# A Matemática da Criptografia RSA

**Isabella Tito de Oliveira Silva**[1] **- isabella.tito@estudante.ufcg.edu.br**
**Maria Débora de Oliveira Silva**[1]**- debora.oliveira@estudante.ufcg.edu.br**
**Daniel Cordeiro de Morais Filho**[1] **- daniel@mat.ufcg.edu.br**

[1]Universidade Federal de Campina Grande, Unidade Acadêmica de Matemática - Campina Grande, PB, Brasil. Parcialmente financiado pelo MEC/FNDE/PET

***Resumo:*** *Desde a antiguidade, a humanidade buscou um jeito de esconder informações sigilosas sem que pessoas indesejadas tivessem acesso a elas. Durante anos, foram buscadas formas para se, acaso uma mensagem fosse interceptada, ela não pudesse ser lida, um exemplo bastante simples são as mensagens cifradas trocando letras por símbolos. Porém, havia um problema: se o interceptor encontrasse o artifício utilizado para esconder as mensagens, o método de criptografia estaria quebrado e não seria mais útil. Dessa forma, era necessário estabelecer uma maneira segura na qual o receptor tivesse acesso ao método utilizado, podendo decodificar e ler a mensagem, gerando o que chamamos Problema da Distribuição de Chaves. Em decorrência desse Problema, surgiu um método muito conhecido e utilizado para a segurança de dados, a Criptografia RSA. Sendo assim, o objetivo desse trabalho é entender como ocorre a codificação e decodificação do método RSA, além de compreender a matemática desse método, que permite a troca segura de mensagens e evita qualquer tipo de violação. Vale ressaltar que o presente trabalho é fruto de uma atividade do Grupo PET-Matemática-UFCG, sob orientação do Tutor Prof. Dr. Daniel Cordeiro de Morais Filho, utilizando bibliografias sobre o assunto, como livros e dissertações.*
***Palavras-chave****: Problema da Distribuição de Chaves; Codificação de mensagens; Números primos.*

## 1. Introdução

Esconder uma mensagem é uma atividade muito comum, seja em uma situação banal, como brincar com a *língua do P* ou decifrar uma frase em um jogo de gibi ou, em outra situação, esconder informações importantes, como dados pessoais ou segredos governamentais. Manter essas informações importantes em segurança é uma tarefa de extrema necessidade, visto que, uma vez em mãos erradas, podem afetar uma nação, causar dívidas, problemas pessoais, entre outros. Por esse motivo, foram criados diversos métodos com a finalidade de que uma mensagem interceptada não pudesse ser decifrada. A técnica utilizada para transmitir informações cifradas chama-se *criptografia.*

Na criptografia, as *chaves* desenvolvem um papel muito relevante, elas guardam as informações utilizadas nos processos de codificação e decodificação, que dão acesso às mensagens. O termo "chave" faz analogia a uma mensagem trancada em uma caixa com um cadeado, onde apenas a chave certa fornece a mensagem guardada. É chamada *chave simétrica ou única* quando tanto o emissor quanto o receptor possuem a chave para abrir o cadeado, enquanto é chamada *chave assimétrica* quando o emissor utiliza um cadeado e apenas o receptor tem a chave para abri-lo.

Inicialmente, foram pensadas em *criptografias de chave simétrica*, como, por exemplo, a troca de letras por símbolos. Neste caso, em um texto extenso, o interceptador consegue perceber um padrão na repetição dos símbolos e, assim, pode facilmente decodificar a mensagem. Outro problema desse método é que o receptor deve conhecer a chave utilizada para criptografar a mensagem, ou seja, o emissor deve informá-lo do método. No entanto, nem sempre é possível informar pessoalmente esse código, tendo de confiar em uma terceira pessoa para fazer o intermédio, arriscando ter essas informações divulgadas.

