HW 10 CMSC/MATH/ENEE 456. Morally DUE Nov 30.

1. (0 points but you MUST DO IT)
   (a) What DAY and TIME are the TIMED FINAL?
   (b) IF that DAY/TIME is not good for you then EMAIL ME.

GOTO NEXT PAGE

2. (20 points) Consider the following pathetic PRG:

$$G(b_1 \cdots b_n) = b_1 \cdots b_n(\sum_{i=1}^{n} b_i \pmod 4 \text{ written in binary}).$$

Example 11001 maps to 11001(1+1+0+0+1 mod 4 written in binary) = 1100111.

Come up with a poly time strategy for Eve for the Psuedo-Random Game that is correct over $\frac{1}{2}$ the time. Note when Eve is SURE that she wins and when she is NOT sure. Prove that Eve wins OVER half the time.

The strategy should begin:

Eve's strategy:

- Eve sees strings $b_1 \cdots b_n b_{n+1} b_{n+2}$ and $c_1 \cdots c_n c_{n+1} c_{n+2}$.
- Eve computes $b_1 + \cdots + b_n \pmod 4$ and writes it in binary as $b'_{n+1} b'_{n+2}$.

GOTO NEXT PAGE

3. (20 points) One way to measure how random a sequence is to measure the following: How often does 0 occur? How often does 1 occur? How close are they? How often does 00 occur? 01? 10? 11? Is it close? (example: 0110 has zero 00, one 01, one 11, one 10) Similar for sequences from $\{0, 1, 2\}$. In this problem we do an empirical study of two stream ciphers and see how random they look.

GOTO NEXT PAGE

(a) (10 points) AN ATTEMPT AT A 0-1 STREAM CIPHER.

Do the following TEN times and format it as specified later. *Pick a RANDOM 10-bit sequence. Let them be* $x_1, \ldots, x_{10}$.

Using that $x_1, \ldots, x_{10}$, *and the recurrence,*

$$x_{n+10} = x_{n+9}x_{n+8} + x_{n+7}x_{n+6} + x_{n+5}x_{n+4} + x_{n+3}x_{n+2} + x_{n+1}x_n \pmod 2$$

find $x_1, \ldots, x_{1000}$.

Find how many 0's are in $x_1, \ldots, x_{1000}$. *1's. PRINT the absolute value of the difference.*

Find how many 00's are in $x_1, \ldots, x_{1000}$. *01's. 10's. 11's. Let MIN be the MIN of these 4 numbers and MAX be the max of these 4 numbers. PRINT MAX-MIN.*

Find how many 000's are in $x_1, \ldots, x_{1000}$. *010's, ..., 111's. Let MIN be the MIN of these 8 numbers and MAX be the max of these 8 numbers. PRINT MAX-MIN.*

You do not have to submit your code. We just want the table in this format (this is just an example which probably bears no relation to reality):

10-bit initial sequence	1-bit diff	2-bit diff	3-bit diff
0110001101	8	49	13
1001010010	18	99	3
⋮	⋮	⋮	⋮

(In your HW you will have ten of these rows.)

(b) (0 points but DO It- this is really the point of the HW) Speculate on if this recurrence is a good stream cipher.

GOTO NEXT PAGE

(c) (10 points) We call elements of $\{0,1,2\}$ *trits*. Do the following TEN times and format it as specified later. *Pick a RANDOM 10-trit sequence. Let them be* $x_1, \ldots, x_{10}$.

Using that $x_1, \ldots, x_{10}$, *and the recurrence:*

$$x_{n+10} = x_{n+9}+x_{n+8}+x_{n+7}+x_{n+6}+x_{n+5}+x_{n+4}+x_{n+3}+x_{n+2}+x_{n+1}+x_n \pmod 3$$

find $x_1, \ldots, x_{1000}$.

