MATH 256 **Name:**_____
Project/Fall 2016
Due: November 21, 2016

CRYPTOGRAPHY

Directions: Complete all portions of this project neatly, either handwritten or by using a word processor. As for technology, feel free to use any standard graphing calculator (e.g., TI-84) or CAS system (e.g., Maple, Sage, etc.). Submit a clearly written, easy-to-read worksheet with all parts labeled. Fix all false starts and/or errors so that they do not interfere with the continuity of the project. Use this sheet as a cover sheet and staple your work to this sheet.

This project delves into the interesting world of hidden messages via a secret code. A **cryptogram** is a message written according to a secret code. This project will explain how you can use matrix multiplication and inverse matrices to encode (hide) and decode (reveal) messages. This type of "covert operation" can be seen in military communication (sending messages), government undertakings (sending classified information), computer security (online banking information, passwords), etc. The list is virtually endless. Some of the most sensitive information in the world passes through matrices before it reaches its target audience.

We begin by assigning a number to each letter in the alphabet (with 0 assigned to a blank space). See the table below.

0	=		9	=	I	18	=	R
1	=	A	10	=	J	19	=	S
2	=	B	11	=	K	20	=	T
3	=	C	12	=	L	21	=	U
4	=	D	13	=	M	22	=	V
5	=	E	14	=	N	23	=	W
6	=	F	15	=	O	24	=	X
7	=	G	16	=	P	25	=	Y
8	=	H	17	=	Q	26	=	Z

Then the message is converted to numbers and partitioned into uncoded row matrices, each having n entries. For example, we can write the uncoded row matrices of order 1×3 for the message LINEAR ALGEBRA RULES. If we partition this message into groups of 3, we get the following uncoded row matrices:

[12	9	14]	[5	1	18]	[0	1	12]	[7	5	2]	[18	1	0]	[18	21	12]	[5	19	0]
L	I	N	E	A	R	_	A	L	G	E	B	R	A	_	R	U	L	E	S	_

Notice the use of a blank space to fill out the last uncoded row matrix.

Next, to encode this message, we choose an $n \times n$ invertible matrix A and multiply the uncoded row matrices (on the right) by A to obtain coded row matrices. In this specific example, $n = 3$. Let's use $A = \begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix}$. Our first coded row matrix is $\begin{bmatrix} 17 & -29 & -5 \end{bmatrix}$ because $\begin{bmatrix} 12 & 9 & 14 \end{bmatrix} \begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix} = \begin{bmatrix} 17 & -29 & -5 \end{bmatrix}$. If you do this for the rest of the message, you obtain the string

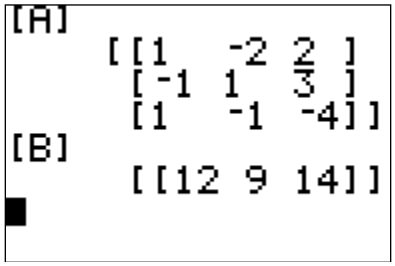
$$\begin{bmatrix} 17 & -29 & -5 \end{bmatrix}\begin{bmatrix} 22 & -27 & -59 \end{bmatrix}\begin{bmatrix} 11 & -11 & -45 \end{bmatrix}\begin{bmatrix} 4 & -11 & 21 \end{bmatrix}\begin{bmatrix} 17 & -35 & 39 \end{bmatrix}\begin{bmatrix} 9 & -27 & 51 \end{bmatrix}\begin{bmatrix} -14 & 9 & 67 \end{bmatrix}.$$

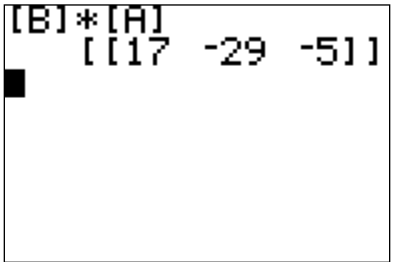
Finally, upon removal of the matrix notation we get the cryptogram

17 −29 −5 22 −27 −59 11 −11 −45 4 −11 21 17 −35 39 9 −27 51 −14 9 67

For those who do not know matrix A, decoding the cryptogram above is a bit of a headache! To do these computations on computer/calculator, you could type…

TI-83 example:





