

SEGUNDO PARCIAL - 29 DE JUNIO DE 2016. DURACIÓN: 3 HORAS Y MEDIA

N° de parcial	Cédula	Apellido y nombre	Salón

Primera parte: Múltiple Opción

MO	
1	2

Ejercicio 1. Austria y Bielorusia quieren acordar una clave común utilizando el protocolo Diffie-Hellman. Para ello toman el primo $p = 499$ y $g = 7$ raíz primitiva módulo p . Austria elige el número $m = 394$ y le envía el número 489 a Bielorusia. Bielorusia elige el número $n = 18$. ¿Cuál es la clave k común que acordaron Austria y Bielorusia?

Indicar cuál de las opciones es correcta:

- A. $k = 331$. B. $k = 77$. C. $k = 80$. D. $k = 64$.

Ejercicio 2. Sean $n = 209$ y $e = 7$. 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. $D(y) = y^{103} \pmod{n}$. C. $D(y) = y^{119} \pmod{n}$.
 B. $D(y) = y^{30} \pmod{n}$. D. $D(y) = y^{163} \pmod{n}$.

Segunda parte: Desarrollo

Ejercicio 3.

- a. Sea $(G, *)$ un grupo finito y H un subgrupo de G . Definimos la siguiente relación en G :

$$g \sim g' \Leftrightarrow g * (g')^{-1} \in H.$$

Probar que la relación definida es una relación de equivalencia.

- b. Sean G, K grupos finitos y $f : G \rightarrow K$ un homomorfismo de grupos. Probar que $\text{Ker}(f)$ es un subgrupo de G .
 c. Probar el teorema de órdenes para grupos:

Sean G y K dos grupos finitos y $f : G \rightarrow K$ un homomorfismo de grupos. Entonces

$$|G| = |\text{Ker}(f)| |\text{Im}(f)|.$$

Ejercicio 4.

- a. Sean G un grupo finito, $g \in G$ y $n \in \mathbb{N}$, probar que $o(g^n) = \frac{o(g)}{\text{mcd}(o(g), n)}$.
 b. Probar que 2 es raíz primitiva módulo 101 y hallar un elemento de $U(101)$ con orden 10.

Ejercicio 5. Sean los grupos $G = \mathbb{Z}_{100}$ y $K = U(101)$.

- a. Probar que los grupos G y K son isomorfos.
 b. Describir todos los isomorfismos entre G y K .