Universidade Federal do Piauí
Centro de Ciências da Natureza
Curso de Pós-graduação em Matemática

Kelvis Moraes da Silva

# *A Criptografia RSA, Matemática e suas Aplicações*

Teresina
2021

Kelvis Moraes da Silva

# *A Criptografia RSA, Matemática e suas Aplicações*

Dissertação apresentada ao programa de Pós-Graduação em Matemática da Universidade Federal do Piauí, na modalidade Profissional, como requisito parcial para a obtenção do grau de Mestre em Matemática.

**Orientador: Professor Dr. Carlos Humberto Soares Júnior**

**Orientador - UFPI**

Teresina

2021

FICHA CATALOGRÁFICA
Universidade Federal do Piauí
Biblioteca Setorial de Ciências da Natureza – CCN
Serviço de Processamento Técnico

S586c Silva, Kelvis Moraes.
A criptografia RSA, matemática e suas aplicações / Kelvis Moraes da Silva. – 2021.
74 f.: il.

Dissertação (Mestrado) – Universidade Federal do Piauí, Centro de Ciências da Natureza, Programa de Pós-Graduação em Matemática, Teresina, 2021.
"Orientador: Prof. Dr. Carlos Humberto Soares Júnior. "

1. Matemática computacional. 2. Criptografia RSA. 3. Teoria dos números. 4. Educação básica. I. Soares Júnior, Carlos Humberto. II. Titulo.

CDD 512.7

Bibliotecária (o): Caryne Maria da Silva Gomes – CRB3/1461

Kelvis Moraes da Silva

*A Criptografia RSA, Matemática e suas Aplicações*

Dissertação apresentada ao programa de Pós-Graduação em Matemática da Universidade Federal do Piauí, na modalidade Profissional, como requisito parcial para a obtenção do grau de Mestre em Matemática.

Aprovado em 27 de fevereiro de 2021

**BANCA EXAMINADORA**

Professor Dr. Carlos Humberto Soares Júnior

Orientador - UFPI

Dr. Manoel Vieira de Matos Neto

Examinador interno - UFPI

Dr. Edvalter da Silva Sena Filho

Examinador externo - UVA

*Quero agradecer, em primeiro lugar, a Deus, pela força e coragem durante toda esta longa caminhada.*
*Agradeço também a minha famílía por tudo que fizeram pra que eu chegasse até aqui.*

# Agradecimentos

Em primeiro lugar, agradeço a Deus por me ajudar a ultrapassar todas as barreiras e obstáculos encontrados durante a minha trajetória de vida.

Aos meus avós, tios, irmãos e esposa que sempre me deram apoio e incentivo durante toda a jornada de curso.

Ao meu orientador Carlos Humberto Soares Júnior, pela sua compreensão em meio as minhas dificuldades, atrasos e pela sua instrução e amizade.

Agradeço a todos os professores que fizeram parte da minha graduação e pós-graduação (PROFMAT) por me proporcionar apoio, conhecimento e incentivo.

Aos meus amigos de turma, por se dedicarem ao máximo em ajudar os colegas, para que todos nós conseguíssemos obter êxito.

Aos meus companheiros de trabalho, pela ajuda e força nesta caminhada.

Enfim, a todos que de forma direta e indiretamente colaboraram para que este grande dia acontecesse.

*"A matemática aplicada necessita da matemática pura, tanto como os formigueiros necessitam das formigas".*

*Paul Halmos*

# Resumo

Esta dissertação tem como objetivo apresentar metodologias voltadas para o ensino de alguns conteúdos comuns da Teoria dos Números na Educação Básica com a criptografia RSA, utilizando para este fim o uso das tecnologias atuais e a própria criptografia. Dessa forma, apresentamos neste trabalho definições e alguns fragmentos históricos da criptografia, bem como sua importância para a segurança de informações nos dias atuais. Apresentamos também definições, teoremas e propriedades da Teoria dos Números e da Congruência Modular necessárias para entender e compreender a criptografia RSA, além de textos cifrados pelo método de César, Vigenère e também pela criptografia RSA. Por fim incluímos uma proposta de aplicação da criptografia mediante de uma simulação prática de roubo de informação em uma plataforma de rede social ao qual deve ser criada e trabalhada em trabalhos futuros.

**Palavras-chave:** criptografia, criptografia RSA, matemática aplicada.

# Abstract

This dissertation aims to present methodologies aimed at teaching some common content of Number Theory in Basic Education with RSA cryptography, using for this purpose the use of current technologies and cryptography itself. Thus, we present in this work a definition and some historical fragments of cryptography, as well as their importance for security today. We also present definitions, theorems and properties of Number Theory and Modular Congruence necessary to understand and understand RSA encryption, as well as texts ciphered by the method of Cézar, Vigenère and also by RSA encryption. Finally, we have included a proposal for the application of cryptography through a practical simulation of information theft on a social network platform that must be created and worked on in future works.

**Keywords:** Cryptography, RSA, Application of RSA cryptography, Number Theory in Basic Education.

# Lista de Figuras

# Sumário

# 1 Introdução

A criptografia é uma ferramenta estratégica voltada para a segurança na troca de informações, a mesma pode atuar principalmente em sites de compras, *apps*, *e-mails*, rede sociais e senhas. Segundo Coutinho (2008, p. 1) a criptografia é o estudo dos "métodos para codificar uma mensagem de modo que só seu destinatário consiga interpretá-la". Como podemos perceber nas palavras do Coutinho, a Criptografia está acoplada a história da humanidade, pois desde cedo o homem sentiu a necessidade de guardar informações e transmiti-las com segurança, como por exemplo em comunicações em que envolvem segredos militares e de estado ou comerciais.

No processo de ensino-aprendizagem são inúmeros os desafios, e em se tratando de matemática, temos como problemáticas principais a relação de conteúdos com situações do cotidiano e o interesse dos alunos pela disciplina. Pensando nesses desafios, elaboramos este trabalho buscando não só o incentivo da criptografia como recurso didático, mas também que a mesma seja desenvolvida como parte da formação dos discente, pois é função social da escola preparar o cidadão para a sociedade atual, uma vez que é perceptível o avanço da tecnologia e com tal avanço tem havido o crescimento de crimes cibernéticos.

Como no Ensino Básico é trabalhado alguns elementos da Teoria dos Números, tais como os números primos, números compostos, MMC e MDC, e tendo em vista os diversos trabalhos realizados sobre o tema criptografia, percebemos a variabilidade de recursos para trabalhar boa parte da criptografia, porém deixando um pouco a desejar na abordagem prática da criptografia RSA em sala de aula, por isso focamos nosso trabalho na aplicação e compreensão da mesma no Ensino Básico por meio de simulações de espionagem durante conversas realizada em rede social criada especificamente para fins didáticos. Assim, a pergunta fomentadora do trabalho foi: de que forma podemos trabalhar Teoria dos Números, Criptografia RSA e a relação destes nos meios digitais na Educação Básica? E nosso objetivo geral constitui-se em trabalhar essas relações, instigando a afinidade pela matemática e tornar cidadãos mais preparados para atuar na sociedade atual.

Este trabalho esta dividido em seis capítulos. O primeiro deles trata da apre-

sentação do conteúdo de criptografia, da estrutura do trabalho e da escolha do tema. O segundo, intitulado “Conhecimentos Preliminares” traz alguns conteúdos clássicos da Aritmética, tais como: divisibilidade, o Algoritmo de Euclides, números primos, mínimo múltiplo comum, máximo divisor comum, congruência e algumas de suas propriedades, pois é de suma importância para a compreensão e aplicação da Criptografia RSA.

O terceiro capítulo detalha a definição de criptografia e percorre desde o campo da Criptologia até o contexto histórico, destacando sua importância na evolução da história, da tecnologia e avanços alcançados ao longo do tempo, apresentando tipos de máquinas e artefatos que possibilitam a criação de cifras e a decodificação das mesmas.

No quarto capítulo apresentamos o conceito e o algoritmo de funcionamento da Criptografia RSA, assim, aplicamos os conteúdos clássicos da Aritmética apresentados no capítulo 2 expondo por meio de exemplos práticos o processo de pré-codificação, codificação, decodificação, o funcionamento e a segurança do método RSA.

Depois de compreendermos o funcionamento da criptografia RSA, destacamos no capítulo cinco uma proposta de aplicação da criptografia, explorando gradativamente seus picos históricos e com foco principal na criptografia RSA.

O sexto capítulo é direcionado as considerações finais, contudo destacamos possibilidades de trabalhos futuros visando a aplicação da proposta apresentada no capítulo anterior.

# 2 Conhecimentos Preliminares

## 2.1 Indução

Nesta seção trataremos do Princípio da Indução Finita, que além de ter relação direta com a criptografia, é uma forte ferramenta para a demonstração de vários teoremas propriedades, alguns expostos aqui. A demonstração será omitida por depender de um poderoso axioma conhecido Princípio da Boa Ordenação, o qual, pelo contexto deste trabalho, não vemos a necessidade de expormos.

No que se segue, denotaremos o conjunto dos números naturais por $\mathbb{N} = \{0, 1, 2, ...\}$

**Proposição 2.1.** (Primeira forma do Princípio de Indução Finita)

Suponhamos que seja dada uma afirmação $P(n)$ dependendo de $n \in \mathbb{N}$ tal que:

i) $P(0)$ é verdadeira, isto é, a sentença é valida para o primeiro valor de $n$ possível.

ii) Para cada $k \in \mathbb{N}, P(k+1)$ é verdadeira sempre que $P(k)$ for verdadeira. Então $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

## 2.2 Divisibilidade

**Definição 2.1.** Se $a$ e $b$ são inteiros, dizemos que $a$ *divide* $b$ se existir um inteiro $c$ tal que $b = ac$ e denotamos por $a|b$. Se $a$ não divide $b$ escrevemos $a \nmid b$.

