Criptografía: Tema 3 –Gestión de claves

Alumno(a) _____
Alumno(a) _____

1) Sea el generador de congruencias lineales G: Xi+1 = (21Xi +17) mod 32 y el alfabeto de 32 letras

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

P	Q	R	S	T	U	V	W	X	Y	Z	Á	É	Í	Ó	Ú
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Genere la clave para cifrar Mcla = CIELO considerando la semilla X0 = 3 y el alg.Afín por desplazamiento

2) Sea el generador de congruencias lineales G: Xi+1 = (11Xi +7) mod 32 y el alfabeto de 32 letras
Genere la clave para descifrar Cripto=QZÓÁJX considerando X0 = 1 y el alg.Afín por desplazamiento

3) Descifre el criptograma Cripto = ùÅg↔▼>╕I↑ utilizando una clave generada por congruencias lineales

con parámetros a = 73, b = 81, n = 256, X0 = 128, el algoritmo de Vernam.

4) Cifre el mensaje: Mcla = INFORMACIÓN mediante el algoritmo de Vernam, si la clave se generó con un LFSR con polinomio característico p(x) = x6 + x5 + 1, desplazamiento a la derecha y semilla X0 = 001001.

Utilice el código de la siguiente tabla

000000	A	010000	P	100000	Ü	110000	¿
000001	B	010001	Q	100001	0	110001	?
000010	C	010010	R	100010	1	110010	¡
000011	D	010011	S	100011	2	110011	!
000100	E	010100	T	100100	3	110100	"
000101	F	010101	U	100101	4	110101	@
000110	G	010110	V	100110	5	110110	#
000111	H	010111	W	100111	6	110111	$
001000	I	011000	X	101000	7	111000	%
001001	J	011001	Y	101001	8	111001	&
001010	K	011010	Z	101010	9	111010	(
001011	L	011011	Á	101011	+	111011	)
001100	M	011100	É	101100	-	111100	;
001101	N	011101	Í	101101	*	111101	,
001110	Ñ	011110	Ó	101110	/	111110	.
001111	O	011111	Ú	101111	=	111111	:

5) Considere ahora el alfabeto de 64 caracteres que se muestra a continuación

A	a	B	b	C	c	D	d	E	e	F	f	G	g	H	h	I	i	J	j	K	k	L	l	M	m
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

N	n	Ñ	ñ	O	o	P	p	Q	q	R	r	S	s	T	t	U	u	V	v	W	w
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	4 5	46	47

X	x	Y	y	Z	z	1	2	3	4	5	6	7	8	9	0
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63

Y genere mediante el generador LFSR con p(x)=x6 + x3 + 1 con corrimiento a la derecha, la secuencia que permita descifrar el Cripto = s u 7 K por el alg. Afín por desplazamiento variable si la semilla es X0 = 110010

6) Determine si la secuencia S=X1X2X3...X14 cumple con los postulados de Golomb. Considere que S se generó mediante el algoritmo BlumBlumShub con p = 163, q = 31, X0 = 1276 y el criterio del bit menos significativo.

7) Cifre el mensaje Mcla = SEIS mediante al algoritmo por desplazamiento con 32 letras. Considere que la clave de cifrado se generó mediante BlumBlumShub con p = 131, q = 67, X0 = 81 y el bit menos significativo. Cada 5 bits representan, en binario, el valor numérico de una letra.

8) Descifre Cripto = PZIÍDOS mediante el algoritmo por desplazamiento con 32 letras, donde la clave de cifrado se obtuvo con un LFSR con polinomio p(x) = x5 + x4 + x3 + x + 1, semilla X0 = 11110 y corrimiento a la izquierda. (cada 5 bits representan, en binario, el valor numérico de una letra).

9) Genere una secuencia aleatoria S de 24 bits mediante el LFSR representado por el polinomio q(x) = x8 + x6 +x5 +x4 + 1, desplazamiento a la derecha y semilla X0 = 10101011, y determine si S cumple con los postulados de Golomb.

10) Obtenga la secuencia pseudoaleatoria S = X1X2X3...X25, si se generó mediante el algoritmo BlumBlumShub con parámetros p = 31, q = 47, X0 = 994 y bit menos significativo.

TRABAJO

El trabajo debe cumplir con las características propias dadas a conocer a través de la rúbrica para trabajos.

Programar dos generadores de claves:

A) Un generador BlumBlumShub que corresponda a parámetros dados en el ejercicio 7
B) Un generador LFSR que corresponda a parámetros dados en el ejercicio 8

Para ambos generadores es necesario presentar: análisis, diseño, selección de herramientas de software, desarrollo (programación), pruebas y conclusiones.
Requisito indispensable entregar en un CD el programa y el ejecutable da cada generador.