Ejercicio 2. Cavani desde París y Rolan desde Burdeos quieren acordar tácticas para el partido contra Jamaica; pero los técnicos jamaiquinos contrataron espías para interceptar sus comunicaciones. Así que no tienen más remedio que aprender un poco de criptografía para poder asegurar privacidad.

a. Al principio Cavani 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 $1 < g < p$. Cavani elige en secreto un entero n y Rolan elige un entero m. Cavani calcula $a = ng \pmod p$ y le manda a a Rolan; Rolan calcula $b = mg \pmod p$ y le manda b a Cavani. Entonces la clave común será $k = ngm \pmod p$, la cual Cavani puede calcular haciendo $k = nb \pmod p$ y Rolan puede calcular $k = am \pmod p$.

i) Si eligen $p = 101$ y $g = 2$. Cavani le manda $a = 19$ y Rolan elige $m = 35$, ¿cuál es la clave común?

ii) Si un observador ve que Cavani manda $a = 19$ y que Rolan 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.

6 - 2.35 = -70

(1) Eligen p primo. g entero $1 < g < p$ en vez $g^1 \pmod p$

Cavani elige n (privado) $\mapsto$ manda $a = n \cdot g \pmod p$

Rolan elige m (privado) $\mapsto$ manda $b = m \cdot g \pmod p$ en vez de g^m

Clave: $k = n \cdot g \cdot m \pmod p$.

(i) $p = 101 \quad g = 2 \quad a = 19 \quad m = 35.$

$= g \cdot n$

La clave es $k = 19 \cdot 35 \pmod{101}$

(ii) $a = 19 \quad b = 35,$

$a = g \cdot n \quad b = gm$ ¿puede obtener $k = g \cdot n \cdot m$?

El observador conoce $p = 101 \quad g = 2 \quad a = 19 \quad b = 35$

$\Rightarrow$ Para hallar k basta conocer $2^{-1} \pmod{101}$:

$k = gnm \equiv gn \cdot gn \cdot g^{-1} \pmod{101}$ porque conmuta!

$\equiv ab \cdot g^{-1} \pmod{101}$

$\equiv 19 \cdot 35 \cdot 51 \pmod{101}$

$\equiv 80 \pmod{101}$

n impar $\quad 2^{-1} \pmod n = \text{coc}(n, 2) + 1$

$\Rightarrow 2^{-1} \pmod{101} = 51$

(iii) $k = (gn)(gm) \cdot g^{-1} = abg^{-1} \pmod{101}$

$\Rightarrow$ Basta calcular $g^{-1} \bmod (101)$ y multiplicar.

Ejercicio 3.

a. Probar que 5 es una raíz primitiva módulo 97.

b. Supongamos que somos espías que interceptamos la conversación entre Alicia y Bob cuando ambos están utilizando el protocolo Diffie-Hellman para acordar una clave común. Alicia y Bob acuerdan $p = 97$ para el módulo y $g = 5$ como generador. Alicia le envía a Bob 3 y Bob le envia a Alicia 7. ¿Cuál es la clave k común que acuerdan Alicia y Bob? (la idea es justo ver que no es fácil descubrir la clave).

c. Supongamos que Diego y Marta quieren utilizar el método Diffie-Helmann de intercambio de clave usando el primo $p = 97$ y $g = 29$. Diego le envia a Marta el número $x = 85$. Marta luego le envía a Diego el número $y = 3$. Recordando que 5 es una raíz primitiva módulo 97 y teniendo como datos los siguientes logaritmos discretos $log_5 29 = 13$ y $log_5 85 = 90$, hallar la clave común.

(a) Hay que ver que $mcd(5,97)=1$ ✓ y que $o(5)=\varphi(97)=96$.
Esto es equivalente a ver que $mcd(5,97)=1$ y $5^{\varphi(97)/p} \neq 1 \quad \forall p \mid \varphi(97)$

$\varphi(97)=96$, luego hay que chequear que $\begin{cases} 5^{96/2} \neq 1 \pmod{97} \\ 5^{96/3} \neq 1 \pmod{97} \end{cases}$
$= 3 \cdot 2^5$

$5^{96/3} = 5^{32}$: Exponenciación Rápida:

i	$5^{2^i} \pmod{97}$	
$i=0$	$5 \pmod{97}$	✓
$i=1$	$25 \pmod{97}$	✓
$i=2$	$25^2 = 625 \pmod{97}$	✓
$i=3$	$6 = 1849 \pmod{97}$	✓
$i=4$	$36 \pmod{97}$	✓
$i=5$	$1296 = 35 \pmod{97}$	✗
$i=6$	$1225 = 61 \pmod{97}$	✓

