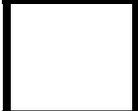


Ejercicio 1	Ejercicio 2	Ejercicio 3	Ejercicio 4	FINAL
				
4 puntos	1.5 puntos	3.5 punto	1 puntos	10

El alfabeto utilizado en todos los ejercicios es el siguiente:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	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

- Interceptamos un mensaje de Marcos que dice

ZQXSMOTIGQ

Sabemos que Marcos siempre firma sus mensajes y que en este caso ha cifrado el mensaje utilizando un cifrado matricial lineal sobre digrafos. Descifrar el mensaje.

- Factorizar 2599 utilizando el método de Kraitchick–Dixon.

- La clave pública RSA de Alberto es $(n, e) = (2599, 2085)$. Alguien le ha enviado el siguiente mensaje:

CDYADB

¿Qué le han querido decir?

- Demostrar que hay infinitos pseudoprimos en base 2.

Ayuda:

- ¿Es 341 un pseudoprimo en base 2?
- Demostrar que si n es pseudoprimo en base 2 entonces $2^n - 1$ también es pseudoprimo en base 2.

Razonar debidamente las respuestas

Incluir todas las cuentas relativas al Algoritmo de Euclides/Teorema de Bezout y cuadrados iterados