CMSC 389 Second Midterm- Some ANSWERS and Grading Issues

1. This is a closed book exam, though ONE sheet of notes is allowed. **You may use a Calculators**. If you have a question during the exam, please raise your hand.
2. There are 5 problems which add up to 100 points. The exam is 2 hours.
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. If you need extra scratch paper **after** you have filled these areas up, please raise your hand.
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:	
TOTAL	

1. (20 points)

   (a) If Alice and Bob use Diffie-Helman with prime p what is the LENGTH of the secret key they will share?

   (b) If Alice and Bob use Diffie-Helman with prime p ROUGHLY how many steps will this take? (Assume that any operation mod p takes $\log p$ steps).

   (c) If Eve uses the Giant-Step/Baby-Step Discrete Log algorithm to try to find the secret key than ROUGHLY how many steps will this take? (Assume that any operation mod p takes $\log p$ steps).

SOLUTION TO PROBLEM ONE

a) $FLOOR(\log_2 p)$.

GRADING: $\log_2 p$ is fine, CEIL, +1, etc. FINE. "the length of p" or "the size of p" is also good, but if this question is on the final it will NOT be. Anything involving g is WRONG- 6 points off.

b) Alice and Bob do roughly $O(\log p)$ operations over mod p. Each one takes $O(\log p)$ steps, so its $O((\log p)^2)$.

GRADING- we accepted any poly in $\log p$.

c) Giant-Step/Baby-step takes $O(\sqrt{p})$ operations over mod p, so this is $O(\sqrt{p}\log p)$.

GRADING- We didn't care if you left off the $\log p$.

2. (20 points) Alice and Bob are going to do Secret Sharing with Cards. $n = 15$. Alice has $\{1, 2, 3, 4, 5\}$, Bob has $\{6, 7, 8, 9, 10, 11, 12\}$ and Eve has $\{13, 14, 15\}$. You can assume that if (later) Alice has a cards, Bob has b cards, Eve has ZERO cards then Alice and Bob can exchange $FLOOR(\log_2 \left(\frac{(a+b)!}{a!b!}\right))$. Alice and Bob use the convention that if they agree on a pair the bits shared is 0 if Alice has the low card,1 if Bob does.

   (a) Give a detailed scenario where every time either Alice or Bob shouts a pair of cards, and Eve has not used up all her cards, she has one of them. How many shared secret bits do Alice and Bob end up sharing? What is the sequence of shared bits? You MUST use the format on the next page.

   (b) Give a detailed scenario where every time either Alice or Bob shouts a pair of cards the other of Alice or Bob has one of them. How many shared secret bits do Alice and Bob end up sharing? What is the sequence of shared bits? You MUST use the format on the next page.

SOLUTION TO PROBLEM TWO

a)

(a) Alice: $\{1, 2, 3, 4, 5\}$, Bob: $\{6, 7, 8, 9, 10, 11, 12\}$, Eve: $\{13, 14, 15\}$.

(b) (Bob has more cards than Alice, so Bob declares the pair.) Bob says $6, 13$. Alice says NO.

Alice: $\{1, 2, 3, 4, 5\}$, Bob: $\{7, 8, 9, 10, 11, 12\}$, Eve: $\{14, 15\}$.

(c) (Bob has more cards so he declares the pair.) Bob says $7, 14$. Alice says NO.

Alice: $\{1, 2, 3, 4, 5\}$, Bob: $\{8, 9, 10, 11, 12\}$, Eve: $\{15\}$.

(d) (Alice and Bob are tied so Alice declares the pair.) Alice says $1, 15$. Bob says NO.

Alice: $\{2, 3, 4, 5\}$, Bob: $\{8, 9, 10, 11, 12\}$, Eve: $\{\}$.

(e) (NOW Eve has 0. Alice has 4 cards, Bob has 5 cards. The union of Alice and Bob's cards is $\{2, 3, 4, 5, 8, 9, 10, 11, 12\}$. Note that Eve has NO IDEA who has which cards.) There are $\binom{9}{4} = \frac{9!}{4!5!} = \frac{9\times8\times7\times6}{4!} = \frac{9\times8\times7}{4} = 9 \times 2 \times 7 = 126$ possible hands. The power of

2 that is just below 126 is $64 = 2^6$. We now do the $e = 0$ case as discussed in class.

