O Algoritmo RSA

Livia Steise Gapar Diniz - 125111410617

O RSA (Rivest-Shamir-Adleman), desenvolvido em 1977, é um dos algoritmos de criptografia assimétrica mais fundamentais e amplamente utilizados. Sua segurança se baseia na dificuldade computacional de fatorar números inteiros grandes , o que o tornou a base para inúmeros protocolos de segurança digital, como HTTPS e SSH, sendo versátil tanto para a criptografia de dados quanto para a criação de assinaturas digitais.

Princípios Matemáticos

A segurança e o funcionamento do RSA estão enraizados em problemas matemáticos complexos e conceitos da teoria dos números:

- **Problema da Fatoração de Números Primos:** A base da segurança do RSA. Dado um número grande que é o produto de dois primos grandes e (), é computacionalmente inviável descobrir e sabendo apenas em um computador clássico.
- **Aritmética Modular:** Operações matemáticas realizadas dentro de um "ciclo" definido por um módulo . O resultado é sempre o resto da divisão pelo módulo, o que é crucial para manter os números em um tamanho gerenciável e para a prova de funcionamento do algoritmo.
- **Função Totiente de Euler ():** Representa a quantidade de inteiros positivos menores que que são coprimos com . Para , o cálculo é , sendo este um componente secreto crucial na geração da chave privada.
- **Teorema de Euler:** Garante o funcionamento da descriptografia. Um corolário direto deste teorema assegura que a descriptografia com a chave privada reverte a criptografia feita com a chave pública ((mod n)).

Funcionamento

O RSA utiliza um par de chaves (pública e privada) matematicamente vinculadas e seu processo se divide em três fases:

1. Geração do Par de Chaves:

1. **Seleção de Primos:** Gerar dois números primos grandes e distintos, e .
2. **Cálculo do Módulo ():** Calcular . Este valor é parte de ambas as chaves e define o tamanho da chave.
3. **Cálculo da Função Totiente ():** Calcular . Este valor deve ser mantido em segredo.
4. **Escolha do Expoente Público ():** Escolher um inteiro tal que e que seja coprimo com .
5. **Cálculo do Expoente Privado ():** Calcular como o inverso modular de em relação a , ou seja, (mod).

- **Chave Pública:** O par , que pode ser distribuída livremente.
- **Chave Privada:** O par , que deve ser mantida em segredo absoluto, assim como os primos e .

2. Criptografia:

- Para criptografar uma mensagem (representada como um número menor que), utiliza-se a chave pública do destinatário:

  Onde é o texto cifrado.

3. Descriptografia:

- Para descriptografar o texto cifrado , o destinatário utiliza sua própria chave privada: Onde é a mensagem original recuperada.

Aplicações Práticas em Segurança da Informação

O RSA consolidou-se como um pilar da segurança digital moderna devido à sua robustez e versatilidade.

Principais Aplicações:

- **Protocolos de Segurança Digital:** É a base para inúmeros protocolos como **HTTPS** e **SSH**.
- **Criptografia de Dados (em sistemas híbridos):** Embora seja mais lento que algoritmos simétricos como o AES, ele é usado em sistemas híbridos para:
    - **Troca de Chaves:** Criptografar uma chave de sessão simétrica (ex: AES), que, por sua vez, será usada para criptografar o grande volume de dados da comunicação.
- **Assinaturas Digitais:** É versátil para a criação de assinaturas digitais que garantem **autenticidade** e **integridade** de documentos e softwares.

Níveis de Segurança Recomendados:

Ano	Tamanho Mínimo (bits)	Segurança Simétrica Equivalente	Status
2010	1024	80 bits	Quebrado
2015	2048	112 bits	Seguro (Padrão Atual)
2025	3072	128 bits	Recomendado
2030	4096	140 bits	Preparação para o Futuro

Ameaças e Futuro:

- **Ameaça Quântica:** O RSA enfrenta uma ameaça existencial com o advento da computação quântica. O **Algoritmo de Shor** pode resolver o problema da fatoração em tempo polinomial, tornando o RSA obsoleto e inseguro. Estima-se que um computador quântico funcional poderia quebrar uma chave RSA de 2048 bits em questão de horas.
- **Criptografia Pós-Quântica (PQC):** A comunidade criptográfica está em transição acelerada para PQC, padronizando novos algoritmos como o **Kyber** (para troca de chaves, substituindo o RSA na confidencialidade) e o **Dilithium** (para assinaturas digitais, substituindo o DSA/ECDSA na autenticidade), ambos baseados em reticulados.

• **Kyber** (Troca de Chaves):

◦ Finalidade: Substituir o RSA e o ECC na troca segura de chaves para protocolos como HTTPS e VPNs.

◦ Vantagens: Extremamente rápido (mais que RSA/ECC), chaves relativamente pequenas (para PQC) e resistente aos algoritmos quânticos conhecidos.

• **Dilithium** (Assinaturas Digitais):

◦ Finalidade: Substituir DSA e ECDSA para garantir a autenticidade e integridade de mensagens e softwares.

◦ Vantagens: Gera assinaturas de forma rápida e com tamanho compacto.

A migração para Kyber e Dilithium representa a substituição direta das funcionalidades do RSA, garantindo confidencialidade e autenticidade em um mundo pós-quântico.