Criptografia RSA

Junior R. Ribeiro

21 de outubro de 2021

1 Criptografia RSA

A Criptografia RSA (Rivest-Shamir-Adleman são os autores deste modelo de criptografia) consiste em um modelo matemático de criptografia assimétrica, isto é, o processo de decodificação é diferente do processo de codificação. Ela é fortemente dependente da **dificuldade de fatoração de números compostos muito grandes**; é isso que lhe garante segurança nos dados.

Os número primos são aqueles que são divisíveis somente por 1 e por ele mesmo, tais como $2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ \ldots$, e os demais números são compostos porque são produtos de números primos, como exemplo $6 = 2 \cdot 3,\ 15 = 3 \cdot 5$, etc.

Fatorar um número composto com milhares de dígitos C pode ser uma tarefa simples, se este número for composto pelo produto de dois números primos P e Q, em que P seja enorme e Q seja pequeno, digamos, 23. Basta fazermos algumas tentativas pelos números primos listados acima, até que encontremos 23 e conseguimos um fator primo para C. Agora, se P e Q forem gitantescos, a tarefa de fatoração é impraticável mesmo com os melhores supercomputadores existentes e a existir, pois precisamos testar cada um dos possíveis números primos anteriores para saber se são um fator para C. É aí que reside a segurança da RSA[1].

2 Modelo

O RSA consiste de duas chaves, a pública e a privada, que são dois números grandes. A chave pública pode ser conhecida por qualquer pessoa, inclusive os hackers. Ela é o produto de dois primos grandes. Para “hackear” o RSA, o hacker precisará fatorar esse produto e descobrir quem são os dois primos que o compõem, o que, como já dito, é impraticável com a tecnologia atual. A chave privada deve ser mantida em segredo pelo responsável pela segurança do sistema. A mensagem é codificada utilizando apenas a chave pública, já a decodificação é feita usando a chave pública e a privada; esta última é calculada a partir dos números primos que geram a chave pública. Por isso é importante criar o par de chaves e destruir os números primos, para que ninguém mais possa quebrar a criptografia; e logicamente guardar a chave privada em segredo.

O modelo a seguir é um modelo particular do RSA, que é mais genérico.

[1] Para mais detalhes, veja, por exemplo, RSA (sistema criptográfico).

Nota: Representamos o resto r da divisão de a por b indicando que a é igual a r módulo b, ou

$$a = r \pmod{b}.$$

Considere dois números primos grandes P e Q escolhidos de modo que deixem resto 5 quando divididos por 6, ou seja, $P = 5 \pmod 6$ e $Q = 5 \pmod 6$.

A chave pública é

$$\alpha = P \cdot Q. \tag{1}$$

A chave privada é

$$\beta = 4k - 1, \tag{2}$$

em que k é calculado por

$$k = \frac{(P-1)(Q-1)+2}{6}$$

A codificação de uma mensagem M é feita tomando o resto da divisão de M^3 pela chave pública α, vamos chamar esse resto de M_r. Escrito de outra maneira, temos

$$M^3 = M_r \pmod{\alpha}.$$

A mensagem codificada é M_r.

A decodificação é feita tomando o resto da divisão de M_r^β pela chave pública α. Ou matematicamente,

$$M_r^\beta = M \pmod{\alpha}.$$

2.1 Exemplo numérico

Tomemos $P = 11$ e $Q = 41$, pois são $11 = 5 \pmod 6$ e $41 = 5 \pmod 6$.

A chave pública é

$$\alpha = 11 \cdot 41 = 451,$$

Calculamos k,

$$k = \frac{(11-1)(41-1)+2}{6} = \frac{10 \cdot 40 + 2}{6} = 67,$$

e obtemos a chave privada

$$\beta = 4 \cdot 67 - 1 = 267.$$

Nossa mensagem não pode ser maior que a chave pública α, para que haja possibilidade de recuperar a mensagem após a codificação e decodificação.

Suponha que nossa mensagem seja $M = 96$. Vamos calcular M_r

$$M^3 = 96^3 = 96^2 \cdot 96 = 9216 \cdot 96 = 196 \cdot 96 = 18816 = 325 \pmod{451}$$

e assim, $M_r = 325$ é a mensagem **codificada**. Perceba em vermelho, que trocamos 96^2 pelo seu resto que é 196 módulo 451. Este é o procedimento quando trabalhamos com a aritmética modular, assunto para você pesquisar.

Agora, vamos decodificar a mensagem $M_r = 325$ usando ambas as chaves.

$$M_r^{267} = 325^{267} \pmod{451}$$

Vejamos como fica M_r^2

$$M_r^2 = 325^2 = 105625 = 91 \pmod{451}.$$

Vamos olhar com cuidado o expoente

$$267 = \underbrace{2 + 2 + ... + 2}_{133 \text{ vezes}} + 1.$$

com isso, podemos substituir no problema original esse resultado (apliação de aritmética modular)

$$M_r^{267} = 325^{267} = \underbrace{91 \times 91 \times ... \times 91}_{133 \text{ vezes}} \times 325 = 325 \cdot 91^{133} \pmod{451}.$$

Veja que o problema era o expoente 267, agora o problema é menor, 133. Vamos fazer essa redução repetidas vezes. Vamos chamar essa base $b_1 = M_r^2 = 91 \pmod{451}$.

