MTH 111
Activity for Unit 5
ENCRYPTION

This activity is a worksheet, print these pages, complete, and turn in to your Instructor. If you find there is not enough room, write up your work neatly and attach it.

In this activity we will be exploring different method for coding messages and why messages coded with matrices are so difficult to "break".

You will need a graphing calculator and a sentence or phrase **15 to 21 letters** long.

YOUR MESSAGE: _____

The first method for coding our method will use a function and its inverse.

Translate your message into numbers using the following assignments:

10 = A	11 = B	12 = C	13 = D	14 = E	15 = F	16 = G	17 = H
18 = I	19 = J	20 = K	21 = L	22 = M	23 = N	24 = O	25 = P
26 = Q	27 = R	28 = S	29 = T	30 = U	31 = V	32 = W	33 = X
34 = Y	35 = Z	36 = _	37 = .	38 = !	39 = ?		

YOUR TRANSLATED MESSAGE:

__ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

Now use the function $f(x) = 3x + 2$ to code your message by plugging each number of your translated message into the function:

YOUR CODED MESSAGE:

__ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

Find the inverse of the function $f^{-1}(x)$: *(Need to review? See section 1.6)*

INVERSE FUNCTION:

Now use $f^{-1}(x)$ to decode your message by plugging each number of your coded message into the inverse function:

YOUR DECODED MESSAGE (in numbers):

__ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

YOUR DECODED MESSAGE (in words):

__ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

When you translate your decoded message back into letters, you should see your original message. What letter (and its corresponding number) appeared most frequently in your message? What happened to that number when you coded your message? Would you be able to "break the code" without using the inverse function?

Now we want to look at coding messages using matrices and their inverses.

Take your translated message and arrange it into an nx3 row matrix, with as many rows as needed. Add some blanks (36) if you need to complete the last row:

__ __ __
__ __ __
__ __ __
__ __ __
__ __ __
__ __ __
__ __ __

Enter the following nonsingular 3x3 matrix as A in your calculator. Use your calculator to find A^{-1} and **save this as matrix B** in your calculator.

$$A = \begin{matrix} 1 & 2 & -1 \\ 2 & 6 & 1 \\ 3 & 6 & -4 \end{matrix} \qquad A^{-1} = B = \begin{matrix} \_\_ & \_\_ & \_\_ \\ \_\_ & \_\_ & \_\_ \\ \_\_ & \_\_ & \_\_ \end{matrix}$$

Then enter your n x 3 message matrix as **matrix C** in your calculator.

Now you are ready to code your message by multiplying your message matrix with matrix A. (**Make sure to write down your coded message, you will need it later**) You will be performing: C * A, **save this as matrix D** in your calculator

CODED MESSAGE MATRIX:

D= ___ ___ ___
___ ___ ___
___ ___ ___
___ ___ ___
___ ___ ___
___ ___ ___

How does your coded message look? Would you be able to "break the code"?

Now it is time to decode your message by multiplying your matrix with A^{-1}, which you have saved as matrix B. You will be performing: D * B

DECODED MESSAGE MATRIX:

___ ___ ___
___ ___ ___
___ ___ ___
___ ___ ___
___ ___ ___
___ ___ ___
___ ___ ___

If you translate your decoded message back into letters, you should see your original message.

___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Now we will do some exploration. Take your inverse matrix, A^{-1} = B, and change any one number in the matrix. Enter this as matrix E. E =

___ ___ ___
___ ___ ___
___ ___ ___

Use this modified inverse matrix to "decode" your message. (D * E)

MODIFIED DECODED MESSAGE MATRIX:

What changed and what stayed the same? Using your knowledge of how matrix multiplication works, explain why. Translate your (mutilated) message back to letters, is there enough correct in your message to figure it out?

Take matrix E and **change a second number in the same <u>column</u> as before**. (So there are two changed values in one column). Again, use this modified matrix to attempt to "decode" your message (D * E_2).

$$E_2 = \begin{matrix} & & \\ & & \\ & & \end{matrix}$$

MODIFIED DECODED MESSAGE, VER. 2:

What changed and what stayed the same? Why?

Go back to the original matrix E again but this time change a **second number in the same row**. (So now there are two changed values in the same row, the rest matches the original E matrix.)

$$E_3 = \begin{matrix} \_ & \_ & \_ \\ \_ & \_ & \_ \\ \_ & \_ & \_ \end{matrix}$$

MODIFIED DECODED MESSAGE, VER. 3:

What happens this time as you attempt to "decode" the message (D* E_3)? Why?

_ _ _
_ _ _
_ _ _
_ _ _
_ _ _
_ _ _
_ _ _

__ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

Other Questions to Consider:
A message that is encoded merely by assigning each letter in the alphabet a different symbol is relatively easy to break, particularly if the message is very long. The letters used most frequently in the English language, such as *e* and *t* and *s*, are assigned to the symbols that appear most frequently in the encoded message and the message is usually readable after a few attempts.

What letter (and its corresponding number) appeared most frequently in your message?
After your message was multiplied by the matrix, what happened to that particular number?

How would using smaller or larger matrices affect the difficulty of breaking your code?

Suppose your enemies have intercepted part of your "decoding" inverse matrix. How much of the correct inverse matrix do you think they would they need to break your code? Would it matter what part of the matrix they had?