Com as descobertas científicas e avanços tecnológicos, os computadores se tornaram amplamente acessíveis às corporações, implicando em um maior uso dos métodos de criptografia, e consequentemente, necessitando de mais pessoas para distribuir as chaves. Este problema foi denominado *Problema da distribuição de chaves*, no qual muitos pesquisadores e estudiosos se dedicaram a resolver. Segundo Singh (2004), um deles foi o matemático Whitfield Diffie (1944- ), que pensou em um método de criptografia no qual a chave utilizada para codificar não pudesse ser usada para decodificar, chamada *criptografias de chave assimétrica.*

No entanto, após anos de estudo junto ao criptógrafo Martin Hellman (1945 - ), ele não conseguiu elaborar um método como havia pensado, mas acreditava em sua ideia. Por isso, em 1975, Diffie publicou um resumo com a teoria da chave assimétrica, dando a largada a corrida pelo método. Os primeiros a passar pela linha de chegada foram os cientistas da computação, Ronald Rivest (1947 - ) e Adi Shamir (1952 - ), e o matemático Leonard Adleman (1945 - ), em 1977, dando início ao sistema *Criptografia RSA*.

A criptografia RSA é principalmente utilizada por sites para gerar certificados digitais que comprovam a autenticidade e integridade de uma mensagem. Um exemplo de empresas que usam esse tipo de criptografia é a *Amazon.com, Inc.* e, segundo Bonfim (2017), o site do Banco do Brasil.

## 2. Metodologia

O trabalho foi realizado em atividades do Grupo PET-Matemática-UFCG, através de revisões bibliográficas com textos renomados sobre o assunto, como o livro *Números Inteiros e Criptografia RSA*, do Professor Doutor Severino Collier Coutinho, e *O livro dos códigos*, de Simon Singh, Ph.D. em Física e ex editor de Ciência da BBC. Após os estudos e análise dos textos, foram realizadas reuniões com o tutor, Prof. Dr. Daniel Cordeiro, para orientação e desenvolvimento do trabalho. Em seguida, foi elaborado uma apresentação para o *XI Workshop Didático-Pedagógico de Prática de Ensino em Matemática*, uma das atividades do Grupo PET-Matemática-UFCG. Neste Workshop foi trabalhado a matemática por trás do método de Criptografia RSA, gerando discussões importantes sobre o assunto e sugestões de melhoria do trabalho.

## 3. Resultado e discussão

Como já citado, a Criptografia RSA é uma criptografia de chave assimétrica, isso significa que são utilizadas duas chaves para o processo, chamadas *Chave pública* e *Chave privada*. A chave pública é aquela divulgada pelo receptor para que as pessoas possam lhe enviar mensagens, enquanto a chave privada deve ser guardada para si, pois ela permite que a mensagem seja descriptografada pela pessoa que a possui. A forma como ocorre o processo de codificação e decodificação e como são definidas as chaves serão explicados mais à frente, mas antes iremos enunciar alguns resultados preliminares estudados.

### 3.1 Resultados preliminares

**Definição 1.** *Seja $\bar{a} \in \mathbb{Z}_n$. Dizemos que a classe $\bar{a'} \in \mathbb{Z}_n$ é o inverso multiplicativo de $\bar{a}$ se a igualdade $\bar{a} \cdot \bar{a'} = \bar{1}$ é satisfeita em $\mathbb{Z}_n$. (COUTINHO, 2005)*

**Teorema 1.** *(Teorema da inversão.) A classe $\bar{a}$ tem inverso multiplicativo em $\mathbb{Z}_n$ se, e somente se, $mdc(a, n) = 1$. (COUTINHO, 2005)*

**Teorema 2.** *(Teorema de Bézout.) Sejam $a, b \in \mathbb{Z}$ e $d = mdc(a, b)$. Então existem $r, s \in \mathbb{Z}$ tais que $d = ra + sb$. (MILIES; COELHO, 2006)*

**Teorema 3.** *(Pequeno Teorema de Fermat.) Seja $p$ um número primo e $a$ um inteiro que não é divisível por $p$. Então $a^{p-1} \equiv 1 \ (mod\ p)$. (COUTINHO, 2005)*

**Definição 2.** *(Função de Euler.) O número $\phi(n)$ é o número de inteiros positivos menores do que ou iguais a $n$, que são relativamente primos com $n$. Em especial, se $p$ é um número primo, então todos os inteiros positivos menores que $p$ são primos com $p$, ou seja, $\phi(p) = p - 1$. (COUTINHO, 2005)*

**Teorema 4.** *Se $m$, $n$ são inteiros positivos tais que $mdc(m, n) = 1$, então $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$. (COUTINHO, 2005)*