. . . .

Vejamos como fica $b_1^2 \pmod{451}$.

$$b_1^2 = 91^2 = 8281 = 163 \pmod{451}.$$

Vamos olhar de novo o novo expoente

$$133 = \underbrace{2 + 2 + ... + 2}_{66 \text{ vezes}} + 1.$$

Com isso, podemos substituir no problema original

$$\begin{aligned} M_r^{267} &= 325^{267} = 325 \cdot 91^{133} = 325 \cdot (\underbrace{163 \times 163 \times ... \times 163}_{66 \text{ vezes}} \times 91) \\ &= 325 \cdot 91 \cdot 163^{66} = 29575 \cdot 163^{66} = 260 \cdot 163^{66} \pmod{451}. \end{aligned}$$

Veja que o problema era o expoente 133, agora o problema é menor, 66. Vamos chamar essa base $b_2 = M_r^4 = 163 \pmod{451}$.

. . . .

Vejamos como fica $b_2^2 \pmod{451}$.

$$b_2^2 = 163^2 = 26569 = 411 \pmod{451}.$$

Vamos olhar de novo o novo expoente

$$66 = \underbrace{2 + 2 + ... + 2}_{33 \text{ vezes}}.$$

Com isso, podemos substituir no problema original

$$M_r^{267} = 325^{267} = 260 \cdot (\underbrace{411 \times 411 \times ... \times 411}_{33 \text{ vezes}}) = 260 \cdot 411^{33} \pmod{451}.$$

Veja que o problema era o expoente 66, agora o problema é menor, 33. Vamos chamar essa base $b_3 = M_r^8 = 411 \pmod{451}$.

. . . .

Vejamos como fica $b_3^2 \pmod{451}$.

$$b_3^2 = 411^2 = 168921 = 247 \pmod{451}.$$

Vamos olhar de novo o novo expoente

$$33 = \underbrace{2 + 2 + ... + 2}_{16 \text{ vezes}} + 1.$$

Com isso, podemos substituir no problema original

$$\begin{aligned} M_r^{267} &= 325^{267} = 260 \cdot (\underbrace{247 \times 247 \times ... \times 247}_{16 \text{ vezes}} \times 411) \\ &= 260 \cdot 411 \cdot 247^{16} = 106860 \cdot 247^{16} = 424 \cdot 247^{16} \pmod{451}. \end{aligned}$$

Veja que o problema era o expoente 33, agora o problema é menor, 16. Vamos chamar essa base $b_4 = M_r^{16} = 247 \pmod{451}$.

. . . .

Vejamos como fica $b_4^2 \pmod{451}$.

$$b_4^2 = 247^2 = 61009 = 124 \pmod{451}.$$

Vamos olhar de novo o novo expoente

$$16 = \underbrace{2 + 2 + ... + 2}_{8 \text{ vezes}}.$$

Com isso, podemos substituir no problema original

$$M_r^{267} = 325^{267} = 424 \cdot (\underbrace{124 \times 124 \times ... \times 124}_{8 \text{ vezes}}) = 424 \cdot 124^8 \pmod{451}.$$

Veja que o problema era o expoente 16, agora o problema é menor, 8. Vamos chamar essa base $b_5 = M_r^{32} = 124 \pmod{451}$.

. . . .

Vejamos como fica $b_5^2 \pmod{451}$.

$$b_5^2 = 124^2 = 15376 = 42 \pmod{451}.$$

Vamos olhar de novo o novo expoente

$$8 = 2 + 2 + 2 + 2.$$

Com isso, podemos substituir no problema original

$$M_r^{267} = 325^{267} = 424 \cdot (42 \times 42 \times 42 \times 42) = 424 \cdot 42^4 \pmod{451}.$$

Veja que o problema era o expoente 8, agora o problema é menor, 4. Vamos chamar essa base $b_6 = M_r^{64} = 42 \pmod{451}$.

. . . .

Vejamos como fica $b_6^2 \pmod{451}$.

$$b_6^2 = 42^2 = 1764 = 411 \pmod{451}.$$

Vamos olhar de novo o novo expoente

$$4 = 2 + 2.$$

Com isso, podemos substituir no problema original

$$M_r^{267} = 325^{267} = 424 \cdot 411 \cdot 411 = 71622504 = 96 \pmod{451}.$$

E obtemos a mensagem original.

2.2 Comentário

O processo de criptografia foi rápido, pois escolhemos um modelo especificamente para essa finalidade. Veja que para codificar, precisamos apenas elevar a mensagem M à terceira potência. O valor de k e de β foi determinado especificamente para esse número três, bem como a exigência de que os números primos sejam iguais a 5 módulo 6.

Já para decodificar, o processo se tornou bem mais árduo porque a chave privada acaba sendo um número grande, e por isso precisamos fazer reduções sucessivas até obtermos a mensagem descriptografada.