Um estudo sobre a Criptografia RSA

Dafne Moraes Deparis Teixeira - Universidade Federal da Fronteira Sul
Raquel Lehrer - Universidade Estadual do Oeste do Paraná

(*Recebido em 06/11/2023. Aceito em 30/11/2023. Publicado em 20/12/2023*)

Resumo: A necessidade da escrita secreta para o homem é um ponto indiscutível; desde a antiguidade até os dias atuais, o sigilo na comunicação deve ser tão velho quanto o surgimento da escrita. No decorrer do tempo, é possível perceber a evolução de códigos e cifras, que foram impulsionados pela ameaça de informações secretas acabarem nas mãos de inimigos, e também devido aos decifradores que ao descobrirem o funcionamento de uma cifra, obrigavam os cifradores a inventarem uma nova cifra desconhecida e mais segura. Apresentamos aqui alguns aspectos da Criptografia RSA, como sua história, método de funcionamento e os conceitos de matemática envolvidos. Finalizamos com um exemplo de como a Criptografia RSA funciona.

Palavras-chave: Criptografia RSA; números primos; Pequeno Teorema de Fermat.

1 Introdução

Por anos, reis e rainhas necessitavam da comunicação secreta para assuntos de disputa de território; manutenção de segredos de estado; transações militares com seus exércitos. No decorrer da história da Criptografia, é possível perceber a evolução de códigos e cifras. Isso trouxe avanços tecnológicos, que começaram com a invenção de instrumentos criptográficos que facilitavam a cifragem; e posteriormente, a invenção do telégrafo, do rádio e de máquinas que evoluíram até chegarem ao ilustre computador.

Conforme Carneiro (2017, p.4), a palavra criptografia tem origem grega, *kryptos* significa oculto, escondido, secreto, e *graphein*, escrita. Apenas ocultar a mensagem, trata-se do método chamado esteganografia, já a criptografia esconde o significado da mensagem, tornando um texto legível em um texto ilegível, para isso utiliza-se códigos ou cifras, de modo que apenas a pessoa (remetente e destinatário) que possuir a chave transformará o texto ilegível em legível novamente. As cifras podem ser classificadas em cifras de transposição e cifras de substituição. Na cifra de transposição, as letras da mensagem são reordenadas. A cifra de substituição consiste em trocar palavras, frases, sentenças ou até mesmo códigos, por outras palavras, frases, sentenças, ou códigos. Para cifrar o transmissor aplica um algoritmo, composto por uma chave, na mensagem original transformando-a no texto cifrado, o receptor da mensagem fará o caminho inverso para decifra-lá, mas para isso precisa conhecer o algoritmo e a chave, que podem ser combinados previamente. A chave é um elemento confidencial que cifra e decifra a mensagem, ela pode ser simétrica ou assimétrica. Nas cifras que usam chave simétrica, geralmente, no processo de decifragem é aplicado o oposto da chave de cifragem, ou ainda, se sabemos a chave para cifrar

obtemos, facilmente, a chave para decifrar. Já na cifra com chave assimétrica temos uma chave para cifragem e outra diferente para decifragem.

É possível observar, ao longo da história da criptografia, que a distribuição de chaves para a codificação e decodificação de mensagens sempre foi um ponto crítico, pois os criptógrafos conviviam com o risco da chave parar em mãos erradas. Além disso, o crescente uso dos computadores para cifrar comunicações importantes, implicou no aumento da demanda por distribuição de chaves, o que tornou-se impraticável tanto logisticamente quanto pelos custos exorbitantes.

Segundo Singh (2020, p. 277-279), o criptógrafo Whitfield Diffie tinha grande interesse pelo problema da distribuição de chaves. Nascido em 1944, graduou-se em matemática no Massachusetts Institute of Technology, em 1965. Ele possuía uma visão de mundo conectado, onde pessoas comuns com seus computadores interligados por linhas telefônicas nas suas casas pudessem trocar informações através de e-mails, comprar produtos pela internet, realizar transações bancárias, mas isso implicaria na necessidade de privacidade digital. Diffie teve sua visão de mundo concretizada com a ARPANet em 1969, evoluindo para Internet em 1982. Diffie conheceu Hellman e Merkle, e os três vislumbravam resolver o problema da distribuição de chaves. De acordo com Singh (2020, p. 280-281), Martin Hellman, nascido em 1945, era professor da Universidade de Stanford na Califórnia, e Ralph Merkle um refugiado intelectual. Juntos concluíram que a solução para o problema da distribuição de chaves era uma função matemática de mão única, ou seja, difícil de reverter. Após uma busca incessante, Hellman conseguiu chegar a um esquema, usando a função modular $Y^x (\text{mod } P)$, na qual não era necessária a troca de chaves, o receptor e o emissor apenas precisavam decidir juntos os valores de Y e P, sendo Y menor que P, podendo fazer isso por telefone, pois esses valores não eram a chave, portanto não eram sigilosos.

Entretanto, Diffie foi além do conquistado pelos três, chegando ao conceito de chave assimétrica. Até o momento, todas as cifras eram formadas por chaves simétricas, ou seja, para o processo de decifragem era aplicado o oposto da chave de cifragem. Já na cifra com chave assimétrica seria uma chave para cifragem e outra diferente para decifragem. Em 1975, Diffie publicou seu trabalho sobre o sistema de chaves assimétricas, porém ele ainda não havia descoberto uma cifra que preenchesse os requisitos do seu sistema.