**Teorema 5.** *(Teorema Chinês dos Restos.)*

*Sejam $n_1, n_2, \ldots, n_k$ inteiros, relativamente primos dois a dois. Então o sistema*

$$\begin{aligned} x &\equiv a_1 \ (mod\ n_1) \\ &\vdots \\ x &\equiv a_k \ (mod\ n_k) \end{aligned}$$

*tem uma única solução em $\mathbb{Z}_{n_1 \cdot n_2 \cdots n_k}$. (MILIES; COELHO, 2006)*

### 3.2 Codificação

Antes de iniciar o processo de codificação é necessário que o receptor disponibilize sua chave pública contendo dois parâmetros: $n$ e $e$. Para isso, o receptor deve escolher dois primos distintos $p$ e $q$, e o produto entre eles será $n$. O parâmetro $e$ deve ser escolhido de forma que seja invertível módulo $\phi(n)$, em outras palavras, pelo Teorema 1, precisamos ter o $mdc(e, \phi(n)) = 1$. Recordando que, pelo Teorema 4 e Definição 2, podemos calcular $\phi(n)$.

Vamos dar um exemplo. Consideraremos $p = 3$ e $q = 17$, logo $n = 51$. Desse modo, aplicando o Teorema 4 e a Definição 2 em $n = 51$, temos $\phi(51) = 32$, e assim, consideraremos $e = 11$, pois $mdc(11, 32) = 1$. Portanto, a chave pública a ser disponibilizada será $(51, 11)$.

Conhecendo a chave pública escolhida pelo receptor, vamos fazer um teste e checar se o método funciona. Desse modo, criptografaremos a frase *Bombas de Turing*, remetendo a máquina criada pelo matemático e criptógrafo Alan Turing (1912–1954). Segundo o Singh (2004), a máquina recebeu esse apelido, pois sua abordagem mecânica tinha uma semelhança passageira com a *bomba de Marian Rejewski (1905-1980)*. Esse mecanismo ajudou a decifrar o código da máquina *Enigma* utilizada pelos alemães durante a guerra.

Dividiremos o processo de codificação em três passos:

1. **Pré-codificação**

   Primeiro de tudo, é necessário transformar a mensagem que desejamos enviar em números. Dessa forma, é utilizada uma tabela pré-formulada e de domínio público. Nesta tabela é necessário que todos os números tenham a mesma quantidade de dígitos para não gerar ambiguidades durante a decodificação. No exemplo a seguir, vamos utilizar a relação estabelecida na Figura 1.

Figura 1: Relação estabelecida pelos autores

| A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** | **Espaço** |
| 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 |

Fonte: Os autores

Fazendo a troca de letras pelos números na frase *Bombas de Turing*, encontramos o seguinte número:

$$12252312112937141537303128192417. \tag{1}$$

2. **Separação em blocos**

   Feito a pré-codificação, o número obtido em (1) deve ser separado em pequenos blocos, de forma a serem menores que o parâmetro $n$ e não podem começar com zero. Vale ressaltar que esta separação não é única, podendo ser feita de diversas formas. Assim, para $n = 51$, separaremos a expressão (1) da seguinte maneira:

$$12 - 25 - 2 - 31 - 21 - 1 - 29 - 37 - 1 - 41 - 5 - 37 - 30 - 3 - 12 - 8 - 19 - 2 - 41 - 7. \tag{2}$$

3. **Codificação**

   Considerando $b$ cada um dos blocos separados em (2), neste passo será utilizado a *Aritmética Modular* para encontrar o resto da divisão de $b^e$ por $n$. Desse modo, basta calcularmos a forma reduzida de

$$C(b) := b^e (mod\ n). \tag{3}$$

Lembrando que o parâmetro $e = 11$, teremos cada um dos blocos elevados a 11.° potência. Desse modo, para facilitar os cálculos, será utilizada a linguagem de programação *Python* com a fórmula $[(b^{**}e)\ \%\ n]$, onde "$**$" indicam o expoente e o símbolo "%" encontra o resto da divisão de $(b^{**}e)$ por $n$. Efetuando as operações usando a *Aritmética Modular*, temos

