HW 4 CMSC 389. DUE Jan 8
THE HW IS TWO PAGES LONG SO DON"T FORGET PAGE 2

1. READ my NOTES on line. What is your name? Write it clearly.

2. (15 points) Alice and Bob are using a matrix code with matrix

$$\mathbf{A} = \begin{pmatrix} 1 & 3 \\ 4 & 7 \end{pmatrix}$$

   Alice wants to send the message *cool*. What does she send? Your answer should be a sequence of four alphabet symbols.

3. (15 points) Alice and Bob are going to use a 1-time pad. They use the key 0110000110101

   (a) Alice wants to send 0000. What does she send?

   (b) Bob wants to reply 111111. What does he send?

   (c) What is the length of the longest message Alice can then send?

4. (15 points) List all of the primes that are between 100 and 150. Note which ones are SAFE primes. (RECALL- a prime p is *safe* if $p-1 = 2q$ where q is a prime.)

5. (15 points) Let $p = 47$. Note that p is a safe prime. Find the smallest generator of Z_p. SHOW ALL WORK!!!! (If you just write down 'The smallest generator is 11' without any work then you will get ZERO points!!!!!!!!!!!!) You may NOT use a calculator. (HINT1: Since p is safe you don't need to do that many calculations of g^a. HINT2: When computing g^a use the repeated squaring technique.)

6. (40 points) Let g be the generator found in the last problem. Assume that Alice and Bob are going to do Diffie Helman with $p = 47$ and this value of g.

   (a) Assume that Alice's secret random number is 10. What does Alice send Bob? (You may NOT use a calculator and you must show all work. HINT: use repeated squaring.)

   (b) Assume that Bob's secret random number is 8. What does Bob send Alice? (You may NOT use a calculator and you must show all work. HINT: use repeated squaring.)

   (c) What is the shared secret key? Express both as a number in $\{0, \ldots, 46\}$ and as a sequence of bits in binary.