

Universidad de la República - Facultad de Ingeniería - IMERL  
Matemática Discreta 2, semipresencial

SOLUCIÓN CUARTA PRUEBA (SEGUNDO PARCIAL) - 1 DE DICIEMBRE DE 2016.

**Ejercicio 1.** (15 puntos) (*Ejercicio 1 del segundo parcial del curso semipresencial de 2015*)

- a. Probar que 2 es raíz primitiva módulo 53.
- b. Hallar todos los  $x \in \mathbb{Z}$  tales que  $x^{19} \equiv 32 \pmod{53}$ .
- c. Archibaldo y Baldomero quieren pactar una clave común empleando el protocolo Diffie-Hellman. Para ésto fijan el primo  $p = 53$  y la raíz primitiva  $g = 2$ . Archibaldo selecciona el número  $m = 28$  y le remite el número 49 a Baldomero. Éste selecciona el número  $n = 5$ . ¿Cuál es la clave común  $k$  que acordaron Archibaldo y Baldomero?

**Solución Ejercicio 1:**

- a. Observemos primero que  $52 = 2^2 \cdot 13$ . Por lo tanto, si queremos probar que 2 es raíz primitiva módulo 53, debemos probar que  $2^{\frac{52}{p}} \not\equiv 1 \pmod{53}$ , para todo  $p$  primo, con  $p|52$ . O sea debemos calcular  $2^4$  y  $2^{26}$ .

$n$	$2^n \pmod{53}$
0	1 (mód 53)
1	2 (mód 53)
2	4 (mód 53)
3	8 (mód 53)
<b>4</b>	<b>16 mód53</b>
5	32 (mód 53)
6	11 (mód 53)
7	22 (mód 53)
8	44 (mód 53)
9	35 (mód 53)
10	17 (mód 53)
11	34 (mód 53)
12	15 (mód 53)
13	30 (mód 53)
14	7 (mód 53)
15	14 (mód 53)
$\vdots$	$\vdots$

Luego  $2^{26} = 2^{13} \times 2^{13} \equiv 900 \pmod{53} \equiv -1 \pmod{53}$ .  
Entonces 2 es raíz primitiva módulo 53.

- b. Como  $32 = 2^5$  la ecuación a resolver se transforma en:  $x^{19} \equiv 2^5 \pmod{53}$ . Por otro lado, como 2 es raíz primitiva módulo 53, entonces para todo  $x \in \mathbb{Z}$  existe  $0 \leq t(x) \leq 52$  tal que  $x = 2^{t(x)}$ . Luego la ecuación a resolver se transforma en:  $2^{t(x)19} \equiv 2^5 \pmod{53}$ . Nuevamente como 2 es raíz primitiva, la ecuación anterior es equivalente a:  $19 \cdot t(x) \equiv 5 \pmod{52}$ . Esto último a su vez es equivalente a  $t(x) \equiv 3 \pmod{52}$ . Luego  $x = 2^3 \pmod{53}$ , o sea  $x = 8 + 53 \cdot z$ , con  $z \in \mathbb{Z}$ .
- c. Archibaldo toma  $m = 28$  y le envía  $2^{28} \equiv 49 \pmod{53}$  a Baldomero. Éste toma  $m = 5$  y le envía  $49^5 \pmod{53}$  a Archibaldo. O sea,  $49^5 \equiv (-4)^5 \pmod{53} = -2^{10} \pmod{53} \equiv -17 \pmod{53} \equiv 36 \pmod{53}$ . O sea que la clave común acordada es  $k = 36$ .