A descoberta da função matemática que satisfazia os requisitos do sistema de chaves assimétricas foi realizada, em 1977, por Ron Rivest, Leonard Adleman e Adi Shamir, dois cientistas da computação e um matemático, respectivamente. Eles eram pesquisadores do Laboratório de Ciência da Computação do MIT, Estados Unidos. Por isso, o método de cifra de chave pública mais influente da criptografia moderna ficou conhecido como RSA. Conforme descreveu Singh (2020, p. 300), a RSA é baseada em uma função modular, na qual é colocado um número, que corresponde a mensagem a ser cifrada, o resultado disso é um texto cifrado, ou seja, outro número. Um aspecto importante dessa função de mão única é a possibilidade de escolha do valor de N, cada pessoa para personalizar sua função pode escolher um valor de N diferente. A flexibilidade de N é o que torna-a uma função de mão única reversível sob certas circunstâncias. O valor de N é obtido através da multiplicação de dois números primos p e q, o número N é a

chave pública de uma pessoa, e os números p e q correspondem à chave particular dela. A pessoa pode divulgar sua chave pública, por exemplo, colocá-la em um lista pública de chaves, onde constem as chaves de diversas pessoas. Para cifrar uma mensagem, obtemos a chave pública N do destinatário e colocamos na forma geral da função de mão única, então temos a função de mão única do destinatário. O destinatário receberá o resultado da aplicação da mensagem na sua função personalizada, ele usará sua chave particular p e q para decifrá-la.

A segurança da RSA reside no fato que os valores de p e q não são públicos, e apenas eles revertem a função de mão única utilizada. E a força da RSA reside na escolha de p e q suficientemente grandes, gerando N ainda maior, para que seja virtualmente impossível fatorar N para chegar na chave particular p e q, capaz de decifrar as mensagens. "O único problema para a segurança da criptografia de chave pública RSA é que, em alguma época no futuro, alguém possa encontrar um modo rápido de fatorar N" (Singh, 2020, p. 303).

O método de criptografia RSA que aqui apresentaremos garante, conforme Carneiro (2017, p. 97), "a transmissão de informações confidenciais através de redes inseguras e ainda a autenticação do usuário extremamente necessária em transações bancárias". Em outras palavras, ele tornou viável a comunicação através da Internet e, possibilitou o desenvolvimento da assinatura digital.

O RSA é um método de criptografia de chave pública bastante utilizado, devido a segurança que ele fornece. Esse fato, conforme já escrevemos nesse trabalho, reside na inexistência de uma forma rápida para fatorar números muito grandes. Sendo assim, na próxima seção faremos uma revisão de alguns conceitos matemáticos necessários para a descrição e fundamentação do método de Criptografia RSA, apresentados na seção 3. Na seção 4 explicaremos por que a Criptografia RSA é segura e na seção 5 apresentaremos um exemplo de como a criptografia RSA é efetivamente aplicada numa mensagem.

2 Preliminares

Nesta seção, apresentaremos os conceitos e resultados necessários para a demonstração da validade do método da criptografia RSA. Algumas demonstrações foram omitidas para uma maior fluidez da leitura, mas sempre foram indicadas referências onde tais demonstrações podem ser encontradas.

Os conjuntos numéricos utilizados serão os seguintes: $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$, o conjunto dos números naturais; $\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$, o conjunto dos números inteiros. Denotaremos por $\mathbb{N}^*$, quando $\mathbb{N} \setminus \{0\}$, e também $\mathbb{Z}^*$, quando for $\mathbb{Z} \setminus \{0\}$.

Definição 1. Sejam a, $b \in \mathbb{Z}$. Dizemos que b *divide* a se existir algum $q \in \mathbb{Z}$ tal que $a = b \cdot q$. Utilizamos a notação $b \mid a$. Caso b não divide a, denotamos por $b \nmid a$.

Definição 2. Um número inteiro p é chamado *número primo* se as seguintes condições se verificam: $p \neq 0$, $p \neq \pm 1$ e os únicos divisores de p são ± 1, $\pm p$.

Se um número inteiro $n \neq \{0, \pm 1\}$ não é primo, então dizemos que n é *composto*. Nesse caso, n não possui apenas os divisores ± 1 e $\pm n$. Dessa maneira, devem existir números inteiros u e v tais que $1 < u < n$ e $1 < v < n$ e $n = u \cdot v$.

Definição 3. Sejam a e b dois números inteiros, $a \neq 0$ ou $b \neq 0$. Dizemos que $d \in \mathbb{Z}$ é o *máximo divisor comum* de a e b se cumpre as seguintes condições:

i) $d > 0$;

ii) $d \mid a$ e $d \mid b$;

iii) se d' é um inteiro tal que $d' \mid a$ e $d' \mid b$, então $d' \mid d$ (ou seja, todo divisor comum de a e b também é divisor de d).

Definição 4. Sejam a e b dois inteiros, $a \neq 0$ ou $b \neq 0$. Dizemos que a e b são *primos entre si (ou coprimos)* quando $mdc(a, b) = 1$.

Definição 5. Sejam a e b inteiros quaisquer e m um inteiro maior que 1. Dizemos que *a é congruente a b módulo m* se $m \mid (a - b)$. Denotamos isto por $a \equiv b (\text{mod } m)$. Se $m \nmid (a - b)$ dizemos que *a é incongruente a b módulo m* e denotamos $a \not\equiv b (\text{mod } m)$.

Segue diretamente das definições acima a seguinte proposição:

Proposição 6. *Se a, b e m são inteiros, com $m > 1$, temos que $a \equiv b (mod\ m)$ se, e somente se, existir um inteiro k tal que $a = b + k \cdot m$.*

Proposição 7. *Seja m um número inteiro tal que $m > 1$.*

(a) Se a e b são inteiros tais que $a \equiv b (mod\ m)$, então $a - b \equiv 0 (mod\ m)$.

(b) Se a, b, c e d são inteiros tais que $a \equiv b (mod\ m)$ e $c \equiv d (mod\ m)$, então $a + c \equiv b + d (mod\ m)$.

(c) Se a, b, c e d são inteiros tais que $a \equiv b (mod\ m)$ e $c \equiv d (mod\ m)$, então $a - c \equiv b - d (mod\ m)$.

(d) Se a, b, c e d são inteiros tais que $a \equiv b (mod\ m)$ e $c \equiv d (mod\ m)$, então $a \cdot c \equiv b \cdot d (mod\ m)$.

(e) Se a e b são inteiros tais que $a \equiv b (mod\ m)$, então $a \cdot x \equiv b \cdot x (mod\ m)$, para todo inteiro x.

(f) Seja d um inteiro tal que $mdc(d, m) = 1$. Se a e b são inteiros tais que $a \cdot d \equiv b \cdot d (mod\ m)$, então $a \equiv b (mod\ m)$.

