

EXAMEN - 17 DE FEBRERO DE 2016. DURACIÓN: 3 HORAS Y MEDIA.

N° de examen	Cédula	Apellido y nombre

**Ejercicio 1.**

- a. Dados  $p, q, n, d$  y  $e$  en las hipótesis del criptosistema RSA y las funciones de cifrado  $E(x) = x^e \pmod{n}$  y descifrado  $D(y) = y^d \pmod{n}$ . Probar que la función de descifrado funciona como tal; es decir, probar que:

$$D(E(x)) = x \pmod{n} \quad \forall x \in \mathbb{Z}_n.$$

- b. Dados los primos  $p = 17$ ,  $q = 19$  y  $e = 11$ , calcular la función de descifrado  $D$ .
- c. Con los mismos datos que en (b) cifrar  $x = 170$ .

**Ejercicio 2.** Sea  $G$  un grupo y  $g \in G$ .

- a. Probar que  $\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$  es un subgrupo de  $G$ .
- b. Probar que  $|\langle g \rangle| = o(g)$
- c. Si  $G$  es finito, probar que  $g^{|G|} = e_G$ .

**Ejercicio 3.**

- a. Hallar todas las soluciones módulo 61 de la ecuación  $3x \equiv 10 \pmod{61}$ .
- b. Sea la ecuación

$$4x \equiv 20 \pmod{100}. \tag{1}$$

- i) Hallar todas las soluciones módulo 100 de la ecuación (1).
- ii) Hallar todas sus soluciones módulo 50 y 25 de la ecuación (1).
- iii) ¿Cuántas soluciones módulo 1000 tiene la ecuación (1)?

**Ejercicio 4.**

- a. Probar que 2 es raíz primitiva módulo 59.
- b. Hallar el orden de 57 módulo 59.
- c. Encontrar todos los homomorfismos  $f : U(59) \rightarrow S_3$ .
- d. Hallar una raíz primitiva módulo 118.