

SEGUNDO PARCIAL - XX DE JULIO DE 2015.

Primera parte: Múltiple Opción

Ejercicio 1. Ana y Belen quieren acordar una clave común utilizando el protocolo Diffie-Hellman. Para ello toman el primo $p = 503$ y $g = 10$ raíz primitiva módulo p . Ana elige el número $m = 434$ y le envía el número 498 a Belen. Belen elige 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. $k = 287$.

Solución:

Tenemos que calcular $498^9 \pmod{503} \equiv (-5)^9 \pmod{503}$. Utilizamos el método de exponenciación rápida, $9 = 8 + 1 = 2^3 + 2^0$ por lo que

$$(-5)^9 \equiv (-5)^{2^3} (-5)^{2^0} \pmod{503}.$$

Computamos la tabla

t	$(-5)^{2^t} \pmod{503}$
0	-5
1	25
2	$625 \equiv 122 \pmod{503}$
3	$14884 \equiv 297 \pmod{503}$

Por lo que $(-5)^9 \equiv 297(-5) \pmod{503} \equiv 24 \pmod{503}$.

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. $D(y) = y^{157} \pmod{n}$.

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 $341 = 11 \cdot 31$, por lo que $\varphi(11 \cdot 13) = 10 \cdot 30 = 300$. Utilizando el algoritmo extendido de Euclides obtenemos $d \equiv 277 \pmod{300}$.

Segunda parte: Desarrollo

Ejercicio 3.

- a. Enunciar y demostrar el Teorema de Lagrange para grupos.

Solución:

Ver teórico.

- b. Sea G un grupo y $x, y \in G$ elementos de orden finito.

- i) Probar que si $xy = yx$ y $\text{mcd}(\text{o}(x), \text{o}(y)) = 1$, entonces $\text{o}(xy) = \text{o}(x)\text{o}(y)$.

Solución:

Ver teórico.

- ii) Mostrar con dos ejemplos que cada hipótesis de la parte anterior es necesaria.

Solución:

- Sea $G = S_3$ y consideremos $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ y $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Tienen ordenes $o(\tau) = 2$ y $o(\sigma) = 3$, así que cumplen $\text{mcd}(o(\tau), o(\sigma)) = 1$. Además

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \sigma\tau.$$

Como $o(\tau\sigma) = 2$ y $o(\sigma\tau) = 3$ vemos que se precisa la hipótesis $\sigma\tau = \tau\sigma$.

- Consideramos ahora el grupo $G = \mathbb{Z}_6$ y $g = 2$, $h = 4$. Cumplen $gh = hg$ porque G es abeliano. Por otro lado $o(g) = 3$, $o(h) = 3$ y $o(g+h) = o(0) = 1 \neq 9 = o(2) \cdot o(4)$.

Ejercicio 4.

- a. Probar que 3 es raíz primitiva módulo 98.

Solución:

Calculamos $\varphi(98) = \varphi(2 \cdot 49) = \varphi(2)\varphi(7^2) = 7^2 - 7 = 42 = 2 \cdot 3 \cdot 7$. Para probar que 3 es raíz primitiva módulo 98 alcanza con probar que $3^{\varphi(98)/p} \not\equiv 1 \pmod{98}$ para $p = 2, 3, 7$. O sea que $3^{21}, 3^{14}, 3^6 \not\equiv 1 \pmod{98}$. Primero

$$3^6 = (3^3)^2 = 27^2 = 729 \equiv 43 \pmod{98}.$$

Luego

$$3^{14} = 3^2 \cdot (3^6)^2 \equiv 9 \cdot 43^2 \pmod{98} \equiv 9 \cdot 1849 \pmod{98} \equiv 9 \cdot (-13) \pmod{98} \equiv 79 \pmod{98}.$$

Por último

$$3^{21} = 3^{14} \cdot 3^6 \cdot 3 \equiv 79 \cdot 43 \cdot 3 \pmod{98} \equiv 65 \cdot 3 \pmod{98} \equiv 195 \pmod{98} \equiv 97 \pmod{98}.$$

Como se cumple lo que dijimos antes, concluimos que 3 es raíz primitiva módulo 98.

- b. ¿Cuántas raíces primitivas módulo 98 hay?