(g) Se a, b e d são inteiros, com $d \neq 0$, tais que $a \cdot d \equiv b \cdot d (mod\ m \cdot d)$, então $a \equiv b (mod\ m)$.

(h) Se a e b são inteiros tais que $a \equiv b (mod\ m)$, então $a^x \equiv b^x (mod\ m)$ para todo natural x.

A demonstração desta proprosição pode ser encontrada em Silva e Gomes (2018, p. 167 - 169).

Definição 8. Sejam a, r e m números inteiros, com $m > 1$. Dizemos que r é um *resíduo de a módulo m* se $a \equiv r(\text{mod } m)$.

Definição 9. Seja $m \in \mathbb{Z}$ tal que $m > 1$. Dizemos que o conjunto de números inteiros $\{r_1, r_2, \ldots, r_m\}$ é um *sistema completo de resíduos módulo m* se

(1) $r_i \not\equiv r_j(\text{mod } m)$ para $i \neq j$;

(2) para todo inteiro n existe um r_i tal que $n \equiv r_i(\text{mod } m)$.

Exemplo 1. Os conjuntos $\{0, 1, 2, 3, 4\}$ e $\{5, 16, 17, 28, 29\}$ são sistemas completos de resíduos módulo 5.

A demonstração da proposição a seguir pode ser encontrada em Santos (2020, p. 34).

Proposição 10. *Se k inteiros $r_1, r_2, \ldots, r_k$ formam um sistema completo de resíduos módulo m então $k = m$.*

Definição 11. Sejam $a \in \mathbb{Z}$ e m um inteiro maior que 1. Uma solução de $a \cdot x \equiv 1(\text{mod } m)$ é chamado de *inverso de a módulo m.*

Proposição 12. *Seja m um inteiro maior que 1. O número inteiro a possui inverso módulo m se, e somente se, $mdc(a, m) = 1$.*

Tal resultado pode ser encontrado em Coutinho (2009, p. 82-83).

Demonstraremos agora dois importantes teoremas em Teoria dos Números e com aplicabilidade no método RSA. Conforme Boyer (2012, p. 310), o Pequeno Teorema de Fermat foi uma conjetura de Fermat, sendo Euler o primeiro a publicar uma demonstração dela. E, a partir disso, Euler demonstrou uma afirmação um pouco mais geral, que trata-se do Teorema de Euler.

Teorema 13. *(Pequeno Teorema de Fermat) Seja p primo. Se $p \nmid a$ então $a^{p-1} \equiv 1(mod\ p)$.*

Prova. Sabemos que o conjunto formado pelos p números $0, 1, 2, \ldots, p-1$ constitui um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de $\{0, 1, 2, \ldots, p-1\}$. Vamos agora considerar os números $a, 2 \cdot a, 3 \cdot a, \ldots, (p-1) \cdot a$. Como $mdc(a, p) = 1$, nenhum destes números $i \cdot a$, $1 \leq i \leq p-1$ é divisível por p, ou seja, nenhum é congruente a zero módulo p. Quaisquer dois deles são incongruentes módulo p, pois $a \cdot j \equiv a \cdot k(\text{mod } p)$ implica $j \equiv k(\text{mod } p)$ e isto só possível se $j = k$, uma vez que ambos j e k são positivos e menores que p e não divisíveis por p. Temos, portanto, um conjunto de $p-1$ elementos incongruentes módulo p e não divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os elementos $0, 1, 2, \ldots, p-1$. Se multiplicarmos estas congruências, membro a membro, teremos:

$$a \cdot (2 \cdot a) \cdot (3 \cdot a) \ldots (p-1) \cdot a \equiv 1 \cdot 2 \cdot 3 \ldots (p-1)(\text{mod } p)$$

ou seja, $a^{p-1} \cdot (p-1)! \equiv (p-1)!(\text{mod } p)$. Mas como, $mdc((p-1)!, p) = 1$, podemos cancelar o fator $(p-1)!$ em ambos os lados, obtendo

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

o que conclui a demonstração. □

Definição 14. Se m é um inteiro positivo, a *função ϕ de Euler*, denotada por $\phi(m)$, é definida como sendo o número de inteiros positivos menores do que ou iguais a m que são coprimos com m.

Definição 15. Um *sistema reduzido de resíduos módulo m* é um conjunto de $\phi(m)$ inteiros $r_1, r_2, \ldots, r_{\phi(m)}$, tais que cada elemento do conjunto é coprimo com m, e se $i \neq j$, então $r_i \not\equiv r_j(\text{mod } m)$.

Exemplo 2. O conjunto $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ é um sistema completo de resíduos módulo 9, portanto $\{1, 2, 4, 5, 7, 8\}$ é sistema reduzido de resíduos módulo 9, ou seja, $\phi(9) = 6$. A fim de obter um sistema reduzido de resíduos de um sistema completo módulo m, basta retirar os elementos do sistema completo que não são coprimos com m.

É possível observar que $\phi(m) \leq m - 1$ para $m \geq 2$. Também para $m \geq 2$, temos que $\phi(m) = m - 1$ se, e somente se, m é um número primo, veja Burton (1980, p.136 - 137). Realmente, m é primo se, e somente se, $\{1, 2, \ldots, m-1\}$ é um sistema reduzido de resíduos módulo m, o que significa $\phi(m) = m - 1$.