**Lema 2.1.** Sejam $a$, $b$, $c$, $d$, $x$ e $y$ inteiros. Tem-se:

*i)* Se $d|a$ e $d|b$, então $d|(ax + by)$;

*ii)* Se $d|a$, então $a = 0$ ou $|d| \leq |a|$;

*iii)* Se $a|b$ e $b|c$, então $a|c$.

**Demonstração de *i)*:** Como $d|a$ e $d|b$, existem inteiros $q$ e $k$ tais que $a = dq$ e $b = dk$, multiplicando ambos os membros das igualdes por $x$ e $y$, respectivamente e adicionando

membro a membro das igualdades, obtemos $ax + by = dqx + dky = d(qx + ky)$ o que implica $d|(ax + by)$.

**Demonstração de *ii)*:** Se $a = 0$ nada há de demonstrar. Se $a \neq 0$, então existe inteiro $q \neq 0$ tal que $a = dq$, assim $|q| \geq 1$ e $|a| = |d||q| \geq |d|$.

**Demonstração de *iii)*:** Como $a|b$ e $b|c$, existem inteiros $q$ e $k$ tais que $b = aq$ e $c = bk$. Substituindo o valor de $b$ em $c = bk$, obtemos $c = a(qk)$ o que implica que $a|c$. ■

## 2.3 O algoritmo de Euclides

**Teorema 2.1.** Sejam $a$ e $b$ dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros $q$ e $r$ tais que $a = bq + r$, com $a \leq r < |b|$.

**Demonstração:** Considere o conjunto

$$S = \{x = a - by, y \in \mathbb{Z}\} \cap \mathbb{N}.$$

Para existência, temos pela propriedade Arquimediana que existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, portanto $a - bn > 0$, o que implica em $S$ não vazio. O conjunto $S$ é limitado inferiormente por 0, logo, pelo Princípio da Boa Ordenação, temos que $S$ possui um menor elemento $r$. Suponhamos então que $r = a - bq$. Sabemos que $r \geq 0$, assim basta mostrarmos que $r < |b|$. Suponhamos por absurdo que $r \geq |b|$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, logo $0 \leq s < r$. Mas isso contradiz o fato de $r$ ser o menor elemento de $S$, pois $s = a - (q \pm 1)b \in S$, com $s < r$.

Para a unicidade, suponhamos que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}, 0 \leq r < |b|$ e $0 \leq s < r$. Assim, temos que $-|b| < r \leq r' - r \leq r' < |b|$. Logo, $|r' - r| < |b|$. Por outro lado, $b(q - q') = r' - r$, o que implica que $|b||q - q'| = |r - r'| < |b|$, o que só é possível se $q = q'$ e $r = r'$. ■

## 2.4 Números Primos

**Definição 2.2.** Um número inteiro $n(n > 1)$ é dito primo se possuir apenas dois divisores positivos $n$ e 1.

Se $n(n > 1)$ não é primo diremos que $n$ é composto.

**Teorema 2.2.** *(Teorema Fundamental da Aritmética)* Todo inteiro maior que 1 pode ser representado de forma única (a menos da ordem) como produto de fatores primos.

**Demonstração:** Se $n$ é primo não há nada a ser demonstrado. Suponhamos $n$ composto. Seja $p_1$ o menor dos divisores de $n$. Note que $p_1$ é primo, pois, se fosse composto existiria $p$, $1 < p < p_1$ tal que $p|n$ o que é absurdo, pois $p_1$ é o menor de seus divisores. Logo, $n = p_1 n_1$.

Se $n_1$ for primo a prova está completa. Caso contrário, tomamos $p_2$ como menor fator de $n_1$. Pelo argumento anterior $p_2$ é primo e temos $n = p_1 p_2 n_2$.

Repetindo este procedimento, obtemos uma sequência de inteiros positivos $n_1$, $n_2$, ..., $n_r$. Como todos estes inteiros são maiores que 1 esse processo certamente deve terminar. Como os primos $p_1$, $p_2$, ..., $p_k$ não são, necessariamente, distintos, $n$ terá em geral a forma:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$$

Para mostrarmos a unicidade usamos indução em $n$. Para $n = 2$ a afirmação é verdadeira. Assumimos, então, que ela se verifica para todos os inteiros maiores do que 1 e menores que do que $n$. Vamos provar que ela também é verdadeira para $n$. Se $n$ é primo, não há nada a provar. Vamos supor, então, que $n$ seja composto e que tenha duas fatorações, isto é,

$$n = p_1 p_2 ... p_s = q_1 q_2 ... q_r.$$

Vamos provar que $s = r$ e que cada $p_i$ é igual a algum $q_j$. Como $p_1$ divide o produto $q_1 q_2 ... q_r$ ele divide pelo menos um dos fatores $q_j$. Sem perda de generalidade podemos supor que $p_1|q_1$. Como são ambos primos, isto implica $p_1 = q_1$. Logo $n/p_1 = p_2 ... p_s = q_2 ... q_r$. Como $1 < n/p_1 < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1 p_2 ... p_s$ e $q_1 q_2 ... q_r$ são iguais.

■

**Teorema 2.3.** (Euclides) A sequência dos números primos é infinita.

**Demonstração:** Vamos supor que a sequência dos números primos seja finita. Seja $p_1$ $p_2$ ..., $p_n$ a lista de todos os primos. Consideramos o número $R = p_1 . p_2 ... p_n + 1$. É claro que $R$ não é divisível por nenhum dos $p_i$ de nossa lista e que $R$ é maior do que qualquer $p_i$. Mas, pelo Teorema 3.1, ou $R$ é primo ou possui algum fator primo e isto implica na

existência de um primo que não pertence à nossa lista. Portanto a sequência dos números primos não pode ser finita. ■

## 2.5 Mínimo Múltiplo Comum (MMC) e Máximo Divisor Comum (MDC)

**Definição 2.3.** O Mínimo Múltiplo Comum $m$ de dois inteiros $a$ e $b$ positivos é o menor inteiro positivo que é divisível por $a$ e $b$, no qual denotaremos por $m = [a, b]$.

**Definição 2.4.** O Máximo Divisor Comum $d$ de dois inteiros $a$ e $b$ não ambos nulos e denotado por $d = (a, b)$, é o maior inteiro que divide $a$ e $b$.

**Definição 2.5.** Os inteiros $a$ e $b$ são relativamente primos(coprimos ou primos entre si) quando $(a, b) = 1$.

**Definição 2.6.** (*Função Totiente de Euler*) O número $\phi(m)$ é o número de inteiros positivos menores que, ou iguais a $m$ que são relativamente primos com $m$.

Note, pela definição, que $\phi(p) = p - 1$ quando $p$ primo, já que ele é coprimo com todos os inteiros positivos menores que ele.

**Teorema 2.4.** Se $a$ e $b$ são inteiros e $a = qb+r$ onde $q$ e $r$ são inteiros, então $(a, b) = (b, r)$.

**Demonstração:** Da relação $a = qb + r$ podemos concluir que todo divisor de $b$ e $r$ é um divisor de $a$ (Lema 3.1). Esta mesma relação, escrita na forma $r = a - qb$, nos diz que todo divisor de $a$ e $b$ é um divisor de $r$. Logo o conjunto dos divisores comuns de $a$ e $b$ é igual ao conjunto dos divisores comuns de $b$ e $r$, o que nos garante o resultado $(a, b) = (b, r)$. ■

**Teorema 2.5.** (*Relação de Bèzout*) Se $d = (a, b)$, então exitem inteiros $x$ e $y$ tais que $d = ax + ay$.

**Demonstração:** Seja $S = \{ax + by \geq 0 |\ x, y \in \mathbb{Z}\}$.

Note que $ka \in S$ para todo $k \geq 0$ inteiro, portanto $S$ é infinito.

Sendo $d'$ o menor elemento positivo de $S$, então $S = \{kd' |\ k \geq 0\ e\ k \in \mathbb{Z}\}$. Como $d'$ é o menor elemento de $S$, então existem inteiros $x$ e $y$ tais que $d' = ax+by$ o que implica em $d|d'$.

Como $a = 1.a + 0.b$, $b = 0.a + 1.b$ e ambos pertencem a $S$, então $d'|a$ e $d'|b$ portanto $d'|d$. Logo, $d' = d$.

■

## 2.6 Congruência

**Definição 2.7.** Se $a, b$ e $m > 0$ são inteiros, dizemos que $a$ é congruente a $b$ módulo $m$ e denotamos por $a \equiv b \ mod \ m$ se $(a - b)$ é múltiplo de $m$. Se $(a - b)$ não é múltiplo de $m$ dizemos que $a$ é incongruente a $b$ e denotamos por $a \not\equiv b \ mod \ m$. Dizer que $a$ é congruente a $b$ módulo $m$ significa que $a$ e $b$ deixam o mesmo resto quando divididos por $m$.

**Exemplo**

a) $10 \equiv 1 \ mod \ 3$, pois $(10 - 1)$ é múltiplo de 3.

b) $20 \not\equiv 3 \ mod \ 2$, pois $(20 - 3)$ não é múltiplo de 2.

Observe em a) que o resto da divisão dos dois números por 3 é igual a 1.

**Proposição 2.2.** Seja $m \in \mathbb{N}$ e $m > 1$, para todos $a, b, c$ e $m$ inteiros, tem-se que:

(1) *(Reflexividade)* $a \equiv a \ mod \ m$;

(2) *(Simetria)* Se $a \equiv b \ mod \ m$, então $b \equiv a \ mod \ m$;

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

(4) *(Compatibilidade com a soma e a diferença)* Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então $a + c \equiv b + d \ mod \ m$ e $a - c \equiv b - d \ mod \ m$. (Desta pode ser concluída uma outra propriedade particular: se $a \equiv b \ mod \ m$, então $ka \equiv kb \ mod \ m$ para todo k inteiro.)

