CMSC 456 Final-VERSION B, Fall 2018

1. This is a closed book exam, though ONE sheet of notes is allowed. **You CANNOT use a Calculator**. If you have a question during the exam, please raise your hand.
2. There are 7 problems which add up to 100 points. The exam is 120 minutes.
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. After the last page there is paper for scratch work.
5. Please write out the following statement: "*I pledge on my honor that I will not give or receive any unauthorized assistance on this examination.*"
6. Fill in the following:

NAME :
SIGNATURE :
SID :

SCORES ON PROBLEMS (FOR OUR USE)

Prob 1:	
Prob 2:	
Prob 3:	
Prob 4:	
Prob 5:	
Prob 6:	
Prob 7:	
TOTAL	

1. (15 points) Zelda wants to do $(3,3)$ information-theoretic secret sharing with polynomials. The players are A_1, A_2, A_3. The secret is 6.

   (a) (8 points) Assume Zelda uses the prime $p = 7$, and works over mod 7. Assume Zelda generates $r_2 = 1$ and $r_1 = 3$ as her two random numbers. What share does she give A_1? What share does she give A_2? What share does she give A_3?

   (b) (7 points) If A_4 comes in later then what can Zelda do to extend this to $(3,4)$ secret sharing?

2. (20 points) For this problem you can assume there are programs to do the following quickly:

   - FIND-PRIME-AND-GEN: given n, find a prime p of length n and a generator g for $\mathbb{Z}_p$.
   - POWER: given a, b, p find $a^b \pmod{p}$ (p need not be a prime).

   And of course you CANNOT say something like *Do the Pallier Public Key Protocol* (that was an example – you won't need to do that.)

   And NOW finally the problem:

   (a) (10 points) Describe the ElGamal Public Key Crypto System.

   (b) (10 points) State carefully what the hardness assumption is for ElGamal.

3. (15 points) Zelda wants to do (t, L) Verifiable Secret Sharing (VSS) with secret s. Here is what she will do:

   - Zelda finds a *safe prime* p where $p \geq s$. All arithmetic is mod p. She then forms a function f in the usual way and, for all $1 \leq i \leq L$, gives A_i the number $f(i)$.
   - Zelda find a generator g.
   - Zelda makes public the information: g, $g^{f(1)}$,..., $g^{f(L)}$.
   - When t people get together everyone says their $f(i)$ and this can be verified by seeing if $g^{f(i)}$ checks out.

   Now the questions:

   (a) (5 points) Why does Zelda use a *safe* prime?

   (b) (10 points) Is there any reasonable hardness assumption HA such that HA implies NO information about the secret leaks? IF YES then state the assumption. If NO then show how some information could leak. (NOTE- the length of the secret is known and is not considered information that leaks.)

4. (20 points) Describe an encryption system that uses the alphabet $\{0, \dots, 6\}$ and has perfect security. You DO NOT need to prove it has perfect security.

5. (15 points) In this problem we develop a technique to help factor numbers

   (a) (2 points) Find a factor of the following number that is not 1 or the number itself.

   $$1023^4 - 512^4.$$

   (HINT: DO NOT calculate this number in your effort to factor it.)

   (b) We want to factor N. We find natural numbers $x, y \geq 1$ such that

   $$x^4 - y^4 = N$$

   i. (8 points) Show how this might help us factor N.

   ii. (5 points) If such an x, y exist, do they always help to find a factor? Either give an x, y such that $x^4 - y^4 = N$ but this does NOT help to factor N, or show that given x, y so $x^4 - y^4 = N$ you can always find a factor.

6. (10 points)

(a) (2 points) Define what it means for a function $F : \{0,1\}^n \rightarrow \{0,1,2\}^{n^2}$ to be a psuedorandom generator. (This is NOT a typo-the domain is $\{0,1\}^n$ and the range is $\{0,1,2\}^{n^2}$.)

(b) (8 points) Assume n is even. Prove that the following function $F : \{0,1\}^n \rightarrow \{0,1,2\}^{n^2}$ is NOT a psuedorandom generator.

If $x \in \{0,1\}^n$ has MORE 0's than 1's then $F(x) = 0^{n^2}$.

If $x \in \{0,1\}^n$ has MORE 1's than 0's then $F(x) = 1^{n^2}$.

If $x \in \{0,1\}^n$ has exactly as many 0's as 1's then $F(x) = 2^{n^2}$.

(You need to show Eve's strategy but you do not need to show the probability that she wins.)

THERE IS A PROBLEM SEVEN ON THE NEXT PAGE

7. (5 points) How does Bitcoin prevent replay attacks?

Scratch Paper