**Ejercicio 2.** (20 puntos)

- Calcular el número de raíces primitivas en  $U(29)$ .
- Encontrar todas las raíces primitivas de  $U(29)$ .  
(Sugerencia: Calcular  $2^n$  (mód 29), para todo  $0 \leq n \leq 14$ , para facilitar los cálculos posteriores.)
- Ordenar en forma creciente las raíces primitivas halladas en el ítem anterior:  $r_1 \leq r_2 \leq r_3 \leq r_4 \leq r_5 \leq \dots$ . Luego escribir la secuencia:  $r_1 r_5 0 r_9 r_3 r_1 r_7$ . Finalmente traducir usando la numeración de los símbolos:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	␣
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

- Utilizando el método de Vigenère **decodificar** el siguiente texto, usando la palabra clave hallada en el ítem anterior:

*OZ\_LPTSOKMS\_BUCBRSNCG*

**Solución Ejercicio 2:**

- El número de raíces primitivas en  $U(n)$  (si hay) es  $\varphi(\varphi(n))$ , siendo  $\varphi$  la función de Euler. En este caso  $\varphi(29) = 28$ , pues 29 es primo. Luego  $\varphi(28) = \varphi(4 \times 7) = \varphi(4) \cdot \varphi(7) = 2 \cdot 6 = 12$ . Entonces el número de raíces primitivas en  $U(29)$  es 12.
- Para encontrar todas las raíces primitivas calculamos los valores sugeridos en la letra del ejercicio, en la siguiente tabla:

$n$	$2^n$ (mód 29)
0	1 (mód 29)
1	2 (mód 29)
2	4 (mód 29)
<b>3</b>	<b>8 mód29</b>
<b>4</b>	<b>16 (mód 29)</b>
<b>5</b>	<b>3 mód29</b>
6	6 (mód 29)
7	12 (mód 29)
8	24 (mód 29)
<b>9</b>	<b>19 mód29</b>
10	9 (mód 29)
<b>11</b>	<b>18 mód29</b>
12	7 (mód 29)
<b>13</b>	<b>14 mód29</b>
<b>14</b>	<b>-1 (mód 29)</b>
$\vdots$	$\vdots$

Luego se concluyen varias cosas de la tabla anterior:

- Por un lado  $2^{14} \not\equiv 1$  (mód 29) y también se verifica:  $2^4 \not\equiv 1$  (mód 29). Entonces  $o(2) = 28$ , concluyendo que 2 es raíz primitiva en  $U(29)$ .
- Como 2 es raíz primitiva, entonces  $2^s$  (mód 29) es raíz primitiva para todo  $s \in \mathbb{N}$  tal que  $\text{mcd}(s, 28) = 1$ . Entonces las que están marcadas en “negrita” en la tabla son también raíces primitivas. Así que tenemos hasta ahora las siguientes raíces primitivas: 2, 3, 8, 14, 18 y 19.

- Por último puede observarse que  $-2, -3, -8, -14, -18$  y  $-19$  son raíces primitivas de  $U(29)$ . O sea,  $27, 26, 21, 15, 11$  y  $10$  son raíces primitivas de  $U(29)$ . Sugerimos tres caminos para probar la última afirmación.
  - Completar la tabla anterior hasta  $n = 28$ .
  - Probar teóricamente que si  $a$  es raíz primitiva en  $U(29)$  entonces  $(-a)$  también.
  - Hacer las cuentas a mano en cada caso.

c. Por lo tanto las raíces primitivas, ordenadas en forma creciente son:

$$2 \leq 3 \leq 8 \leq 10 \leq 11 \leq 14 \leq 15 \leq 18 \leq 19 \leq 21 \leq 26 \leq 27.$$

La palabra clave es: CLASICO (sería CLÁSICO).

d. Por último decodificando el mensaje oculto

*OZ\_LPTSOKMS\_BUCBRNCG*

utilizando Vigenère, obtenemos el mensaje:

*NO\_TIREN\_MAS\_GARRAFAS*

**Ejercicio 3.** (10 puntos) Describir el “Método de Fermat” de ataque al RSA, y demostrar la validez del algoritmo planteado.

### **Solución Ejercicio 3**

Ver los apuntes de Teórico, Capítulo 5, ítem 5.3.4, Método de Fermat de ataque al RSA.