(5) *(Compatibilidade com o produto)* Se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então $ac \equiv bd \ mod \ m$.

Em particular, se $a \equiv b \ mod \ m$, então $a^k \equiv b^k \ mod \ m$ para todo $k \in \mathbb{N}$.

(6) *(Cancelamento)* Se $(c, m) = 1$, então $ac \equiv bc \ mod \ m \Leftrightarrow$ a $\equiv b \ mod \ m$.

(7) Se $c \neq 0$, *então*ac $\equiv bc \ mod \ m \Leftrightarrow$ a $\equiv b \ mod \ \dfrac{m}{(c, m)}$.

**Demonstração**:

(1) Como $0 = (a - a) = m.0$, isto é, $(a - a)$ é múltiplo de $m$, decorre da definição que $a \equiv a \ mod \ m$.

(2) Se $a \equiv b \ mod \ m$, então $m|(a-b)$ uma vez que $(a-b)$ é múltiplo de $m$. Portanto, existe um inteiro $k$ tal que $(a-b) = mk \Leftrightarrow \ (b-a) = m(-k) \ \Leftrightarrow \ m|(b-a) \ \Rightarrow$ $b \equiv a \ mod \ m$.

(3) $\begin{cases} a \equiv b \ mod \ m \Rightarrow \ m|(b-a) \\ b \equiv c \ mod \ m \Rightarrow \ m|(b-c) \end{cases}$ segue do lema 2.1 que $m|(b-a)+(c-b)$ $\Rightarrow \ m|(c-a) \ \Rightarrow$ a $\equiv c \ mod \ m$.

(4) Suponha que $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$. Deste modo $m|(b-a)$ e $m|(d-c)$ isso implica que $m|(b-a) \pm (d-c) \ e \ m|(b \ \pm d) - (a \ \pm c)$.

(5) Como $m|(b-a)$ e $m|(d-c)$ segue que $m|d(b-a)$ e $m|a(d-c)$. Desta forma pode-se concluir que $m|d(b-a)+a(d-c)$, ou seja, $m|bd-ac$. ■

Deixamos os itens (6) e (7) como exercício ao leitor.

Algumas propriedades adicionais que serão utilizadas:

**Proposição 2.3.** Sejam $a, b \in \mathbb{Z}$ e $m$, $n$, $m_1$, ..., $m_r$ inteiros maiores que 1. Tem-se que:

(1) se $a \equiv b \ mod \ m$ e $n|m$ então $a \equiv b \ mod \ n$;

(2) $a \equiv b \ mod \ m_i$, $\forall i = 1$, ..., $r \Leftrightarrow a \equiv b \ mod \ [m_1, ..., m_r]$;

(3) se $a \equiv b \ mod \ m$, então $(a, m) = (b, m)$.

**Demonstração**:

(1) Se $a \equiv b \ mod \ m$, então $m|(b-a)$. Como $n|m$, segue-se que $n|(b-a)$. Logo, $a \equiv b \ mod \ n$.

(2) Se $a \equiv b \ mod \ m_i$, $i = 1, ..., r$, então $m_i|(b-a)$, para todo $i$. Sendo $b-a$ um múltiplo de cada $m_i$, segue-se que $[m_1, ..., m_r]|(b-a)$, o que prova que $a \equiv b \ mod$ $m_1, ..., m_r$.

A recíproca decorre do primeiro item.

(3) Se $a \equiv b \ mod \ m$, então $m|(b-a)$ e, portanto, $b = a + tm$ com $t \in \mathbb{Z}$. Logo, pelo **Teorema 2.3**, tem-se que

$$(a, m) = (a + tm, m) = (b, m).$$

■

**Teorema 2.6.** *(Pequeno Teorema de Fermat)* Seja $p$ um número primo, tem-se

que $p$ divide o número $a^p - a$, para todo número inteiro $a$.

Em notação de congruências, temos

**Teorema 2.7.** Sejam $a \in \mathbb{Z}$ e $p$ um número primo tem-se que $a^p \equiv a \; mod \; p$.

Deste teorema, decorre o seguinte corolário:

**Corolário 2.1.** Se $p$ é um inteiro e se $a$ é um natural não divisível por $p$, então $p$ divide $a^{p-1} - 1$.

Em notação de congruências, temos

**Corolário 2.2.** Sejam $a \in \mathbb{Z}$ e $p$ um número primo tais que $(a, p) = 1$. Tem-se que $a^{p-1} \equiv 1 \; mod \; p$.

As demonstrações dos teoremas **2.6**, **2.7** e corolário **2.1**, **2.2** são encontradas em Hefez (2014).

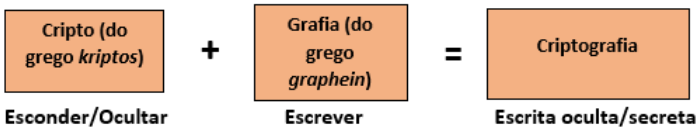
**Definição 2.8.** Seja $\bar{a}$ um inteiro de forma que $\bar{a}a \equiv 1 \; mod \; m$. Dizemos que $\bar{a}$ é um inverso de $a$ módulo $m$.

**Teorema 2.8.** Se $a$ e $m$ são inteiros primos entre si e $m > 1$, então um inverso de $a$ módulo $m$ existe.

**Demonstração:** Como $(a, m) = 1$, então pela relação de Bézout existem inteiros $q$ e $k$ tais que $aq + mk = 1 \Rightarrow \; aq + mk - 1 = 0 = 0.m$, daí, pela definição de congruência $aq + mk \equiv 1 \; mod \; m$. Como $mk \equiv 0 \; mod \; m$, segue-se que $aq \equiv 1 \; mod \; m$, logo $q$ é inverso de $a$ módulo $m$. ■

# 3 Criptografia

Ao ouvirmos a palavra criptografia certamente nos lembramos dos computadores, internet ou algo complicado relacionado exclusivamente a aparelhos digitais, mas se pararmos para analisar a origem desta palavra, veremos que a mesma vem do grego onde é formada pela seguinte combinação:




Fonte: autor

Assim, podemos concluir que criptografia é uma técnica de escrita oculta ou secreta, isto é, transpor uma mensagem da forma legível para uma forma ilegível de modo a garantir o sigilo da comunicação.

> Durante milhares de anos, reis, rainhas e generais dependeram de comunicações eficientes de modo a governar seus países e comandar seus exércitos. Ao mesmo tempo, todos estavam cientes das consequências de suas mensagens caírem em mãos erradas, revelando segredos preciosos a nações rivais ou divulgando informações vitais para forças inimigas. Foi a ameaça da interceptação pelo inimigo que motivou o desenvolvimento de códigos e cifras, técnicas para mascarar uma mensagem de modo que só o destinatário possa ler seu conteúdo. (Singh, Simon, 2004, pag. 11)

A criptografia é antes de tudo uma ramificação da criptologia, essa por sua vez é o estudo que reúne as habilidades e os conhecimentos essenciais para a ocultação de informações (criptografia) e a ruptura das informações ocultas (criptoanálise). Existem dois modos diferentes de ocultar uma informação, uma é omitindo a existência da mensagem (esteganografia) e a outra é tornando apenas a mensagem incompreensível (criptografia). A título de exemplos de aplicação da esteganografia, temos a marcas d'água em imagens e cédulas por razões de proteção dos direitos autorais ou assegurar a legitimidade, e minúsculos pontos amarelos em toda página empregados por impressoras digitais atuais, os pontos são pouco visíveis e contém codificados os números de série, bem como a

data e a hora da impressão. Simplificando, Esteganografia é a técnica de camuflar uma mensagem ou informação.

Por outro lado, a criptografia é a técnica de tornar a mensagem ininteligível (sem a preocupação de escondê-la) de modo que só o remetente e o receptor possam decodificá-la através de uma chave. Segundo Coutinho (2005, p.1) "decodificar é o que um usuário legítimo do código faz quando recebe uma mensagem codificada e deseja lê-la. Já decifrar significa ler uma mensagem codificada sem ser um usuário legítimo". A criptografia pode ocorrer através de códigos ou cifras.

Os códigos são caracteres (barras, letras, números, etc.) empregados para exibir uma mensagem. Como exemplo prático do dia-a-dia temos o código de barras e os números de controle (ex: CPF).

O outro método usado para criptografar mensagens é a cifra, técnica na qual o conteúdo da mensagem é cifrado através da mistura e/ou substituição das letras da mensagem original. A mensagem é decifrada fazendo-se o processo inverso ao ciframento e são divididas em:

1. Cifras Assimétricas: possue um par de chaves, uma pública e outra privada, por isso é também conhecida como cifra de chave pública e tem como principal algoritmo de utilização o sistema de criptografia RSA. Mostraremos exemplos no capítulo 4.

2. Cifras Siméticas: dispõe de uma única chave, que é compartilhada entre o destinador e o destinatário podendo ser dividida em:

2.1 Simétrica por Transposição: quando os caracteres da mensagem cifrada são os mesmos da mensagem original diferindo entre si apenas na ordem a qual foram empregados, isto é, a informação cifrada é composta de anagramas das palavras originais. Tem como ponto negativo a facilidade em ser decifrada, já que todas os símbolos da mensagem original são conhecidos pelo decifrador, bastando assim montar o quebra-cabeça. A exemplo de cifras por transposição, temos a palavra ESPERTO que pode ser transformada em ESPORTE.

