Math 373/578 Homework, Week 7, Due Day 2/29/2012

Instruction: In doing this set of problems, you can use any electronic devise to help your computation. But you need to present conclusions based on the analysis of your computation.

The English Alphabet: Unless otherwise stated, we will use the English alphabet with $A - Z$ represented by the mod 26 numbers 0 - 25, respectively, as shown below.

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10| 11| 12| 13| 14| 15| 16| 17| 18| 19| 20| 21| 22| 23| 24| 25 |

1. What is a cryptosystem? (Give the answer in your own language based on your understanding. It is OK to go to library to find information in a book, or to use google to find information in the web for you to answer this question. However, when you quote something that is not your origination, please give a reference of the source, such as a book, an article in a journal, and an url of a website.)

Purpose of this exercise: Train us to know how to find answers by using resources around us.

2. Solve the system of equations in $\mathbb{Z}_{26}$

\[
\begin{pmatrix}
2 & 3 \\
7 & 8
\end{pmatrix}
\begin{pmatrix}
x \\
y
\end{pmatrix}
=
\begin{pmatrix}
1 \\
-1
\end{pmatrix}
\]

by doing the following two steps: (No credit for solutions not doing these two steps).

(i) Let $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$. Find $A^{-1}$ in $\mathbb{Z}_{26}$.

(ii) Multiply both sides of the equations by $A^{-1}$ from the left to get the solutions of system of equations.

Purpose of this exercise: To become more familiar with matrix operations.

3. We have intercepted the following messages $QVNAYQHI$ and $FWMDIQ$. Intelligence agents have informed us that the cipher texts were encoded by the a cryptosystem using digraphs with a fixed but unknown enciphering matrix $A$. Moreover, the plain text of first six letters of $QVNAYQHI$ are $NOANSW$.

(i) Find the enciphering matrix $A$ and the deciphering matrix $A^{-1}$.

(ii) Decrypt the cipher text $QVNAYQHI$.

(iii) Decrypt the cipher text $FWMDIQ$.

Purpose of this exercise: To become more familiar with matrix operations, and how they are used in cryptosystem.