Calculando Chaves RSA

Prof.: Thiago H. Bom Conselho
UNATEC- Rede de Computadores

Objetivo do Apresentação

- **Entender a complexidade da criptografia assimétrica**

Teoria das Chaves

1. Escolha **p e q,** 2 inteiros primos
2. Calcule $n = p * q$
3. Calcule $\Phi(n) = (p-1) * (q-1)$
4. Escolha **e** inteiro, $1 < e < \Phi(n)$,tal que $mdc(e, \Phi(n))=1$
5. Calcule **d** inteiro, $1 < d < \Phi(n)$ tal que $e*d = 1 \bmod \Phi(n) \Rightarrow d = (k \times \Phi(n) + 1) / e$

- As chaves utilizadas serão:
- **KP = {e, n}** ***(pública) e*** **KU = {d,n}** ***(privada)***

Resumindo a Teoria

- P e Q – Números primos
- N = P * Q
- Z = (P – 1) * (Q – 1)
- E, numero primo em relação a Z (MDC(Z))
- (D * E) mod Z = 1

- As chaves utilizadas serão:
- **KP = {e, n}** ***(pública) e*** **KU = {d,n}** ***(privada)***

Cifrando e Decifrando

- Cifrando:
- (Texto Plano ^ E) mod N = Texto Cifrado
- Decifrando:
- (Texto Cifrado ^ D) mod N = Texto Plano

- OBS: **KP = {e, n}** ***(pública) e*** **KU = {d,n}** ***(privada)***

Exemplo de calculo de chaves

- Para facilitar o calculo iniciaremos com dois números primos pequenos
  - P=17 e Q=11
- Próximo passo é calcular o valor de **N** e de **Z**:
  - N = 17 * 11 = 187
  - Z = (17-1) * (11-1) = 160
- Definimos E como um numero primo em relação a Z (MDC(e,z) = 1)
  - E = 7

Continuação

- Calculamos os números D aceitos no algoritmo e escolhemos um:
  - D = 1 => (1 * 7) mod 160 = 7
  - D = 2 => (2 * 7) mod 160 = 14
  - D = 3 => (3 * 7) mod 160 = 21
  - ...
  - D = 23 => (23 * 7) mod 160 = 1
  - ...
  - D = 183 => (183 * 7) mod 160 = 1
  - ...
  - D = 343 => (343 * 7) mod 160 = 1
  - ...
  - D = 503 => (503 * 7) mod 160 = 1
  - ...
- Escolhemos entao D = 23, para facilitar o calculo.

Montando as chaves

- Chave Publica = e,n
  - Kp {7, 187}
- Chave Privada = d,n
  - Ku {23, 187}

Cifrando com a chave K Publica

- Para o exemplo utilizaremos o numero 5 para a cifra, sendo assim:
  - (5 ^ 7) mod 187
  - 78.125 mod 187
  - 146

- O texto cifrado é 146

Decifrando com a chave K Privada

- Recebido o texto cifrado 146, decriptografamos:
  - (146 ^ 23) mod 187
  - 60.272.011.127.891.400.000.000.000.000.000.00 0.000.000.000.000.000,00 mod 187
  - 5

- O texto plano é 5

Bibliografia

- Coutinho,S.C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA 2005.