Maple example:

```
with(LinearAlgebra) :
A := Matrix([[1,-2, 2], [-1, 1, 3], [1,-1,-4]]);
```

$$\begin{bmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{bmatrix}$$

```
x := Vector[row]([12, 9, 14]);
```

$$\begin{bmatrix} 12 & 9 & 14 \end{bmatrix}$$

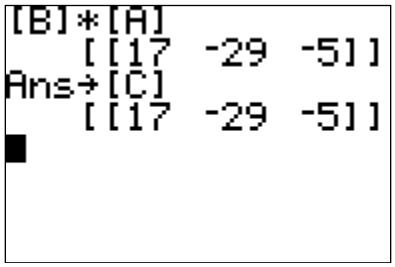
```
y := evalm(x&*A);
```

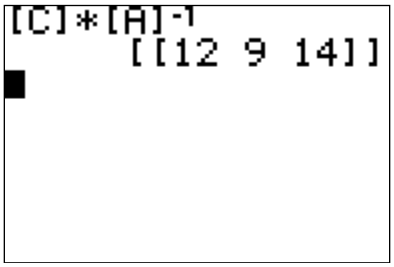
$$\begin{bmatrix} 17 & -29 & -5 \end{bmatrix}$$

At this point, you could continue doing the other calculations or write a program to complete all calculations in one quick step.

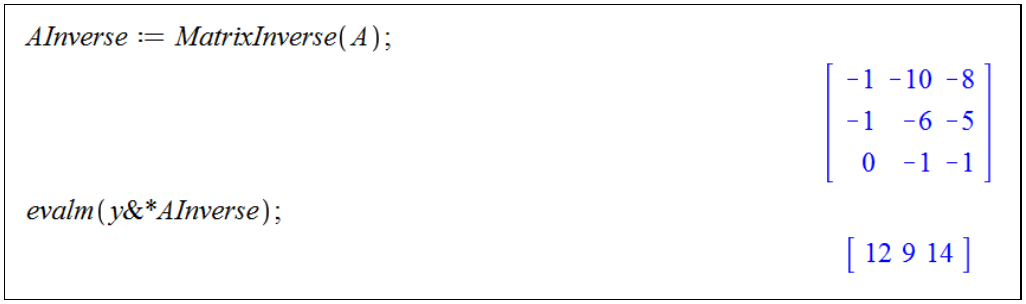
Once your message has arrived at its target destination, this person will want to read your message. The message can now be decoded by using A^{-1}. See the sample code below.

TI-83 example:





Maple example:



Notice that the above sequence 12 9 14 gives the first three letters of the original message. If the receiver continues to decode in this manner, he/she will eventually get the string of row vectors

[12 9 14][5 1 18][0 1 12][7 5 2][18 1 0][18 21 12][5 19 0]

or, more simply

12 9 14 5 1 18 0 1 12 7 5 2 18 1 0 18 21 12 5 19 0.

In other words, the receiver would conclude that LINEAR_ALGEBRA_RULES_.

Use these ideas to solve the problems below.

Problem 1: Consider the message COME HOME SOON. Encode this message by using 1×2 row matrices and the encoding matrix $A=\begin{bmatrix}1 & 2\\ 3 & 5\end{bmatrix}$.

Problem 2: Consider the matrix $A = \begin{bmatrix} 3 & -2 \\ -4 & 3 \end{bmatrix}$ and the cryptogram

–45	34	36	−24	−43	37	−23	22	−37	29	57	−38	−39	31

Find A^{-1} and reveal the message.

Problem 3: Consider the matrix $A = \begin{bmatrix} 4 & 2 & 1 \\ -3 & -3 & -1 \\ 3 & 2 & 1 \end{bmatrix}$ and the cryptogram

33	9	9	55	28	14	95	50	25	99	53	29	−22	−32	−9

Find A^{-1} and reveal the message.

Problem 4: The cryptogram below was encoded with a 2×2 matrix:

4	118	−5	145	−50	100	−2	4	−41	127	−12	132	4	28
9	153	8	146	−39	123	−8	16	−31	107	−18	216		

The last part of the message reads REST. What is the message?

Problem 5: **(5 points extra)** Make up your own secret message and encode it using some matrix A. Store your encoded message using row vectors as in the above discussion. Finally, write some code or a program to decode the message so that it is revealed. