Ejercicios:
Cifrado en flujo con clave secreta

3.1) Descifra el criptograma c = |^M|É| = 13 144$_{(ASCII)}$ sabiendo que se ha utilizado el método Vernam con la secuencia cifrante de 16 bits obtenida mediante el algoritmo RC4 con 3 bits de salida por iteración y semilla k = [7,6,5,4,3,2,1,0].

3.2) Descifra el criptograma c = |^E|,|~| = 05 44 126$_{(ASCII)}$ sabiendo que se ha utilizado el método Vernam con la secuencia cifrante de 24 bits obtenida mediante el algoritmo RC4 con 2 bits de salida por iteración y semilla k = [2,1,3].

3.3) Descifra el criptograma c = Ë = 203$_{(ASCII)}$ sabiendo que se ha utilizado el método Vernam con la secuencia cifrante de 8 bits obtenida mediante el algoritmo RC4 con 4 bits de salida por iteración.
La clave para el algoritmo viene dada por la cadena de 64 bits obtenida a partir de la palabra ALIMENTO codificada en ASCII.
El texto en claro corresponde a una vocal.
Ten en cuenta la siguiente tabla:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
ASCII	65	66	67	68	69	70	71	72	73	74	75	76	77	78
HEX	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E

	O	P	Q	R	S	T	U	V	W	X	Y	Z	Ë
ASCII	79	80	81	82	83	84	85	86	87	88	89	90	203
HEX	4F	50	51	52	53	54	55	56	57	58	59	05	CB

3.4) Describe, brevemente, el esquema fundamental de un cifrador en flujo (qué hace el emisor del mensaje m, que hace el receptor del criptograma c, …)

3.5) Todo registro de desplazamiento realimentado linealmente con n celdas tiene asociado un polinomio de realimentación de grado *n*. En el caso de que este polinomio sea primitivo, explica qué tipo de secuencia se obtendría.

3.6) Explica brevemente las características generales del algoritmo de cifrado A5.

3.7) Explica brevemente las características generales del algoritmo de cifrado E0.