Códigos y Criptografía (GIINF)

Práctica sobre camino hacia la clave pública.
Intercambio de claves de Diffie y Hellmann

ALBERTO LUQUE RIVAS

1. Todo número natural tiene una expresión única en base 2. Escribir en base 2 los siguientes números naturales:

	128	64	32	16	8	4	2	1
17	0	0	0	1	0	0	0	1
61	0	0	1	1	1	1	0	1
-18	-	-	-	-	-	-	-	-
110	0	1	1	0	1	1	1	0
135	1	0	0	0	0	1	1	1

2. Utilizar el algoritmo de potenciación rápida (binaria) para hallar las siguientes potencias:

(a) 3^{17} mod 9:

$$3^{17} = 3^{2^4+2^0} = 3^{2^4} \cdot \; 3^{2^0} = 0\, mod(9) \cdot 3\, mod(9) = 0\, mod(9)$$

(b) 5^{61}mod 11

$$5^{61} = 5^{2^5+2^4+2^3+2^2+2^0} = 5^{2^5} \cdot 5^{2^4} \cdot 5^{2^3} \cdot 5^{2^2} \cdot 5^{2^0} = 5^{2^3} \cdot 5^{2^3} \cdot 5^{2^3} 5^{2^3} \cdot 5^{2^4} \cdot 5^{2^3} \cdot 5^{2^2} \cdot 5^{2^0} \; mod\, 11 = 4\, mod(11) \cdot 4\, mod(11) \cdot 4\, mod(11) \cdot 4\, mod(11) \cdot 4\, mod(11) \cdot 4\, mod(11) \cdot 4\, mod(41) \cdot 3\, mod(11) \cdot 3\, mod(11) = 6\, mod(11) \cdot 9\, mod(11) \cdot 5\, mod(11) = 5\, mod(11)$$

(c) 70^{110}mod 21

$$70^{110} = 70^{2^6+2^5+2^3+2^2+2^1} = \left(70^{2^3} \cdot 70^{2^3} \cdot 70^{2^3} \cdot 70^{2^3} \cdot 70^{2^3} \cdot 70^{2^3} \cdot 70^{2^3} \cdot 70^{2^3}\right) \cdot \left(70^{2^3} \cdot \; 70^{2^3} \cdot \; 70^{2^3} \cdot \; 70^{2^3}\right) \cdot \left(70^{2^3}\right) \cdot \left(70^{2^2}\right) \cdot \left(70^{2^1}\right) = 7\; mod\, 21$$

3. Comprobar si el número natural a **es generador del cuerpo finito Z_p con** p **primo, usando la definición:**

(a)a= 0,p= 7 , no es generador.

(b)a= 2,p= 6, no es generador porque el cuerpo finito no genera el 3 ni el 5.

(c)a= 3,p= 5, si es generador.

[3^0**,**3^1**,**3^2**,**3^3**]** = **[**1 mod 5**,**3 mod 5**,**4 mod 5**,** 2 mod 5]

Conjunto generador {1,3,4,2}

(d)a= 2,p= 7 , no es generador porque el cuerpo finito no genera el 3 ni el 5 ni el 6.

(e)a= 2.5,p= 11 , el numero no es natural es real.

4. Comprobar en los casos anteriores si el número naturala es generador del cuerpo finito Z_p usando el criterio alternativo estudiado en clase.

(a)a= 0,p= 7 , no es generador.

(b)a= 2,p= 6, si es generador.

$$p \;=\; 6-1 \;=\; 5\,;a=2;\,2^{\frac{5}{5}} \;=\; 2\;!=1$$

(c)a= 3,p= 5, si es generador.

