TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA

Examen 14-11-2024

APELLIDOS, NOMBRE: _____

1	2	3	4	5	FINAL
30	20	10	10	10	80

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. En un criptosistema matricial afín sobre digrafos sobre el alfabeto

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

sabemos que el nombre `JAVIER` se ha cifrado como `UASPLM`.

(a) Calcular la función de cifrado.

(b) Calcular la función de descifrado.

(c) Descifrar `KP`.

---

2. Mi clave pública RSA es $(n, e) = (12091, 4749)$. Utilizando el alfabeto:

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

alguien ha utilizado esta clave pública para mandarme el siguiente mensaje:

`ADI`

Pero como soy muy despistado, no encuentro donde guardé mi clave secreta para poder descifrar el mensaje. Calcula mi clave secreta y descifra el mensaje.

---

3. Sabemos que el número 340531 es producto de dos primos. Calcular estos primos.

---

4. (a) Demostrar que 3 divide a $2^{14} - 1$ sin calcular explicitamente 2^{14}.

(b) Factorizar el número $(2^{14} - 1)/3$ sabiendo que los primos menores de 130 son

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127$$

---

5. Sea $b \in \mathbb{N}$, $b > 1$ y p un primo impar. Definimos $n = \dfrac{b^{2p} - 1}{b^2 - 1}$. Demuestra:

(a) n es compuesto;

(b) n es impar;

(c) n es primo con b.
