TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA

Examen 7-11-2025

APELLIDOS, NOMBRE: _____

1	2	3	4	FINAL
30	30	20	20	100

Razonar debidamente las respuestas

- **Incluir** todas las cuentas relativas al Algoritmo de Euclides/Teorema de Bezout y cuadrados iterados
- **Factorización:** No se puede mediante fuerza bruta. Describe los algoritmos que utilices.

---

1. Consideramos un criptosistema matricial afín sobre *digrafos* con alfabeto dado por la correspondencia

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	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

El cifrado de un digrafo $v \in (\mathbb{Z}/25\mathbb{Z})^2$ está dado por

$$C(v) = Av + b \pmod{25},$$

donde $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z})$ y $b = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \in (\mathbb{Z}/25\mathbb{Z})^2$.

La clave del cifrado matricial (A, b) se escribe en base 25 como

$$m_{(A,b)} = a_{11} + a_{12} \cdot 25 + a_{21} \cdot 25^2 + a_{22} \cdot 25^3 + b_1 \cdot 25^4 + b_2 \cdot 25^5.$$

Mi clave pública RSA es $(n, e) = (416021, 37703)$.
Para enviarme un mensaje se usa un criptosistema híbrido:

- La clave de cifrado matricial $m = m_{(A,b)}$ se envía mediante RSA obteniendo

$$c = 362463 \qquad (\text{i.e. } c \equiv m^e \pmod{n}).$$

- Posteriormente se usa el cifrado matricial afín $C : (\mathbb{Z}/25\mathbb{Z})^2 \longrightarrow (\mathbb{Z}/25\mathbb{Z})^2$.

He recibido el mensaje cifrado `SUCA`. ¿Qué me han querido decir?

---

2. En nuestra red de mensajería usamos el criptosistema de ElGamal en el grupo de unidades del cuerpo $\mathbb{F}_8$, tomando como generador $g = x$. Donde $\mathbb{F}_8$ lo identificamos con $\mathbb{F}_2[x]/(x^3 + x + 1)$ (observar que $x^3 + x + 1$ es irreducible sobre $\mathbb{F}_2$). A los elementos de $\mathcal{U}(\mathbb{F}_8)$ le asignamos los siguiente caracteres:

A	E	I	M	S	T	R
1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1

(a) Comprueba que $\mathcal{U}(\mathbb{F}_8) = \langle x \rangle$.
(b) Nuestra clave pública es $h = g^{11}$ y hemos recibido el mensaje

$$(M, I), (I, R), (T, A)$$

¿Qué nos han querido decir?

Continúa en la siguiente página

3. Sabemos que $n = 530821$ es el producto de dos primos. Factorizar n aplicando el método Kraitchik–Dixon con las siguientes factorizaciones de los valores $a_k = k^2 \pmod{n}$:

k	factorización de a_k
729	$2^2 \cdot 5 \cdot 31$
730	$3^3 \cdot 7 \cdot 11$
733	$2^2 \cdot 3 \cdot 7^2 \cdot 11$
734	$3 \cdot 5 \cdot 23^2$
736	$3 \cdot 5^3 \cdot 29$
737	$2^2 \cdot 3^2 \cdot 7^3$

---

4. Decide de manera razonada si las siguientes afirmaciones son verdaderas o falsas. Recuerda que si son verdaderas tienes que dar una demostración y si son falsas un contraejemplo:
(a) Sean p y q primos distintos. Entonces

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

(b) Sea $n = 2p$ con p primo impar. Entonces

$$a^{n-1} \equiv a \pmod{n}.$$
