HW 1 CMSC 389. DUE Jan 5
NOTE- THE HW IS TWO PAGES LONG

1. (0 points) READ the syllabus- Content and Policy. READ my NOTES on line. What is your name? Write it clearly. Staple your HW. What is the day and time of the first midterm? Are you free then? (if not then SEE ME IMMEDIATELY) What is the day and time of the second midterm? Are you free then? (if not then SEE ME IMMEDIATELY) When is the final? Are you free then? (if not then SEE ME IMMEDIATELY)

2. (0 points VERY IMPORTANT). I emailed the entire class a message. I want to make sure that I have everyones email correctly. SO- if you GOT the message, write it down. If NOT then EMAIL Me your email address AS SOON AS POSSIBLE. (Email will be the main way I communicate with the class so its important I have all of your email addresses.)

3. (25 points)

   (a) Vulcans use an alphabet of 40 letters. If they use an affine cipher of the form $f(x) = ax+b$ then what are the restrictions on a, b.

   (b) Ferengi use an alphabet of 50 letters. If they use an affine cipher of the form $f(x) = ax+b$ then what are the restrictions on a, b.

4. (25 points) In this problem we work in mod 12

   (a) Write down all of the numbers in $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ that are relatively prime to 12.

   (b) For each number in the first part write down its multiplicative inverse mod 12. (NOTE- nothing fancy needed, brute force is fine, though I will tell you a better way to do this later.)

5. (25 points)

   (a) Either find a prime $p \geq 11$ such that $f(x) = x^2 \pmod{p}$ is 1-1 OR show that no such p exists.

   (b) Either find a prime $p \geq 11$ and a number $a \in \{1, \ldots, p-1\}$ such that $f(x) = x^2 + ax \pmod{p}$ is 1-1 OR show that no such p exists.

6. (25 points) Alice and Bob want to use an affine cipher where x maps to $3x + 2$.

   (a) Write the table that they can use to CODE messages.

   (b) Write the table that they can use to DECODE messages.