HW 2 CMSC 389. DUE Jan 6
SOLUTIONS
NOTE- THE HW IS TWO PAGES LONG

1. (0 points) Write your name!

2. (25 points)

   (a) Alice wants to use a keyword cipher with keyword *Vince Xavier Zell*. Write the table of what a maps to, what b maps to, etc. Show your work.

   (b) Alice wants to send the message *Alan Turing*. What does Alice send?

3. (25 points) Find all of the solutions to $x^2 + 6x + 5 \equiv 0 \pmod{12}$ by just plugging in $x = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$. You will find that there are MORE THAN two. Since quadratics have at most 2 roots over the reals (and over the complex numbers) there must be something about mod 12 that is DIFFERENT than the reals. Speculate on what that is. (Your answer need not be correct, but it must be coherent.)

4. (25 points)

   (a) Look up on the web an easy formula for finding the inverse of a 2×2 matrix. NOTE- the formula should only work if the determinant is NOT zero.

   (b) We are doing codes with the standard 26 letter alphabet, so we are working mod 26. Write down two 2×2 matrices that CAN be used for a matrix code.

   (c) Write down the inverses of those matrices.

5. (25 points) (In this problem the alphabet is the usual $\{0, \ldots, 25\}$ so all arithmetic is mod 26.) You are Eve. You know that Alice and Bob are using a matrix cipher with a 2×2 cipher. You know that the message $(1, 3, 25, 4)$ mapped to $(2, 3, 5, 11)$. FIND the matrix.

   Assume the matrix is

   $$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

   All $\equiv$ are mod 26.

   Since $(1, 3)$ maps to $(2, 3)$ we have that

   EQ1: $a + 3b \equiv 2$

   EQ2: $c + 3d \equiv 3$

   Since $(25, 4)$ maps to $(5, 11)$ we have that

   $25a + 4b \equiv 5$

   $25c + 4d \equiv 11$

SHORT CUT: $25 \equiv -1 \pmod{26}$. SO we rewrite the last equation as

EQ3: $-a + 4b \equiv 5$

EQ4: $-c + 4d \equiv 11$.

ADD EQ1 and EQ3 to get

$7b \equiv 7$, so $b \equiv 1$.

$a + 3b \equiv 2$ so $a + 3 \equiv 2$ so $a \equiv -1 \equiv 25$.

ADD EQ2 and EQ4 to get

$7d \equiv 14$, so $d \equiv 2$.

$-c + 4d \equiv 11$, so $-c + 8 \equiv 11$, so $c \equiv -3 \equiv 23$.

HENCE we have

$$\mathbf{A} = \begin{pmatrix} 25 & 1 \\ 23 & 2 \end{pmatrix}$$