CMSC 389 PROJECT- DUE FRIDAY JAN 20

NOTE- This should be written so that someone who does not know this course can understand it. I want it to be well enough written that I could give it to next winters students as a helpful handout.

THERE ARE THREE PAGES

1. (a) Plutonians use an alphabet with 3^9 symbols. How many affine ciphers are there? Explain your reasoning briefly.

   (b) Daleks use an alphabet with $2^9 \times 3^{12}$ symbols. How many affine ciphers are there? Explain your reasoning briefly.

2. Alice and Bob want to use a variant of Vigenere where they code a sequence of 3×3 matrices rather than a sequence of shift ciphers. (Some matrices don't work- but assume Alice and Bob do this with a sequence of matrices that have inverses)

   (a) Explain carefully exactly how Alice and Bob take a sequence of 3×3 matrices and encode a text. Give an EXAMPLE.

   (b) Give a short description (no pseudocode needed) of how Eve can crack the code.

3. Let $p = 2903$. This entire problem is in mod 2903.

   (a) Test if $2, 3, 4 \ldots$ is a generator until you find one. Let g be the first one that you find.

   (b) Fill in the XXX in the following question and explain your answer.
   If Alice uses a and Bob uses b and $(a, b) \in XXX$ then Eve can find the shared secret key EASILY.

THERE IS ANOTHER PAGE

4. (For this problem you will need to write a computer program and run it.) Take your name. Let F be the number of letters in your first name and L be the number of letters in your last name. Vorlons use a $L + 2F$-letter alphabet.

   (a) Find all (a, b, c) such that Vorlons can use the quadratic cipher with $f(x) = ax^2 + bx + c$. LIST THEM. No explanation required.

   (b) Find all (a, b, c) such that Vorlons can use the quadratic cipher with $f(x) = ax^2 + bx + c$. AND both the code and decode tables are the same. LIST THEM. No explanation required.

5. For each of the following ciphers

   - Describe the cipher and give an instructive example that is YOURS, not from my notes, not from Wikipedia, etc.
   - Discuss PROS and CONS for Alice and Bob's ease of use
   - Discuss ways Eve might crack it. (What can you assume Eve knows? Your discussion should include that as well, like "If Eve knows ... then she can do ...")

   (a) General 2-char cipher.

   (b) General 20-char cipher

   (c) Keyword shift cipher

   (d) Keyword mixed cipher

6. Alice and Bob do RSA.

   (a) Alice picks $p = 13$ and $q = 17$. List all values of e they could use.

   (b) What is the smallest e they could use?

   (c) Alice is going to use the smallest e. What is the FIRST THING tha Alice Broadcasts? (NOTE- Bob and Eve can both hear it.)

   (d) What is the largest number Bob can send?

   (e) If Bob want to send 5, what does he send? (NOTE- Alice and Eve can both hear it.)

THERE IS ANOTHER PAGE

7. Zelda wants to share a secret with 10 friends, $A_1, \ldots, A_{10}$ such that if any TWO get together they can recover the secret, but only one alone cannot. She uses the poly method and mod 13. If A_1 gets 5 and A_2 gets 7 then what is the secret? (We do not need to know what everyone else gets.)