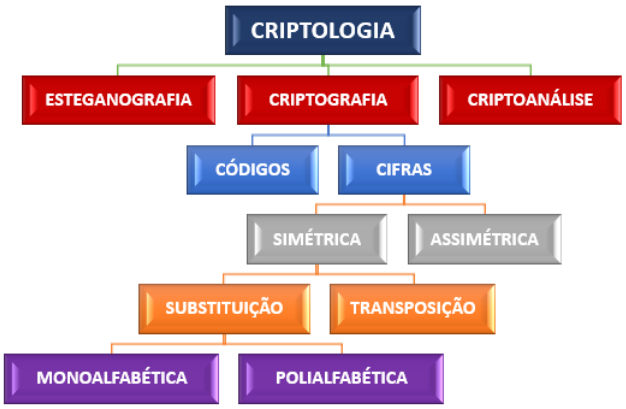
2.2 Simétrica por Substituição: cada letra do alfabeto em questão é substituída por outra letra ou símbolo. Para que haja comunicação é necessário que o remetente e o receptor tenha em mãos dicionários chave idênticos. As cifras simétricas por substituição que apresentam um único alfabeto em sua composição são chamadas de monoalfabéticas

e as que apresentam mais de um são chamadas de poli-alfabéticas. Exemplo em **3.1.5**

Com o surgimento da criptografia surge também a criptoanálise, essa por sua vez é o conjunto de técnicas e métodos para a decifração de caracteres pertencentes a uma escrita de sistema desconhecido.

Para compreendermos melhor as subdivisões da criptologia vejamos o organograma abaixo:

Figura 3.1: Organograma.




Fonte: autor

## 3.1 Desenvolvimento da Criptografia

Conhecer o processo de desenvolvimento de um conteúdo é tão importante quanto conhecer o produto, que é o próprio conteúdo. O pensamento nesse processo foi o que nos motivou na descrição de alguns picos da criptografia e sua contribuição para a humanidade. Em meio ao processo de ensino e aprendizagem é possível que o discente compreenda quais as necessidades e os conteúdos empregados, pois:

> "A história deve ser o fio condutor que direciona as explicações dadas aos porquês da Matemática. Assim, pode promover uma aprendizagem significativa, pois propicia ao estudante entender que o conhecimento matemático é construído historicamente a partir de situações concretas e necessidades reais (MIGUEL e MIORIM, 2004).

### 3.1.1 Primeiros Relatos

Segundo estudiosos da criptografia, os primeiros relatos de escritas em cifras se deram por volta de 1900 a.C. onde os escribas resolveram usar alguns símbolos em

hieróglifos não tanto comuns ao invés de alguns já familiares no túmulo do grande chefe e arquiteto egípcio Khnumhotep II, que serviu durante o reinado dos faraós Amenemhat II e Senusret II da 12ª dinastia , Reino Médio. Escritas ao qual chamamos hoje de criptografia de cifra simétrica por substituição monoalfabética.

Figura 3.2: Hieróglifos da tumba de Khnumhotep II.

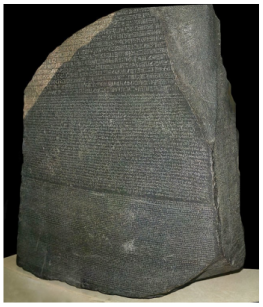
Fonte: Machinae

### 3.1.2 Esteganografia

Há relatos sobre escritas secretas do século V a.C. nos nove livros *As Histórias de Heródoto,* historiador grego. Os livros de Heródoto relatam que as informações enviadas aos gregos, de como e quando Xerxes, o rei da Pérsia, iria atacá-los, eram escritas em fragmentos de madeira e cobertas com cera. Há também episódio destes mesmos livros que relata sobre um jovem raspar a cabeça para escrever uma mensagem em seu couro cabeludo, onde é levada em segurança ao destinatário coberta pelo cabelo já crescido e é revelada raspando novamente a cabeça. Porém, essas escritas secretas não se tratavam de criptografia e sim de esteganografia, pois como podemos observar a grande preocupação era em esconder a mensagem e não torná-la inelegível.

### 3.1.3 Pedra de Roseta

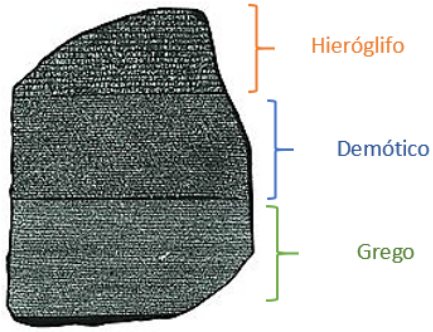
Figura 3.3: Pedra de Roseta



Fonte: *https://pt.wikipedia.org/wiki/Pedra-de-Roseta*

A pedra de Roseta é um fragmento de granito, encontrada na cidade de Roseta, próxima a Alexandria, pelas tropas de Napoleão em 1799 após sua derrota para o Reino Unido. Consiste em um artefato de quase uma tonelada, medindo 118 centímetros de comprimento, 77 centímetros de largura e 30 centímetros de espessura na qual contém por escrito um decreto de 196 a.C. elaborado pelo conselho de sacerdotes e promulgado em nome do faraó Ptolemeu V. Sua contribuição para a criptografia não está ligado diretamente ao conteúdo, mas a forma como foi escrito, pois trata de uma mensagem escrita a partir de três alfabetos distintos: grego, hieróglifos e demótico, além de ter sido escrito em duas línguas.

Figura 3.4: Pedra de Roseta: Detalhes




Fonte: autor

A consumação da tradução se deu em 1822 com o estudante francês Jean-François Champollion, nascido em 1970, quando percebeu que a técnica egípcio admitia sinais que indicavam ideias e outras caracterizavam sons.

Figura 3.5: Jean-François Champollion

Fonte: *https://pt.wikipedia.org/wiki/Jean-Francois-Champollion*

### 3.1.4 Cítala ou Bastão de Licurgo

Figura 3.6: Bastão de Licurgo

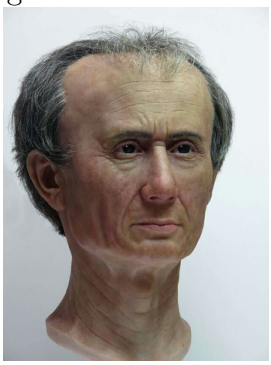
Fonte: *https://educalingo.com/pl/dic-pl/skytale*

A **Cítala ou Bastão de Licurgo** é uma técnica de criptografia utilizada pelos espartanos para envio de mensagens de modo que as tornassem inelegíveis e consiste em uma cifra de transposição, conhecida por ser o primeiro dispositivo criptográfico militar, com origem no séc. V a.C.

A cifragem com o Bastão de Licurgo fundava-se em envolver uma fita de couro ou pergaminho em um mastro de madeira de dada espessura, como na figura acima, e em seguida, escrever o texto a ser cifrado na fita sobreposta ao mastro no sentido do seu comprimento, desenrolada e emiti-la embuçada (como um cinto por exemplo) e ao chegar ao destinatário deveria ser enrolada em um outro mastro congruente ao primeiro para que a mensagem fosse decifrada.

### 3.1.5 Cifra de César

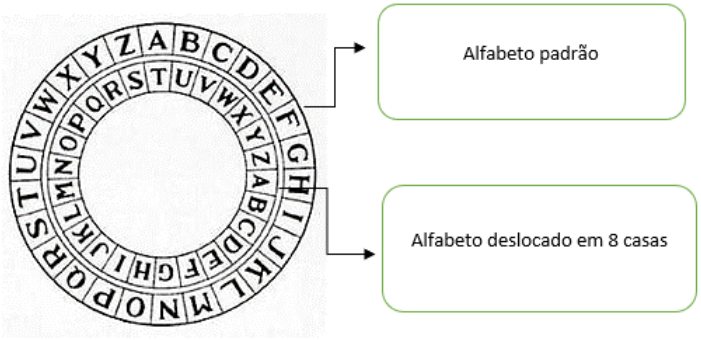
Figura 3.7: Júlio César



Fonte: *https://www.hypeness.com.br/2018/07/reconstrucao-3d-mostra-como-era-rosto-do-imperador-romano-julio-cesar/*

Tendo em vista a fragilidade da esteganografia, pois, caso o mensageiro fosse pego por tropas inimigas seus planos seriam inúteis, César ex-ditador da Roma Antiga por volta de 58 a.C. criou um método para minimizar chances de que a mensagem fosse decifrada por quem a interceptasse indesejavelmente, o método de César, conhecido

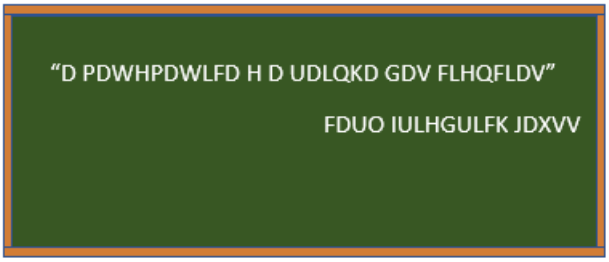
também como cifra de César consiste em deslocar o alfabeto um número x de vezes, onde $1 \leq x \leq$ *número de caracteres do alfabeto em questão*, por exemplo, usando o alfabeto português atual e a tabela abaixo, onde o alfabeto foi deslocado 8 casas no sentido horário, temos que a letra A passa ser escrita como T, o B como U e assim sucessivamente, portanto a palavra MATEMÁTICA passaria a ser escrita como FTMXFTMBVT.




Fonte: autor

Note que o receptor da mensagem criptografada pela cifra de César precisa saber exatamente quantas vezes o alfabeto foi deslocado e qual sentido (horário ou anti-horário) para que consiga decodificá-la, ou seja, ele precisa de informações a qual chamamos de chave. Logo, uma mensagem cifrada a partir da Cifra de César compõe-se de duas partes, uma para codificá-la e outra para decodificá-la.

