RMU
REVISTA MATEMÁTICA UNIVERSITÁRIA

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

Revista Matemática Universitária, vol. 2, 2021
ISSN: 2675-5254 — **DOI:** 10.21711/26755254/rmu20219

RETICULADOS E NÚMEROS BINÁRIOS: UM ATAQUE À CRIPTOGRAFIA RSA

JOSÉ LAUDELINO DE M. NETO

Resumo. Descrevemos um ataque ao criptosistema RSA, desenvolvido por May e Ritzenhofen em [1], que consiste em fatorar simultaneamente, utilizando teoria de reticulados, dois números inteiros positivos $N_1 = p_1q_1$ e $N_2 = p_2q_2$, onde p_1, p_2, q_1 e q_2 são números primos ímpares. Mas, para tal feito é necessário ter duas dicas a respeito destes números N_1 e N_2, a saber: p_1 e p_2 devem ter alguns bits finais em comum e q_1 e q_2 devem ter a mesma quantidade de bits.

1. Introdução

Nos dias atuais, a criptografia se encontra em voga, pois basta reparar que ao iniciar uma conversa no aplicativo de mensagens *WhatsApp*, somos surpreendidos com um aviso alertando que *"As mensagens e as chamadas são protegidas com a criptografia de ponta a ponta (...)"*. E o que é criptografia? Podemos dizer que é a arte de codificar uma mensagem, transformando um texto legível e entendível em um texto que fique não compreensível para leitores não autorizados. Apenas leitores autorizados terão acesso ao texto original.

Exemplificando o que foi dito no parágrafo acima: o seguinte texto original *"BOM"* é cifrado, por algum método criptográfico, no texto *"ABBDLG"*. Então, somente pessoas autorizadas terão como descriptografar o texto cifrado e recuperar a mensagem original. Os leitores não autorizados, terão acesso apenas ao texto cifrado e não compreensível.

Um dos métodos criptográficos mais famosos é o RSA, criado por Rivest, Shamir e Adleman. Sua segurança consiste na dificuldade em fatorar um número como um produto de primos, pois o cerne do RSA é um número N positivo, produto de dois números primos ímpares, p e q [4]. Este número $N = pq$ é chamado de *RSA moduli*.

Desde o surgimento de técnicas criptográficas, pesquisam-se maneiras de quebrar a criptografia e desvendar o texto cifrado. Não é diferente com o RSA e é isso que apresentaremos neste texto, um ataque a criptografia RSA, desenvolvida por May e

Data de aceitação: Agosto de 2021.
Palavras chave. Álgebra Linear; Teoria dos Números; Congruência.

Ritzenhofen [1], na tentativa de fatorar um *RSA moduli* $N = pq$ utilizando números binários e teoria de reticulados.

2. Reticulados

Ressaltamos que, na literatura matemática, o termo reticulado é usado em duas situações distintas. Numa delas, um assunto se refere a conjuntos parcialmente ordenados [5], que não é o do nosso interesse, e na outra se refere a subconjuntos de um espaço vetorial real [3]. Portanto, para entender reticulados no contexto de álgebra linear, é necessário ter conhecimento prévio sobre: conjunto de vetores Linearmente Independentes (LI), espaço vetorial, base de um espaço vetorial, norma de um vetor etc.

Um reticulado inteiro L é um subgrupo discreto e aditivo de $\mathbb{Z}^n$. Equivalentemente, sejam $d, n \in \mathbb{N}$ e $\mathbf{b}_1, \ldots, \mathbf{b}_d \in \mathbb{Z}^n$ vetores LI, um reticulado inteiro L é o conjunto de todas as combinações lineares inteiras dos vetores $\mathbf{b}_i$, ou seja,

$$L = \{a_1\mathbf{b}_1 + \ldots + a_d\mathbf{b}_d; a_i \in \mathbb{Z}\}.$$

Neste caso, dizemos que o conjunto $\{\mathbf{b}_1, \ldots, \mathbf{b}_d\}$ é uma base do reticulado L.

