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?

SOLUTION TO PROBLEM ONE

$$f(x) = r_2x^2 + r_1x + s = x^2 + 3x + 6 \pmod 7$$

a)

A_1 gets $f(1) = 10 = 3$.

A_2 gets $f(2) = 2^2 + 3 \times 2 + 6 = 4 + 6 + 6 \equiv 4 - 2 \equiv 2$

A_3 gets $f(3) = 3^2 + 3 \times 3 + 6 = 9 + 9 + 6 \equiv 2 + 2 - 1 \equiv 3$.

b) A_4 gets

$f(4) = 4^2 + 3 \times 4 + 6 \equiv 16 + 12 + 6 \equiv 2 - 2 + 6 \equiv 6$.

END OF SOLUTION TO PROBLEM ONE

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.

SOLUTION TO PROBLEM TWO

a) ElGamal:

(a) The security parameter is n.

(b) Alice picks prime p of length n and generator g for $\mathbb{Z}_p$. Alice sends (p, g). All arithmetic is mod p.

(c) Alice picks secret $a \in \{1, \ldots, p-1\}$. She computes and sends g^a.

(d) Bob picks secret $b \in \{1, \ldots, p-1\}$. He computes and sends g^b.

(e) Alice computes $s = (g^b)^a$. Bob computes $s = (g^a)^b$. Now they both have the same number s. They both compute s^{-1}.

(f) NOW Bob wants to send message m to Alice. He sends $c = ms$ to Alice.

(g) Alice can decode by computing $s^{-1}m = s^{-1}ms = m$

END OF SOLUTION TO PROBLEM TWO

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, $g^{f(1)}, \ldots, g^{f(L)}$.
   - 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.)

SOLUTION TO PROBLEM THREE

All arithmetic is mod p.

a) Zelda uses a safe prime so that its easy to find a generator

b) NO there is NO reasonable hardness assumption to prevent leaking. If there exists $i < j$ such that $f(i) = f(j)$ then everyone KNOWS this since $g^{f(1)}, \ldots, g^{f(L)}$ are all public. Hence a group of $t-1$ that includes A_i but not A_j would know $t-1$ points PLUS $f(j)$, so they can find the secret.

NOTE ADDED AFTER GRADING IT: Many students thought that Discrete Log being hard. But the above scenario shows that no – the scheme is just plain insecure.

Also- some students said things like: If the players are all powerful then no scheme is info-theoretic secure. That is correct. However, here we are asking about making the players NOT all powerful. Note that in class we DID give a VSS scheme with a hardness assumption, so it is possible. The confusion here was with the phrase 'no information about the secret leaks' - that means that GIVEN that the players satisfy a hardness condition, they can't learn any info, which was the case for the VSS scheme we did in class.

NOTE ADDED AFTER SOME REGRADE REQUESTS.

Some students wrote that information is leaked because $A_1, \ldots, A_{t-1}$ people can get together and brute force (this would take 2^n steps if the shares are of length n) see which share of for A_t they can verify.

I asked Is there an HA that prevents ALL attacks.

The above answer give AN Attack – but for that attack there is a reasonable HA – that all of the players operation in poly time.

END OF SOLUTION TO PROBLEM THREE

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

SOLUTION TO PROBLEM FOUR

We give two solutions.

SOLUTION ONE:

A variant of the 1-time pad. Alice and Bob agree on a RANDOM strings in $\{0,1,2,3,4,5,6\}^N$ for a LARGE N. Say the string is $b_0 b_1 \cdots b_L$.

$$ENC(m_0, m_1, \ldots, m_L) = (m_0 + b_0 \pmod 7, \ldots, m_L + b_L \pmod 7)$$

$$DEC(c_0, c_1, \ldots, c_L) = (c_0 - b_0 \pmod 7, \ldots, c_L - b_L \pmod 7)$$

SOLUTION TWO:

Code 0 as 000

Code 1 as 001

Code 2 as 010

Code 3 as 011

Code 4 as 100

Code 5 as 101

Code 6 as 110

NOW do the normal 1-time pad. Even though 111 cannot be coded, the ones left are still equally likely. That is, if Eve sees Alice send Bob 010 she knew ahead of time it didn't code to 111 and still knows that, but what it does code to she has no information about.

END OF SOLUTION TO PROBLEM FOUR

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.

SOLUTION TO PROBLEM FIVE

a)

$$1023^4 - 512^4 = (1023^2 - 512^2)(1023^2 + 512^2) = 511 \cdot 1535 \cdot (1023^2 - 512^2)$$

b)

i.

$$(x-y)(x+y)(x^2+y^2) = N$$

One of these might be a factor.

ii. There is no such x, y. The only way this would not help is if every factor is 1 or N.

Since $x - y < x + y$ you would need to have

$x - y = 1$.

Then $x + y \neq 1$ so $x + y = N$

But then $x^2 + y^2 > N$. So such an x, y is ALWAYS helpful.

END OF SOLUTION TO PROBLEM FIVE

6. (10 points)

(a) (2 points) Define what it means for a function $F : \{0,1\}^n \to \{0,1,2\}^{n^2}$ 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 $F : \{0,1\}^n \to \{0,1,2\}^{n^2}$ 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

SOLUTION TO PROBLEM SIX

a) $F : \{0,1\}^n \to \{0,1,2\}^{n^2}$ is a psuedorandom generator if there exists a neg function $e(n)$ such that, for all PPT Eve, the prob Eve wins the following game is $\leq \frac{1}{2} + e(n)$

(a) Alice picks a random string $x_0 \in \{0,1,2\}^{n^2}$ and a random string $y \in \{0,1\}^n$. She then computes $x_1 = F(y)$.

(b) Alice gives Eve (z_0, z_1) which is $\{x_0, x_1\}$ in some order, picked with prob $\frac{1}{2}$.

(c) Eve has to say $i \in \{0,1\}$ as a way to pick z_0 or z_1. i If $z_i = x_1$ (the psuedorandom string) then Eve wins!

b) Here is Eve's strategy.

If there exists $i \in \{0,1\}$ such that $z_i \in \{0^{n^2}, 1^{n^2}, 2^{n^2}\}$ and $z_{1-i} \notin \{0^{n^2}, 1^{n^2}, 2^{n^2}\}$ then Eve guesses i. If not then Eve flips a coin to pick 0 or 1.

The prob that Eve LOSES is the prob that two things happen:

ONE- $x_0 \in \{0,1,2\}^{n^2}$. Prob $\frac{3}{3^{n^2}} = \frac{1}{3^{n^2-1}}$.

TWO- Eve picks the wrong one. Prob $\frac{1}{2}$.

So Prob Eve LOSES is $\frac{1}{2 \times 3^{n^2-1}}$.

So the prob that Eve wins is $1 - \frac{1}{2 \times 3^{n^2-1}}$.

NOTE ADDED AFTER WE GRADED IT: Some students seem to want to use Psuedo random FUNCTIONS rather than a Psuedo Random Generator.

END OF SOLUTION TO PROBLEM SIX

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

SOLUTION TO PROBLEM SEVEN

Each coin can only be spend once.

Each transactions destroy the input coin and create new ones.

NOTE ADDED AFTER WE GRADED IT:

Digital Signature Alone Do Not prevent replay attacks.

END OF SOLUTION TO PROBLEM SEVEN

Scratch Paper