A partir da criptoanálise a cifra de César foi decifrada por volta de 1000 anos depois de seu império, a proeza foi dos árabes que utilizaram para isso Análise de Frequência, de modo geral, qualquer cifra demasiada que provém da substituição de uma letra por símbolos pode ser facilmente decifrada com o uso deste método, pois, basta para isto comparar o símbolo mais frequente com a letra mais frequente, o segundo símbolo mais frequente com a segunda letra mais frequente e assim sucessivamente até conseguir deduzir a chave da cifra do alfabeto em questão.Vejamos um exemplo:

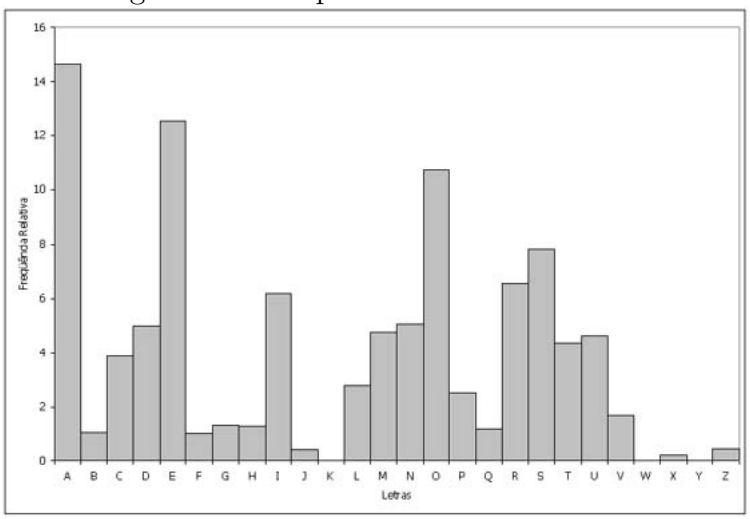



Fonte: autor

Sabendo que a frase na imagem acima é monoalfabética e foi cifrada a par-

tir do alfabeto português atual, podemos deduzir a chave da cifra, uma vez que em “D PDWHPDWLFD H D UDLQKD GDV FLHQFLDV” a letra D surge oito vezes, P duas vezes, W duas vezes, H três vezes, L quatro vezes, F três vezes, U uma vez, Q duas vez, K uma vez, G uma vez, V duas vezes e que a frequência de surgimento de cada letra em um texto demasiado da lingua portuguesa em porcentagem é aproximadamente:

Figura 3.8: Frequência de uso das letras




Fonte: *https://pt.wikipedia.org/wiki/Ficheiro:Frequencia-de-uso-das-letras-PT.png*

Como D e H surgem sozinhas e a letra D aparece com maior frequência é razoável cogitar que a letra D corresponde a letra A e que H corresponde a letra E, portanto podemos deduzir que a frase foi cifrada a partir da cifra de César abaixo:

Alfabeto Normal:

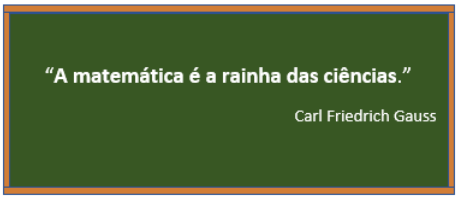
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Alfabeto Cifrado:

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

Fonte: autor

Logo, fazendo as respectivas substituições temos:




Fonte: autor

Os esforços dos árabes para decifrar o código de César trouxe consigo uma competição entre criadores e decifradores de códigos, gerando cada vez mais, códigos resistentes a serem decifrados, um destes é a Cifra Indecifrável ou Cifra de Vigenère que nada mais é que uma evolução da Cifra de César.

Figura 3.9: Blaise de Vigenère

Fonte: *https://www.britishmuseum.org/collection/object/P-1927-1008-87*

Blaise de Vigenère, nascido em 5 de abril de 1523, foi um diplomata e criptógrafo francês. A Cifra de Vigenère foi assim atribuída a sua autoria no século XIX de forma bastante curiosa, pois esse método de cifragem foi descrito primeiramente pelo criptologista italiano Giovan Battista Bellaso em um livro de 1553 de nome “La cifra del. Sig. Giovan Battista Bellaso”. A cifra de Vigenère trata de um método de criptografia por substituição polialfabética na qual utiliza uma variedade de cifras de César distintas distribuidas em forma de tabela, na qual uma palavra é escolhida como “palavra-chave”, e cada letra desta palavra vai indicar a linha a ser utilizada para cifrar ou decifrar uma letra da mensagem.

Figura 3.10: Tabela ou quadro de Vigenère

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

Fonte: *https://pt.wikipedia.org/wiki/Cifra-de-Vigenère*

Para melhor compreensão, vamos encriptar a frase “um tempo para cada propósito”, usando como palavra-chave a palavra “eclesiastes”. A palavra-chave deve ser repetida sucessivamente até completar o comprimento da mensagem a ser enviada, da seguinte forma:

Figura 3.11: Exemplo de cifragem pelo método de Vigenère

| | |
|---|---|
| Mensagem: | um tempo para cada propósito |
| Palavra-chave: | ec lesia stes ecle siastesec |
| Texto cifrado: | yo eieu htvs gcoe hzohhwaxq |

Fonte: autor

A primeira letra do texto, que é a letra “u”, é cifrada com o alfabeto da linha “e”, que é a primeira letra da palavra-chave. Procuramos a letra referente ao cruzamento da linha “e”com a coluna “u”, obtendo como resultante a letra “y”. Esta será a primeira letra do texto cifrado. Passando para a segunda letra do texto normal, que é “m”, procuramos a linha correspondente à letra “c”, segunda letra da chave, e localizamos a letra que esteja na intersecção dessa linha com a coluna da letra procurada, m. No caso, a letra é “o”, segunda letra do texto cifrado. E assim sucessivamente, até o final da cifragem.

Para decriptar o texto, estudamos à tabela na linha correspondente a cada letra da palavra-chave, encontramos a letra do texto cifrado na linha, e então temos o letreiro da coluna como texto plano (decriptado). No exemplo acima, na linha “e”, a letra “y”do texto cifrado (primeira letra), surge na coluna “u’, que é assim a primeira letra do texto decifrado. Na linha da segunda letra da chave, “c”, encontramos a segunda letra do texto cifrado, “o”, que corresponde à coluna “m”– esta é a segunda letra do texto original – e assim sucessivamente.

### 3.1.6 A Criptografia na Segunda Guerra Mundial

Por volta do fim da primeira e início da Segunda Guerra Mundial os alemães criaram uma poderosa máquina eletromecânica de criptografia com rotores capaz de cifrar e decifrar mensagem a qual foi batizada de **enigma** a qual foi patenteada por **Arthur Scherbius** em 1918, engenheiro electrotécnico alemão. A enigma era uma maquina de cifrar mensagens composta por três misturadores de letras e com 6 tomadas interligadas por plugs capazes de gerar um código com mais de um sextilhão

(1.000.000.000.000.000.000.000) de chaves. Os primeiros modelos foram exibidos nos congressos da União Postal Universal de 1923 e 1924. Tratava-se de um modelo semelhante a uma máquina de escrever, com as medidas de 65x45x35 *cm* e pesando cerca de 50 *kg*.

Figura 3.12: Enigma

Fonte: *https://revistagalileu.globo.com/Sociedade/Historia/noticia/2019/09/icone-da-criptografia-na-2-guerra-mundial-maquina-enigma-tem-exemplar-no-brasil.html*

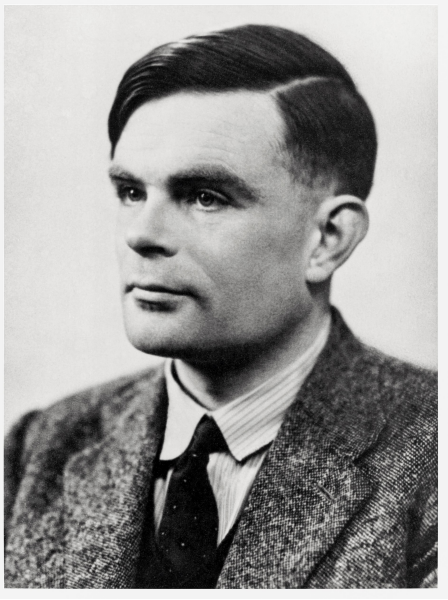
Os alemães começaram a utilizar a enigma na década de 20, gerando assim uma motivação para diversos países na busca por quebrar as cifras geradas pela mesma, alguns destes se destacaram como a França que conseguiu comprar informações sobre o funcionamento da enigma através de serviços de espionagens e a Polônia que após receber informações da França sobre o funcionamento da enigma, percebeu que um criptoanalista que tivesse fundamentos científicos poderia fazer grandes avanços na quebra das cifras geradas pela enigma, pois apesar de já existir criptoanalistas, quase todos eram linguistas, isto é, conheciam a estrutura da linguagem, mas para decifrar a enigma precisavam conhecer a estrutura mecânica, por isso, foram atrás do matemático **Marian Adam Rejewski** por ser também um grande conhecedor da língua alemã.

Figura 3.13: Marian Adam Rejewski 1905-1980

Fonte: *https://www.geni.com/people/Marian-Rejewski/6000000044584559304*

Sabendo que os alemães enviavam uma nova senha duplicada através da senha do dia anterior no inicio do texto, senha a qual definia a posição dos três misturadores, Marian Adam Rejewski foi juntando dados em uma tabela durante dias até descobrir determinado padrão e construir as primeiras máquinas decifradoras conhecidas como **Bombas de Rejewski**, que eram capazes de calcular as possibilidades para cada misturador da enigma. O problema é que ao iniciar realmente a segunda guerra mundial os alemães aprimoraram a enigma passando de 3 para 5 misturadores e de 6 para 10 o número de tomadas, assim os poloneses resolveram compartilhar os conhecimentos com os franceses e os ingleses. Com as grandes descobertas e avanços dos poloneses o matemático inglês **Alan Mathison Turing**, que já havia se dedicado a criação de máquinas capazes de processar qualquer tipo de informação, pode aprimorar a técnica de Rejewski criando uma máquina super complexa a qual ficou conhecida como **colossus**, capaz de quebrar em 3 horas uma cifra criada pela enigma, na qual foi fundamental para a vitória dos aliados na segunda guerra mundial, conhecida também por ser a propulsora dos computadores atuais.