Teorema 16. *Sejam a um inteiro positivo tal que $mdc(a, m) = 1$. Se $r_1, r_2, \ldots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m, então $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(m)}$ é, também, um sistema reduzido de resíduos módulo m.*

Prova. Na sequência $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(m)}$ temos $\phi(m)$ elementos, é necessário mostrar que todos eles são coprimos com m e, dois a dois, incongruentes módulo m. Como $mdc(a, m) = 1$ e $mdc(r_i, m) = 1$, temos que $mdc(a \cdot r_i, m) = 1$ (Hefez (2016), p. 71). Logo, nos resta mostrar que $a \cdot r_i \not\equiv a \cdot r_j(\text{mod } m)$ se $i \neq j$. Mas, como $mdc(a, m) = 1$, pelo item (f) da Proposição 7, de $a \cdot r_i \equiv a \cdot r_j(\text{mod } m)$ temos $r_i \equiv r_j(\text{mod } m)$, o que implica $i = j$, uma vez que $r_1, r_2, \ldots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m, o que conclui a demonstração. □

Proposição 17. *As seguinte propriedades da função ϕ de Euler são válidas:*

i) Sejam p um número primo e k um natural não nulo. Então $\phi(p^k) = p^k - p^{k-1}$.

ii) $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$, sempre que $m, n \in \mathbb{N}^*$ e $mdc(m, n) = 1$.

iii) Se $n = p_1^{a_1} \cdot p_2^{a_2} \ldots p_t^{a_t}$ é a fatoração de n em números primos, onde $n > 1$, então

$$\phi(n) = (p_1^{a_1} - p_1^{a_1-1}) \cdot (p_2^{a_2} - p_2^{a_2-1}) \ldots (p_t^{a^t} - p_t^{a_t-1}).$$

A demonstração de tal proposição pode ser encontrada em Silva e Gomes (2018, p. 212 - 214).

Teorema 18. *(Euler) Sejam m, $a \in \mathbb{Z}$ com $m > 1$ e $mdc(a, m) = 1$, então*

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

Prova. O Teorema 16 mostra que os elementos $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(m)}$ constituem um sistema reduzido de resíduos módulo m se $mdc(a, m) = 1$ e $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ for um sistema reduzido de resíduos módulo m. Isto significa que $a \cdot r_i$ é congruente a exatamente um dos r_j, $1 \leq j \leq \phi(m)$, e portanto o produto dos $a \cdot r_i$ deve ser congruente ao produto dos r_j módulo m, isto é,

$$a \cdot r_1 \cdot a \cdot r_2 \cdots a \cdot r_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} (\text{mod } m),$$

ou seja,

$$a^{\phi(m)} \cdot r_1 \cdot r_2 \cdots r_{\phi(m)} \equiv r_1 \cdot r_2 \cdots r_{\phi(m)} (\text{mod } m).$$

Como

$$mdc\left(\prod_{i=1}^{\phi(m)} r_i, m\right) = 1,$$

pelo item (f) da Proposição 7, podemos cancelar

$$\prod_{i=1}^{\phi(m)} r_i$$

em ambos os lados para obter $a^{\phi(m)} \equiv 1(\text{mod } m)$. □

Como para p primo, $\phi(p) = p - 1$, o Teorema de Euler é uma generalização do Pequeno Teorema de Fermat.

3 Codificação e Decodificação

A primeira etapa para conseguirmos aplicar o método de criptografia RSA trata-se de uma pré-codificação, que consiste na substituição das letras da mensagem por números, o que transforma a mensagem em uma sequência numérica. A substituição é realizada usando a seguinte tabela:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Os espaços entre as palavras serão substituídos pelo número 36.

Observamos que a escolha desses números para substituir as letras em vez de 1, 2, 3, ..., e assim sucessivamente, é para evitar ambiguidades. Por exemplo, ao corresponderemos A e B aos números 1 e 2, respectivamente, no decorrer do texto, o número 12 resultaria na dúvida, é A e B ou é L?

Posteriormente, determinamos os parâmetros do método de criptografia RSA, escolhendo dois números primos p e q. O par (n, e) é a chave de codificação do sistema RSA, sendo $n = p \cdot q$ e e um número inteiro, tal que e é inversível módulo $\phi(n)$. Como vimos na seção anterior, a função ϕ é conceituada pela Definição 14, e os cálculos de $\phi(n)$ podem ser realizados usando a Proposição 17, isto é, $\phi(n) = (p_1^{a_1} - p_1^{a_1-1}) \cdot (p_2^{a_2} - p_2^{a_2-1}) = (p^1 - p^0) \cdot (q^1 - q^0) = (p-1) \cdot (q-1)$. Já o número e para ser inversível módulo $\phi(n)$ precisa seguir o disposto na Proposição 12, ou seja, $mdc(e, \phi(n)) = 1$.

Para finalizar a pré-codificação, a sequência numérica será dividida em blocos, sendo cada bloco denotado por b. A divisão em blocos seguirá regras, os blocos não podem iniciar com o número 0 e deverão ser menores que n, para evitar problemas na decodificação; e para maior segurança, não corresponder a palavras ou letras, o que torna impossível a análise de frequência.

O bloco b codificado será $C(b) = a$, que é igual ao resto da divisão de b^e por n, ou ainda,

$$b^e \equiv a (\text{mod } n), \text{ com } 0 < a < n. \tag{1}$$

Cada bloco b passará pela etapa de codificação separadamente. A mensagem codificada é uma sequência blocos codificados $(C(b_1), C(b_2), \ldots, C(b_n))$. Vale salientar que os blocos codificados devem ser mantidos separados, para não tornar impossível a decodificação da mensagem.

A chave de decodificação do sistema RSA é o par (n, d), onde d é o inverso de e módulo $\phi(n)$. Assim como acontece com e, o $mdc(d, \phi(n)) = 1$. É possível obter d pelo método das divisões sucessivas, resolvendo a equação diofantina que resulta da equação de congruência linear $e \cdot d \equiv 1 (\text{mod } \phi(n))$ (Definição 11).

A decodificação trata-se de encontrar o bloco da mensagem original. O bloco da mensagem decodificado será $D(a) = l$, que é igual ao resto da divisão de a^d por n, ou seja,

$$a^d \equiv l (\text{mod } n) \text{ com } 0 < l < n. \tag{2}$$

Para calcularmos as congruências (1) e (2), é possível aplicar os Teoremas de Fermat e de Euler e também a Proposição 7.