Solución:

Como existe una raíz primitiva módulo $n = 98$ entonces hay exactamente $\varphi(\varphi(98)) = \varphi(2 \cdot 3 \cdot 7) = 2 \cdot 6 = 12$ raíces primitivas módulo 98

- c. Listar todas las raíces primitivas módulo 98 (pueden expresarlas como potencia).

Solución:

Como 3 es raíz primitiva módulo 98 sabemos que todos los elementos de $U(98)$ son de la forma 3^k para algún k . Aplicando la relación de ordenes en un grupo finito G , que dice que si $g \in G$ y $k \in \mathbb{N}$ entonces

$$o(g^k) = \frac{o(g)}{\text{mcd}(o(g), k)}$$

podemos ver que 3^k es raíz primitiva módulo 98 si y sólo si $\text{mcd}(k, \varphi(98)) = 1$. Por lo tanto, las raíces primitivas módulo 98 son:

$$3^k \text{ para } k = 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.$$

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.

- a. $G = \mathbb{Z}_9$, $K = U(24)$.

Solución:

Como $|G| = 9$ y $|K| = \varphi(24) = 8$ son coprimos entonces no hay morfismos no triviales entre ellos, ya que por el teorema de Lagrange $|\text{Im}(f)| \mid |K|$ y por el Teorema de órdenes, $|\text{Im}(f)| \mid |G|$. Y entonces $|\text{Im}(f)| = 1$ y por lo tanto f es trivial-

b. $G = U(9)$, $K = \mathbb{Z}_{12}$.

Solución:

Tenemos que G es cíclico, $G = U(9) = \langle 2 \rangle$ y de orden 6, por lo tanto un morfismo $f : G \rightarrow K$ es de la forma $f(2^n) = \underbrace{f(2) + \cdots + f(2)}_{n \text{ veces}}$ con la condición que $\text{o}(f(2)) \mid \text{o}(2)$. Es decir, basta con elegir

$f(2)$ un elemento de \mathbb{Z}_{12} cuyo orden divida a 6. Por ejemplo, podemos tomar $f(2) = 2$ y por lo tanto $f(2^n) = n \cdot 2 \in \mathbb{Z}_{12}$.

c. $G = U(15)$, $K = \mathbb{Z}_6$.

Solución:

El grupo G tiene orden $\varphi(15) = 2 \cdot 4 = 8$ y no es cíclico por el teorema de la raíz primitiva. Si existe $f : G \rightarrow K$ entonces sabemos que $|\text{Ker}(f)| |\text{Im}(f)| = |G| = 8$. Además $|\text{Im}(f)| \mid |K| = 6$ y entonces si f no es trivial tiene que cumplir $|\text{Im}(f)| = 2$ y $|\text{Ker}(f)| = 4$.

El único subgrupo de orden 2 de \mathbb{Z}_6 es $\{0, 3\}$ y por lo tanto $\text{Im}(f) = \{0, 3\}$.

Por otro lado, $\text{Ker}(f)$ es un subgrupo de $U(15)$ de orden 4.

Un subgrupo de G de orden 4 es $\{1, 2, 4, 8\} = \langle 2 \rangle$, por lo tanto una posibilidad es que $\text{Ker}(f) = \langle 2 \rangle$ (y que $\text{Im}(f) = \{0, 3\}$). Es decir que $f(1) = f(2) = f(4) = f(8) = 0$ y que $f(7) = f(11) = f(13) = f(14) = 3$.

Falta verificar que f es un homomorfismo; es decir que $f(x \cdot y) = f(x) + f(y)$ para todo $x, y \in U(15)$.

Tenemos que $\text{ker}(f) = \{2^k : k \in \mathbb{Z}\}$ y que $\{7, 11, 13, 14\} = \{-8, -4, -2, -1\} = \{-2^k : k \in \mathbb{Z}\}$.

Y como

- $f(2^k \cdot 2^l) = f(2^{k+l}) = 0 = 0 + 0 = f(2^k) + f(2^l)$,
- $f((-2^k) \cdot 2^l) = f(-2^{k+l}) = 3 = 3 + 0 = f(-2^k) + f(2^l)$ y
- $f((-2^k) \cdot (-2^l)) = f(2^{k+l}) = 0 = 3 + 3 = f(-2^k) + f(-2^l)$,

tenemos que f es homomorfismo.