Figura 3.14: Alan Mathison Turing 1912-1954



Fonte: *https://www.biography.com/scientist/alan-turing*

*Sugestões de filmes de ficções científicas inspirados em fatos reais que retratam a relação entre homem e tecnologia ao longo da história da humanidade*

**A Rede Social (2010)**

O filme retrata o cotidiano de Mark Zuckerberg na criação do Facebook, aquela que ainda é a maior rede social do mundo, com mais de 50 milhões de usuários.

O longa mostra a visão empreendedora de Zuckerberg, ao conseguir identificar os anseios das pessoas em se conectar, mas também alerta para os riscos no tratamento e compartilhamento dos dados na rede.

**O jogo da imitação (2014)**

Durante a Segunda Guerra Mundial, o governo britânico monta uma equipe que tem por objetivo quebrar o Enigma, o famoso código que os alemães usam para enviar mensagens aos submarinos. Um de seus integrantes é Alan Turing (Benedict Cumberbatch), um matemático de 27 anos estritamente lógico e focado no trabalho, que tem problemas de relacionamento com praticamente todos à sua volta. Não demora muito para que Turing, apesar de sua intransigência, lidere a equipe. Seu grande projeto é construir uma máquina que permita analisar todas as possibilidades de codificação do Enigma em apenas 18 horas, de forma que os ingleses conheçam as ordens enviadas antes que elas sejam executadas.

**Risk (2016)**

O filme conta a história de como Julian Assange iniciou a criação do WikiLeaks, plataforma responsável por vazar centenas de documentos privados do governo dos Estados Unidos e de outros países.

O escandaloso vazamento de dados provocado pelo WikiLeaks reacendeu o debate sobre o tratamento e a governança de dados na internet. No último ano, Assange foi preso depois de passar 12 anos em exílio na embaixada do Equador, em Londres.

# 4 Criptografia RSA

## 4.1 Conceito e Algoritmo

O método de criptografia RSA é um tipo de criptografia de cifras assimétricas baseado exclusivamente em teoremas clássicos da teoria dos números, este método foi criado em 1978, por três professores do MIT (Massachusests Institute of Technology), R. L. Rivest, A. Shamir e L. Adleman. É um código de chave pública, usado principalmente em aplicações comerciais e bancárias, estando ligado diretamente a transações feitas pela internet.

A criptografia RSA possui um par de chaves, uma chave pública (que pode ser conhecida por todos) e uma chave privada (que deve ser mantida em sigilo). Toda mensagem cifrada usando uma chave pública só pode ser decifrada usando a respectiva chave privada. Para a geração das chaves precisamos:

1) Escolher de forma aleatória dois números inteiros e primos muito grandes $p$ e $q$; (Obs: existem fórmulas matemáticas as quais possibilita encontrar primos grandes, a caráter de exemplo, temos o pequeno teorema de Fermat ou também podemos fazer o teste probabilístico para a primalidade)

2) Calcular n tal que $n = p.q$;

3) Calcular a Função Totiente de Euler (**Definição 2.6**) em n onde $\phi(n) = (p-1)(q-1)$;

4) Escolher um inteiro $e$, tal que $1 < e < \phi(n)$ onde $e$ e $\phi(n)$ sejam coprimos; (**Definição 2.5**)

5) Calcular $d$ de forma que $de \equiv 1 \ mod \ \phi(n)$, ou seja, $d$ é o inverso multiplicativo de $e$ em $mod \ \phi(n)$. (**Definição 2.8**)

Diremos que o par $(n, e)$ será a chave de codificação e o par $(n, d)$ chave de decodificação.

## 4.2 Pré-codificação

Com base na sequência dada acima, podemos perceber que a mensagem a ser criptografada em RSA deve está escrita apenas com números, portanto, devemos criar uma maneira de converter a mensagem em uma sequência de números, quando a mesma é um texto heterogêneo e também quando não há números, apenas palavra. É possível criptografar, sem a necessidade de conversão, uma mensagem na qual a informação é escrita apenas com números, porém a criptografia se torna mais frágil.

O processo de pré-codificação advém de convertemos os algarismos, espaçamento entre as palavras e as letras em números usando uma tabela de conversão de domínio público, como por exemplo a tabela abaixo, e em seguida dividimos em blocos menores $b_i$.

Figura 4.1: Tabela de pré-codificação

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| A<br>10 | B<br>11 | C<br>12 | D<br>13 | E<br>14 | F<br>15 | G<br>16 | H<br>17 | I<br>18 | J<br>19 |
| K<br>20 | L<br>21 | M<br>22 | N<br>23 | O<br>24 | P<br>25 | Q<br>26 | R<br>27 | S<br>28 | T<br>29 |
| U<br>30 | V<br>31 | W<br>32 | X<br>33 | Y<br>34 | Z<br>35 | ESPAÇAMENTO<br>36 | | | |
| 0<br>37 | 1<br>38 | 2<br>39 | 3<br>40 | 4<br>41 | 5<br>42 | 6<br>43 | 7<br>44 | 8<br>45 | 9<br>46 |

Fonte: autor

Vale salientar que precisamos fazer cada número ou letra corresponder a um número com igual quantidade de algarismos para evitar ambiguidades. Se fizéssemos, por exemplo, A corresponder ao número 1, B ao 2, e assim por diante, não teríamos como distinguir AB de L. A divisão da mensagem codificada em blocos $0 < b_i < n$ deve ser arbitrária. Por exemplo, usando a tabela a cima, podemos converter a frase ”Meu Piauí”no número ou bloco geral $B$

$$B = 2214303625181030 18.$$

Como $b_i < n$, temos antes de tudo que conhecermos o valor de $n = pq$, por exemplo, se escolhermos $p = 5$ e $q = 11$, então $n = 55$. Neste caso, a mensagem, cuja conversão numérica foi feita acima, pode ser decomposta nos seguintes blocos:

$b_1 = 2$, $b_2 = 21$, $b_3 = 4$, $b_4 = 30$, $b_5 = 36$, $b_6 = 2$, $b_7 = 51$, $b_8 = 8$, $b_9 = 10$, $b_{10} = 30$, $b_{11} = 18$.

Note que a pré-codificação acima não é única, pois como foi dito acima a escolha dos blocos $b_i$ é arbitrária e que a decodificação ficaria comprometida se iniciarmos um bloquinho com 0, já que, por exemplo, não temos como distinguir o bloco 018 do bloco 18.

## 4.3 Codificação

Agora que sabemos o que é e como fazer a pré-codificação podemos ir a codificação propriamente dita. Nesta etapa precisaremos seguir os passos de 1) a 4) da subseção 4.1, isto é, escolher dois números inteiros e primos $p$ e $q$, calcular $n = pq$, calcular a Função Totiente de Euler em $n$ ($\phi(n) = (p-1)(q-1)$ definição **2.7** ) e escolher um inteiro $e$, tal que $1 < e < \phi(n)$ onde $e$ e $\phi(n)$ sejam coprimos, visto que $(n, e)$ é a chave de codificação e os passos elencados se faz necessários para escolhermos o $e$. Todo bloco $b_i$ que adquirimos no passo da pré-codificação será codificado à parte e a mensagem codificada consistirá na sequencia dos blocos codificados.

Em nosso exemplo temos $n = 5.11 = 55$ e $\phi(n) = (5-1)(11-1) = 40$. Para facilitar os cálculos escolheremos o $e$ como o menor primo que não divide 40, logo $e = 3$, portanto temos como chave de codificação pública o par $(n, e) = (55, 3)$. A codificação de um bloco $b_i$ será dada pela seguinte definição ou regra de codificação

$C(b_i)$ = resto da divisão de ${b_i}^e$ por $n$, sendo $b_i$ um bloco da mensagem.

Em expressões de aritmética modular dizemos,

$C(b_i) \equiv {b_i}^e \ mod\ n$, com $0 < C(b_i) < n$.

Portanto, codificando todo bloco $b_i$ do exemplo acima adquirimos:

Como $b_1 = 2 = b_6$, temos $2^3 \equiv\ 2^3\ mod\ 55$, então $\mathbf{C(2) = 2^3 = 8}$.

Como $b_2 = 21$, temos $\begin{cases} 21 \equiv 21\ mod\ 55 \\ 21^2 \equiv 1\ mod\ 55 \end{cases}$, então pela propriedade 1) decorrente da **definição 2.8** $21.21^2 \equiv\ 21.1\ mod\ 55 \Leftrightarrow 21^3 \equiv\ 21\ mod\ 55$, logo, $\mathbf{C(21) = 21}$.

Como $b_3 = 4$, temos $4^3 = 64$ e $64 - 9 = 55$, então $4^3 \equiv\ 9\ mod\ 55$, logo, $\mathbf{C(4) = 9}$.

Como $b_4 = 30 = b_{10}$, temos $\begin{cases} 30 \equiv 30 \ mod\ 55 \\ 30^2 \equiv 20 \ mod\ 55 \end{cases}$, então pela propriedade 1) decorrente da **definição 2.8** $30.30^2 \equiv 30.20 \ mod\ 55 \Leftrightarrow 30^3 \equiv 600 \equiv 50 \ mod\ 55$, logo, $\mathbf{C(30) = 50}$.

Como $b_5 = 36$, temos $\begin{cases} 36 \equiv 36 \ mod\ 55 \\ 36^2 \equiv 31 \ mod\ 55 \end{cases}$, então pela **proposição 2.2** $36.36^2 \equiv 36.31 \ mod\ 55 \Leftrightarrow 36^3 \equiv 1116 \equiv 16 \ mod\ 55$, logo, $\mathbf{C(36) = 16}$.

