HW 1 CMSC 389. DUE Jan 4

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) When is the final? Are you free then? (if not then SEE ME IMMEDIATELY) NOTE that the MIDTERM and FINAL are both 4:30-6:00 so NOT the standard class time so IMPORTANT to make sure you are free and to CONTACT ME if you are not.

2. (0 points VERY IMPORTANT). I emailed the entire class a message. I want to make sure that I have everyone's 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 it's important I have all of your email addresses.)

3. (20 points)

   (a) Vulcans use an alphabet of 39 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 51 letters. If they use an affine cipher of the form $f(x) = ax+b$ then what are the restrictions on a, b.

4. (20 points) In this problem we work in mod 17

   (a) Write down all of the numbers in $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ that are relatively prime to 17.

   (b) For each number in the first part write down its multiplicative inverse mod 17. (NOTE- nothing fancy needed, brute force is fine, though I will tell you a better way to do this later.)

5. (20 points) Let $\phi(a)$ be the number of numbers in $\{1, \ldots, a-1\}$ that are relatively prime to a.

   (a) Find a formula fo $\phi(2^n)$. HINT: Try both reasoning and many examples.

   (b) Find a formula fo $\phi(3^n)$. HINT: Try both reasoning and many examples.

6. (20 points) Alice and Bob use a shift cipher and notice the CODING table and the DECODING table are the same. What is the Shift? Prove your answer but DO NOT give us the tables.

7. (20 points) (I DID NOT COVER THIS IN CLASS. READ THE NOTES AND DO THIS PROBLEM.) Alice and Bob use the Keyword-Shift cipher with code word MATH and shift 7.

   (a) Write the CODE and DECODE tables.

   (b) Code the statement: MATH IS FUN.

   (c) Does the fact that the keyword is the first word of the phrase make cracking the code easier for Eve?

8. (For fun, not for points, and don't hand in) Find ALL a, b such that the function $f(x) = ax^2 + bx \pmod{26}$ is a bijection. Try to do this with Math, not with a program. The notes give you a head start.

9. (For Fun, not for points, and don't hand in). Look up permutation polynomials on the web and see if you can characterize all cubics that are bijections over $\{0, \ldots, 25\}$ mod 26.