

SEGUNDO PARCIAL - 29 DE JUNIO DE 2016.

### Primera parte: Múltiple Opción

**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.  $k = 64$ .

**Solución:**

Tenemos que calcular  $489^{18} \pmod{499} \equiv (-10)^{18} \pmod{499} \equiv ((-10)^3)^6 \pmod{499} \equiv (-1000)^6 \pmod{499} \equiv (-2)^6 \pmod{499} \equiv 64 \pmod{499}$ .

**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.  $D(y) = y^{163} \pmod{n}$ .

**Solución:**

La función de descifrado es  $D(y) = y^d \pmod{n}$  donde  $d$  es tal que  $d \equiv e^{-1} \pmod{\varphi(n)}$ . La factorización de  $n$  es  $209 = 11 \cdot 19$ , por lo que  $\varphi(11 \cdot 19) = 10 \cdot 18 = 180$ . Utilizando el algoritmo extendido de Euclides obtenemos  $d \equiv 103 \pmod{180}$ .

### 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*

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

**Solución:** Ver la segunda demostración del Teorema de Ordenes de las notas, Teorema 3.9.8.

#### Ejercicio 4.

- a. Sean  $G$  un grupo finito,  $g \in G$  y  $n \in \mathbb{N}$ , probar que  $o(g^n) = \frac{o(g)}{\gcd(o(g), n)}$ .

**Solución:** Ver Proposición 3.7.8 parte 7 de las notas.

- b. Probar que 2 es raíz primitiva módulo 101 y hallar un elemento de  $U(101)$  con orden 10.

**Solución:** Para ver que 2 es r.p. módulo 101, alcanza con ver  $2^{50} \not\equiv 1 \pmod{101}$  y  $2^{20} \not\equiv 1 \pmod{101}$ , ya que  $\varphi(101) = 100 = 2^2 \cdot 5$  y  $100/2 = 50$ ,  $100/5 = 20$ . Entonces  $2^{20} = (2^{10})^2 \equiv (1024)^2 \pmod{101} \equiv 14^2 \pmod{101} \equiv 196 \pmod{101} \equiv 95 \pmod{101} \not\equiv 1 \pmod{101}$ . También  $2^{50} = (2^{20})^2 \cdot 2^{10} \equiv (95)^2 \cdot 14 \pmod{101} \equiv (-6)^2 \cdot 14 \pmod{101} \equiv 36 \cdot 14 \pmod{101} \equiv 504 \pmod{101} \equiv -1 \pmod{101}$ . Con eso probamos que 2 es r.p. módulo 101.

Para hallar un elemento de orden 10 utilizamos la parte anterior y el hecho que el orden de 2 es 100. Utilizamos  $n = 10$  y obtenemos

$$o(2^{10}) = \frac{o(2)}{\gcd(o(2), 10)} = \frac{100}{\gcd(100, 10)} = \frac{100}{10} = 10.$$

Por lo tanto  $o(14) = 10$ .

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

- a. Probar que los grupos  $G$  y  $K$  son isomorfos.

**Solución:** Dado que  $\bar{1}$  es generador de  $G$  y tiene orden 100 que es el orden de 2 en  $K$ , el morfismo  $f : G \rightarrow K$  dado por  $f(\bar{n}) = 2^n \pmod{101}$  es un morfismo bien definido. Es fácil ver que es inyectivo ya que  $f(n) = 1$  si y solo si  $2^n \equiv 1 \pmod{101}$ , o sea si  $n \equiv 0 \pmod{100}$ . Como  $G$  y  $K$  tienen igual orden entonces es biyectivo y por lo tanto es un isomorfismo.

- b. Describir todos los isomorfismos entre  $G$  y  $K$ .

**Solución:** En la parte anterior podemos cambiar  $f$  por  $f_k$  donde  $f_k(n) = 2^{kn} \pmod{101}$  y  $k$  otro elemento de orden 100 de  $\mathbb{Z}_{100}$ . El nuevo  $f_k$  es isomorfismo de igual manera que antes. Por el ejercicio anterior vemos que los  $k$  que cumplen que son generadores de  $\mathbb{Z}_{100}$  son los que cumplen  $\gcd(k, 100) = 1$ . Y por lo tanto obtuvimos todos los isomorfismos entre  $G$  y  $K$ .