$$12^{11} \equiv 6\ (mod\ 51) \quad 25^{11} \equiv 19\ (mod\ 51) \quad 2^{11} \equiv 8\ (mod\ 51) \quad 31^{11} \equiv 10\ (mod\ 51) \quad 21^{11} \equiv 30\ (mod\ 51)$$
$$1^{11} \equiv 1\ (mod\ 51) \quad 29^{11} \equiv 23\ (mod\ 51) \quad 37^{11} \equiv 7\ (mod\ 51) \quad 41^{11} \equiv 14\ (mod\ 51) \quad 5^{11} \equiv 11\ (mod\ 51)$$
$$30^{11} \equiv 21\ (mod\ 51) \quad 3^{11} \equiv 24\ (mod\ 51) \quad 8^{11} \equiv 2\ (mod\ 51) \quad 19^{11} \equiv 25\ (mod\ 51) \quad 7^{11} \equiv 31\ (mod\ 51).$$

Assim, chegamos nos seguintes blocos codificados:

$$6 - 19 - 8 - 10 - 30 - 1 - 23 - 7 - 1 - 14 - 11 - 7 - 21 - 24 - 6 - 2 - 25 - 8 - 14 - 31. \tag{4}$$

O número enviado para o receptor é o encontrado em (4). Não devemos juntar os blocos novamente, pois caso o fizesse, poderia causar confusão no momento da decodificação.

### 3.3 Decodificação

Na etapa de decodificação dos blocos cifrados, o receptor precisará apenas de duas informações: $n$ e o inverso de $e$ em $\phi(n)$ (Teorema 1) que chamaremos de $d$. Pelo Teorema 2, temos $ed = 1 + k\phi(n)$, com $k$ inteiro, e assim pode-se obter $d$ da seguinte forma:

$$d \cdot e \equiv 1\ (mod\ (p-1)(q-1)).$$

Como apenas o receptor conhece os números primos $p$ e $q$, somente ele conseguirá facilmente resolver a equação usando *Aritmética Modular* sem precisar fatorar $n$, chegando em $d = 3$. Assim, a chave privada, que deve ser apenas do conhecimento do receptor, será $(p, q, d)$.

Por último, para decodificar a mensagem cifrada, ele deve encontrar o resto da divisão de $a^d$ por $n$, onde $a$ é cada um dos blocos codificados de (4). Isto é,

$$D(a) := a^d\ (mod\ n). \tag{5}$$

Aplicando os blocos (4) da mensagem codificada em (5), obtemos

$$6^3 \equiv 12\ (mod\ 51) \quad 19^3 \equiv 25\ (mod\ 51) \quad 8^3 \equiv 2\ (mod\ 51) \quad 10^3 \equiv 31\ (mod\ 51) \quad 30^3 \equiv 21\ (mod\ 51)$$
$$1^3 \equiv 1\ (mod\ 51) \quad 23^3 \equiv 29\ (mod\ 51) \quad 7^3 \equiv 37\ (mod\ 51) \quad 14^3 \equiv 41\ (mod\ 51) \quad 11^3 \equiv 5\ (mod\ 51)$$
$$21^3 \equiv 30\ (mod\ 51) \quad 24^3 \equiv 3\ (mod\ 51) \quad 2^3 \equiv 8\ (mod\ 51) \quad 25^3 \equiv 19\ (mod\ 51) \quad 31^3 \equiv 7\ (mod\ 51).$$

Observe que reescrevendo os blocos com essa nova relação de congruência, temos

$$12 - 25 - 2 - 31 - 21 - 1 - 29 - 37 - 1 - 41 - 5 - 37 - 30 - 3 - 12 - 8 - 19 - 2 - 41 - 7,$$

justamente o conjunto de blocos obtidos em (2). Neste momento, podemos juntar os números novamente e separá-los de dois em dois para utilizar a relação entre números e letras da Figura 1. Feita a relação chegamos na mensagem desejada: *Bombas de Turing*.

### 3.4 Por que funciona?

Já vimos como ocorre o processo de codificação e decodificação do método RSA, mas até agora só mostramos um caso particular. A pergunta que fica é: será que o método funciona para outros números que seguem as condições citadas, ou esse foi um caso isolado? E se funcionar para qualquer número, por que funciona? Nesta seção pretendemos responder essas perguntas.

A ideia do método é que os passos de codificação e decodificação sejam inversos, ou seja, conseguiremos voltar para o bloco pré-codificado utilizando as funções (3) e (5), além dos parâmetros definidos. Em outras palavras, desejamos mostrar que $D(C(b)) \equiv b \ (mod\ n)$, onde $C(b)$ é o resto da divisão de $b^e$ por $n$ e $D(a)$ é o resto da divisão de $a^d$ por $n$. Dessa forma, $D(C(b)) \equiv (b^e)^d \ (mod\ n) \equiv b^{ed} \ (mod\ n)$.

Logo, pelo Teorema 2, como o $mdc(e, \phi(n)) = 1$ existem $d$ e $k$ inteiros tais que $ed = 1 + k\phi(n)$. Além disso, pelo Teorema 1, concluímos que $d$ é inverso de $e$ módulo $\phi(n)$. Portanto,

$$b^{ed} \equiv b^{1+k\phi(n)} \equiv b \cdot (b^{\phi(n)})^k \equiv b \cdot b^{k(p-1)(q-1)} \ (mod\ n).$$

Sabendo que $p$ e $q$ são números primos distintos e $n = pq$, pelo Teorema 5, podemos calcular a forma reduzida de $b^{ed}$ módulo $p$ e $b^{ed}$ módulo $q$. Comecemos por $p$. Assim, temos dois casos a considerar: $p$ não divide $b$ ou $p$ divide $b$. Se a primeira situação ocorre, então pelo Teorema 3, segue

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

Caso contrário, temos

$$b^{p-1} \equiv 0(mod\ p) \Rightarrow b^{ed} \equiv b \ (mod\ p).$$

De forma análoga, fazemos para módulo $q$ e chegamos a conclusão de que a congruência vale para quaisquer $p$ e $q$. Em outras palavras, $b^{ed} - b$ é divisível por $p$ e $q$. Além disso, $p$ e $q$ são números primos distintos tais que $mdc(p, q) = 1$, então temos $b^{ed} - b$ é divisível por $n$, concluindo

$$b^{ed} \equiv b \ (mod\ n), \text{ para qualquer inteiro } b.$$

Um fator muito importante para a segurança desse método é a escolha dos números $p$ e $q$. A nível de exemplo, utilizamos números primos muito pequenos, de forma que facilmente o parâmetro $n$ possa ser fatorado, o que permite a qualquer pessoa obter $p$ e $q$ e decifrar a mensagem. Dessa forma, é necessário utilizar números primos muito grandes, dificultando ainda mais a fatoração do parâmetro $n$ e garantindo que ninguém além do receptor irá ler as mensagens enviadas. No livro de Coutinho (2005) explica como escolher esses números para o uso do método, pois não podemos apenas escolher números primos grandes, mas devemos nos certificar que a diferença entre eles não é pequena.

## 4. Conclusões

Durante o processo de criptografia apresentado neste trabalho, é possível perceber o quão importante a matemática foi para o desenvolvimento do método RSA. As propriedades da *Aritmética Modular* e o uso dos números primos, possibilitaram o desenvolvimento desse método seguro. Vale salientar, que a dificuldade de identificar a fatoração de números muito grandes em produtos de potências de primos, torna a mensagem cifrada difícil de ser quebrada.

## Agradecimentos

O presente trabalho foi parcialmente financiado pelo FNDE, Fundo Nacional de Desenvolvimento da Educação-Brasil, por meio da bolsa fornecida para o Grupo PET-Matemática-UFCG, do qual os autores fazem parte.

## Referências

BONFIM, D. H. *Criptografia RSA*. [s.n.], 2017. 49-51 p. Disponível em: ⟨https://teses.usp.br/teses/disponiveis/55/55136/tde-06042017-164507/publico/DanieleHelenaBonfim_revisada.pdf⟩. Citado na página 2.

COUTINHO, S. *Números inteiros e criptografia RSA*. [S.l.]: IMPA, 2005. Citado 2 vezes nas páginas 2 e 5.

MILIES, C. P.; COELHO, S. P. *Números: uma Introdução à Matemática*. [S.l.]: Edusp, 2006. ISBN 978-8531404580. Citado na página 2.

SINGH, S. *O livro dos códigos*. RECORD, 2004. ISBN 9788501055989. Disponível em: ⟨https://books.google.com.br/books?id=yUpTa5WLWv0C⟩. Citado 2 vezes nas páginas 1 e 3.