4 Por que o método de Criptografia RSA funciona e é seguro?

O método funciona se, decodificando um bloco codificado, conseguimos obter o bloco correspondente da mensagem original. Considerando as notações adotadas anteriormente, temos um sistema de Criptografia RSA de parâmetros p e q, $n = p \cdot q$, a chave de codificação (n, e) e a chave de decodificação (n, d), e queremos mostrar que se b é um inteiro e $1 \leq b \leq n - 1$, então

$D(C(b)) \equiv b(\text{mod } n)$. Com a orientação de dividirmos a mensagem original em blocos menores do que n, temos b e $D(C(b))$ estão entre 1 e $n-1$, ou seja, só podem ser congruentes módulo n se são iguais. Sendo assim, precisamos provar apenas que $D(C(b)) \equiv b(\text{mod } n)$. De (1) e (2), contamos com $C(b) \equiv b^e \equiv a(\text{mod } n)$ e $D(a) \equiv a^d \equiv l(\text{mod } n)$, o que resulta em

$$D(C(b)) \equiv (b^e)^d \equiv b^{e \cdot d}(\text{mod } n). \tag{3}$$

Dessa forma, e retomando o fato que $n = p \cdot q$, onde p e q são números primos distintos, calcularemos, separadamente,

$$b^{e \cdot d} \equiv b(\text{mod } p) \tag{4}$$

e

$$b^{e \cdot d} \equiv b(\text{mod } q). \tag{5}$$

Sabemos que d é o inverso de e módulo $\phi(n)$, logo, pela Definição 11, $e \cdot d \equiv 1(\text{mod } \phi(n))$, o que corresponde a $e \cdot d = 1 + k \cdot \phi(n)$ pela Proposição 6. Usando a Proposição 17,

$$e \cdot d = 1 + k \cdot (p-1) \cdot (q-1), \text{ para algum inteiro } k. \tag{6}$$

Substituindo (6) em (4) e (5),

$$b^{e \cdot d} \equiv b^{1+k \cdot (p-1) \cdot (q-1)} \equiv b \cdot b^{k \cdot (p-1) \cdot (q-1)}(\text{mod } p). \tag{7}$$

e

$$b^{e \cdot d} \equiv b^{1+k \cdot (p-1) \cdot (q-1)} \equiv b \cdot b^{k \cdot (p-1) \cdot (q-1)}(\text{mod } q). \tag{8}$$

Primeiramente, mostraremos que $b^{e \cdot d} \equiv b(\text{mod } p)$. Supondo que $p \mid b$, logo $b = 0 + k \cdot p$, para algum k inteiro, o que resulta em, pela Proposição 6, $b \equiv 0(\text{mod } p)$, e também $b^{e \cdot d} \equiv 0(\text{mod } p)$. Logo,

$$b^{e \cdot d} \equiv b(\text{mod } p). \tag{9}$$

Agora, supondo que $p \nmid b$, pelo Pequeno Teorema de Fermat,

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

Assim, dos itens (h) e (e) da Proposição 7, obtemos, respectivamente,

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

e

$$(b^{(p-1)})^{k \cdot (q-1)} \cdot b \equiv 1 \cdot b \equiv b(\text{mod } p) \tag{10}$$

De, (7) e (10), $b^{e \cdot d} \equiv b(\text{mod } p)$. Portanto, $b^{e \cdot d} \equiv b(\text{mod } p)$ para qualquer b inteiro. Analogamente, $b^{e \cdot d} \equiv b(\text{mod } q)$ para qualquer b inteiro.

Acabamos de mostrar as congruências $b^{e \cdot d} \equiv b(\text{mod } p)$ e $b^{e \cdot d} \equiv b(\text{mod } q)$ para qualquer b inteiro. A Definição 5 de congruência nos permite dizer que p e q dividem $b^{e \cdot d} - b$. Como

$mdc(p, q) = 1$, segue que $n = p \cdot q$ divide $b^{e \cdot d} - b$ (vide Hefez (2016, p. 71)). Portanto, podemos concluir que $b^{e \cdot d} \equiv b (\text{mod } n)$. Isto encerra a demonstração de que o método RSA funciona.

Como vimos anteriormente, a criptografia RSA é um método de chave pública, considerando os parâmetros do sistema adotados anteriormente, sendo eles os números primos p e q, e $n = p \cdot q$. A chave de codificação ou chave pública (n, e) é acessível a qualquer usuário, já a chave de decodificação (n, d) é privada. Por isso, o método RSA só será seguro se for difícil de calcular d, quando conhecemos apenas n e e.

Para calcular d aplicamos o método das divisões sucessivas a $\phi(n)$ e e. No entanto, para calcular $\phi(n)$ é necessário fatorar n para obter p e q. Se n for um número grande, fatorá-lo torna-se muito difícil por não existirem algoritmos rápidos para fatoração.

Então, acredita-se que quebrar o código RSA é equivalente a fatorar n. Por isso é importante a escolha de primos suficientemente grandes.

5 Exemplo

Para ilustrar o método de criptografia RSA descrito acima, faremos um exemplo, codificando a mensagem **"PIERRE DE FERMAT"**.

Primeiramente, faremos a etapa de pré-codificação usando a tabela da seção 3, o que nos dá a seguinte sequência numérica:

2518142727143613143615142722 1029

Os parâmetros escolhidos são $p = 5$ e $q = 17$, então temos $n = p \cdot q = 5 \cdot 17 = 85$ e $\phi(n) = (p-1) \cdot (q-1) = 4 \cdot 16 = 64$. O número 3 é inversível módulo $\phi(85) = 64$, então tomaremos $e = 3$. Lembrando que os blocos devem ser menores que $n = 85$, obtemos os seguintes blocos da sequência numérica acima:

2-51-81-42-72-71-43-61-31-43-61-51-42-72-2-10-2-9

Seja $(85, 3)$ a chave de codificação e $C(b) \equiv b^e (\text{mod } n)$ a fórmula, iniciemos a codificação dos blocos:

1. $b_1 = 2$: Como $2^3 = 8$ e $8 \equiv 8 (\text{mod } 85)$. Logo $C(2) = 8$.

2. $b_2 = 51$: Como $51^3 = 132651$ e $132651 \equiv 51 (\text{mod } 85)$. Logo $C(51) = 51$.

3. $b_3 = 81$: Como $81 \equiv -4 (\text{mod } 85)$, então $81^3 \equiv (-4)^3 \equiv -64 \equiv 21 (\text{mod } 85)$. Logo $C(81) = 21$.