O Problema do Menor Vetor, em inglês *Shortest Vector Problem*, é uma das pesquisas na área [2] e consiste em determinar o vetor de menor comprimento de um reticulado. Ou seja, denotamos $\|\mathbf{v}\|$ como a norma euclidiana do vetor $\mathbf{v}$, e o Problema do Menor Vetor consiste em determinar $\mathbf{0} \neq \mathbf{a} \in L$ tal que $\|\mathbf{a}\| \leq \|\mathbf{v}\|$ para qualquer vetor $\mathbf{v}$ de L. Adotamos a norma tradicional euclidiana, porém o problema também pode ser proposto para outras normas usuais. Se $\mathbf{a}$ é o menor vetor do reticulado L, então escrevemos $\|\mathbf{a}\| = \lambda_1(L)$.

Para um caso de dimensão n qualquer, resolver o Problema do Menor Vetor não é uma tarefa fácil. Entretanto, para um reticulado bidimensional L, no caso em que $n = 2$, é possível utilizar um algoritmo chamado de Redução de Gauss, o qual resolve o Problema do Menor Vetor.

O Algoritmo da Redução de Gauss funciona calculando uma sequência de bases $\{\mathbf{a}, \mathbf{b}\}$ de um reticulado bidimensional L, que satisfaz a propriedade

$$\|\mathbf{a}\| \leq \|\mathbf{a} - \mathbf{b}\| < \|\mathbf{b}\|,$$

e, ao final de uma quantidade finita de iterações, retorna uma base $\{\mathbf{a}, \mathbf{b}\}$ tal que $\|\mathbf{a}\| = \lambda_1(L)$.

Algoritmo da Redução de Gauss
Entrada: Base de um reticulado bidimensional L, $\{\mathbf{a}, \mathbf{b}\}$.
Saída: Base $\{\mathbf{a}, \mathbf{b}\}$ do reticulado L satisfazendo $\|\mathbf{a}\| = \lambda_1(L)$.

(1) Se $\|\mathbf{a}\| > \|\mathbf{b}\|$, então troque $\mathbf{a}$ por $\mathbf{b}$ e vá para (2). Caso contrário, vá para (2).
(2) Se $\|\mathbf{a} - \mathbf{b}\| > \|\mathbf{a} + \mathbf{b}\|$, então $\mathbf{b} := -\mathbf{b}$ e vá para (3). Caso contrário, vá para (3).
(3) Se $\|\mathbf{b}\| \leq \|\mathbf{a} - \mathbf{b}\|$, então pare e retorne $\{\mathbf{a}, \mathbf{b}\}$. Caso contrário, vá para (4).
(4) Se $\|\mathbf{a}\| \leq \|\mathbf{a} - \mathbf{b}\|$, então vá para (6). Caso contrário, vá para (5).
(5) Se $\|\mathbf{a}\| = \|\mathbf{b}\|$, então pare e retorne $\{\mathbf{a}, \mathbf{a} - \mathbf{b}\}$. Caso contrário, vá para (6).

(6) Determine $\mu \in \mathbb{Z}$ tal que $\|\mathbf{b} - \mu\mathbf{a}\|$ é o menor possível, faça $\mathbf{a} := \mathbf{b} - \mu\mathbf{a}$, $\mathbf{b} := \mathbf{a}$. Se $\|\mathbf{a} - \mathbf{b}\| > \|\mathbf{a} + \mathbf{b}\|$, faça $\mathbf{b} := -\mathbf{b}$. Se $\{\mathbf{a}, \mathbf{b}\}$ satisfizer $\|\mathbf{a}\|, \|\mathbf{b}\| < \|\mathbf{a} - \mathbf{b}\|, \|\mathbf{a} + \mathbf{b}\|$, então pare e retorne $\{\mathbf{a}, \mathbf{b}\}$. Caso contrário, refaça (6).

