CMSC 456 Final, Fall 2020

1. This is an open-book, open-slides, open-web exam. If you have a question please go to class Zoom site or post to private piazza.
2. You may use calculators or programs you find online or programs you wrote for the class on any of the problems.
3. There are 5 problems which add up to 100 points. The exam is 120 minutes.
4. 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.
5. After the last page there is paper for scratch work.
6. Please SIGN the following statement, which you can do by typing if this is being done online in (say) LaTeX.

   "*I pledge on my honor that I will not give or receive any unauthorized assistance on this examination.*"

7. Fill in the following:

NAME :
SIGNATURE :
UID :

1. (20 points) (This problem has 5 parts, 2 on this page and 2 on the next page and 1 on the next page after that. Do this problem in the space provided after each question.) Give SHORT answers to all of these questions.

   (a) What is an advantage of using the public-key LWE rather than RSA?

   (b) What is an advantage of using RSA rather than public-key LWE?

(c) What is an advantage of using the randomized-shift cipher rather than the shift cipher?

(d) The Eric-3 cipher is as follows: Let S be the set of all 3-blocks of letters (aaa, aab, $\ldots$, zzz). Take a random perm of S (e.g., pqz, ppq, uvb might be the first three). Use this for your key and for you mapping (e.g., in the above aaa maps to pqz).

And NOW for the question: What is an advantage of using the Eric-3 cipher rather than the 3×3 matrix cipher?

(e) What is an advantage of using the 3×3 matrix cipher rather than the Eric-3 cipher?

2. (20 points) (Do this problem on this page and, if needed, the next page.) Alice and Bob have an idea! They will do Diffie Helman using $\mathbb{N}$ (the naturals) instead of mod p. They do not need to pick a prime. They will pick g, a, b such that $g, a, b \in \{2, \ldots, L\}$ where L is a security parameter. (We assume that calculations with $g, a, b \in \{2, \ldots, L\}$ do not take much time and that space is abundant and hence not an issue.) They call their protocol DHON (Diffie-Helman-Over-N).

   GRADING The three parts were 8 points, 4 points, 8 points.

   (a) Give READABLE psuedo code for DHON. It should look like
   ALICE does BLAH BLAH
   BOB does BLAH BLAH
   BLAH BLAH BLAH
   and their shared secret is BLAH BLAH

   (b) If $g = 3$, $a = 2$, and $b = 5$ then what is the shared secret key? Express in base 2.

   (c) Why is DHON worse than DH? (Recall that we are assuming calculation is fast and space is abundant so neither speed nor space are an issue.)

3. (20 points) (Do this problem on this page and, if needed, the next page.) READ THIS NOW!: In this problem you will likely use a calculator or an online program OR the program you wrote for class. However, you should **show work** as follows: If I ask you what (say) R is, you can't just write down $R = 6769$, you need to write down how you got R, for example (THIS IS NOT TRUE) $R = \lceil p^2 \lg q \rceil = \lceil 101 * \lg(103) \rceil = 676$. You an use English if you need to, like (THIS IS NOT TRUE) for example "R is the inverse of p mod q so R is the inverse of 101 mod 103 which is BLAH".

   AND NOW FOR THE PROBLEM:

   Alice and Bob are going to do RSA. Alice is using $p = 101$, $q = 103$, and $e = 11$. In this problem we use the notation for RSA from the slides.

   (a) What is N? (REMEMBER- show work, though you can use a calculator or a program on the web.)

   (b) What is R? (REMEMBER- show work, though you can use a calculator or a program on the web.)

   (c) What is d? (REMEMBER- show work, though you can use a calculator or a program on the web.)

   (d) Bob wants to send plaintext 40. What does he send? (REMEMBER- show work, though you can use a calculator or a program on the web.)

   (e) (This problem is NOT connected to part (d).) Lets say Alice sees that Bob sent her ciphertext 7534. What is the plaintext? (REMEMBER- show work, though you can use a calculator or a program on the web.)

4. (20 points) (Do this problem on this page and, if needed, the next page.) A Zan-Prime is a prime p such that $p-1 = 6q$ where q is prime. ASSUME we have a fast program that will, given a number, determine if it is prime. (You do not need to do trial division or anything to optimize this program.) You also have a random number generator.

   (a) Write pseudo code for a program that will, on input L, output a random L-bit Zan-Prime. (The left most bit has to be 1.
   The result must be exactly L bits, so $2^{L-1} \le p < 2^L$.

   (b) Write pseudo code for a program that will, given a Zan-Prime p and a number $g \in \{1, \ldots, p-1\}$, determine if g is a generator in $O(\log p)$ time. (HINT: Use that p is a Zan-prime.)

5. (20 points) (Do this problem on the next page and, if needed, the page after that.) For this problem we assume that m is a perfect square so $\sqrt{m}$ is a natural. Let sq be $\sqrt{m}$.

   Zelda has a secret s. She wants to share it with $A_1, \ldots, A_m$. We assume

   If $A_1, \ldots, A_{sq}$ (or any superset) get together they can learn the secret.

   If $A_2, \ldots, A_{sq+1}$ (or any superset) get together they can learn the secret.

   $\vdots$

   If $A_{m-sq+1}, \ldots, A_m$ (or any superset) get together they can learn the secret.

   If $A_{m-sq+2}, \ldots, A_m, A_1$ (or any superset) get together they can learn the secret.

   If $A_{m-sq+3}, \ldots, A_m, A_1, A_2$ (or any superset) get together they can learn the secret.

   $\vdots$

   If $A_m, A_1, \ldots, A_{sq-1}$ (or any superset) get together they can learn the secret.

   (So any consecutive segment of sq people, including wrap-around.)

   NO OTHER set of people who get together can learn the secret. (For Example, A_1, A_3, A_5, A_7 cannot learn the secret.)

   (a) EXPLAIN a secret sharing scheme Zelda can use. Specify: (1) What Zelda gives to each person, and (2) What each group does to obtain the secret.

   (b) Let $|s|$ be the length of the secret. ROUGHLY how many bits does each A_i get? Your answer should be of the form $O(f(|s|, m))$. (NOTE THAT the answer is a function of $|s|$ and m NOT just $|s|$.)

EXTRA PAGE IF YOU NEED IT