4. $b_4 = 42$: Como $42^3 = 74088$ e $42^3 \equiv 53 (\text{mod } 85)$. Logo $C(42) = 53$.

5. $b_5 = 72$: Como $72^3 = 373248$ e $72^3 \equiv 13 (\text{mod } 85)$. Logo $C(72) = 13$.

6. $b_6 = 71$: Como $71^3 = 357911$ e $71^3 \equiv 61(\text{mod } 85)$. Logo $C(71) = 61$.

7. $b_7 = 43$: Como $43^3 = 79507$ e $43^3 \equiv 32(\text{mod } 85)$. Logo $C(43) = 32$.

8. $b_8 = 61$: Como $61^3 = 226981$ e $61^3 \equiv 31(\text{mod } 85)$. Logo $C(61) = 31$.

9. $b_9 = 31$: Como $31^3 = 29791$ e $31^3 \equiv 41(\text{mod } 85)$. Logo $C(31) = 41$.

10. $b_{10} = 43$: Como $43^3 = 79507$ e $43^3 \equiv 32(\text{mod } 85)$. Logo $C(43) = 32$.

11. $b_{11} = 61$: Como $61^3 = 226981$ e $61^3 \equiv 31(\text{mod } 85)$. Logo $C(61) = 31$.

12. $b_{12} = 51$: Como $51^3 = 132651$ e $132651 \equiv 51(\text{mod } 85)$. Logo $C(51) = 51$.

13. $b_{13} = 42$: Como $42^3 = 74088$ e $42^3 \equiv 53(\text{mod } 85)$. Logo $C(42) = 53$.

14. $b_{14} = 72$: Como $72^3 = 373248$ e $72^3 \equiv 13(\text{mod } 85)$. Logo $C(72) = 13$.

15. $b_{15} = 2$: Como $2^3 = 8$ e $8 \equiv 8(\text{mod } 85)$. Logo $C(2) = 8$.

16. $b_{16} = 10$: Como $10^3 = 10^2 \cdot 10$, $10 \equiv 10(\text{mod } 85)$ e $10^2 \equiv 15(\text{mod } 85)$, então $10^3 \equiv 15 \cdot 10 \equiv 65(\text{mod } 85)$. Logo $C(10) = 65$.

17. $b_{17} = 2$: Como $2^3 = 8$ e $8 \equiv 8(\text{mod } 85)$. Logo $C(2) = 8$.

18. $b_{18} = 9$: Como $9^3 = 9^2 \cdot 9 = 81 \cdot 9$ e $81 \equiv (-4)(\text{mod } 85)$, então $9^3 \equiv (-4) \cdot 9 \equiv -36 \equiv 49(\text{mod } 85)$. Logo $C(9) = 49$.

Portanto, a mensagem codificada é

8-51-21-53-13-61-32-31-41-32-31-51-53-13-8-65-8-49

Agora, o objetivo é decodificar, então será necessário a chave de decodificação $(85, d)$, mas ainda não conhecemos o d. O que sabemos é que d é o inverso de e módulo $\phi(n)$, logo $3 \cdot d \equiv 1(\text{mod } 64)$, o que implica, $64 \cdot k + 3 \cdot (-d) = 1$. Aplicando o método das divisões sucessivas de 64 por 3, temos que $1 = 64 + 3 \cdot (-21)$. Logo, o inverso de 3 módulo 64 é -21, mas precisamos de d positivo, pois usaremos como expoente de potências, então $d = 64 - 21 = 43$ que é o menor inteiro positivo congruente a -21 módulo 64. Agora, já possuímos a chave de decodificação (85, 43) e a fórmula $D(a) \equiv a^d(\text{mod } n)$, então podemos ilustrar o processo de decodificação dos blocos:

1. $a_1 = 8$: Como $8^3 = 512$, $512 \equiv 2(\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned} 8^3 &\equiv 2(\text{mod } 85) \\ (8^3)^{14} &\equiv 2^{14} \equiv 16384 \equiv 64(\text{mod } 85) \\ 8^{42} \cdot 8 &\equiv 64 \cdot 8(\text{mod } 85) \\ 8^{43} &\equiv 2(\text{mod } 85). \end{aligned}$$

Logo $D(8) = 2$.

2. $a_2 = 51$: Como $51^3 = 132651$, $132651 \equiv 51(\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned} 51^3 &\equiv 51(\text{mod } 85) \\ (51^3)^{14} &\equiv 51^{14} \equiv 51^3 \cdot 51^3 \cdot 51^3 \cdot 51^3 \cdot 51^2 \equiv 51 \cdot 51 \cdot 51 \cdot 51 \cdot 51^2(\text{mod } 85) \\ 51^{42} &\equiv 51^3 \cdot 51^3 \equiv 51 \cdot 51(\text{mod } 85) \\ 51^{42} \cdot 51 &\equiv 51 \cdot 51 \cdot 51 \equiv 51^3 \equiv 51(\text{mod } 85) \\ 51^{43} &\equiv 51(\text{mod } 85). \end{aligned}$$

Logo $D(51) = 51$.

3. $a_3 = 21$: Como $21^4 = 194481$, $194481 \equiv 1(\text{mod } 85)$ e $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned} 21^4 &\equiv 1(\text{mod } 85) \\ (21^4)^{10} &\equiv 1^{10} \equiv 1(\text{mod } 85) \\ 21^{40} &\equiv 1(\text{mod } 85) \\ 21^{40} \cdot 21^3 &\equiv 1 \cdot 21^3 \equiv 9261 \equiv 81(\text{mod } 85) \\ 21^{43} &\equiv 81(\text{mod } 85). \end{aligned}$$

Logo $D(21) = 81$.

4. $a_4 = 53$: Como $53^4 = 7890481$, $7890481 \equiv 16(\text{mod } 85)$, $16^2 = 256 \equiv 1(\text{mod } 85)$ e $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned} 53^4 &\equiv 16(\text{mod } 85) \\ (53^4)^{10} &\equiv 16^{10} \equiv (16^2)^5 \equiv 1^5 \equiv 1(\text{mod } 85) \\ 53^{40} &\equiv 1(\text{mod } 85) \\ 53^{40} \cdot 53^3 &\equiv 1 \cdot 53^3 \equiv 148877 \equiv 42(\text{mod } 85) \\ 53^{43} &\equiv 42(\text{mod } 85). \end{aligned}$$

Logo $D(53) = 42$.