A HAND is an ordered pair with has 4 elements of $\{2, 3, 4, 5, 8, 9, 10, 11, 12\}$ in the first set, and the OTHER 5 in the second set. For example $(\{2, 4, 5, 11\}, \{3, 8, 9, 10, 11, 12\}$.

Alice picks 63 HANDS at random NOT including the one that Alice-Bob currently have She then lists them out in a random order. We think of them as H_{000000}, H_{000001}, ..., H_{111111}. In OUR scenario Alice makes her hand H_{011001}. The shared sequence is 011001.

GRADING: Many people did not have Alice and Bob go in the correct order, i.e. they had Alice shout pairs even when she had fewer cards than Bob. We did not take off for this except in extreme cases.

Quite commonly people GOT everything up to the $e = 0$ case, but then did NOT do the $e = 0$ case properly (or explained it badly). That cost them FIVE points. However, there will be a HW problem that is worth 5 points ON THE MIDTERM for those who missed it.

b)

Alice and Bob use the convention that if there is a pair and Alice has the low card then the bit is 0, if Bob has the low card then the bit is 1.

(a) Alice: $\{1, 2, 3, 4, 5\}$, Bob: $\{6, 7, 8, 9, 10, 11, 12\}$, Eve: $\{13, 14, 15\}$.

(b) (Bob has more cards, so he declares the pair.) Bob says $1, 12$. Alice says YES. They share the bit 0.

Alice: $\{2, 3, 4, 5\}$, Bob: $\{6, 7, 8, 9, 10, 11\}$, Eve: $\{13, 14, 15\}$.

(c) (Bob has more cards, so he declares the pair.) Bob says $5, 11$. Alice says YES. They share the bit 0.

Alice: $\{2, 3, 4\}$, Bob: $\{6, 7, 8, 9, 10\}$, Eve: $\{13, 14, 15\}$.

(d) (Bob has more cards, so he declares the pair.) Bob says $4, 10$. Alice says YES. They share the bit 0.

Alice: $\{2, 3\}$, Bob: $\{6, 7, 8, 9\}$, Eve: $\{13, 14, 15\}$.

(e) (Bob has more cards, so he declares the pair.) Bob says $3, 9$. Alice says YES. They share the bit 0.

Alice: $\{2\}$, Bob: $\{6, 7, 8\}$, Eve: $\{13, 14, 15\}$.

(f) (Bob has more cards, so he declares the pair.) Bob says $2, 8$. Alice says YES. They share the bit 0.

Alice: $\{\}$, Bob: $\{6, 7\}$, Eve: $\{13, 14, 15\}$.

Alice is out of cards, so the game is over. Alice and Bob share the bit sequence 00000.

The following is an example of the format you MUST use: (We use a DIFFERENT scenario than the one in the problem.) I also give COMMENTS on the format the are NOT part of the format.

FORMAT:

COMMENT: Must state what cards everyone has and what cards are in play.

Alice: $\{1, 2, 3\}$, Bob: $\{4, 5, 8\}$, Eve: $\{6, 7, 9, 10\}$.

Cards in play are $\{1, \ldots, 10\}$.

(a) Alice says 1,8
COMMENT: This is shorthand for 'Alice says 'I have one of 1,8'

(b) Bob says YES Alice and Bob share bit 0.
COMMENT: must state what the hands are now and what cards are in play.
Hands are now:
Alice: $\{2, 3\}$, Bob: $\{4, 5\}$, Eve: $\{6, 7, 9, 10\}$.
Cards in play: $\{2, 3, 4, 5, 6, 7, 9, 10\}$.

(c) Alice says 2,6

(d) Bob says NO. Alice and Bob do not get to share a bit.

(e) Alice says 2.

(f) Alice: $\{3\}$, Bob: $\{4, 5\}$, Eve: $\{7, 9, 10\}$.
Cards in play: $\{3, 4, 5, 7, 9, 10\}$.

