
- [6] SEABRA, D. F. S. **Criptologia: uma abordagem histórica e matemática**. 2010. 43 f. Trabalho de Conclusão de Curso (Especialização)-Departamento de Matemática, Universidade Federal de São Carlos, São Carlos, 2010.
- [7] SHOKRANIAN, S. **Números notáveis**. Brasília: Editora Universidade de Brasília, Brasília, 2002.
- [8] SHOKRANIAN, S.; SOARES, M. V.; GODINHO, H. **Teoria dos números**. Brasília: Editora Universidade de Brasília, 1999.
- [9] SILVA, E. V. P. da. **Introdução à Criptografia RSA**. Disponível em: http://www.impa.br/opencms/pt/eventos/downloads/jornadas_2006/trabalhos/ Acesso em Nov. de 2015.
- [10] SILVA, F T. da; PAPANI, F. G. **Um pouco da história da criptografia**. Disponível em: <http://projetos.unioeste.br/cursos/cascavel/matematica/xxiisam/artigos/16> Acesso em Nov. de 2015.

- [11] PIMENTEL, E. G. **Teoria de números e criptografia RSA**. Disponível em: <http://www.mat.ufmg.br/~elaine/OBMEP/criptografia.pdf> Acesso em Nov. de 2015.