CMSC 456 Project

The PROJECT is due LAST day of class, MONDAY DEC 14 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 14, 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 40 letter alphabet. The alphabet is $\{0, \ldots, 39\}$ and their math is mod 40. 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.

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

6. (10 points) Describe why plain RSA is insecure and how to fix it so that it is secure.

7. (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 $n - 1$.

8. (10 point) Describe the Pollard-Rho factoring algorithm and give an example of its use.