CMSC 456 Project

NOTE- THE PROJECT IS FIVE PAGES LONG

The PROJECT is due LAST day of class, MONDAY DEC 10. 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 10, 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 might want to 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 TWO PAGES

1. Martians use a 100 letter alphabet. The alphabet is $\{0, \ldots, 99\}$ and their math is mod 100. For each of the following either give an example or prove there is no such example.

   (a) (5 points) A 2×2 matrix that they can use with the matrix cipher where all of the entries are the same.

   (b) (5 points) A 2×2 matrix that they cannot use with the matrix cipher where all of the entries are different and between 4 and 40.

2. (5 points) Describe the VIG cipher and give an example of its use.

3. (5 points) Describe how to crack the VIG cipher and give an example of this.

GOTO NEXT PAGE

4. (5 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 decode.)

5. (5 points) Describe why plain RSA is insecure and how to fix it so that it is secure.

6. (10 points) Describe Rabin Encryption. Give one PRO and one CON.

7. (10 points) Describe the Blum-Williams variant of Rabin Encryption. Give one PRO and one CON.

8. (10 points) Describe the Goldwasser-Micali Encryption. Give one PRO and one CON.

9. (10 points) Describe the Blum-Goldwasser Encryption. Give one PRO and one CON.

10. (10 points) Show that there is NO INFORMATION-THEORETIC (t, L) secret sharing scheme with a secret of length n can have ANY person get a share of length $n - 1$.

11. (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.

12. (10 points) Show that there IS (using a Hardness Assumption) a (t, L) 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.