RSA

Universidade Federal do Ceará - Campus Quixadá

Roberto Cabral
rbcabral@ufc.br

26 de Março de 2021

Criptografia

RSA - Introdução

- Martin Hellman e Whitfield Diffie o primeiro artigo sobre criptografia assimétrica em 1976.
- Ronald Rivest, Adi Shamir e Leonard Adleman propuseram o criptosistema assimétrico RSA em 1977.
- Até agora, o RSA é o criptosistema assimétrico mais amplamente utilizado, embora a criptografia de curva elíptica (ECC) esteja se tornando cada vez mais popular.
- O RSA é usado principalmente em duas aplicações:
    - Transporte de chaves (isto é, compartilhamento de chave simétrica).
    - Assinaturas digitais.

Encriptação e Decriptação

- As operações do RSA são feitas sobre aneis inteiros Z_n (isto é, aritmética módulo n), onde $n = p \times q$, com p e q sendo primos grandes.
- A Encriptação e a decriptação não passa de exponenciação no anel.

Definition

Given the public key *(n,e)* = k_{pub} and the private key *d* = k_{pr} we write

$$y = e_{k_{pub}}(x) \equiv x^e \bmod n$$

$$x = d_{k_{pr}}(y) \equiv y^d \bmod n$$

where x, y ε Z_n.

We call $e_{k_{pub}}()$ the encryption and $d_{k_{pr}}()$ the decryption operation.

Encriptação e Decriptação

- Na pratica, x, y, n e d são numeros inteiros muito grandes. (> 1023 bits).
- A segurança do esquema recai no fato de que é difícil derivar o "expoente privado" d dado a chave pública (n, e).

Geração de Chaves

- Como todos os esquemas assimétricos, o RSA tem uma fase de inicialização onde são geradas as chaves pública e privada.

Algorithm: RSA Key Generation

Output: public key: $k_{pub} = (n, e)$ and private key $k_{pr} = d$

1. Choose two large primes p, q
2. Compute $n = p * q$
3. Compute $\Phi(n) = (p-1) * (q-1)$
4. Select the public exponent $e \in \{1, 2, \ldots, \Phi(n)-1\}$ such that $\gcd(e, \Phi(n)) = 1$
5. Compute the private key d such that $d * e \equiv 1 \bmod \Phi(n)$
6. **RETURN** $k_{pub} = (n, e)$, $k_{pr} = d$

Geração de Chaves

- Observações:
  - A escolha de dois primos grandes e distintos p, q (no Passo 1) não é trivial.
  - $\texttt{gcd}(e, \phi(n)) = 1$ garante que e tem um inverso e, assim, que sempre existe uma chave privada d.

RSA - Exemplo

ALICE		BOB
Message $\boldsymbol{x = 4}$		1. Choose $p = 3$ and $q = 11$
		2. Compute $n = p * q = 33$
		3. $\Phi(n) = (3-1) * (11-1) = 20$
		4. Choose $e = 3$
	$\xleftarrow{K_{pub} = (33,3)}$	5. $d \equiv e^{-1} \equiv 7 \bmod 20$
$y = x^e \equiv 4^3 \equiv 31 \bmod 33$		
	$\xrightarrow{y = 31}$	
		$y^d = 31^7 \equiv \boldsymbol{4 = x} \bmod 33$

Aspectos de Implementação

- O sistema criptográfico RSA usa apenas uma operação aritmética (exponenciação modular) que torna conceitualmente um esquema assimétrico simples
- Mesmo sendo conceitualmente simples, devido ao uso de números muito longos, o RSA é ordens de magnitude mais lenta do que esquemas simétricos, por exemplo, DES, AES
- Ao implementar o RSA (especialmente em um dispositivo restrito, como smartcards ou telefones celulares), deve-se prestar muita atenção à escolha correta dos algoritmos aritméticos.
- O algoritmo de quadrado e multiplicação permite uma rápida exponenciação, mesmo com números muito longos...

RSA

Universidade Federal do Ceará - Campus Quixadá

Roberto Cabral
rbcabral@ufc.br

26 de Março de 2021

Criptografia