

Tarea 3

2 de diciembre, 2017

Problema 1. Para cada caso, encuentre los valores de x .

- $4^{56} \equiv x \pmod{7}$
- $25^{24} \equiv x \pmod{13}$
- $5^{124} \equiv x \pmod{14}$
- $8^{88} \equiv x \pmod{15}$
- $7^{39} \equiv x \pmod{19}$
- $11^{25} \equiv x \pmod{21}$

Problema 2. El objetivo de este juego es el envío y recepción segura de mensajes.

1. Formar equipos de tres o cuatro personas; cada equipo debe identificarse visiblemente.
2. Cada equipo debe desarrollar su clave pública RSA: un número N y un exponente e .
3. La clave pública debe ser anunciada visiblemente al resto de los equipos.
4. Cada equipo debe enviar un mensaje a otro equipo (de su elección), utilizando la clave pública del destinatario, y usando como mensajero a un tercer equipo. El mensajero debe entregar el mensaje cifrado inmediatamente, pero puede leerlo y guardarlo.
5. El equipo que actúe como mensajero intentará descifrar el mensaje.
6. Se considerará un éxito:

- para el equipo remitente, el envío de un mensaje cifrado al destinatario sin que haya sido descifrado por el mensajero;
- para el equipo mensajero, un mensaje descifrado exitosamente; y
- para el equipo destinatario, la recepción de un mensaje sin que haya sido descifrado por el mensajero.

7. El equipo con el mayor número de éxitos será el ganador.

Los mensajes deben convertirse a números de acuerdo a la siguiente tabla.

A	11	B	12	C	13	D	14
E	15	F	16	G	17	H	18
I	19	J	20	K	21	L	22
M	23	N	24	Ñ	25	O	26
P	27	Q	28	R	29	S	30
T	31	U	32	V	33	W	34
X	35	Y	36	Z	37	espacio	45
,	55	.	56	;	57	:	58
i	75	!	76	¿	85	?	86