taller

May 29, 2023

1) ¿Cuál es el mensaje oculto en la siguiente lista de enteros, si se sabe que se ha usado el RSA con p=7919, q=17389 y e=96558349?

[116427824, 71262391, 95967677, 108216637, 130284225, 44866252, 16356886, 121976595, 16896540, 44866252, 106409323, 44866252, 130284225, 71262391, 95967677, 108216637, 95967677, 16356886, 108216637, 16356886, 95967677, 106409323, 162951, 16356886, 122552340, 13783210, 87965332, 121976595, 108216637, 86661090, 71262391, 122552340, 108216637, 31583046, 87965332, 130284225, 16356886, 122552340, 108216637, 86661090, 71262391, 95967677, 44866252, 105050342, 116427824, 16356886, 108216637, 116427824, 71262391, 108216637, 44866252, 36622724, 86661090, 71262391, 95967677, 44866252, 105050342, 116427824, 16356886, 108216637, 36622724, 44866252, 16356886, 121976595, 16896540, 122552340, 87965332, 95967677, 108216637, 12960247, 162951, 16356886, 108216637, 116427824, 71262391, 95967677, 108216637, 86661090, 71262391, 116427824, 44866252, 16896540, 44866252, 130284225, 71262391, 95967677, 108216637, 86661090, 71262391, 122552340, 108216637, 31583046, 87965332, 130284225, 16356886, 122552340, 108216637, 116427824, 71262391, 108216637, 86661090, 71262391, 95967677, 44866252, 105050342, 116427824, 16356886, 108216637, 44866252, 36622724, 86661090, 71262391, 95967677, 44866252, 105050342, 116427824, 16356886]

2) ¿Cuál es el mensaje oculto en la siguiente lista de enteros, si se sabe que se ha usado el RSA con p=7919, q=17389 y e=96558349?

[94132717, 122552340, 87965332, 121976595, 108216637, 86661090, 87965332, 122552340, 16896540, 16356886, 108216637, 96593042, 16356886, 108216637, 116427824, 87965332, 95967677, 108216637, 96593042, 44866252, 106409323, 44866252, 130284225, 162951, 116427824, 16896540, 87965332, 96593042, 16356886, 95967677, 108216637, 86661090, 71262391, 122552340, 108216637, 116427824, 87965332, 95967677, 108216637, 12960247, 162951, 16356886, 108216637, 87965332, 16896540, 122552340, 87965332, 13625048, 44866252, 16356886, 95967677, 87965332, 108216637, 16356886, 116427824, 108216637, 36622724, 162951, 121976595, 96593042, 71262391, 108216637, 95967677, 16356886, 108216637, 96593042, 16356886, 105050342, 16356886, 121976595, 108216637, 87965332, 108216637, 12960247, 162951, 16356886, 108216637, 116427824, 71262391, 95967677, 108216637, 44866252, 94132717, 121976595, 71262391, 122552340, 87965332, 121976595, 16896540, 16356886, 95967677, 108216637, 16356886, 95967677, 16896540, 87965332, 121976595, 108216637, 130284225, 71262391, 36622724, 86661090, 116427824, 16356886, 16896540, 87965332, 36622724, 16356886, 121976595, 16896540, 16356886, 108216637, 95967677, 16356886, 94132717, 162951, 122552340, 71262391, 95967677, 108216637, 11752584, 108216637, 116427824, 71262391, 95967677, 108216637, 44866252, 121976595, 16896540, 16356886, 116427824, 44866252, 94132717, 16356886, 121976595, 16896540, 16356886, 95967677, 108216637, 116427824, 116427824, 16356886, 121976595, 71262391, 95967677, 108216637, 96593042, 16356886, 108216637, 96593042, 162951, 96593042, 87965332, 95967677]

3. Usando RSA con p=7919, q=17389 y e=96558349, encripte el siguiente mensaje:

`"las matematicas pueden ser definidas como aquel tema del cual no sabemos nunca lo que decimos ni si lo que decimos es verdadero"`

4. Usando RSA con p=7919, q=17389 y e=96558349, encripte el siguiente mensaje:

`"lo mas dificil de aprender en la vida es que puente hay que cruzar y que puente hay que quemar"`

5) ¿Cuál es el mensaje oculto en la siguiente lista de enteros, si se sabe que se ha usado el RSA con p=104729, q=224737 y e=554039341?

[21820245060, 16973863343, 16647907597, 5351085797, 18648503124, 18273004418, 15817170431, 7381433519, 15585396102, 4443772741, 1656337393, 14754433457, 22946763748, 5135880178, 6542531552, 2051320888, 18050988245, 4994899630, 17668156117, 11269362579]

6) ¿Cuál es el mensaje oculto en la siguiente lista de enteros, si se sabe que se ha usado el RSA con p=104729, q=224737 y e=554039341?

[20071683819, 18754823901, 15281925738, 22431087988, 18578136847, 14565167928, 20363208149, 23164154654, 19883031733, 17926748637, 22540995446, 9667978832, 3356165928, 20768696878, 7232548727, 17445960483, 17408203534, 18047748783, 11480314056, 20135029456, 21596106087, 21071138629, 12152023796, 18248646084, 9103249568, 22310161636]

7. Usando RSA con p=163841, q=350377 y e=4180452401, encripte el siguiente mensaje:

`"paren el mundo que me quiero bajar"`

8. Usando RSA con p=163847, q=350381 y e=8584779379, encripte el siguiente mensaje:

`"estos son mis principios y si no le gustan le tengo otros"`

Manuscrito Para encriptar un mensaje, el primer paso es convertirlo en una secuencia de números como lo indica la siguiente tabla:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W
11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34

y al espacio entre palabras le asignamos los dígitos 38. Así, “hola mundo” se convierte en 18262211382332241426.

H	O	L	A		M	U	N	D	O
18	26	22	11	38	23	32	24	14	26

Para realizar en manuscrito.

1) Usando el módulo $m = pq = 319$ y el exponente $e = 3$, que es coprimo con $\varphi(m) = 280$, encripte el mensaje `saludos a todos`.

2) Hace mucho, mucho tiempo en una galaxia muy lejana, te encontrabas en una misión ultra-secreta llevando en tu memoria las claves secretas $p = 23$, $q = 29$ y exponente $e = 5$. Llegas al Hotel Electiva2, donde te alojas, para “descansar” después de un día arduo de trabajo y

estudio; poco después de la media noche alguien toca a tu puerta y un misterioso mensajero te deja un papel con el mensaje encriptado siguiente:

[222, 330, 329, 232, 460, 329, 237, 41, 195, 329, 645]

Tu misión, si la aceptas, es aprobar el primer parcial del Hotel Elevtiva2, si sigues la orden del mensaje anterior.