TAREA ALGORITMO RSA

Matemáticas II



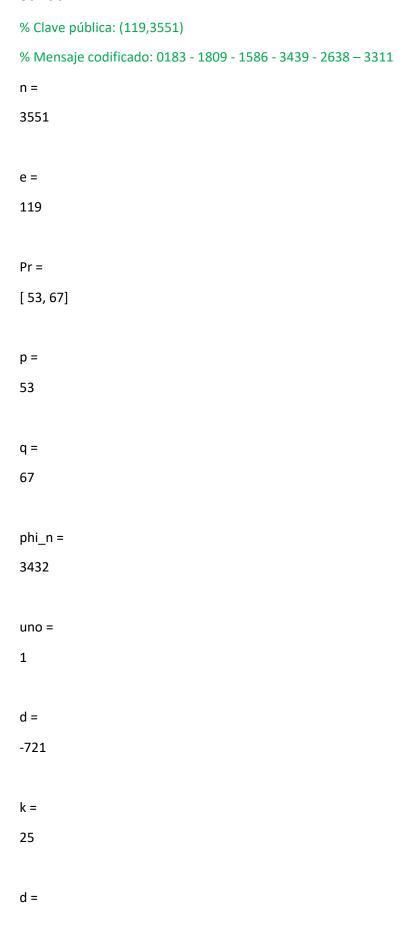
Por: Ismael Da Palma Fernández

Ejercicio Algoritmo RSA 1

Comandos de Matlab:

```
%% ----- Ejercicio RSA 1 -----
%Clave pública: (119,3551)
%Mensaje codificado: 0183 - 1809 - 1586 - 3439 - 2638 - 3311
응
clc
%Guardamos los valores de la clave pública
diary TareaAlgoritmoRSA1.txt
n = sym(3551)
e=sym(119)
%Factorizamos n y obtenemos p y q
Pr=factor(n)
p=Pr(1)
q=Pr(2)
%Con p y q obtenemos phi(n)
phi n = (p-1) * (q-1)
%Calculamos d
[uno d k]=gcd(e,phi n)
%Como d sale negativa hacemos su modulo
d=mod(d,phi n)
%Obtenemos la clave privada: (1463,3351)
%Comprobamos que todo es correcto:
mod(e*d,phi n)
%Descodificamos el mensaje
C=sym([0183 1809 1586 3439 2638 3311])
M=mod(C.^d,n)
%El mensaje descodificado es:
%CANGURO ROJO
diary off
```

Salida:



```
2711

ans =
1

C =
[ 183, 1809, 1586, 3439, 2638, 3311]

M =
```

[301, 1407, 2219, 1600, 1916, 1016]

% El mensaje descodificado es: **CANGURO ROJO**

Ejercicio Algoritmo RSA 2

Comandos de Matlab:

```
%% ----- Ejercicio RSA 2 -----
%Clave pública: (121,3053)
%Mensaje codificado: 2689 - 2741 - 0803 - 2179 - 2741 - 1152 - 2997 - 0830
clc
%Guardamos los valores de la clave pública
diary TareaAlgoritmoRSA2.txt
n = sym(3053)
e=sym(121)
%Factorizamos n y obtenemos p y q
Pr=factor(n)
p=Pr(1)
q=Pr(2)
%Con p y q obtenemos phi(n)
phi n = (p-1) * (q-1)
%Calculamos d
[uno d k]=gcd(e,phi n)
%Como d sale negativa hacemos su modulo
d=mod(d,phi n)
%Obtenemos la clave privada: (2041,3053)
%Comprobamos que todo es correcto:
mod(e*d,phi n)
%Descodificamos el mensaje
C=sym([2689 2741 0803 2179 2741 1152 2997 0830])
M=mod(C.^d,n)
%El mensaje descodificado es:
%NOS VEMOS LUEGO
diary off
```

Salida:

% Clave pública: (121,3053) % Mensaje codificado: 2689 - 2741 - 0803 - 2179 - 2741 - 1152 - 2997 - 0830 n = 3053 e = 121 Pr = [43, 71] p = 43 q = 71 phi_n = 2940 uno = 1 d = -899 k = 37

```
d =
2041

ans =
1

C =
[ 2689, 2741, 803, 2179, 2741, 1152, 2997, 830]

M =
[ 1416, 2000, 2305, 1316, 2000, 1222, 507, 1600]
```

% El mensaje descodificado es: NOS VEMOS LUEGO