Ejercicio 5. (Parcial 2, Semestre 1, 2021)

a. Hallar el menor $x \in \mathbb{Z}^+$ que verifica $\begin{cases} x \equiv 10 \pmod{13} \\ x \equiv 91 \pmod{101} \end{cases}$.

b. Sea E la función de cifrado **RSA** con clave (n, e). Describir la función de descifrado D, y probar que descifra.

c. Si $(n, e) = (1313, 271)$, cifrar la letra K. Sugerencia: usar TCR con $1313 = 101 \times 13$.

a) buscamos el menor $x \in \mathbb{Z}^+$ tal que

$$\begin{cases} x \equiv 10 \pmod{13} \\ x \equiv 91 \pmod{101} \end{cases}$$

$$\Leftrightarrow \quad x \equiv x_0 \pmod{\overbrace{13 \cdot 101}^{1313}}$$

x_0 ↑ solución particular

* vamos a buscar una solución particular

$x \equiv 91 \pmod{101} \longrightarrow 91$ y $91 \equiv 0 \pmod{13}$ ✗

$\longrightarrow 192$ y $192 \equiv 10 \pmod{13}$ ✓

tenemos $\begin{cases} 192 \equiv 91 \pmod{101} \\ 192 \equiv 10 \pmod{13} \end{cases}$

$x_0 = 192$ es solución particular

$\Rightarrow$ $\boxed{x \equiv 192 \pmod{1313}}$

b) Criptosistema RSA

Ana va a recibir mensajes cifrados

① elige dos primos distintos grandes p, q (secretos)

② calcula $n = pq$ $\quad$ n es público

③ calcula $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$

④ elige un número e tal que

$1 < e < \varphi(n)$ y $\text{mcd}(e, \varphi(n)) = 1$

La clave pública es (n, e)

la función de cifrado es:

$$E : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$
$$E(x) = x^e \pmod n$$

¿Cómo hace Ana para descifrar el mensaje que recibe?

como $\text{mcd}(e, \varphi(n)) = 1$, tenemos que e es invertible modulo n

$\Rightarrow$ existe $d \in \mathbb{Z}^+$ tal que $de \equiv 1 \pmod{\varphi(n)}$

la función descifrado es:

$$D : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$
$$D(x) = x^d \pmod n$$

$$D(E(x)) = x$$

c) la clave pública es $(n, e) = (1313, 271)$

función de cifrado es:

$$E : \mathbb{Z}_{1313} \longrightarrow \mathbb{Z}_{1313}$$
$$E(x) \equiv x^{271} \pmod{1313}$$

Queremos cifrar la letra K:

a la letra K le corresponde el número 10

entonces queremos calcular $E(10)$

$$E(10) \equiv 10^{271} \pmod{1313} \iff \begin{cases} E(10) \equiv 10^{271} \pmod{101} \\ E(10) \equiv 10^{271} \pmod{13} \end{cases}$$

$1313 = 101 \cdot 13$

(primos)

* $10^{271} \pmod{101}$

10 y 101 son coprimos entonces podemos aplicar el teorema de Euler

$\varphi(101) = 100$

entonces $10^{\varphi(101)} \equiv 1 \pmod{101}$

$\Rightarrow 10^{100} \equiv 1 \pmod{101}$

$271 = 2 \cdot 100 + 71$

$10^{271} \equiv 10^{2 \cdot 100 + 71} \pmod{101}$

$\equiv (10^{100})^2 10^{71} \pmod{101}$

$\equiv 10^{71} \pmod{101}$

$10^2 \equiv 100 \equiv -1 \pmod{101}$

$10^{271} \equiv 10^{71} \pmod{101}$

$\equiv 10^{2 \cdot 35 + 1} \pmod{101}$

$\equiv (10^2)^{35} \cdot 10 \pmod{101}$

$\equiv (-1)^{35} \cdot 10 \pmod{101}$

$\equiv -10 \pmod{101}$

$\equiv 91 \pmod{101}$

$\Rightarrow E(10) \equiv 10^{271} \equiv 91 \pmod{101}$

* $10^{271} \pmod{13}$

como 13 y 10 son coprimos, podemos aplicar el teorema de Euler.

$\varphi(13) = 12$

entonces $10^{12} \equiv 1 \pmod{13}$

$271 = 22 \cdot 12 + 7$

$10^{271} \equiv 10^{22 \cdot 12 + 7} \pmod{13}$

$\equiv (10^{12})^{22} \cdot 10^7 \pmod{13}$

$\equiv 10^7 \pmod{13}$

$7 = 4 + 2 + 1$

$\Rightarrow 10^7 = 10^4 \cdot 10^2 \cdot 10$

$10^2 \equiv 100 \equiv 9 \pmod{13}$

$10^4 \equiv (10^2)^2 \equiv 9^2 \equiv 81 \equiv 3 \pmod{13}$

$10^7 \equiv 10^4 \cdot 10^2 \cdot 10 \pmod{13}$

$\equiv 3 \cdot 9 \cdot 10 \pmod{13}$

$\equiv 3 \cdot 90 \pmod{13}$

$\equiv 3(-1) \pmod{13}$

$\equiv -3 \pmod{13}$

$\equiv 10 \pmod{13}$

$$\boxed{10^{271} \equiv 10^7 \equiv 10 \pmod{13}}$$

$$E(10) \equiv 10^{271} \pmod{1313} \iff \begin{cases} E(10) \equiv 10^{271} \pmod{101} \\ E(10) \equiv 10^{271} \pmod{13} \end{cases}$$

$$\iff \begin{cases} E(10) \equiv 91 \pmod{101} \\ E(10) \equiv 10 \pmod{13} \end{cases}$$

$$\iff E(10) \equiv 192 \pmod{1313}$$

entonces el mensaje cifrado es 192.

