**HW 12 CMSC 456. MORALLY DUE Dec 10**
**NOTE- THE HW IS FOUR PAGES LONG**

1. (0 points) READ the syllabus- Content and Policy. What is your name? Write it clearly. What is the day of the final? READ the slides and notes on Perfect and Comp Secrecy.

**GOTO NEXT PAGE**

2. (40 points)

All of the arithmetic in this problem is mod 2.

Write a program do do the following.

Input $c_0, c_1, c_2, c_3 \in \{0, 1\}$ and do the following:

(a) Let

$$f(s_3, s_2, s_1, s_0) = (c_3 s_3 + c_2 s_2 + c_1 s_1 + c_0 s_0, s_3, s_2, s_1)$$

(ADDED: This is CORRECT. Earlier version had

$$(c_3 s_3 + c_2 s_2 + c_1 s_1 + c_0 s_1, s_3, s_2, s_1)$$

which was INCORRECT.)

(b) For all $b_0, b_1, b_2, b_3 \in \{0, 1\}$ compute
$v_0 = (b_3, b_2, b_1, b_0)$
$v_1 = f(v_0)$
$v_2 = f(v_1)$
$\vdots$
UNTIL you find $i < j$ such that $f(v_i) = f(v_j)$. Keep track of the $j$'s seen (see next step). (So you will need to store all of the $v_1, v_2, \ldots$. Since there are only 16 possibilities you can do this in an inelegant but easy way. And DO NOT WORRY- I am NOT going to ask you to later to it for 10 bits or 100 bits or something that would require a clever way to store it.)

(c) For each $(c_3, c_2, c_1, c_0)$ note which $(b_3, b_2, b_1, b_0)$ lead to the LARGEST sequence without a repeat- so the largest $j$.

You final output should look like this (I made up the numbers and only give the first two rows. Yours should have 16 rows).

| $c$-vector | best $b$-vector | length of sequence |
|---|---|---|
| 0000 | 1100 | 2 |
| 0001 | 1010 | 13 |

**GOTO NEXT PAGE**

3. (30 points) All of the arithmetic in this problem is mod 2.

   Let

$$f(s_3, s_2, s_1, s_0) = (s_3 s_2 + s_1 + s_0, s_3, s_2, s_1)$$

   (ADDED: No problem here. The above IS correct and always has been. Some students THOUGHT it was a typo to have $s_3 s_2$ but its NOT. This is close to the function I proposed on Nov 19, slide titled *Nonlinear Feedback Shift Register* )

   Write a program do do the following.

   (a) For all $b_0, b_1, b_2, b_3$ compute

   $v_0 = (b_3, b_2, b_1, b_0)$

   $v_1 = f(v_0)$

   $v_2 = f(v_1)$

   $\vdots$

   UNTIL you find $i < j$ such that $f(v_i) = f(v_j)$. Keep track of the $j$'s seen (see next step). (So you will need to store all of the $v_1, v_2, \ldots$. Since there are only 16 possibilities you can do this in an inelegant but easy way. And DO NOT WORRY- I am NOT going to ask you to later to it for 10 bits or 100 bits or something that would require a clever way to store it.)

   (b) For each $(b_3, b_2, b_1, b_0)$ output the length of the sequence before a repeat. sequence without a repeat.

   You final output should look like this (I made up the numbers and only gave the first two rows. Yours should have 16 rows.)

| $b$-vector | length of sequence |
|---|---|
| 0000 | 5 |
| 0001 | 19 |

**GOTO NEXT PAGE**

4. (30 points) Give a rigorous definition of a psuedorandom FUNCTION that uses a game. It should begin with $F_k(x)$ where $k$ is unif in $\{0,1\}^n$. $F_k$ goes from $\{0,1\}^n$ to $\{0,1\}^n$.

   (ADDED HINT:

   - Use a Game!
   - In class we have defined roughly two kinds of games: Here is an example of each: (1) Defining perfect security. Here Eve picks $m_0, m_1$, Alice encodes one of them into $c$, gives Eve $c$, and eve has to tell which one it was $m_0$ or $m_1$. (2) Defining Psuedorandom GEN: Here ALICE picks a truly random string and a psuedorandom string and Eve has, gives one of them to Eve, Eve has to tell which one it was.
   - The definition of Psuedorandom Function will be more like that of psuedorandom generator.
   - When Alice gives Eve a function, Eve will have black box access to it.

   )