

MAC0336/5723 Criptografia para Segurança de Dados

Lista 1

Mateus Agostinho dos Anjos

NUSP: 9298191

Exercício 1.

1. Temos como entrada: n e $\Phi(n)$
2. Sabemos que no algoritmo do RSA: $n = p * q$ e $\Phi(n) = (p - 1) * (q - 1)$
3. Queremos descobrir p e q para fatorar n

Podemos manipular essas equações da seguinte forma:

$$p - 1 = \frac{\Phi(n)}{(q - 1)} \quad , \quad (q - 1) > 0$$
$$p = \frac{\Phi(n)}{q - 1} + 1 \tag{I}$$

Substituindo (I) em $n = p * q$ temos:

$$n = \left(\frac{\Phi(n)}{q - 1} + 1 \right) * q$$
$$n = (\Phi(n) + q - 1) * q$$
$$n = \Phi(n) * q + q^2 - q$$
$$n = q^2 + (\Phi(n) - 1) * q \tag{II}$$

Note que, se isolássemos q em (I) chegaríamos em:

$$n = p^2 + (\Phi(n) - 1) * p$$

Portanto as soluções de p e q são simétricas.

Como temos n e $\Phi(n)$ podemos achar as raízes r_1 e r_2 de (II), sendo que $p = r_1$ e $q = r_2$, uma vez que p e q são primos a fatoração de n será $p * q$, portanto temos um algoritmo *rápido* (solução de uma equação de segundo grau, podendo utilizar *bhaskara*) para encontrar a fatoração de n .



Exercício 2.

1. $n = 21$ e $a = 5$

Fatorando $n - 1$ temos: $20 = 2^2 * 5$

Portanto $t = 2$ e $c = 5$ Agora calcularemos os módulos

$$(5^5)^1 \bmod 21 = 17$$

$$(5^5)^2 \bmod 21 = 16$$

$$(5^5)^4 \bmod 21 = 4$$

$$r_0 = 17, r_1 = 16, r_2 = 4$$

Como nenhum r_x é igual a $+1$ ou -1 temos que o número 21 é composto.

Esta resposta final está correta, uma vez que 21 é divisível por 3 e por 7 ele possui mais do que os 2 divisores naturais triviais, portanto não é primo.

2. $n = 13$ e $a = 2$

Fatorando $n - 1$ temos: $12 = 2^2 * 3$

Portanto $t = 2$ e $c = 3$ Agora calcularemos os módulos

$$(2^3)^1 \bmod 13 = 8$$

$$(2^3)^2 \bmod 13 = 12$$

$$(2^3)^4 \bmod 13 = 1$$

$$r_0 = 8, r_1 = 12, r_2 = 1$$

Como r_2 é igual 1 e r_x imediatamente anterior a ele é $r_1 = 12 (-1)$ o número n é dado como primo.

Esta resposta final está correta, uma vez que 13 é primo.

Exercício 3.

Exercício 4.