Mini-aula: Criptografia RSA — conceitos e passo a passo

1) Ideia central

RSA é um sistema de criptografia de chave pública: cada participante tem um par de chaves (pública e privada).

Com a chave pública de alguém podemos criptografar; só a chave privada correspondente consegue descriptografar.

RSA baseia-se em operações com inteiros grandes e na dificuldade de fatorar grandes números (produto de dois primos).

2) Elementos matemáticos (resumo prático)

- Escolhemos dois primos grandes p e q.

- Calculamos n = p * q — módulo público.

- Calculamos $\phi(n) = (p-1)(q-1)$ (função totiente de Euler).

- Escolhemos um expoente público e tal que $\gcd(e, \phi(n)) = 1$ (por exemplo 65537 é comum).

- Calculamos o expoente privado d como o inverso multiplicativo de e mod $\phi(n)$.

- Chave pública: (n, e). Chave privada: (n, d).

3) Criptografia e descriptografia

- Cifrar: $c \equiv m^e \bmod n$

- Decifrar: $m \equiv c^d \bmod n$

Observação prática: usa-se padding (OAEP, PKCS#1 v1.5). OAEP é o padrão moderno.

4) Boas práticas

- Chaves $\geq$ 2048 bits.

- Padding OAEP para criptografia e PSS para assinaturas.

- Não implementar do zero: use bibliotecas auditadas.

- Proteja a chave privada e use fonte de entropia segura (OsRng).

5) Fluxo prático (exemplo que o código faz)

- Gera par de chaves RSA (2048 bits)

- Exporta em PEM (PKCS#8 e PKCS#1)

- Criptografa uma string com OAEP + SHA-256

- Descriptografa e verifica igualdade

- Mostra como salvar e carregar chaves PEM