A etapa (6) é um loop, pois é necessário tornar a repetir o procedimento em (6), até chegarmos ao objetivo. O medo seria o da etapa (6) entrar em um loop infinito, porém isso não ocorre, pois o valor de $\|\mathbf{a}\|$ ou $\|\mathbf{b}\|$ diminui a cada iteração e, como existe uma quantidade finita de vetores de L menores que $\|\mathbf{a}\| + \|\mathbf{b}\|$, então o algoritmo irá finalizar após uma quantidade finita de iterações [2]. Além disso, o problema para determinar μ na etapa (6) é contornado ao considerarmos a Proposição abaixo, pois garante um intervalo de números inteiros positivos para μ. É justo por isso que μ pode ser calculado de modo eficiente, pois vamos testando todos os valores de μ deste intervalo garantido pela Proposição, até encontrarmos um $\mu \in \mathbb{Z}$ tal que $\|\mathbf{b} - \mu\mathbf{a}\|$ é o menor possível.

Proposição: *Sejam* $\mathbf{a}, \mathbf{b}$ *vetores tais que* $\|\mathbf{b}\| > \|\mathbf{b} - \mathbf{a}\|$. *Então, podemos calcular de modo eficiente um inteiro* μ *tal que* $\|\mathbf{b} - \mu\mathbf{a}\|$ *é o menor possível. Além disso,* $1 \leq \mu \leq 2\frac{\|\mathbf{b}\|}{\|\mathbf{a}\|}$.
Demonstração: A demonstração detalhada desta Proposição é encontrada na referência [2]. ■

3. Fatorando dois *RSA moduli* simultaneamente

Apresentamos o tema principal deste texto, descrito no Teorema abaixo, que foi a técnica desenvolvida por May e Ritzenhofen [1], a fatoração simultânea de dois *RSA moduli*, onde duas dicas são dadas. No caso, sejam $N_1 = p_1q_1$ e $N_2 = p_2q_2$ dois *RSA moduli* e a primeira dica dada é que p_1 e p_2 na sua forma binária possuem alguns dígitos finais em comum, ou seja, alguns bits finais iguais. A segunda dica é que q_1 e q_2 tem a mesma quantidade de dígitos na sua escrita em binário, o que equivale a dizer que q_1 e q_2 tem a mesma quantidade de bits.

Com o intuito de apresentar a prova do Teorema, lembramos a construção do anel de inteiros módulo n, onde n é um número inteiro positivo. Dizemos que dois números inteiros a e b são congruentes módulo n se e somente se n divide $a - b$. Neste caso, escrevemos $a \equiv b (\text{mod } n)$. A relação $\equiv$ é de equivalência e o conjunto das classes de equivalência é denotado por $\mathbb{Z}_n$. As operações de soma e multiplicação induzidas de $\mathbb{Z}$ em $\mathbb{Z}_n$ o tornam um anel comutativo. Verifica-se que uma classe de equivalência $\bar{a} \in \mathbb{Z}_n$ tem inverso multiplicativo se e somente se $\text{mdc}(a, n) = 1$.

Teorema: *Sejam* $N_1 = p_1q_1$ *e* $N_2 = p_2q_2$ *dois RSA moduli distintos, onde* q_i *tem* α *bits. Suponhamos que* p_i *possuem* $t > 2(\alpha + 1)$ *bits finais em comum. Então,* N_1 *e* N_2 *podem ser fatorados simultaneamente.*
Demonstração: Como p_1, p_2 possuem t bits finais em comum, temos

$$p_1 = 2^t\widetilde{p_1} + p \quad \text{e} \quad p_2 = 2^t\widetilde{p_2} + p.$$

Assim, $N_i = (p + 2^t\widetilde{p_i})q_i$, implicando que $pq_i \equiv N_i (\text{mod } 2^t), i = 1, 2$. Sendo q_i primos ímpares, então possuem inversos multiplicativos em $\mathbb{Z}_{2^t}$. Logo,

$$N_1q_1^{-1} \equiv N_2q_2^{-1} (\text{mod } 2^t) \Rightarrow (N_1^{-1}N_2)q_1 - q_2 \equiv 0 (\text{mod } 2^t). \tag{1}$$

O conjunto de soluções

$$L = \left\{(x_1, x_2) \in \mathbb{Z}^2; (N_1^{-1}N_2)x_1 - x_2 \equiv 0 (\text{mod } 2^t)\right\}$$

forma um grupo aditivo e discreto de $\mathbb{Z}^2$. Isto é, L é um reticulado bidimensional.

