A Matemática por Trás do

SISTEMA RSA

GRUPO

Andrey de Freitas Souza	823217536
Gabrielle Garcia Paz	823126085
Bianca Alves Ribeiro	8222240261
Bruno de Oliveira Santos	823223513
Webster Diógenes Rodrigues	8222242764

INTRODUÇÃO

O RSA (Rivest–Shamir–Adleman) é um dos algoritmos de criptografia assimétrica mais amplamente utilizados no mundo, sendo empregado em várias aplicações de segurança, incluindo a transmissão de dados de maneira segura. A principal vantagem do RSA é a utilização de um par de chaves: uma pública e uma privada.

GERAÇÃO DE NÚMEROS PRIMOS

A criptografia RSA depende da multiplicação de dois grandes números primos p e q para gerar uma chave segura. O método de geração de números primos pode ser descrito matematicamente da seguinte forma:

1. Escolhem-se dois números primos grandes p e q.
2. Calcula-se o produto n, onde:

$$n = p \times q$$

Esse valor n será utilizado tanto na chave pública quanto na chave privada.

EXEMPLO:

$p = 61$

$q = 53$

$n = 61 \times 53 = 3233$

A FUNÇÃO TOTIENTE DE EULER Φ(N)

A função totiente de Euler $\phi(n)$ (ou função ϕ de Euler) é crucial para garantir a segurança do sistema RSA. Ela é definida como o número de inteiros positivos menores que n que são coprimos com n, ou seja, que possuem máximo divisor comum (MDC) igual a 1.

Para $n = p \times q$, onde p e q são primos, a função $\phi(n)$ é calculada como:

$$\phi(n)=(p-1)\times(q-1)$$

Isso ocorre porque, para cada número primo p, $\phi(p)=p-1$, já que todos os números menores que um primo são coprimos com ele.

EXEMPLO:

$$\phi(n)=(61-1)\times(53-1) = 3120$$

GERAÇÃO DAS CHAVES

Com n e $\phi(n)$ calculados, podemos gerar o par de chaves.

1. A chave pública é composta por dois valores: e (um número primo pequeno, geralmente 65537) e n:

$$\text{Chave pública} = (e, n)$$

2. A chave privada é composta por d, que é calculado como o inverso multiplicativo modular de e em relação a $\phi(n)$, ou seja:

$$d \times e \equiv 1 \bmod \phi(n)$$

Isso significa que d é o valor que, quando multiplicado por e, resulta em 1 no módulo $\phi(n)$.

GERAÇÃO DAS CHAVES

EXEMPLO

Chave Pública:

$e = 65537$

$n = 3233$

Chave privada:

Calcula-se d como $d = e^{-1} \mod 3120 = 2753$

CRIPTOGRAFIA

A criptografia no RSA é baseada na exponenciação modular. Quando o remetente deseja enviar uma mensagem para o destinatário, ele criptografa a mensagem M (convertida em número inteiro) usando a chave pública (e,n). A criptografia é dada pela fórmula:

$$C = M^e \bmod n$$

Onde C é o texto cifrado.

EXEMPLO:

Mensagem M = 65

Texto cifrado $C = 65^{65537} \bmod 3233 = 2790$

DESCRIPTOGRAFIA

A descriptografia é feita de maneira semelhante à criptografia, mas usando a chave privada (d,n). Para recuperar o texto plano M, aplicamos:

$$M = C^{d} \mod n$$

EXEMPLO:

Texto cifrado C = 2790

Mensagem recuperada = $2790^{2753} \mod 3233 = 65$

CONCLUSÃO

O RSA é um sistema criptográfico robusto, baseado em problemas matemáticos difíceis, como a fatoração de grandes números primos. A segurança do RSA depende do fato de que é fácil multiplicar grandes números primos, mas extremamente difícil fatorar o produto deles. Entender a matemática por trás do RSA, como a função totiente de Euler e o cálculo do inverso modular, é fundamental para compreender como ele protege a comunicação digital.

Obrigado pela atenção!