

Criptografia Assimétrica: RSA

RSA são as iniciais dos autores deste algoritmo (Rivest, Shameir e Adleman). A segurança deste método está baseada em dois princípios:

- A dificuldade computacional esperada (mais ainda não provada) em fatorar grandes números. Este fato vai ser melhor estudado nas próximas aulas, quando vocês serão desafiados a “quebrar” o método RSA.
- A garantia de que quem diz ser alguém de fato o é. Esta garantia é obtida pela certificação digital.

Trocando em miúdos, para o RSA funcionar, a chave pública de todo mundo deve ser sempre conhecida e espera-se ter certeza de que quem diz ser o proprietário do certificado é de fato quem diz ser.

Algoritmo RSA A seguir, as etapas necessárias para calcular as chaves pública e privada e depois como criptografar e decryptografar mensagens.

Para o cálculo de CP e CS há que se escolher 2 números primos p e q	Por exemplo: p = 3 e q = 7
Calcula-se n = p x q	n = 21
Calcula-se f = (p-1) x (q-1)	f = 2 x 6= 12
Escolhe-se c, tal que o mdc entre c e f seja 1	c = 5 já que mdc(5,12) = 1
Escolhe-se d tal que (c x d) mod f = 1	5 x d mod 12 tem que ser 1, d =17 já que 5 x 17 = 85 e 85 mod 12 = 1
A CP do indivíduo é (c,n)	CP = (5,21)
A CS do indivíduo é (d,n)	CS = (17,21)
Quando alguém quer mandar uma mensagem para o indivíduo, quebra a mensagem m em blocos (números)	digamos que m = 3, 14, 9
Para cifrar m, esse alguém faz $CP(m) = m^c \bmod n$	$3^5 \bmod 21 = 12$, $14^5 \bmod 21 = 14$, $9^5 \bmod 21 = 18$
Quando a mensagem chega, há que se fazer $m' = [CP(m)]^d \bmod n$	$12^{17} \bmod 21 = 3$, $14^{17} \bmod 21 = 14$, $18^{17} \bmod 21 = 9$

Para fazer este exercício você deverá ter acesso a um computador, e nele deverá programar a seguinte função para auxiliar na tarefa de elevar grandes números a grandes expoentes:

- ```
1: inteirolongo função XELEVADOAY (inteirolongo X, Y, N) {algoritmo
 ADDITION CHAINING, SCH96, pag. 244}
2: inteirolongo TMP
3: se Y = 1 então
4: devolva (X mod N) {em C ou Python: X % N}
5: senão
6: se (Y mod 2) = 0 então
7: TMP ← XELEVADOAY (X, (Y/2), N)
8: devolva (TMP * TMP) mod N
9: senão
10: TMP ← XELEVADOAY (X, ((Y-1)/2), N)
11: TMP ← (TMP * TMP) mod N
12: TMP ← (TMP * X) mod N
13: devolva TMP
14: fim se
15: fim se
16: fim função
```

Depois de digitar, use os seguintes exemplos para testar o programa  
 $(2^3) \bmod 20 = 8$   
 $(5387^{2189}) \bmod 3311 = 1668$   
 $(7752^{4156}) \bmod 12981 = 4812$

Para criptografar uma mensagem qualquer, você deve:

1. Converter a mensagem (caracteres) em números
2. Escolher o par de números que usará como chave (a,b)
3. Para cada número, calcular  $(numero^a) \bmod b$  e enviar o resultado

Para decryptografar uma mensagem qualquer, supostamente já em forma de números, você deve:

1. Recuperar a chave oposta usada na criptografia, na forma (c,d)
2. Para cada número recebido, calcular  $(numero^c) \bmod d$
3. Recuperar o caractere usando a tabela

|   |   |   |   |   |    |   |    |   |    |   |    |   |    |
|---|---|---|---|---|----|---|----|---|----|---|----|---|----|
|   |   | D | 5 | H | 9  | L | 13 | P | 17 | T | 21 | X | 25 |
| A | 2 | E | 6 | I | 10 | M | 14 | Q | 18 | U | 22 | Y | 26 |
| B | 3 | F | 7 | J | 11 | N | 15 | R | 19 | V | 23 | Z | 27 |
| C | 4 | G | 8 | K | 12 | O | 16 | S | 20 | W | 24 | / | 28 |

## Exemplo

Erasmus (cuja chave publica é [1153,4757] mandou a mensagem 3568, 386. O que ela significa ?  
Resposta: O / (a letra O e um espaço)

Agora você quer mandar a mensagem "AS" para a Frida (chave pública da Frida é [763,3953]). Como fica ?  
Resposta: 453, 867

A mensagem "447, 686" só deve ser lida por você (sua chave secreta é [193,1829]. O que é ?  
Resposta: J A (as letras J e A)

Você quer assinar a mensagem LH, usando a sua chave secreta. Como fica ?  
Resposta: 1375 e 390

## 🔗 Para você fazer

1. Eis as chaves públicas conhecidas

Alice=(1343,6887), Bento=( 347,2537)  
Carlos=( 475,2479), Dante=( 901,4661)  
Erasmus=(1187,4897), Frida=(1687,8633)

2. Sua chave pública é ( 211,1147 ) e sua chave secreta é ( 691 )

Obs: Note que a sua CS e CP compartilham o segundo número. Ele só não é escrito na CS, já que não dá para chamá-lo de secreto.

3. Você recebeu a seguinte mensagem (alfabética) de alice  
Mensagem:

997 269 3282 149 5857 3282 6124 5854 149 3965  
269 3282 5187 5187 3282 2299 5187 576 149 997  
269 3282 149 5857 3282 5342 576 5187 149 5857  
3282 149 4511 5854 5854 4511 2828 5857 4511

Qual é a mensagem ?

A=\_\_\_\_\_.

Dica: decodifique usando a CP do remetente

4. Você quer mandar a mensagem abaixo para carlos  
Mensagem:

ENCONTRA/SOB/AS/MAOS/O/DURO/CRANIO

B=\_\_\_\_\_.

Dica: codifique com a CP do destinatário

5. A mensagem abaixo só deve ser lida por você. Qual é?  
Mensagem:

965 1008 541 617 176 143 10 516 176 68  
617 643 1008 27 617 1041 797 68 617 1008  
516 617 281 387 10 541 1008 516 617 965  
1008 541 1008 643 68

C=\_\_\_\_\_.

Dica: decodifique usando a sua CS

6. Esta mensagem vai assinada por você  
Mensagem:

E/AS/DURAS/FADIGAS/DA/GUERRA/PROVEI

D=\_\_\_\_\_.

Dica: codifique com a sua CS

Agora responda as questões, usando A, B, C e D calculados acima

|       |       |       |       |
|-------|-------|-------|-------|
| A[11] | A[39] | B[17] | B[34] |
|       |       |       |       |
| C[29] | C[35] | D[10] | D[35] |
|       |       |       |       |