Afirmamos que L possui os vetores $\mathbf{b}_1 = (1, N_1^{-1}N_2)$ e $\mathbf{b}_2 = (0, 2^t)$ como base. Com efeito, $\mathbf{b}_1, \mathbf{b}_2 \in L$ e são LI. Por outro lado, seja $(x_1, x_2) \in L$. Então, $x_2 = (N_1^{-1}N_2)x_1 - k2^t$, para algum $k \in \mathbb{Z}$. Assim, $(x_1, x_2) = x_1\mathbf{b}_1 - k\mathbf{b}_2$.

Pela Equação (1), vemos que $\mathbf{q} = (q_1, q_2) \in L$. Entretanto, $\mathbf{q}$ ainda está indeterminado. Para deteminar explicitamente quem é $\mathbf{q}$, utilizamos o Algoritmo da Redução de Gauss nos vetores $\mathbf{b}_1$ e $\mathbf{b}_2$. Após aplicarmos o referido algoritmo, obtemos como retorno que $\mathbf{q}$ é o menor vetor de L, ou seja, $\|\mathbf{q}\| = \lambda_1(L)$ (para maiores detalhes desta passagem, ver [1]). Consequentemente, temos material suficiente para fatorar N_1 e N_2 simultaneamente. ■

O Teorema acima nos garante o algoritmo a seguir:
Entrada: dois RSA moduli N_1 e N_2 satisfazendo as hipóteses do Teorema.
Saída: q_1 e q_2, onde $N_1 = p_1q_1$ e $N_2 = p_2q_2$.

(1) Calcule $N_1^{-1}N_2 \in \mathbb{Z}_{2^t}$.
(2) Considere L o reticulado gerado por $\mathbf{a} = (1, N_1^{-1}N_2)$ e $\mathbf{b} = (0, 2^t)$.
(3) Utilize o Algoritmo da Redução de Gauss para determinar o menor vetor $\mathbf{q} = (q_1, q_2)$ do reticulado L.

Para visualizarmos melhor, consideremos um caso prático. Sejam $N_1 = p_1q_1 = 372581$ e $N_2 = p_2q_2 = 493571$ dois *RSA moduli* tais que p_1 e p_2 possuem 12 bits finais em comum e q_1 e q_2 possuem 4 bits, ou seja, N_1 e N_2 satisfazem as condições do Teorema. Sendo assim, estamos aptos para utilizar o algoritmo apresentado acima. Primeiro, calculamos $N_1^{-1}N_2$ módulo $2^{12} = 4096$,

$$N_1^{-1}N_2 \equiv 1863 (\text{mod } 4096).$$

Seja L o reticulado gerado pelos vetores $\mathbf{a} = (1, 1863)$ e $\mathbf{b} = (0, 4096)$. Então, chegamos na etapa de aplicar o Algoritmo da Redução de Gauss. Observamos que os vetores $\mathbf{a}$ e $\mathbf{b}$ satisfazem as etapas (1) a (4) do Algoritmo da Redução de Gauss e, da etapa (4), vamos para a etapa (6), que, como mencionado antes, funciona como um loop até chegarmos a base procurada do reticulado.

Para o loop da etapa (6), vamos iniciar a primeira iteração com $\mathbf{a}_0 = \mathbf{a}$ e $\mathbf{b}_0 = \mathbf{b}$. Utilizando a Proposição, obtemos que

$$1 \leq \mu \leq 2\frac{\|\mathbf{b}_0\|}{\|\mathbf{a}_0\|} \approx 4.$$

Assim, para $\mu \in \{1, 2, 3, 4\}$, testando caso a caso, concluimos que o menor valor possível para $\|\mathbf{b}_0 - \mu\mathbf{a}_0\|$ é quando $\mu = 2$. Logo,

$$\mathbf{a}_1 = \mathbf{b}_0 - 2\mathbf{a}_0 = (-2, 370), \quad \mathbf{b}_1 = \mathbf{a}_0 = (1, 1863).$$

