EXAMEN - 22 DE JULIO DE 2015. DURACIÓN: 3:30 HORAS

N° de parcial	Cédula	Apellido y nombre	Salón

Primera parte: Múltiple Opción

MO	
1	2

Ejercicio 1. Sean $n = 319$ y $e = 19$. Para los datos anteriores sea función de descifrado $D : \mathbb{Z}_n \to \mathbb{Z}_n$ definida por el protocolo RSA. Indicar cuál de las opciones es correcta:

A. $D(y) = y^{42} \pmod{n}$.

B. $D(y) = y^{59} \pmod{n}$.

C. $D(y) = y^{84} \pmod{n}$.

D. $D(y) = y^{67} \pmod{n}$.

Ejercicio 2. Sea $0 \leq m < 325$ tal que $m \equiv 435^{241} \pmod{325}$. Indicar cuál de las opciones es correcta:

A. $m = 65$. **B**. $m = 110$. **C**. $m = 300$. **D**. $m = 175$.

Segunda parte: Desarrollo

Ejercicio 3. Dado los siguientes sistemas, investigar si tienen solución, y en caso que tenga encontrar todas sus respectivas soluciones.

a. $\begin{cases} x \equiv 2 \pmod{11} \\ x \equiv 5 \pmod{8} \\ x \equiv 14 \pmod{15} \end{cases}$.

b. $\begin{cases} x \equiv 9 \pmod{20} \\ x \equiv 5 \pmod{24} \\ x \equiv 35 \pmod{66} \end{cases}$.

Ejercicio 4.

a. Definir la funcion $\varphi : \mathbb{N}^+ \to \mathbb{N}$ de Euler.

b. Probar que si $\operatorname{mcd}(n, m) = 1$ entonces

$$\varphi(nm) = \varphi(n)\varphi(m).$$

c. Calcular:

i) $\varphi(125)$.

ii) $\varphi(108)$.

d. Sabiendo que 2 es raíz primitiva módulo 25 y 125, hallar todos los homomofismos

$$f : U(125) \to U(25).$$

Ejercicio 5.

a. Sea G un grupo finito, y $g \in G$ tal que $\operatorname{o}(g) = m$. Probar que

$$\operatorname{o}\left(g^k\right) = \frac{m}{\operatorname{mcd}(k, m)}.$$

b. Probar que si existe una raíz primitiva módulo n entonces hay exactamente $\varphi(\varphi(n))$ raíces primitivas módulo n.

c. Sea p un primo y g una raíz primitiva módulo p.

i) Probar que si n es el orden de g en $U(p^2)$ entonces $p - 1 \mid n$.

ii) Probar que g o $g + p$ es raíz primitiva módulo p^2.

d. Hallar una raíz primitiva módulo 11^2.