CMSC 456 Project

The PROJECT is due LAST day of class, MONDAY DEC 9 BEFORE CLASS. Since (1) this is being given to you WAY ahead of time, and (2) this is a courtesy, there is NO dead-cat policy. That means its DUE DUE on Monday Dec 9, no extensions WHATSOEVER!!!!!!!!!!!!!

I will not look at it unless after the FINAL you have a grade of D or F. If you have a D and IF THE PROJECT IS GOOD then you get a C-. If you have an F and IF THE PROJECT IS GOOD then you get a D. I am NOT going to define GOOD for you!!!!!! DO NOT even try to game the system.

You should consider this project insurance against getting a D or F. ALSO, for ALL students, you should do this project as it is a good review for the final. Solutions will NOT be posted.

In this project it is important to be CLEAR. The problems where I ask you to describe a cipher will be read by a non-crypto person (no, I don't mean Dr. Gasarch :-)). Clarity is VERY IMPORTANT for this project!!!!!!

THIS PROJECT IS THREE PAGES

1. (5 points) Martians use a 30 letter alphabet. The alphabet is $\{0, \ldots, 29\}$ and their math is mod 30. Either give a 3×3 matrix that they can use with the matrix cipher where all of the entries are even OR show that no such exists. (This is the ONLY paroblem with a 30-letter alphabet.)

2. (5 points) Describe the VIG cipher and give an example of its use. (26 letter alphabe, English)

3. (5 points) Describe how to crack the VIG cipher and give an example of this. (26 letter alphabe, English)

4. (5 points) Describe the one-time pad and give an example of its use.

GOTO NEXT PAGE

5. (15 points) Bill wants to assign a problem where the students work out the quadratic sieve algorithm on the number 231158591 (which he knows is the product of two primes). Help him! Design a problem that students can really do and do it. The students (and you) are allowed to have a calculator and to use Wolfram Alpha (and should). Note that YOU will have to find B and M to work with.

   Hand in the problem AND the solution. What you hand it should be good enough that Bill can put it on a HW when he teaches this class next fall.

6. (15 points) First reread Hw03, Problem 5 and the solution. In this problem we ended up NOT cracking the code :-(. Make up a version of this problem, where the word you are looking for is BILL instead of ERIK, and the final equations DO have a solution (so you'll need to replace ABCD by something else that makes it all work out).

   Hand in the problem AND the solution. What you hand it should be good enough that BILL can put it on a HW when he teaches this class next fall.

GOTO Next Page

7. (10 points) Describe plain RSA and give an example of its use. (NOTE- in this problem and the ones below when we say to DESCRIBE an encryption we just mean tell us what Alice does to set it up, what Bob does to encrypt, and what Alice does to decrypt.)

8. (10 points) Describe why plain RSA is insecure and how to fix it so that it is secure.

9. (10 points) Show that there is NO INFORMATION-THEORETIC (t, m) secret sharing scheme where the secret is of length n and SOME person gets a share of length $n - 1$.

10. (10 points) Show that there IS (using a Hardness Assumption) a (t, L) secret sharing scheme where every person gets a share of length $< n$. Give the hardness assumption, the size of the shares, and of course the protocol.

11. (10 points) Show that there IS (using a Hardness Assumption) a (t, m) secret sharing scheme where every group of t can VERIFY what everyone in the group says is their share. You do not need to give the Hardness Assumption. (Use the one I did in class even though it does not quite work. Don't just copy it, put it in your own words and UNDERSTAND it.)