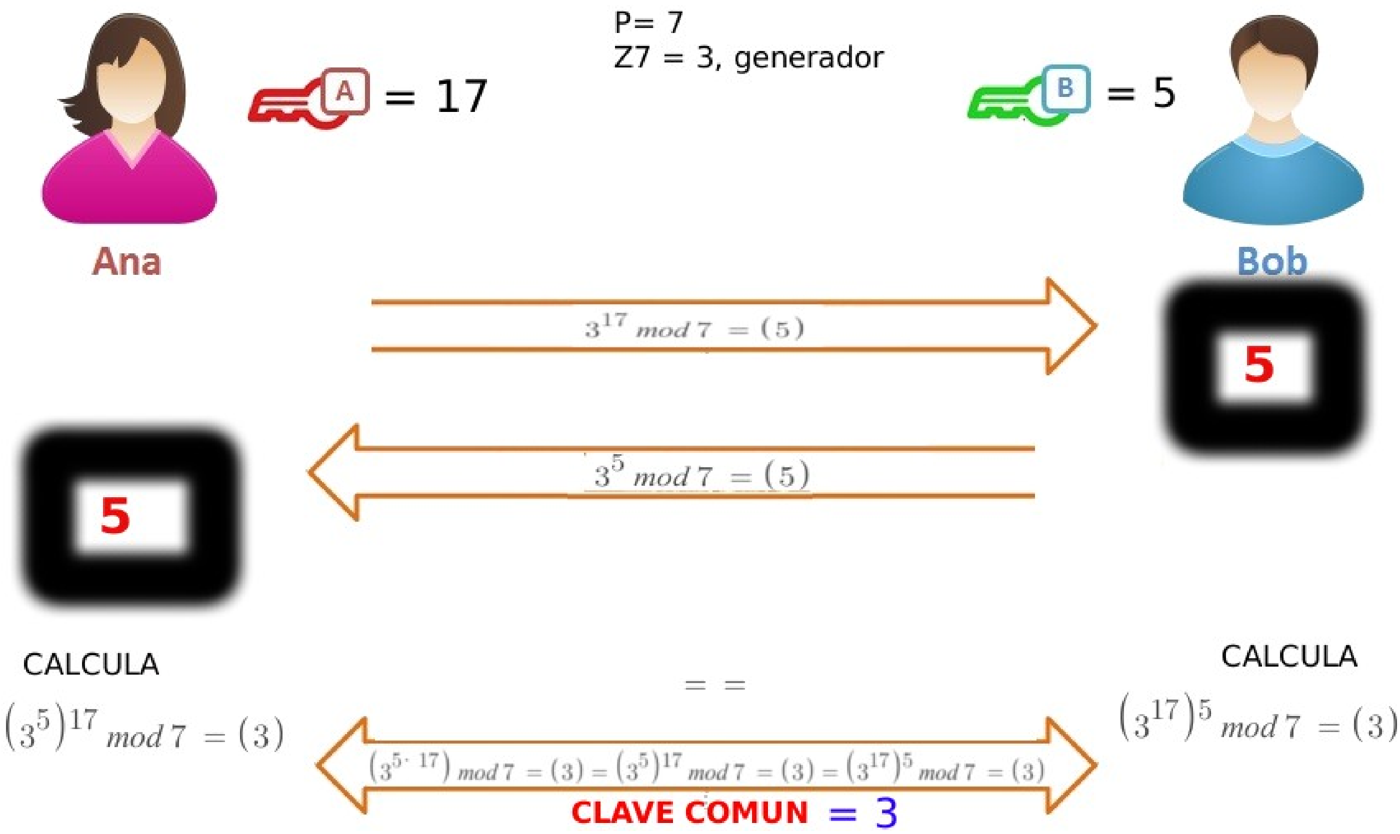
$$p \;=\; 5-1 \;=\; 4\,;a=3;\,3^{\frac{4}{2}} \;=\; 9\;!=1$$

(d)a= 2,p= 7 , si es generador.

$$p \;=\; 7-1 \;=\; 6=3\cdot 2\,;a=2;\,2^{\frac{6}{2}} \;=\; 8\;!=1\;\&\&\;2^{\frac{6}{3}} \;=\; 4\;!=1$$

(e)a= 2.5,p= 11 , el numero no es natural es real.

5. Dos individuos A y B se ponen de acuerdo en el valor de un primo, 7, y de un generadorde Z_7, 3. A partir de dichos valores y de dos valores aleatorios a y b generados por A y B respectivamente, describir como se construiría una clave común. Aplicarlo a los valores a= 17 y b= 5.



Se verifica que no es fácil de criptoanalizar por:

- a != 1 y b != 1 , 3^{17} != 3 y 3^5 != 3
- 17 != 7-1 y 5 != 7-1 , 3^{17} != 1 y 3^5 != 1