Los generadores de números aleatorios, también conocidos como RNG por sus siglas en inglés de *Random Number Generators,* son algoritmos determinísticos que dependes de un valor inicial o semilla, para producir una variable al azar especificada por una distribución, por lo tanto cada elemento de una secuencia pseudoaleatoria es reproducible a partir de su semilla; así, en criptografía, la selección de un buen generador no debe de tomarse a la ligera y es altamente recomendable realizar las pruebas estadísticas suficientes que garanticen la calidad del generador antes de utilizar una secuencia cifradora.

1. Con base en tres de las pruebas estadísticas emitidas por el NIST:

Frequency – Monobit , *Frequency – Block* , *Run Test*.

Indique a qué se refieren, determine si la secuencia $S=X_1X_2X_3...X_{50}$ cumple cada una de ellas y finalmente señale qué tán recomendable es utilizar la secuencia generada. Considere que S se generó mediante el algoritmo BlumBlumShub con p = 163, q = 31, X_0 = 1276 y el criterio del bit menos significativo.

2. Descifre el Cripto=LPJC si se sabe que fue cifrado mediante el algoritmo Afín por desplazamiento puro variable con el alfabeto de 32 letras que se muestra a continuación:

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

La clave de cifrado se obtuvo mediante BlumBlumShub con p = 131, q = 67, X_0 = 81 y el bit menos significativo. Cada 5 bits representan, en binario, el valor numérico de una letra.

3. Descifre el Cripto = 288CRVo~ mediante el algoritmo Afín por desplazamiento y el alfabeto de 64 caracteres que se muestra a continuación, donde la clave de cifrado se obtuvo con un LFSR con polinomio $p(x) = x^6 + x^5 + x^2 + x + 1$, semilla X_0 = 101011 y corrimiento a la derecha. Determine qué tan recomendable es utilizar como secuencia cifradora la secuencia generada.

Tenga presente que el alfabeto utilizado es:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	P	Q	R	S	T	U	V	W	X	Y
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	16	17	18	19	20	21	22	23	24	25

Z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o~	p	q	r	s	t	u	v	w
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50

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

4. Descifre Cripto = EKCW mediante el algoritmo Afín por desplazamiento y el alfabeto de 32 letras del ejercicio anterior, donde la clave de cifrado se obtuvo con un LFSR con polinomio $p(x) = x^5 + x^4 + x^3 + x + 1$, semilla $X_0 = 11110$ y corrimiento a la izquierda. Determine si la secuencia utilizada para cifrar es seguramente confiable. Para recuperar el Mcla considere que cada 5 bits representan, en binario, el valor numérico de una letra. Tenga presente que:

• el grado n de su polinomio característico indicará el número de celdas y se producirá una secuencia de período 2^n-1.

• el valor del término independiente es a_0=1, y representa la entrada realimentada.

• el polinomio debe ser primitivo; es decir, no puede reducirse o factorizarse en polinomios de grado menor y además divide a $x^{(2^n)-1}-1$; todo en módulo dos.

• debe evitarse la secuencia nula.

5. Descifre Cripto = PZIÍDOS mediante el algoritmo Afín por desplazamiento y el alfabeto de 32 letras del ejercicio anterior, donde la clave de cifrado se obtuvo con el LFSR de polinomio $p(x) = x^5 + x^4 + x^3 + x + 1$, mostrado a continuación, semilla $X_0 = 11110$ y corrimiento a la izquierda. Cada 5 bits representan, en binario, el valor numérico de una letra. Tenga presente que: