Taller para descifrar mensajes

La tabla contiene los caracteres básicos para escribir un texto común y corriente y que respectivamente van desde “a” hasta “SP” (ver tabla).

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	SP						

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

SE PIDE:

1. Utilice la función lineal y=a.x+b mediante la cual se encripten mensajes, donde la variable “x” corresponde a la posición del carácter de la lista (**únicamente**); “a” es el coeficiente de x en la función lineal y “b” es el término independiente. Los valores de “a” y de “b” serán números que tendrán una extensión de hasta 14 cifras, cambiarán aleatoriamente cada vez que se realice una encriptación. Aunque siempre puede encriptarse con la función, deberá tener en cuenta que debe encriptar siempre mcd(n, a)=1; es decir, a y n tienen que ser primos relativos para poder descifrar luego en mensaje. Por lo tanto, determine con la función que descifra el mensaje enviado.

2. Haga que si un usuario envía un mensaje cifrado o encriptado, utilizando para los caracteres de la tabla 1, respectivamente representados por la cadena hexadecimal de la tabla 2, haga un informe en MS-Word en que descifre dicho mensaje y muestre tanto el mensaje encriptado como el descifrado. Considere, que deberá localizar los valores de a y b, para poder descifrarlo; en esto consistirá el éxito de la prueba, en vista de la posición de la clave o cambio de esta. Efectivamente, el valor del número “a” estará al comienzo del mensaje y al final encontrará el valor del número “b”. Dichos valores estarán separados del mensaje por el carácter “&”. Su informe deberá determinar, después de identificar el valor de “a”, si tiene o no invertible en $\mathbb{Z}n$. En caso afirmativo procederá a identificar el mensaje; en caso contrario deberá poner “el mensaje enviado no es descifrable”.

Tabla 2: cadena de hexadecimales representativos de los caracteres de la tabla 1

0061	0062	0063	0064	0065	0066	0067	0068	0069	006ª	006B
006C	006D	006E	006F	0070	0071	0072	0073	0074	0075	0076
0077	0078	0079	007ª	00E1	00E9	00ED	00F3	00FA	0041	0042
0043	0044	0045	0046	0047	0048	0049	004A	004B	005C	004D
004E	004F	0050	0051	0052	0053	0054	0055	0056	0057	0058
0059	005ª	00C1	00C9	00CD	00D3	00DA	0031	0032	0033	0034
0035	0036	0037	0038	0039	001A	002A	002B	002C	002D	002E
002F	0023	0024	0025	0040	003A	003B	003C	003D	003E	003F
00A1	0021	005F	0028	0029	005B	005D	007B	007D	005E	00AC
00F1	00D1	00FC	00DC	0020						

3. Por ejemplo, digamos que el mensaje que deberá descifrarse es:
   76283476234887&005D003F005F00D1&37628524277374

Valor de a	Separador	Mensaje	Separador	Valor de b
76283476234887	&	005D003F005F00D1	&	37628524277374

   El valor de a=76283476234887 MOD 104= 103 y b=37628524277374 MOD 104=30.
   103^{-1} en Z_{104}=103
   La función que encripta es: y=103x+30 en Z_{104}
   El mensaje que sale encriptado en hexadecimal es: 005D003F005F00D1
   La función para descifrar es: x= (y - 30)*103 en Z_{104}
   El mensaje descifrado en hexadecimal es: 0048004F005C0041
   El mensaje descifrado en lenguaje corriente corresponde a: HOLA

4. Se considerará como valor agregado para lo cual se asignarán 3 décimas del parcial para quienes establezcan hagan un aplicación en MatLab/C#/Java que establezca una comunicación inalámbrica entre dos PC y envíen y muestren los mensajes encriptados, localizando el IP de los computadores intercomunicados y, en efecto, realicen lo indicado en los numerales anteriores.

PROBLEMA 1: a=53179246802375; b=48795874858719

P1: encripte: ¿eN la LomiTa?

P2: descifre: ñ)}F¿ vY _x sG

PROBLEMA 2: a=12345678909876; b=98765432789098

P1: encripte: ñ)}F¿ vY _x sG

P2: descifre: ¿eN la LomiTa?