Como $b_7 = 51$, temos $51 \equiv -4 \ mod\ 55$, então $51^3 \equiv -64 \equiv -9 \equiv 46 \ mod\ 55$, logo, $\mathbf{C(51) = 46}$.

Como $b_8 = 8$, temos $8^3 = (2^1.2^2)^3$ e $\begin{cases} 2^3 \equiv 8 \ mod\ 55 \\ 2^6 \equiv 9 \ mod\ 55 \end{cases}$, então pela **proposição 2.2** $2^3.2^6 \equiv 8.9 \equiv 72 \equiv 17 \ mod\ 55$ , logo, $\mathbf{C(8) = 17}$.

Como $b_9 = 10$, temos $10^3 \equiv 1000 \equiv 10 \ mod\ 55$, então $\mathbf{C(10) = 10}$.

Como $b_{11} = 18$, temos $\begin{cases} 18 \equiv 18 \ mod\ 55 \\ 18^2 \equiv 49 \ mod\ 55 \end{cases}$, então pela **proposição 2.2** $18.18^2 \equiv 18.49 \ mod\ 55 \Leftrightarrow 18^3 \equiv 882 \equiv 2 \ mod\ 55$, logo, $\mathbf{C(18) = 2}$.

Assim, fazendo a substituição de cada bloco $b_i$ original pelos correspondentes blocos $b'_i = C(b'_i)$ codificados, obtemos:

$b'_1 = 8$, $b'_2 = 21$, $b'_3 = 9$, $b'_4 = 50$, $b'_5 = 16$, $b'_6 = 8$, $b'_7 = 46$, $b'_8 = 17$, $b'_9 = 10$, $b'_{10} = 50$, $b'_{11} = 2$.

Portanto, a mensagem codificada $(8-21-9-50-16-8-46-17-10-50-2)$ pode ser enviada em quaisquer meios de comunicação sem grandes riscos de ser decifrada (mais detalhes de sua segurança em **4.6**) caso seja interceptada por terceiros.

## 4.4 Decodificação

A decodificação de uma cifra criptografada pelo método RSA é o processo que o receptor da mensagem faz para transformar cada bloco codificado em seu respectivo bloco original e depende do par $(n, d)$ o qual chamamos de chave privada ou chave de decodificação. De acordo com o item 5) da subseção 2.1, temos que a regra na qual

permite encontrarmos o valor de $d$ é dada por:

$de \equiv 1 \ mod \ \phi(n)$, onde $d$ é o inverso multiplicativo de $e$ em $\ mod \ \phi(n)$.

Note que para o exemplo acima temos como um dos valores possíveis $d = 27$, pois $27.3 \equiv 1 \ mod \ 40$, porém em exemplos mais complexos teríamos grandes dificuldades em encontrarmos o valor de $d$ por tentativas aleatórias. Portanto, em casos onde o valor de $d$ não for perceptível, usaremos o algoritmo de Euclides estendido a $e$ e $\phi(n)$. Em nosso caso temos que $n = 55$, $e = 3$ e $\phi(n) = 40$. Aplicando o algoritmo para encontrar $d$ temos que

$40 = 13.3 + 1$, donde $1 = 40 + (-13).3$

Logo, o inverso multiplicativo de 3 módulo 40 é -13. Precisamos que $d$ seja positivo, pois vamos usar $d$ como expoente de potências. Portanto, $d = 40 - 13 = 27$ que é o menor inteiro positivo congruente a -13 módulo 40.

Conhecendo $d$ e sendo $b'_i$ um bloco da mensagem codificada, temos que a decodificação do bloco $b'_i$ será dada pela seguinte definição ou regra de decodificação

$D(b'_i)$ = resto da divisão de $b'^{d}_i$ por $n$.

Em termos de aritmética modular dizemos,

$b'^{d}_i \equiv \ D(b'_i) \ mod \ n$, com $0 < D(b'_i) < n$.

Portanto, para decodificar o primeiro bloco $b'_1 = 8$ da mensagem codificada precisamos calcular o resto da divisão de $8^{27}$ por 55, isto é, calcular $D(8)$, onde

$8^{27} \equiv \ D(8) \ mod \ 55$.

Como $8^3 \equiv 17 \ mod \ 55$, então pela **proposição 2.2**,

$(8^3)^3 \equiv 17^3 \ mod \ 55$

$\equiv 17^2.17 \ mod \ 55$

$\equiv 14 \ . \ 17 \ mod \ 55$

$\equiv 238 \ mod \ 55$

$\equiv 18 \ mod \ 55$

Assim $8^9 \equiv 18 \ mod \ 55$, dai,

$(8^9)^3 \equiv 18^3 \ mod \ 55$

$\equiv 18^2.18 \ mod \ 55$

$\equiv 49.18 \ mod \ 55$

$\equiv 882 \ mod \ 55$

$\equiv 2 \ mod \ 55$

Logo, $D(8) = 2$, que é o primeiro bloco da mensagem pré-codificada. O processo é análogo para os demais blocos da mensagem codificada, por isso apresentaremos apenas os resultados

$D(21) = 21$, $D(9) = 4$, $D(50) = 30$, $D(16) = 36$, $D(46) = 51$, $D(17) = 8$, $D(10) = 10$, $D(2) = 18$.

## 4.5 Funcionamento do RSA

Para que o método acima funcione e seja realmente útil, precisamos encontrar a mensagem original ao decodificar a mensagem criptografada. Portanto, adotando as notações usadas anteriormente, onde $p$ e $q$ são primos distintos, $n = pq$, $(n, e)$ chave de codificação, $(n, d)$ chave de decodificação, $0 < b_i < n$ bloco da mensagem pré-codificação, $b'_i = C(b_i)$ bloco da mensagem codificada e $D(b'_i)$ a decodificação do bloco $b'_i$, provaremos que:

Se $D(b'_i) \equiv \ b_i \ mod \ n$, então, $\ D(b'_i) = b_i$.

Já que tanto $D(b'_i)$ quanto $b_i$ estão no intervalo fechado de 1 a $n - 1$, logo só podem ser congruentes módulo $n$ se forem iguais. Isto esclarece porque carecemos eleger $b_i$ inferior que $n$ e porque havemos de manter os blocos separados, inclusive depois da codificação. Se não assumíssemos estes cuidados, continuaríamos obtendo blocos congruentes depois da decodificação, mas eles não seriam necessariamente iguais. Em outras palavras, não teríamos de volta a mensagem original o que, convenhamos, não seria muito satisfatório.

Portanto, o que devemos mostrar é que

$D(b'_i) \equiv \ b_i \ mod \ n$, daí, $\ D(b'_i) = b_i$.

Por definição e o processo, temos que

i) $C(b_i) = b'_i \equiv \ b_i^e \ mod \ n$

ii) $C(b_i)^d = b_i'^d \equiv\ D(C(b_i))\ mod\ n$

Como $d$ é o inverso de $e$ módulo $\phi(n)$, então

iii) $ed = 1+k\phi(n)$ para algum $k$ inteiro. Assim, pela **proposição 2.2** e usando as equações i) e ii), temos que:

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

Usando iii):

iv) $b_i^{1+k\phi(n)} \equiv\ D(C(b_i))\ mod\ n$

Se $p|b_i$ implica que

$b_i \equiv 0\ mod\ p$,

então

$b_i^{ed} \equiv 0\ mod\ p$.

Implicando assim que $b_i^{ed} \equiv\ b_i\ mod\ p$,

portanto

$D(C(b_i)) \equiv\ b_i\ mod\ p$.

Analogamente se $q|b_i$. Agora, supondo que $p$ e $q$ não dividam $b_i$, pelo Pequeno Teorema de Fermat tem-se que

v) $b_i^{p-1} \equiv 1\ mod\ p$,

e

vi) $b_i^{q-1} \equiv 1\ mod\ q$,

o que implica

vii) $b_i^{(p-1)(q-1)} \equiv 1^{q-1}\ mod\ p$,

e

viii) $b_i^{(p-1)(q-1)} \equiv 1^{p-1}\ mod\ q$.

Usando vii) e viii), e a **proposição 2.3**, temos que

$b_i^{\phi(n)} \equiv 1\ mod\ pq$

logo

$b_i^{\phi(n)^k} b \equiv\ b\ mod\ n$.

Usando transitividade e iv) obtem-se

$D(C(b_i)) \equiv b_i \ mod \ n.$

Logo o bloco $b_i$ é igual ao bloco $D(b'_i)$.

## 4.6 Segurança

Como o sistema RSA é um sistema de chave pública, e tem $p$, $q$ e $n = pq$ como parâmetros do sistema, sendo a chave de codificação $(n, e)$ a chave pública (acessível para qualquer usuário) e a chave de decodificação $(n, d)$ a chave privada (restrito), o sistema somente será seguro se for difícil calcular $d$ quando apenas $n$ e $e$ são conhecidos.

Como visto anteriormente, precisamos encontrar $p$ e $q$ para podermos calcular $\phi(n) = (p-1)(q-1)$ e em seguida resolvermos a congruência $ed \equiv 1 \mathrm{mod} \phi(n)$, para encontrarmos, portanto, $d$. Para Coutinho (2003) só podemos quebrar códigos se conseguirmos fatorar $n$, mas quando esse $n$ é grande, fatorá-lo é uma tarefa difícil já que não conhecemos algoritmos de fatoração rápidos que tornem a atividade fácil.

Então quão grande deve ser $n$? Segundo a RSA security (empresa fundada pelos criadores do sistema RSA), as chaves de 2048 bits são suficientes para manter informações em segurança até 2030. Uma chave RSA de 3072 bits de comprimento deveria ser usada se a segurança for necessária para além de 2030.

