SCI 2000
Introduction to Encryption, Assignment 3
Due March 5th at the start of class.

Questions will be marked both on correctness and clarity of presentation. Poor writing and sloppy/illegible presentation both impact the clarity of your work and so will be penalized. You must show all steps in your computations to get credit.

Question 1: In class, we defined the LFSRsum cipher using the 3-bit LFSR $b_3 = b'_2 + b'_1$ and the 5-bit LFSR $c_5 = c'_4 + c'_2 + c'_1$. For this question, replace the 5-bit LFSR from class with the a new 5-bit LFSR given by

$$c_5 = c'_3 + c'_2.$$

Use this new register, together with the same 3-bit register as above, to create a new version of LFSRsum. Use it to encrypt the plain text:

$$0\ 1\ 1\ 1\ 1 \quad 0\ 0\ 1\ 0\ 1.$$

Question 2: Use the same 3-bit and 5-bit registers as in the previous question to create a new version of BabyCSS. Use it to encrypt the plain text from Question 1.

Question 3:

ASCII allows us to convert letters to binary according to the entries in the following table:

a	= 01100001	A	= 01000001
b	= 01100010	B	= 01000010
c	= 01100011	C	= 01000011
d	= 01100100	D	= 01000100
e	= 01100101	E	= 01000101
f	= 01100110	F	= 01000110
g	= 01100111	G	= 01000111
h	= 01101000	H	= 01001000
i	= 01101001	I	= 01001001
j	= 01101010	J	= 01001010
k	= 01101011	K	= 01001011
l	= 01101100	L	= 01001100
m	= 01101101	M	= 01001101
n	= 01101110	N	= 01001110
o	= 01101111	O	= 01001111
p	= 01110000	P	= 01010000
q	= 01110001	Q	= 01010001
r	= 01110010	R	= 01010010
s	= 01110011	S	= 01010011
t	= 01110100	T	= 01010100
u	= 01110101	U	= 01010101
v	= 01110110	V	= 01010110
w	= 01110111	W	= 01010111
x	= 01111000	X	= 01011000
y	= 01111001	Y	= 01011001
z	= 01111010	Z	= 01011010

Notice that the leftmost bits are always "01", and that the bit in the third position from the left simply determines whether or not the letter is uppercase, or lowercase. For this question, we will therefore take the rightmost five bits and use them to represent letters, which by convention we will write in uppercase. E.g. 00001 will be "A", 00010 is "B", etc. Note that some combinations of five bits do not correspond to letters, e.g. 11111 is no letter.

Here is the question. Someone is sending messages using BabyCSS, but using the LFSRs from Question 1 (i.e. their 3-bit register is the same as in class, but their 5-bit register is different). The ciphertext you have intercepted is

1 1 1 1 0 0 0 0 0 1

You discover that the first letter of their message is "H", and the seed used for their 3-bit LFSR is either 001 or 101 (recall seeds always end in 1).

(a) Which seed did they use for their 3-bit LFSR? Justify your answer.

(b) Which seed did they use for their 5-bit LFSR? Justify your answer.

(c) What was the message? Justify your answer.

Question 4: Draw an example of a graph on 10 vertices with a perfect code. Circle the vertices corresponding to the perfect code to indicate your answer.