3. (20 points) In this problem show all work. Use the method shown in class.

   (a) Find the inverse of 30 mod 101.

   (b) Find the inverse of 31 mod 101.

   SOLUTION TO PROBLEM 3.

   Omitted.

   GRADING: Each part was 10 points. For each part— If you GOT that you need to do the GCD that was 5 points. If you GOT that you had to do the 'write 1 as a linear combo of 30 and 101' that was 3 points. If you actually did the arithmetic correct, that was 2 points.

   (Most people got 16,18, or 20 on this one).

   NOTE- If a problem asks for the Inverse SAY CLEARLY WHERE IT IS. If I had a hard time finding it I didn't take off this time but I WILL on the final. Say clearly

   THE INVERSE OF 30 MOD 101 IS:

4. (20 points) Alice and Bob are going to use the Diffie-Helman key exchange to obtain a shared secret key. They use $p = 11$ and $g = 2$. (On the next page you will see ALL powers of 2 mod 11— you can use that.)

   (a) If Alice picks $a = 4$ and Bob picks $b = 8$ then what is their shared secret key?

   (b) If Alice picks $a = 8$ and Bob picks $b = 9$ then what is their shared secret key?

   SOLUTION TO PROBLEM 4

   Omitted.

   GRADING: Each part was 10 points. For part a (part b is similar) If you GOT that it was $2^{4\times 8}$ that was 5 points. If you then got the arithmetic right, that was 5 more points.

   Note that the arithmetic is EASY because you have the table and you can use tricks like (for the second part)

   $2^{8\times 9} \equiv 2^{72} = (2^{10})^7 \times 2^2 \equiv 1^7 \times 2^2 \equiv 4.$

All $\equiv$ on this page are mod 11.

$2^1 \equiv 2$.

$2^2 \equiv 4$.

$2^3 \equiv 8$.

$2^4 \equiv 5$.

$2^5 \equiv 10$.

$2^6 \equiv 9$.

$2^7 \equiv 7$.

$2^8 \equiv 3$.

$2^9 \equiv 6$.

$2^{10} \equiv 1$.

5. (20 points) For each of the following say if it's TRUE or FALSE and WHY

   (a) Alice and Bob want to use Diffie-Helman so that Eve cannot crack it. Does it suffice to use a prime p such that it's hard for Eve to do $O(p)$ operations mod p.

   (b) Alice and Bob have set up Diffie-Helman so they can exchange 10 bits. They plan to use this to share two 5-bit numbers so that they can then use a linear cipher. Does this work? If not then is their a modification of this scheme that will work?

   (c) If Alice and Bob use a 1-time pad with true random bits then Eve cannot crack it.

   (d) The NSA is WAY AHEAD of academic researchers in terms of crypto research.

a) FALSE. Alice and Bob need to make sure that p is such that $\sqrt{p}$ is large since Eve could use the Giant/Baby algorithm for Discrete Log.

GRADING: Anyone who wrote TRUE got it wrong. Anyone who wrote FALSE but did not mention the Giant/Baby step algorithm requiring $\sqrt{p}$ steps (i.e., anyone who did not give a valid reason why) got it wrong.

b) FALSE. Alice and Bob do not control what the two numbers would be, so you could end up transmitting a value of a that is NOT rel prime to 26.

GRADING: Some people interpreted it differently and essentially said that Alice and Bob shouldn't use linear cipher since its easily cracked.

There will be a HW problem similar to this problem that ANYONE who got this one wrong can submit. However, this time DO NOT misread it.

c) TRUE. Eve cannot tell ANYTHING about the text. All texts are equally likely to be the real one.

SEE NEXT PAGE FOR d).

d) FALSE. Their are many excellent academics working on cryptography (Jon Katz and Larry Washington are two of them) and they have the freedom to TALK to each other and to people at other schools which helps them. The NSA lacks that freedom which impedes their ideas. (NOTE- this is my opinion but it SEEMS to be true.)

GRADING- Other reasonable reasons are fine, but you MUST give a reason as the problem said “True or False and WHY”. Even a TRUE is fine if you gave a good reason for it.

Scratch Paper