Name:
PIN:

Applied Matrix Algebra
Cryptology

Objective The objective of this project is to illustrate how Matrices can be used in cryptology using *Mathematica*.

Narrative If you have not already done so, read Section 3.7 of the text. Cryptology is the science of transferring information in such a way that only the intended recipient can understand the message. Of course cryptology is also the study of how to intercept and understand messages that are intended to be secret. Our book briefly discusses some of the ways that have been used to send secret messages, but dwells only on the complexities of trying to break secret codes using the most basic ciphers. The study of code breaking for more complex ciphers is beyond the scope of this course.

Some informal terminology that we will be using:

- *cipher* - the transformation used to hide a message.
- *encode* - the act of applying the cipher to a *plain text* message in order to convert it to an *encrypted* message.
- *decode* - the act of applying the inverse cipher to an encrypted message in order to convert it to a plain text message.

In class we talked about modular arithmetic and how matrix multiplication and modular arithmetic can be used to encode and decode a message and to disguise the frequency distribution of the characters in the message. Here is how we can use *Mathematica* to do some of the work.

First we must make some decisions about the cipher we will use. For the purposes of this exercise we will encode messages using four characters at a time. Thus we need to choose a modulus and a 4x4 matrix that is invertible in that modulus. Because of some theorems in Number Theory it is easier to find an invertible matrix if we use a prime number as our modulus. We also need to choose a modulus that is larger than the largest number we will use to represent the characters in our message. Because of some convenient functions in *Mathematica*, will use the ascii character set which are numbers between 0 and 255. So our modulus needs to be bigger than 255. We will use a modulus of 263.

The following code sets up the modulus and a 4x4 matrix that we will use for our encoding.

```
p=263;
M=Transpose[{{1,2,3,4},{8,1,6,5},{9,1,10,15},{5,1,5,1}}];
MatrixForm[M]
```

Now suppose that we wish to encode the words "math is cool". *Mathematica* has some nice utilities that allow us to convert characters to numbers (and numbers to characters). Observe the output to the following command:

```
ToCharacterCode["Math is cool"]
```

Notice that this gives us the ascii code for the twelve characters we wish to encode. Next form the plain text message and use modular matrix multiplication to encode the message.

```
nplain = Transpose[{{77, 97, 116, 104}, {32, 105, 115, 32},
   {99, 111, 111,108}}]
ncipher = Mod[M.nplain,p]
```

Notice that the plain message has repeated characters, but the encrypted message (matrix) does not. We would send the encrypted message to our agent with less fear that the enemy would be able to understand what it says.

Now when the agent receives the encrypted message, they will need to decode it by multiplying by the inverse of the matrix used to encrypt it. So the agent will need to know what modulus was used and how to calculate the matrix inverse. The following steps show the decryption process.

```
Mi = Inverse[M,Modulus->p];
ndecode = Mod[Mi.ncipher, p];
MatrixForm[ndecode]
FromCharacterCode[Transpose[ndecode]]
```

Note that the columns of **ndecode** has the characters of the words in our message.

Task

(1) Suppose that the modulus and matrix used to encode a message are 271 and

$$\begin{bmatrix} 12 & 9 & 15 & 103 \\ 23 & 56 & 67 & 31 \\ 34 & 33 & 81 & 53 \\ 35 & 11 & 17 & 73 \end{bmatrix}$$

decipher the following message: 72, 21, 247, 260, 226, 114, 135, 30, 159, 263, 27, 35, 179, 210, 116, 98, 268, 240, 170, 218, 244, 40, 151, 37, 163, 162, 241, 76.

(2) On pages 191 and 192, do problems 1, 2, and 4.