PROBLEMA 3: Aplicación de teoría de números en Criptografía- RSA

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	á	é	í	ó	ú	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	Á	É	Í	Ó	Ú	1	2	3	4
5	6	7	8	9	0	+	-	*	/	^
%	#	$	@	SP	,	;	.	:	¿	?
¡	!	_	(	)	[	]	{	}	\	=
¬	ñ	Ñ	ü	Ü						

Tabla 1: matriz de caracteres con “SP” carácter en blanco

Se pretende, con este problema que, usted implemente una versión reducida del esquema de encripción y firmas digitales RSA. Efectivamente, usted deberá entregar una aplicación en Python con un paquete de funciones que cumpla con las siguientes tareas:

1. Forme la lista anterior de los caracteres (ver Lista) que va a utilizar para cifrar y/o descifrar mensajes y que corresponde a la lista de 103 caracteres: Tenga en cuenta que, el subíndice de esta lista inicia en 0 y va hasta 102.

Lista=[“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”, “á”, “é”, “í”, “ó”, “ú”, “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”, “Á”, “É”, “Í”, “Ó”, “Ú”, “1”, “2”, “3”, “4”, “5”, “6”, “7”, “8”, “9”, “0”, “+”, “-”, “*”, “/”, “^”, “%”, “#”, “$”, “@”,“ ”, “,”, “;”, “.”, “:”, “¿”, “?”, “¡”, “!”, “(”, “)”, “[”, “]”, “{”, “}”, “\”, “=”, “¬”, “ñ”, “Ñ”, “ü”, “Ü”]

2. Ingrese 2 números primos arbitrarios diferentes que, a partir de este momento se llamarán p, q tales que, tengan al menos 2 cifras.

3. Calcule el valor de n, el cual será la base Zn (de enteros no negativos menores que n) como el producto de p y q; es decir, n=p*q.

4. Calcule la función cociente de Euler phi(n) que corresponde a la cantidad de enteros entre 1 y n que son primos relativos de n, el cual nos interesa en el sistema RSA para n=p*q, siendo p y q números primos diferentes. Veamos,

   phi(n)= phi(p.q)=p.q-p-q+1=(p-1).(q-1)

5. Genere las claves (pública y privada).
   Clave pública (e): es un número aleatorio primo relativo entre 1 y phi(n)
   Seleccione, de manera aleatoria, un número entre 1< e < phi(n), tal que, mcd(e, phi(n))=1. Dicho valor corresponderá a la clave publica “e”.

Clave privada (d): corresponde al número del módulo del producto de los números enteros entre 1 y phi por la clave publica “e”, con phi(n). Es decir,

$$d(e,phi(n))=(e*(1< e< phi(n))) \text{ MOD } phi(n)=1$$ (que es único).

6. Envíe clave pública al EMISOR que corresponde a los parámetros n y e, la cual pueden ver todos. Entre el EMISOR y el RECEPTOR envían de manera oculta la clave privada n y d.

7. Cifrado: envíe el mensaje que corresponde a la lista M de las posiciones de cada carácter. Luego, forme una lista C con los caracteres cifrados. Efectivamente, forme una lista C con los módulos n de la potencia cada posición de la lista M, elevada a la clave pública. Dicha lista resultante corresponderá al mensaje encriptado. Ahora, muestre el mensaje cifrado; basta con concatenar o enlistar, según la lista C, con los caracteres de la lista L.

8. Descifrado: calcule los módulos n de la potencia cada posición de la lista C, elevada a la clave privada. Dicha lista resultante corresponderá al mensaje descifrado. Para mostrar el mensaje descifrado, concatene los caracteres de la lista L, según las posiciones de dichos caracteres.