HW 7 CMSC 389. DUE Jan 13
HOMEWORK IS TWO PAGES

1. (0 points) READ my NOTES on RSA, NOT FOR THIS HW BUT TO PREPARE FOR THE NEXT LECTURE. NOTE- Because the midterm was during Class Time we are a bit behind so I want to go fast next lecture- HENCE you should read the RSA notes ahead of time. ALSO READ my notes in ciphers.pdf on AUTOCODE-GOOD.

2. (30 points) Alice and Bob are Martians. They have the following conversation. I will later ask you what all the possible value of XXX could be.

   Alice says to Bob: Too bad our alphabet has XXX letters. NOT every affine cipher with nonzero a works, but if our alphabet was of size XXX+2 then any affine cipher with nonzero a would work.

   Bob says to Alice: I'm glad that XXX≤ 20 since otherwise our alphabet would be hard to deal with.

   Alice says to Bob: I'm glad that XXX≥ 10 since otherwise our alphabet would not be able to spell much.

   From the above conversation XXX is uniquely determined! What is XXX?

3. (30 points)

   (a) (10 points) What is *Kerckhoff's Principle*? (You will find this in the notes so it is not hard.)

   (b) (20 points) Tell me something about Kerckoff's principle that is NOT in the notes for the course. Make it between a third of a page and two-thirds of a page. (You can use Wikipedia or any other online resource, but you should UNDERSTAND what you are writing and not just copy it.)

THERE IS ANOTHER PAGE!!!!!!!!!!!!!!!

4. (40 points) Alice and Bob are going to use the Autocode (from AUTOCODE-GOOD section). Write a program (using psuedocode) to help them. That is, write a program that will, given a Text T and a number s, produce the autocoded T.