Ejercicio 3. Ofelia desde Colonia y Lucía desde Artigas quieren intercambiar un mensaje de forma privada. Así que no tienen más remedio que aprender un poco de criptografía.

a. Al principio Ofelia no entendió bien el método de Diffie-Hellman y propone el siguiente método para fijar una clave común: eligen (públicamente) un primo p y un entero $1 < g < p$. A su vez, Ofelia elige en secreto un entero n y Lucía elige un entero m. Ofelia calcula $a = ng \pmod p$ y le manda a a Lucía. Lucía calcula $b = mg \pmod p$ y le manda b a Ofelia. La clave común será: $k = ngm \pmod p$; la cual Ofelia puede calcular haciendo $k = nb \pmod p$, y Lucía haciendo $k = am \pmod p$.

i) Eligen $p = 101$ y $g = 2$. Ofelia le manda $a = 19$ y Lucía elige $m = 35$, ¿cuál es la clave común?

ii) Un observador ve que Ofelia manda $a = 19$, y que Lucía manda $b = 35$. ¿Puede obtener la clave? En caso afirmativo, hallarla.

iii) Describir un método para encontrar la clave en general, conociendo p, g, a y b.

a) ① Eligen publicamente un primo p y un entero $1 < g < p$

② Ofelia elige un entero n (en secreto)

③ Lucía elige un entero m (en secreto)

④ Ofelia calcula $a \equiv ng \pmod p$ y le manda a a Lucía

⑤ Lucía calcula $b \equiv mg \pmod p$ y le manda b a Ofelia

la clave común: $k \equiv ngm \pmod p$

i) eligen $p = 101$, $g = 2$

Ofelia le manda $a = 19$ y Lucía elige $m = 35$

$k \equiv \underbrace{ngm}_{\text{"19}} \pmod p$

$\Rightarrow k \equiv 19 \cdot 35 \pmod{101}$

$k \equiv 59 \pmod{101}$

$\Rightarrow$ la clave común es 59

ii) $p = 101$ y $g = 2$

observamos que { Ofelia manda $a = 19$; Lucía manda $b = 35$

podemos encontrar la clave?

podemos descubrir cuanto vale n?

$a \equiv ng \pmod p$

$19 \equiv n \cdot 2 \pmod{101}$

$x \equiv - \pmod p$

$x = \pmod q$

$2x \equiv 1 \pmod{101}$

$2 \cdot 51 \equiv 102 \equiv 1 \pmod{101}$

$\rightarrow$ el inverso de 2 modulo 101 es 51

$$19 \equiv 2n \pmod{101}$$

$$\Rightarrow 19 \cdot 51 \equiv 51 \cdot 2n \pmod{101}$$

$$\Rightarrow 19 \cdot 51 \equiv n \pmod{101}$$

$$\Rightarrow \boxed{60 \equiv n \pmod{101}}$$

$K \equiv \underbrace{mgn}_{b} \pmod{101} \quad \Rightarrow K \equiv 35 \cdot 60 \pmod{101}$

$$\Rightarrow \boxed{K \equiv 80 \pmod{101}}$$

iii) método para encontrar la clave conociendo p, g, a y b.

$\rightarrow$ usar a para encontrar n

$$a \equiv ng \pmod{p}$$

p es primo, $1 < g < p$ $\Rightarrow$ g es invertible módulo p

$$\Rightarrow ag^{-1} \equiv ngg^{-1} \pmod{p}$$

$$\Rightarrow n \equiv ag^{-1} \pmod{p}$$

$\rightarrow$ la clave es $K \equiv mgn \pmod{p}$

$$\boxed{K \equiv bag^{-1} \pmod{p}}$$

b. Lucía lee el libro y entiende que hay que usar potencias en vez de multiplicaciones; así que Lucía y Ofelia utilizan el método **Diffie-Hellman** correcto para acordar una clave común. Toman como primo $p = 89$ y $g = 7$. Lucía elige el número secreto $m = 86$ y Ofelia le envía $b = g^n \equiv 17 \pmod{p}$. ¿Cuál es la clave secreta K que acuerdan?

eligen un primo $p = 89$ y una raíz primitiva $g = 7$ modulo 89

$\rightarrow$ Ofelia elige n y calcula $b \equiv g^n \pmod{p}$

$\rightarrow$ le envía b a Lucía

* Lucía elige m y calcula $a \equiv g^m \pmod p$

2> le envía a a Ofelia

la clave común es $K \equiv g^{nm} \pmod p$

Tenemos $p = 89$, $g = 7$

Lucía elige $m = 86$ y Ofelia le envía $\underbrace{b \equiv 17 \pmod{89}}_{b}$

$7^n \equiv 17 \pmod{89}$

¿Cuál es la clave?

$$K \equiv 7^{n \cdot m} \pmod{89}$$
$$\equiv (7^n)^{86} \pmod{89}$$
$$\equiv 17^{86} \pmod{89}$$