

SEGUNDO PARCIAL - 06 DE JULIO DE 2015. DURACIÓN: 3 HORAS

N° de parcial	Cédula	Apellido y nombre	Salón

### Primera parte: Múltiple Opción

MO	
1	2

**Ejercicio 1.** Ana y Belen quieren acordar una clave común utilizando el el protocolo Diffie-Hellman. Para ello toman el primo  $p = 503$  y  $g = 10$  raíz primitiva módulo  $p$ . Ana elije el número  $m = 434$  y le envía el número 498 a Belen. Belen elije el número  $n = 9$ . ¿Cuál es la clave  $k$  común que acordaron Ana y Belen? Indicar cuál de las opciones es correcta:

- A.  $k = 24$ .                      B.  $k = 297$ .                      C.  $k = 247$ .                      D.  $k = 287$ .

**Ejercicio 2.** Sean  $n = 341$  y  $e = 13$ . Para los datos anteriores sea función de descifrado  $D : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  definida por el protocolo RSA. Indicar cuál de las opciones es correcta:

- A.  $D(y) = y^{12} \pmod{n}$ .                      C.  $D(y) = y^{277} \pmod{n}$ .  
 B.  $D(y) = y^{105} \pmod{n}$ .                      D.  $D(y) = y^{157} \pmod{n}$ .

### Segunda parte: Desarrollo

#### Ejercicio 3.

- Enunciar y demostrar el Teorema de Lagrange para grupos.
- Sea  $G$  un grupo y  $x, y \in G$  elementos de orden finito.
  - Probar que si  $xy = yx$  y  $\text{mcd}(\text{o}(x), \text{o}(y)) = 1$ , entonces  $\text{o}(xy) = \text{o}(x)\text{o}(y)$ .
  - Mostrar con dos ejemplos que cada hipótesis de la parte anterior es necesaria.

#### Ejercicio 4.

- Probar que 3 es raíz primitiva módulo 98.
- ¿Cuántas raíces primitivas módulo 98 hay?
- Listar todas las raíces primitivas módulo 98 (pueden expresarlas como potencia).

**Ejercicio 5.** Averiguar si para los siguientes pares de grupos existen morfismos  $f : G \rightarrow K$  no triviales entre ellos. En caso de que existan, construir alguno (justificando que es homomorfismo) y en caso contrario explicar por qué.

- $G = \mathbb{Z}_9$ ,  $K = U(24)$ .
- $G = U(9)$ ,  $K = \mathbb{Z}_{12}$ .
- $G = U(15)$ ,  $K = \mathbb{Z}_6$ .