Segundo Rosseau e Saint-Aubin (2015) desde a implementação do sistema RSA, muitos estudos tem sido desenvolvidos necessariamente sobre métodos de fatoração, mas sem muito sucesso, já que o sistema permanece não quebrado. Para os autores, não é possível saber ainda se quebrar o RSA é equivalente a descobrir a fatoração ou se existem alternativas mais baratas, porém o que se sabe é que todos os esforços até o momento em quebrá-lo usando técnicas que não envolvam a fatoração de $n$ não tiveram sucesso.

# 5 Proposta pedagógica para o estudo da matemática por meio da Criptografia RSA no Ensino Básico

Apesar da criptografia esta intimamente ligada ao nosso dia-a-dia, como por exemplo na troca de emails e compras na internet, poucas pessoas a conhecem ou utilizam apenas de forma passiva. Entretanto, mesmo com toda a sua utilidade e avanços tecnológicos, este ainda é um tema pouco presente nos livros didáticos, principalmente no ensino fundamental.

A Criptografia RSA é um recurso próprio que pode ser incrementado no ensino da matemática, uma vez que os principais algoritmos criptográficos fazem uso de vários conteúdos da mesma. Além disso é um tema que desperta interesse por si, pois permite ao professor desenvolver estrategias e abordagens capazes de provocar o interesse dos alunos pela matemática, mostrando não somente o "como funciona", mas também o "quando não funciona". Portanto, com o auxilio de uma plataforma de rede social, que é um dos elementos desta proposta, o professor pode explorar o conteúdo de criptografia de forma gradativa, pois, após revelar as informações discutidas entre os dois alunos, o professor poderá sugerir para os dois alunos integrantes da conversa, criar um outro diálogo e fazer a conversão para a cifra de César e com isso reapresentar a turma. Assim, espera-se que todos percebam que mesmo com acesso a mensagem, não se sabe o conteúdo da mesma, o que permite ao o professor explorar a área da Criptoanálise junto aos alunos e mostrar a fragilidade da cifra de César. Assim, o professor pode percorrer todo o campo histórico da Criptografia, isso explica a criação da plataforma de rede social.

## 5.1 Objetivos

Neste capítulo propomos uma atividade com o objetivo de introduzir aplicações matemáticas junto a noção de criptografia RSA, mostrando como ela é importante em nosso dia a dia, principalmente em transações feitas pela internet, e para seu desenvol-

vimento, se faz necessário a criação de uma plataforma de rede social com finalidade didática na qual é possível de forma proposital a interceptação da comunicação entre duas pessoas de forma que ambas não percebam a presença do terceiro. Portanto, sendo o professor o interceptador da conversa entre dois alunos com tema previamente escolhido pelo professor, o mesmo pode expor para todos da turma o seu conteúdo, fazendo com que os mesmos façam analogia e questionamentos quanto a segurança de outras redes sociais, compras na internet, uso do cartão de credito, entre outros e percebam a necessidade de criar métodos que protejam não somente as conversas como também dados bancários e qualquer outra transação feita com o uso da tecnologia. Portanto a atividade a ser desenvolvida é uma tentativa de relacionar conteúdos matemáticos com suas aplicações, pois poderá ser aplicada em momento oportuno de aula em parceria com a plataforma de rede social. É importante que a atividade seja aplicada ao término do capítulo de Múltiplos e Divisores para os alunos do 6º ano e para os alunos de um nível maior, após uma breve revisão do capítulo citado.

## 5.2 Planejamento da proposta

Para uma melhor aplicação da proposta de atividade, se faz necessário, indispensavelmente, uma breve apresentação do contexto histórico da criptografia, ao qual sugerimos a apostila 7: Criptografia de Severino Collier Coutinho e O Livro dos Códigos de Simon Singh. Apresentar ou revisar conteúdos clássicos da Teoria dos Números como: Divisibilidade e Congruências.

A exploração destes conteúdos pode ser feita em no mínimo 4 encontros, nos quais podemos dividi-los da seguinte maneira:

**Encontro 1** Trabalhar o conteúdo de Múltiplos e Divisores com o objetivo dos discentes saber elaborar e resolver problemas de Máximo Divisor comum, usando o Algoritmo da Divisão, resolver problemas que envolvam os conceitos de Máximo Divisor Comum e Mínimo Múltiplo Comum e números primos.

**Encontro 2** Trabalhar o conteúdo de Congruência explorando suas propriedades, para o qual deixamos como sugestão a apostila 7: Criptografia de Severino Collier Coutinho.

**Encontro 3** Nesse encontro deve ser trabalhado os fragmentos históricos da

Criptografia, destacando seu papel ao longo da história da humanidade.

**Encontro 4** Aqui o professor deve unir os conteúdos matemáticos trabalhados nos encontros 1 e 2 com a criptografia apresentada no encontro 3 para que se possa pôr em desenvolvimento a atividade descrita a seguir.

Identificação: Atividade prática de Matemática

Prof. Kelvis Moraes da Silva

E. M. Antonio Pereira Lopes

Série: 7º ano do ensino fundamental

Tema: Múltiplos e Divisores uma abordagem por meio da Criptografia

Situação problema: Codificar e decodificar uma mensagem usando tabelas e operações aritméticas.

Objetivos específicos: Trabalhar a ideia de criptografia através de simulações de situações presente no cotidiano.

Conceitos-chave: Múltiplos, Divisores e Criptografia.

Conhecimentos prévios: Analise de gráficos e tabelas, operações aritméticas.

Recursos necessários: Computador/ celular com internet, lousa e pincel.

Tempo: 2 h/aulas(120 min)

Avaliação: Envolvimento na atividade e cooperação.

## 5.3 Aplicação da proposta

O professor deve escolher em meio a turma dois alunos(aluno 1 e aluno 2) e pedir que:

1) ambos acessem a plataforma de rede social, efetuem o cadastro e em seguida o login;

2) o aluno 1 deverá enviar a mensagem (oi) para o aluno 2 e o aluno 2 respondê-lo com o intuito de averiguar se o chat está funcionando corretamente;

3) O aluno 1 deverá repassar o texto abaixo para o aluno 2 no chat sem que os demais alunos veja.

Texto: *A Criptografia RSA, Matemática e suas aplicações*

4) O professor deverá compartilhar sua tela para os demais alunos e mostrar o conteúdo exposto pelo aluno 1 para o aluno 2.

5) O professor deverá expor o conceito de criptografia e seu contexto histórico.

6) O professor deverá explicar o funcionamento da Cifra de César. Sugerimos para os passos 5) e 6) o capítulo 3 desse trabalho.

7) O professor deverá pedi para o aluno 1 repassar a mesma mensagem(*A Criptografia RSA, Matemática e suas aplicações*) criptografada pelo método de Cézar para o aluno 2.

8) O professor deverá explicar para os alunos que mesmo com acesso a conversa entre os alunos 1 e 2 aparentemente não é possível identificar seu conteúdo.

9) O professor deverá mostrar aos alunos que a mensagem pode ser decifrada usando a contagem de frequência das letras. Logo, se faz necessário o uso de uma cifra mais forte.

10) Como consequência do passo 9) e 6), o professor deverá explicar aos alunos como pré-codificar e codificar usando criptografia RSA.

11) O professor deverá pedi para que o aluno 1 criptografe e repassa a mesma mensagem(*oi*) criptografada pelo método de Criptografia RSA para o aluno 2 e em seguida repetir o passo 4). Se julgar necessário, o professor pode sortear outros dois alunos.

12) O professor deverá explicar para os alunos que é possível decriptar a mensagem.

13) O professor deverá explicar para os alunos porque o método de criptografia RSA funciona.

*A proposta de atividade acima teve sua aplicação comprometida devido a ocorrência da pandemia do corona vírus.*

# 6 Considerações Finais

No decurso desse trabalho tivemos como objetivo a elaboração de um material adequado para enriquecer a prática do professor de matemática atuante na Educação Básica, lhe ofertando um embasamento teórico e prático sobre criptografia, de forma que ele possa se utilizar desses para contextualizar conteúdos do currículo básico escolar.

A Criptografia é um tema interessante e motivante, porém a falta de conhecimento da mesma, nos fez mergulhar na sua história, conhecendo sua importância no desenvolvimento da sociedade e nos surpreendendo com o relevante envolvimento da matemática na sua evolução e por sua vez elaborar propostas de engajamento da mesma em sala de aula, enriquecendo a aplicação do conteúdo matemático e oferecendo maior preparo aos discentes em relação aos meios digitais. Ainda que a criptografia tenha achado na matemática a solução para seus problemas de segurança obtendo uma cifra excepcionalmente eficaz, essa pode esta ligeiramente ameaçada com o avanço da computação quântica ao qual deixamos o aprofundamento sobre tal tema ao leitor, porém deixamos como sugestão de leitura o livro “Computação Quântica: A Realidade de uma Nova era”de Claude Falbriard e Ines Brosso.

# Referências Bibliográficas


[1] COUTINHO, Severino Collier. **Criptografia**. 1 ed. Rio de Janeiro. IMPA. 2015.

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

[3] COUTINHO, Severino Collier: **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2005, ISBN 9788524401249

[4] SINGH, Simon. **O Livro dos Códigos**. trad. Jorge Calife. 4 ed. Rio de Janeiro. Record. 2004.

[5] COUTO, Sérgio Pereira. **Códigos & Cifras da antiguidade à era moderna**. 1 ed. Rio de Janeiro. Novaterra. 2008.

[6] **Coleção de recursos educacionais.** Disponível em: <https://m3.ime.unicamp.br/recursos/search:criptografia>. Acesso em: 23 mar. 2020.

[7] MIGUEL, A.; MIORIM, M. A. **História na educação matemática: propostas e desafios**. Belo Horizonte: Autêntica, 2004.

[8] ROSSEAU, C.; SAINT-AUBIN, Y. **Matemática e Atualidade** Volume 1. 1. ed. Rio de Janeiro: SBM, 2015. (Coleção PROFMAT).

[9] HEFEZ, A. Aritmética. 1. ed. Rio de Janeiro: SBM, 2014.