CMSC-MATH-ENEE 456 Timed Final, Fall 2021

1. This is an open-book, open-slides, open-web exam.
2. There are 4 problems which add up to 50 points.
3. In order to be eligible for as much partial credit as possible, show all of your work for each problem, **write legibly**, and **clearly indicate** your answers. Credit **cannot** be given for illegible answers.
4. Please write out the following statement: "*I pledge on my honor that I will not give or receive any unauthorized assistance on this examination.*"

5. Fill in the following:

NAME :
SIGNATURE :
UID :

1. (4 points) To set up RSA, Zelda sends Alice $(77, 31)$, so $N = 77$ and $e = 31$. Find the value of d. Show work, though you can use a calculator or Wolfram Alpha.

GOTO NEXT PAGE

2. (24 points- 4 points each) For each of the following questions give a short answer (no more than five sentences). Your answer has to really be about the cipher in question. For example, you CANNOT SAY

   The matrix cipher is not used because Alice and Bob have to meet

   since that is true of MANY ciphers.

   (a) Why is the Matrix Cipher not used in the real world?

GOTO NEXT PAGE

(b) There are three reasons people often use RSA with $e = 2^{16} + 1$. One is that e is prime, so no need to test if its rel prime to d. Another is that e is large. What is the third reason?

GOTO NEXT PAGE

(c) Why do people use a safe prime when doing Diffie-Helman?

GOTO NEXT PAGE

(d) Why do people use a pair of safe primes when doing RSA?

GOTO NEXT PAGE

(e) Why would someone use LWE-PUBLIC rather than RSA?

GOTO NEXT PAGE

(f) When doing Diffie-Helman, Alice and Bob use a prime p and a generator g. Why do they use a generator?

GOTO NEXT PAGE

3. (12 points) Zelda is doing $(2, 2)$ secret sharing with A_1 and A_2 over $\mathbb{Z}_7$.
   Zelda gives A_1 the number 2.
   Zelda gives A_2 the number 1.
   What is the secret? Show your work.

GOTO NEXT PAGE

4. (10 points) Alice and Bob are going to do LWE-PRIVATE with parameters:

   $\vec{k} = (12, 203, 44, 47)$. (RECALL- this is private)

   $p = 2009$. (RECALL- this is public)

   $\gamma = 10$. (RECALL- this is public. This is smaller than recommended, but that's not an issue for this problem.)

   Find TEN values of x such that if Bob receives $(1, 2, 3, 4; x)$ then Bob KNOWS that Eve tampered with the message.