5. $a_5 = 13$: Como $13^2 = 169$, $169 \equiv -1(\text{mod } 85)$ e $43 = 2 \cdot 21 + 1$, temos

$$\begin{aligned} 13^2 &\equiv -1(\text{mod } 85) \\ (13^2)^{21} &\equiv (-1)^{21} \equiv -1(\text{mod } 85) \\ 13^{42} &\equiv -1(\text{mod } 85) \\ 13^{42} \cdot 13 &\equiv -1 \cdot 13 \equiv -13 \equiv 72(\text{mod } 85) \\ 13^{43} &\equiv 72(\text{mod } 85). \end{aligned}$$

Logo $D(13) = 72$.

6. $a_6 = 61$: Como $61^4 = 13845841$, $13845841 \equiv 21(\text{mod } 85)$, $21^4 \equiv 1(\text{mod } 85)$ e $43 = 4 \cdot 10 + 3$, temos

$$61^4 \equiv 21(\text{mod } 85)$$

$$\begin{aligned}(61^4)^{10} &\equiv (21)^{10} \equiv (21^4)^2 \cdot 21^2 \equiv 1^2 \cdot 441 \equiv 16(\text{mod } 85)\\ 61^{40} &\equiv 16(\text{mod } 85)\\ 61^{40} \cdot 61^3 &\equiv 16 \cdot 226981 \equiv 16 \cdot 31 \equiv 496 \equiv 71(\text{mod } 85)\\ 61^{43} &\equiv 71(\text{mod } 85).\end{aligned}$$

Logo $D(61) = 71$.

7. $a_7 = 32$: Como $32^2 = 1024$, $1024 \equiv 4(\text{mod } 85)$, $43 = 2 \cdot 20 + 3$, temos

$$\begin{aligned}32^2 &\equiv 4(\text{mod } 85)\\ (32^2)^{20} &\equiv 4^{20} \equiv 2^{40} \equiv (2^8)^5 \equiv 1^5 \equiv 1(\text{mod } 85)\\ 32^{40} \cdot 32^3 &\equiv 1 \cdot 32^2 \cdot 32 \equiv 4 \cdot 32 \equiv 128 \equiv 43(\text{mod } 85)\\ 32^{43} &\equiv 43(\text{mod } 85).\end{aligned}$$

Logo $D(32) = 43$.

8. $a_8 = 31$: Como $31^4 = 923521$, $923521 \equiv 81 \equiv -4(\text{mod } 85)$, $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned}31^4 &\equiv -4(\text{mod } 85)\\ (31^4)^{10} &\equiv (-4)^{10} \equiv 2^{20} \equiv (2^8)^2 \cdot 2^4 \equiv 1^2 \cdot 16 \equiv 16(\text{mod } 85)\\ 31^{40} \cdot 31^3 &\equiv 16 \cdot 29791 \equiv 16 \cdot 41 \equiv 61(\text{mod } 85)\\ 31^{43} &\equiv 61(\text{mod } 85).\end{aligned}$$

Logo $D(31) = 61$.

9. $a_9 = 41$: Como $41^4 = 2825761$, $2825761 \equiv 21(\text{mod } 85)$, $21^4 \equiv 1(\text{mod } 85)$ e $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned}41^4 &\equiv 21(\text{mod } 85)\\ (41^4)^{10} &\equiv (21)^{10} \equiv (21^4)^2 \cdot 21^2 \equiv (1)^2 \cdot 441 \equiv 1 \cdot 16 \equiv 16(\text{mod } 85)\\ 41^{40} \cdot 41^3 &\equiv 16 \cdot 68921 \equiv 16 \cdot 71 \equiv 1136 \equiv 31(\text{mod } 85)\\ 41^{43} &\equiv 31(\text{mod } 85).\end{aligned}$$

Logo $D(41) = 31$.

10. $a_{10} = 32$: Como $32^2 = 1024$, $1024 \equiv 4(\text{mod } 85)$, $43 = 2 \cdot 20 + 3$, temos

$$\begin{aligned}32^2 &\equiv 4(\text{mod } 85)\\ (32^2)^{20} &\equiv 4^{20} \equiv 2^{40} \equiv (2^8)^5 \equiv 1^5 \equiv 1(\text{mod } 85)\\ 32^{40} \cdot 32^3 &\equiv 1 \cdot 32^2 \cdot 32 \equiv 4 \cdot 32 \equiv 128 \equiv 43(\text{mod } 85)\\ 32^{43} &\equiv 43(\text{mod } 85).\end{aligned}$$

Logo $D(32) = 43$.

11. $a_{11} = 31$: Como $31^4 = 923521$, $923521 \equiv 81 \equiv -4(\text{mod } 85)$, $43 = 4 \cdot 10 + 3$, temos

$$31^4 \equiv -4(\text{mod } 85)$$

$$\begin{aligned}(31^4)^{10} &\equiv (-4)^{10} \equiv 2^{20} \equiv (2^8)^2 \cdot 2^4 \equiv 1^2 \cdot 16 \equiv 16(\text{mod } 85)\\ 31^{40} \cdot 31^3 &\equiv 16 \cdot 29791 \equiv 16 \cdot 41 \equiv 61(\text{mod } 85)\\ 31^{43} &\equiv 61(\text{mod } 85).\end{aligned}$$

Logo $D(31) = 61$.

12. $a_{12} = 51$: Como $51^3 = 132651$, $132651 \equiv 51(\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned}51^3 &\equiv 51(\text{mod } 85)\\ (51^3)^{14} &\equiv 51^{14} \equiv 51^3 \cdot 51^3 \cdot 51^3 \cdot 51^3 \cdot 51^2 \equiv 51 \cdot 51 \cdot 51 \cdot 51 \cdot 51^2(\text{mod } 85)\\ 51^{42} &\equiv 51^3 \cdot 51^3 \equiv 51 \cdot 51(\text{mod } 85)\\ 51^{42} \cdot 51 &\equiv 51 \cdot 51 \cdot 51 \equiv 51^3 \equiv 51(\text{mod } 85)\\ 51^{43} &\equiv 51(\text{mod } 85).\end{aligned}$$

Logo $D(51) = 51$.

