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?

   If factoring can be done quickly, Public-Key LWE remains secure. (e.g., quantum computers can break RSA but not LWE.)

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

   RSA has withstood the test of time. It has been out there so long that it has been attacked and improved so now it seems secure.

   Also, it is much faster and easier to implement, and has much smaller key sizes.

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

Randomized is not vulnerable to NY, NY problem

(d) The Eric-3 cipher is as follows: Let S be the set of all 3-blocks of letters (aaa, aab, ..., 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?

3 x 3 matrix can be broken up by solving as a system of equations

Eric-3 is strictly stronger, since its keyspace is strictly larger (every matrix is a permutation, but not the other way around)

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

A 3 x 3 matrix can be represented by a string of length 9, while a permutation is length 52728.

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

      i. Alice picks a g in $\{2, \ldots, 100\}$. She broadcasts it.
      ii. Alice picks an $a \in \{2, \ldots, 100\}$. She broadcasts g^a.
      iii. Bob picks a $b \in \{2, \ldots, 100\}$. He broadcasts g^b.
      iv. Alice computes $(g^b)^a = g^{ab}$.
      v. Bob computes $(g^a)^b = g^{ab}$.
      vi. Their shares secret is g^{ab}.

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

   The shared secret is $g^{ab} = 3^{10} = 59049$ which is 1110011010101001.

   (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.)

   Eve knows g and she sees g^a. Over $\mathbb{N}$ she can EASILY compute the log and get a. So DHON is insecure, whereas DH seems to be secure.

   COMMENT ON GRADING No other answer made sense. In particular, some students said that brute force was easier over $\mathbb{N}$ than over $\mathbb{Z}_p$, but this is not true.

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.)
   $N = pq = 10403$.

   (b) What is R? (REMEMBER- show work, though you can use a calculator or a program on the web.)
   $R = (p-1)(q-1) = 100 \times 102 = 10200$

   (c) What is d? (REMEMBER- show work, though you can use a calculator or a program on the web.)
   d is the inverse of e mod R, so
   d is the inverse of 11 mod 10200.
   I'll do it by hand, but you can use a calculator for this
   $10200 = 11 * 927 + 3$
   $11 = 3 * 3 + 2$
   $3 = 2 * 1 + 1$
   SO
   $1 = 3 - 2 = 3 - (11 - 3 * 3) = 3 * 4 - 11 = (10200 - 11 * 927) * 4 - 11$
   $1 = 4 * 10200 - 11 * 4 * 927 - 11 = 4 * 10200 - 11 * (4 * 927 + 1) = 4 * 10200 - 11 * 3709$
   $1 \equiv -11 * 3709 \pmod{10200}$

SO the inverse of 11 is $-3709 \equiv 6491$.

SO $d = 6491$.

(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.)

To send m Bob sends $m^e \pmod{N}$.

This is

$40^{11} \equiv 8623 \pmod{10403}$.

SO Bob sends 8623.

(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.)

Alice sees 7534

To decode she does $7534^{6491} \pmod{10403}$ which is

$8623^{6491} \equiv 41 \pmod{10403}$.

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 $2^{L-1} \leq p < 2^L$.

   (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.)

   Your pseudocode may vary, but the gist is:

   (a) Keep generating random ps and check if p is prime and $(p-1)/6$ is prime until you get a Zan-prime

   (b) ALL arithmetic in this solution are mod p.

   Recall that g is a gen mod p iff for all non-trivial factors x of $p-1$, $g^x \not\equiv 1$. Since $p = 6q+1$ the only non-trivial factors of $p-1$ are $2, 3, 6, q, 2q, 3q$. With that in mind, here is the program:

   Compute $g^2, g^3, g^6, g^q, g^{2q}, g^{3q}$. If NONE of them ae 1, then you have a generator. Computing $g^2, g^3, g^6, g^q, g^{2q}, g^{3q}$ takes $O(\log p)$ steps.

   GRADING POLICY If you did any kind of brute force search then you got 0 on this part. Hence, if that is what you did, and you do a regrade request, you will lose points.

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 $|s|$.)

   ANSWER:

   (a) Let $1 \leq i \leq m$. We deal with the group $A_i, \ldots, A_{i+sq-1 \pmod m}$. For all $0 \leq j \leq m-1$ Zelda does the following: Generates random strings $r_0, \ldots, r_{sq-2 \pmod m}$.

Give A_{i+j} (i, r_j).

Give $A_{i+sq-1 \pmod m}$ $(i, r_0 \oplus \cdots \oplus r_{sq-2 \mod m})$.

To recover the secret they just $\oplus$ all of their strings together.

(b) Each A_i is involved in sq groups. Hence A_i gets sq strings of length $O(|s|)$, so A_i gets $O(|s|m^{1/2})$. That is not quite right- the marker saying what group you are in takes $O(\log m)$ bits, so its really $O(\log m + |s|m^{1/2})$, but I did not take off for that.

COMMENT ON GRADING For part b if you wrote anything other than $O(|s|m^{1/2})$ or similar, and possibly with a $\log m$, 0 points.

EXTRA PAGE IF YOU NEED IT