1 Introdução

O RSA é um dos algoritmos de criptografia mais populares, utilizado para garantir a segurança das comunicações digitais. Ele funciona por meio de um par de chaves: uma chave pública, que pode ser compartilhada, e uma chave privada, que deve ser mantida em segredo. Abaixo, explicamos o processo de geração e uso dessas chaves passo a passo.

2 Passo a Passo do Algoritmo RSA

Passo 1: Escolha de dois números primos

Escolha dois números primos grandes e diferentes, que chamaremos de p e q. Exemplo:

$$p = 61 \quad \text{e} \quad q = 53.$$

Passo 2: Calcule n (o módulo)

Multiplique p e q para obter n:

$$n = p \times q.$$

Exemplo:

$$n = 61 \times 53 = 3233.$$

O número n será usado como módulo tanto na chave pública quanto na privada.

Passo 3: Calcule $\varphi(n)$ (a função totiente)

Calcule $\varphi(n)$, que é dado por $(p-1) \times (q-1)$:

$$\varphi(n) = (p-1) \times (q-1).$$

Exemplo:

$$\varphi(n) = (61-1) \times (53-1) = 60 \times 52 = 3120.$$

Passo 4: Escolha o expoente público e

Escolha um número e que seja coprimo com $\varphi(n)$ e esteja entre 1 e $\varphi(n)$. Isso significa que o máximo divisor comum (MDC) entre e e $\varphi(n)$ deve ser 1. Exemplo:

$$e = 17 \quad \text{(pois 17 e 3120 são coprimos).}$$

Agora temos uma parte da chave pública: o par (e, n).

Passo 5: Calcule o expoente privado d

Encontre o valor de d, que é o inverso multiplicativo de e módulo $\varphi(n)$. Em outras palavras:

$$d \times e \equiv 1 \,(\mathrm{mod}\, \varphi(n)).$$

Este valor d é a parte secreta da chave e serve para descriptografar a mensagem. Exemplo: para $e = 17$ e $\varphi(n) = 3120$, $d = 2753$, pois

$$(2753 \times 17) \mod 3120 = 1.$$

Agora temos a chave privada: o par (d, n).

Nota: A expressão $\mod n$ significa que deve-se calcular o **resto da divisão** do resultado por n. O termo **mod** n indica a operação de obter o resto quando dividimos o número por n.

Criptografar uma mensagem

Para criptografar uma mensagem M, o emissor converte o conteúdo da mensagem em um número M menor que n. Exemplo: $M = 123$.

O emissor então usa a chave pública (e, n) para criptografar a mensagem:

$$C = M^e \mod n.$$

Exemplo:

$$C = 123^{17} \mod 3233 = 855.$$

O valor C é o texto cifrado, ou seja, a mensagem criptografada.

Descriptografar a mensagem

Para descriptografar a mensagem, o destinatário usa a chave privada (d, n) e realiza a operação:

$$M = C^d \mod n.$$

Exemplo:

$$M = 855^{2753} \mod 3233 = 123.$$

O resultado é o valor original da mensagem M, que o destinatário pode agora ler.

3 Resumo das Operações Principais

- **Chave Pública**: (e, n)
- **Chave Privada**: (d, n)
- **Criptografia**: $C = M^e \mod n$
- **Descriptografia**: $M = C^d \mod n$

4 Conclusão

A segurança do RSA depende da dificuldade de fatorar o número n em seus fatores primos p e q. Quando p e q são números primos muito grandes, essa fatoração se torna extremamente difícil, tornando o algoritmo seguro para uso em criptografia de dados.