$5^{32} \equiv 35 \pmod{97}$
$\neq 1 \pmod{97}$ ✓

$5^{48} = 5^{32+16}$
$= 35 \cdot 36 \pmod{97}$
$= (-1) \pmod{97}$ ✓

(b) $p=97 \quad g=5 \quad a \equiv g^n \equiv 3 \pmod{97} \quad b \equiv g^m \equiv 7 \pmod{97}$
$k = (g^n)^m = (g^m)^n \pmod{97}$

Necesitamos calcular m o n : n tq $5^n \equiv 3 \pmod{97}$.
m tq $5^m \equiv 7 \pmod{97}$ (notar: $5^{31} \equiv 7 \pmod{97}$)
$\Rightarrow m = 31$

$\Rightarrow k = a^n = 3^{31} \pmod{97}$ (Hacer la cuenta)

(c) $p=97 \quad g=29 \quad x \equiv g^n \equiv 85 \ (97) \quad y \equiv g^m \equiv 3 \ (97)$

$5^{13} \equiv 29 \ (97)$ * $5^{90} \equiv 85 \ (97)$ *

Queremos hallar $K \equiv (g^n)^m = (g^m)^n \pmod{97}$ $\boxed{g=29}$

$85 \equiv 29^n \equiv 5^{13 \cdot n} \pmod{97}$ *, por otra parte

$85 \equiv 5^{90}$ *

$\rightarrow 5^{13 \cdot n} \equiv 5^{90} \pmod{97}$ si y sólo si $13 \cdot n \equiv 90 \ \varphi(97)$

$\Leftrightarrow \quad 13 \cdot n \equiv 90 \ (96)$

$\Leftrightarrow \quad \boxed{13 \cdot n - 96k = 90}$ *

Hay que hallar un par (n,k) que resuelva * (AEE)

Luego $K \equiv (g^m)^n \equiv 3^n \pmod{97}$.

Ejercicio 5.

Supongamos que n es un número muy díficil de factorizar. Bernardo utiliza un criptosistema RSA con clave (n, e_1), al mismo tiempo que Bruno utiliza la clave (n, e_2), con $mcd(e_1, e_2) = 1$. Adriana les envía el mismo texto x a ambos, calculando $y_1 = x^{e_1} \pmod{n}$ e $y_2 = x^{e_2} \pmod{n}$ (envía y_1 a Bernardo e y_2 a Bruno). Alguien que intercepta los mensajes realiza los siguientes cálculos:
1. c_1 y c_2 positivos tales que $c_1 e_1 + c_2 e_2 \equiv 1 \pmod{\varphi(n)}$. 2. $x_1 = y_1^{c_1}(y_2^{c_2}) \pmod{n}$.

(a) Probar que x_1 calculado en el paso 2 es el texto x. Por lo tanto, si bien el criptosistema es seguro, el mensaje puede ser descifrado en este caso.

(b) Descifrar el mensaje si $y_1 = 9983$ e $y_2 = 4026$, sabiendo que $n = 16123, e_1 = 27$ y $e_2 = 29$.

Este criptosistema creado por Rivest, Shamir y Adleman (RSA) en el año 1977 es uno de los criptosistemas de clave pública más famosos. La idea detrás de este criptosistema es el de construir una función que sea fácil de calcular (en este caso multiplicar dos primos), pero que su inversa sea difícil de calcular (en este caso dado un número que es producto de 2 primos, hallar esos primos). Veamos en qué consiste.

1. Ana elige dos primos (distintos) grandes p y q y calcula $n = pq$.
2. Luego calcula:
$$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1).$$
3. Luego elige un número aleatorio e con:
$$1 < e < \varphi(n) \text{ y } \operatorname{mcd}(e, \varphi(n)) = 1.$$
4. Finalmente Ana tiene definida una función (función de cifrado) definida por:
$$E : \mathbb{Z}_n \to \mathbb{Z}_n : E(x) = x^e \pmod{n}.$$

La clave pública de Ana viene dada por el par (n, e) que puede ser publicada en una guía de claves públicas. Observemos que el par (n, e) nos brinda toda la información necesaria para calcular la función de cifrado E.

Alguien que desee mandarle un mensaje confidencial x a Ana, busca la clave pública de Ana en la guía y le envía el mensaje cifrado $E(x)$.

Si queremos mandar x: enviamos $E(x)$ y Ana lo va a desencriptar con una función $D(y)$ tq $D(E(x)) = x$.

La inversa es $D(y) = x^d \pmod{n}$ donde $ed \equiv 1 \ \varphi(n)$.

$\left.\begin{matrix} n \text{ es público} \\ e \text{ es público} \end{matrix}\right\}$ $\left.\begin{matrix} p \\ q \end{matrix}\right\}$ son privados $\Rightarrow$ $\varphi(p)\varphi(q) = \varphi(n)$ es privado.
Luego D es privada.