13. $a_{13} = 53$: Como $53^4 = 7890481$, $7890481 \equiv 16(\text{mod } 85)$, $16^2 = 256 \equiv 1(\text{mod } 85)$ e $43 = 4 \cdot 10 + 3$, temos

$$\begin{aligned}53^4 &\equiv 16(\text{mod } 85)\\ (53^4)^{10} &\equiv 16^{10} \equiv (16^2)^5 \equiv 1^5 \equiv 1(\text{mod } 85)\\ 53^{40} &\equiv 1(\text{mod } 85)\\ 53^{40} \cdot 53^3 &\equiv 1 \cdot 53^3 \equiv 148877 \equiv 42(\text{mod } 85)\\ 53^{43} &\equiv 42(\text{mod } 85).\end{aligned}$$

Logo $D(53) = 42$.

14. $a_{14} = 13$: Como $13^2 = 169$, $169 \equiv -1(\text{mod } 85)$ e $43 = 2 \cdot 21 + 1$, temos

$$\begin{aligned}13^2 &\equiv -1(\text{mod } 85)\\ (13^2)^{21} &\equiv (-1)^{21} \equiv -1(\text{mod } 85)\\ 13^{42} &\equiv -1(\text{mod } 85)\\ 13^{42} \cdot 13 &\equiv -1 \cdot 13 \equiv -13 \equiv 72(\text{mod } 85)\\ 13^{43} &\equiv 72(\text{mod } 85).\end{aligned}$$

Logo $D(13) = 72$.

15. $a_{15} = 8$: Como $8^3 = 512$, $512 \equiv 2(\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned}8^3 &\equiv 2(\text{mod } 85)\\ (8^3)^{14} &\equiv 2^{14} \equiv 16384 \equiv 64(\text{mod } 85)\\ 8^{42} \cdot 8 &\equiv 64 \cdot 8(\text{mod } 85)\\ 8^{43} &\equiv 2(\text{mod } 85).\end{aligned}$$

Logo $D(8) = 2$.

16. $a_{16} = 65$: Como $65^3 = 274625$, $274625 \equiv 75 \equiv -10(\text{mod } 85)$, $10^2 \equiv 100 \equiv 15(\text{mod } 85)$, $15^5 \equiv 759375 \equiv 70(\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned} 65^3 &\equiv -10(\text{mod } 85) \\ (65^3)^{14} &\equiv (-10)^{14} \equiv (10^2)^7 \equiv 15^7 \equiv 15^5 \cdot 15^2 \equiv 70 \cdot 225 \equiv 70 \cdot 55 \equiv 3850 \equiv 25(\text{mod } 85) \\ 65^{42} \cdot 65 &\equiv 25 \cdot 65 \equiv 1625 \equiv 10(\text{mod } 85) \\ 65^{43} &\equiv 10(\text{mod } 85). \end{aligned}$$

Logo $D(65) = 10$.

17. $a_{17} = 8$: Como $8^3 = 512$, $512 \equiv 2(\text{mod } 85)$ e $43 = 3 \cdot 14 + 1$, temos

$$\begin{aligned} 8^3 &\equiv 2(\text{mod } 85) \\ (8^3)^{14} &\equiv 2^{14} \equiv 16384 \equiv 64(\text{mod } 85) \\ 8^{42} \cdot 8 &\equiv 64 \cdot 8(\text{mod } 85) \\ 8^{43} &\equiv 2(\text{mod } 85). \end{aligned}$$

Logo $D(8) = 2$.

18. $a_{18} = 49$: Como $49^2 = 2401$, $2401 \equiv 21(\text{mod } 85)$, $21^4 \equiv 1(\text{mod } 85)$ e $43 = 2 \cdot 21 + 1$, temos

$$\begin{aligned} 49^2 &\equiv 21(\text{mod } 85) \\ (49^2)^{21} &\equiv 21^{21} \equiv (21^4)^5 \cdot 21 \equiv 1^5 \cdot 21 \equiv 21(\text{mod } 85) \\ 49^{42} \cdot 49 &\equiv 21 \cdot 49 \equiv 1029 \equiv 9(\text{mod } 85) \\ 49^{43} &\equiv 9(\text{mod } 85). \end{aligned}$$

Logo $D(49) = 9$.

Logo, a sequência decodificada será

2-51-81-42-72-71-43-61-31-43-61-51-42-72-2-10-2-9,

reescrevendo a sequência temos

25-18-14-27-27-14-36-13-14-36-15-14-27-22-10-29.

Agora, já podemos fazer a conversão para letras usando a tabela da seção 3.1:

P-I-E-R-R-E–D-E–F-E-R-M-A-T.

Portanto, a mensagem é PIERRE DE FERMAT, assim concluindo a decodificação e o nosso exemplo do método.

Referências

BOYER, C. B. *História da matemática*, 3 ed. - São Paulo: Blucher, 2012.

BURTON, D. M. *Elementary Number Theory*, revised printing, Boston: Allyn and Bacon, 1980.

CARNEIRO, F. J. F. *Criptografia e Teoria dos Números.* Rio de Janeiro: Editora Ciência Moderna Ltda., 2017.

COUTINHO, S. C. *Números Inteiros e Criptografia RSA*, Rio de Janeiro: IMPA, 2009.

HEFEZ, A. *Exercícios resolvidos de Aritmética.* 1ª ed. Rio de Janeiro: SBM, 2016.

SANTOS, J. P. O. *Introdução à Teoria do Números.* 3ª ed. Rio de Janeiro: IMPA, 2020.

SILVA, J. C.; GOMES, O. R. *Estruturas Algébricas para Licenciatura: Elementos de Aritmética Superior.* V. 2. São Paulo: Blucher, 2018.

SINGH, S. *O livro dos códigos.* 5ª ed. Rio de Janeiro: Record, 2005.