250 FINAL

Do not open this exam until you are told.

READ THE INSTRUCTIONS

1. This is a closed book exam, though ONE sheet of notes is allowed. **No calculators, or other aids are allowed**. 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 2 hours. (You shouldn't need that much.)
3. For each question show all of your work and **write legibly**. **Clearly indicate** your answers. No credit 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. Scratch paper must be turned in with your exam, with your name and ID number written on it, but scratch paper **will not** be graded.
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 :
SECTION NUMBER :

SCORES ON PROBLEMS

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

1. (10 points) Give an example of a Boolean Formula on the FIVE variables x_1, x_2, x_3, x_4, x_5 (your formula MUST include all five) such that its truth table has exactly TWO rows that say TRUE. (That is, there are exactly TWO satisfying assignments.)

2. (15 points) Let T be defined by:

   $T(0) = 1$

   $T(1) = 3$

   $(\forall n \geq 2)[T(n) \leq 4T(n-1) + 5T(n-2)]$.

   Using constructive induction find A and B, both natural numbers, such that

   $$(\forall n \geq 1)[T(n) \leq AB^n].$$

3. (15 points) Prove that there is no $(x_1, \ldots, x_{14})$ (all natural numbers) such that :

$$x_1^4 + x_2^4 + \cdots x_{14}^4 = 1599.$$

(HINT: Use mod 16)

4. (15 points) For each of the following say if it's TRUE or FALSE. If it's TRUE then give a SHORT PROOF. If it's FALSE then give a COUNTEREXAMPLE.

   You must clearly state TRUE or FALSE before giving your proof or counterexample.

   (a) There is a 1-1 and onto function between the natural numbers and the integers.

   (b) If $x < y$ are rationals then there exists an irrational z such that $x < z < y$.

   (c) If A is a set whose powerset has size 5 then A is infinite.

5. (15 points) Alice and Bob are going to use the Diffie-Helman key exchange to obtain a shared secret key. They use $p = 1201$. Fill in the blanks:

   (a) Alice and Bob want to test if g is a generator. FOR HOW MANY values of x do they need to test "$g^x \equiv 1 \pmod{1201}$?" (SHOW YOUR WORK.)

   (b) Alice and Bob agree to use the generator $g = 2$. Notice that if Alice picks $a = 1$ then Eve will immediately RECOGNIZE it when she sees $2^1 = 2$. Notice that if Alice picks $a = 2$ then Eve will immediately RECOGNIZE it when she sees $2^2 = 4$. (Eve thinks *4-WOW! I know that* $2^2 = 4$ *so* $2^2 \equiv 4 \pmod{1201}$.) We therefore want to AVOID using values for a that are EASILY recognizable from g^a. Find XXX such that the following holds: If Alice uses a value $a \leq XXX$, then Eve can EASILY determine the value of a, but if Alice uses a value of $a \geq XXX + 1$ then Eve will have a harder time. Give a value for XXX and explain why Eve would have a harder time breaking g^a in that case.

6. (15 points) Let $A = \{1, 2, \ldots, 101\}$ and $B = \{1, 2, \ldots, 100\}$. For the problems below you should use exponential or factorial notation. (E.g, if the answer is 20! then DO NOT multiply it out, just leave it as 20!.) SHOW YOUR WORK.

   (a) How many relations are there with domain A and co-domain B?

   (b) How many functions are there with domain A and co-domain B?

   (c) How many onto functions are there with domain A and co-domain B?

7. (15 points) For each of the following either give an a, b that works, and prove they work, OR show that there is NO SUCH a, b that works, and prove that fact.

   (a) (a, b) such that for all 4-colorings of the $a \times b$ grid there is a monochromatic rectangle.

   (b) (a, b) such that for all 4-colorings of the $a \times b$ grid there are 2015 monochromatic rectangles OF THE SAME COLOR.

Scratch Paper