Como $\|\mathbf{b}_1\|$ não é menor que $\|\mathbf{a}_1 - \mathbf{b}_1\|$, repetimos o procedimento e, para $\mu \in \{1, 2, \ldots, 10\}$, analisando caso a caso, temos que o menor valor possível para $\|\mathbf{b}_1 - \mu\mathbf{a}_1\|$ é quando $\mu = 5$. Então,

$$\mathbf{a}_2 = \mathbf{b}_1 - 5\mathbf{a}_1 = (11, 13), \quad \mathbf{b}_2 = \mathbf{a}_1 = (-2, 370).$$

Mais uma vez, como $\|\mathbf{b}_2\|$ não é menor que $\|\mathbf{a}_2 - \mathbf{b}_2\|$, fazemos o procedimento e, para $\mu \in \{1, 2, \ldots, 42\}$, calculando todas as opções disponíveis, temos que o menor valor possível para $\|\mathbf{b}_2 - \mu\mathbf{a}_2\|$ é quando $\mu = 17$. Logo,

$$\mathbf{a}_3 = \mathbf{b}_2 - 17\mathbf{a}_2 = (-189, 149), \quad \mathbf{b}_3 = \mathbf{a}_2 = (11, 13).$$

Neste caso, temos que $\|\mathbf{a}_3\|$ e $\|\mathbf{b}_3\|$ são menores que $\|\mathbf{a}_3 - \mathbf{b}_3\|$ e $\|\mathbf{a}_3 + \mathbf{b}_3\|$. Então, temos que $\mathbf{q} = (11, 13)$ e $(-189, 149)$ é uma base do reticulado L que satisfaz $\|\mathbf{q}\| = \lambda_1(L)$. Portanto,

$$N_1 = 372581 = p_1 q_1 \quad \text{e} \quad N_2 = 493571 = p_2 q_2,$$

onde $q_1 = 11, q_2 = 13$ e, consequentemente, $p_1 = 33871$ e $p_2 = 37967$.

Em binário, temos

$$\begin{aligned} p_1 &= (1000010001001111)_2, \\ p_2 &= (1001010001001111)_2 \\ q_1 &= (1011)_2, \\ q_2 &= (1101)_2. \end{aligned}$$

Referências

[1] Alexander May & Maike Ritzenhofen, *Implicit Factoring: On Polynomial Time Factoring Given Only an Implicit Hint*, In Stanislaw Jarecki and Gene Tsudik, editores, Public Key Cryptography, volume 5443 of Lecture Notes in Computer Science, p. 1-14. Springer, 2009.

[2] Daniele Micciancio & Shafi Goldwasser, *Complexity of lattice problems: a cryptographic perspective*, Kluwer Academic Publishers, 2002.

[3] Fernando Daniel Moreira Coelho, *O Algoritmo LLL e Aplicações*, Dissertação de Mestrado, Faculdade de Ciências e Tecnologia, Universidade de Coimbra, 2007.
<http://www.mat.uc.pt/~jsoares/research/mest_Fernando_Coelho.pdf>
Acesso em: 12/05/2021.

[4] Manoel Lemos, *Criptografia, Números Primos e Algoritmos*, IMPA, 2010.
<https://impa.br/wp-content/uploads/2017/04/PM_04.pdf> Acesso em: 13/06/2021.

[5] Michell Lucena Dias, *Introdução à Teoria dos Reticulados e Reticulados de Subgrupos*, Trabalho de Conclusão de Curso, Unidade Acadêmica de Matemática, Universidade Federal de Campina Grande, 2013.
<http://mat.ufcg.edu.br/pgmat2/wp-content/uploads/sites/2/2015/06/TCC-Michell.pdf>
Acesso em: 12/05/2021.

Departamento de Ciências Exatas
Centro de Ciências Aplicadas e Educação (CCAE)
Universidade Federal da Paraíba (UFPB)
Rio Tinto, PB
Email address: laudelino@dcx.ufpb.br