

## Práctica 6: RSA por bloques

### Modelo 4

4 de mayo de 2021

Supongamos que una red local de usuarios utiliza el sistema criptográfico RSA en modo bloques. Se conocen las claves públicas de los usuarios del sistema, así como las factorizaciones (pues los usuarios no han sido muy hábiles al generar sus claves). Los datos vienen indicados en la tabla siguiente:

| usuario | $n$                       | $e$       | factorización de $n$                |
|---------|---------------------------|-----------|-------------------------------------|
| Pepa    | 62439738695706104201747   | 356812573 | $249879448303 \cdot 249879448349$   |
| Benito  | 743330222539755158153     | 80263681  | $27264083009 \cdot 27264083017$     |
| María   | 8849169404252643679       | 196413997 | $2974755337 \cdot 2974755367$       |
| Juan    | 5244938048376303456108649 | 114340249 | $2290182972661 \cdot 2290182972709$ |

Se sabe que la información está escrita en el alfabeto

$alf = \text{“abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ$   
 $\text{áéíóúÁÉÍÓÚ0123456789 ,:!.?()”}$

y que para la codificación numérica del alfabeto, a cada símbolo  $\alpha$  se le asigna el número  $n(\alpha) = p(\alpha) - 1$ , donde  $p(\alpha)$  es la posición que ocupa  $\alpha$  dentro del alfabeto. Se pide descifrar el mensaje cifrado del *Modelo 4* que podéis encontrar en el archivo *datos\_6*, sabiendo que es un mensaje que Juan envió a María.

mensaje en claro

**AVISO:** En el mensaje cifrado no tengáis en cuenta las comillas que aparecen al comienzo y al final.  
**AVISO:** Para escribir el mensaje en claro tenéis que considerar los dos espacios como un cambio de línea y no tener en cuenta los espacios que aparecen al final del mensaje en claro.