Find how many 0's are in $x_1, \ldots, x_{1000}$. *1's. 2's. Let MIN be the MIN of these 3 numbers and MAX the MAX of these 3 numbers. PRINT MAX-MIN.*

Find how many 00's are in $x_1, \ldots, x_{1000}$. *01's. 02's. 10's. 11's. 12's. 20's. 21's. 22's. Let MIN be the MIN of these 9 numbers and MAX be the max of these 9 numbers. PRINT MAX-MIN.*

Find how many 000's are in $x_1, \ldots, x_{1000}$. *001's. 002's.* $\cdots$ *222's. Let MIN be the MIN of these 27 numbers and MAX be the max of these 27 numbers. PRINT MAX-MIN.*

You do not have to submit your code. We just want the table in this format (this is just an example which probably bears no relation to reality):

10-bit initial sequence	1-trit diff	2-trit diff	3-trit diff
2110021101	8	49	13
1021020012	18	99	3
⋮	⋮	⋮	⋮

(In your HW you will have ten of these rows.)

(d) (0 points but DO It- this is really the point of the HW) Speculate on if this recurrence is a good stream cipher.

GOTO NEXT PAGE

4. (20 points) Alice and Bob are going to do Public Key LWE.

   Prime $p = 37$. Public. Bob adds $\lfloor \frac{37}{2} \rfloor = 18$ when he sends $b = 1$.

   Length of vector $n = 5$. Public.

   Number of equations is $m = 4$. So $\gamma = \lfloor \frac{37}{8} \rfloor = 4$. Both public.

   Alice's private key is $(1, 3, 5, 8, 22)$.

   The noisy equations Alice makes public are:

$$2k_1 + 4k_2 + 6k_3 + 8k_4 + 18k_5 \sim 24 \pmod{37}$$

$$3k_1 + 6k_2 + 9k_3 + 15k_4 + 20k_5 \sim 0 \pmod{37}$$

$$4k_1 + 5k_2 + 6k_3 + 7k_4 + 9k_5 \sim 7 \pmod{37}$$

$$10k_1 + 9k_2 + 8k_3 + 7k_4 + 6k_5 \sim 7 \pmod{37}$$

   (a) (7 points) Bob wants to send $b = 0$. He chooses the first and third equations (note that he does not need to pick a random error). What does he send? Describe what Bob does and show work.

   (b) (7 points) Bob wants to send $b = 1$. He chooses the first and fourth equations (note that he does not need to pick a random error). What does he send? Describe what Bob does and show work.

   (c) (6 points) Alice receives the equation

$$17k_1 + 11k_2 + 15k_3 + 21k_4 + 29k_5 \sim 25 \pmod{37}.$$

   Describe what Alice does to find the bit Bob sent, and tell us the bit.

   (d) (0 points. DO THIS- we will discuss it in class.) This turns out to be a terrible set of equation for secrecy. This is NOT because the the p, n, m are too small. There is ANOTHER reason. Speculate on what that is.

GOTO NEXT PAGE

5. (20 points) Alice and Bob are going to do secret sharing with cards. So Alice, Bob, and Eve are at a table.

   (a) (0 points) What DAY and TIME are the TIMED FINAL? IF that DAY/TIME is not good for you then EMAIL ME. How many students will STILL not read this even though its not problem 1 they tend to skip over? How many students will ask me to take it a different time the DAY of the timed final? Should I accommodate them?

   (b) (0 points, but you will need to do this for the later.) Recall that
   $(\forall n \ge 0)[\binom{n}{0} = 1]$
   $(\forall k \le n)[\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}]$
   Use these equations to write a program that, given n, k, computes $\binom{n}{k}$. You should use dynamic programming, not recursion.

   (c) (0 points, but you will need to do this for the later.) Write a program that, on input $x \in \mathbb{N}$, outputs $\lfloor \lg x \rfloor$.

   (d) (0 points, but you will need to do this for the later.) In class we discussed what happens if m is EVEN and the cards start as (m, m, m), in the worst case. Think about what happens when m is ODD.

   (e) (20 points) Write a program that will, given n, find the least m such that, in the worst case (m, m, m) produces $\ge n$ bits. You DO NOT need to submit the program. You need to run it on $n = 100, 200, \ldots, 3000$ and produce at table of the following form (the numbers in the table are made up).

n	m
100	110
200	220
300	330
$\vdots$	$\vdots$
3000	3330

   Your table will NOT have DOT-DOT-DOT.

   (DO NOT use the approximations I did in class. We want the actual numbers.)