RSA

Eduardo Lundgren

- Algoritmo RSA
  - p = Numero primo grande
  - q = Numero primo grande
  - n = p x q
  - phi = (p - 1)*(q - 1)

- Algoritmo RSA
- mod(phi, e) = 1
- Isso significa que “phi” e “e” são primos entre si
- 1 < e < phi
- d = Math.pow(e, -1) * mod(phi)

- Algoritmo RSA
  - Par de chaves públicas: n, e
  - Par de chaves privadas: n, d

- Criptografia
- M < n (plaintext)
- e - Chave pública
- C = Math.pow(M, e) * mod(n)

- Decriptografia
- C (texto cifrado)
- d - Chave privada
- M = Math.pow(C, d) * mod(n)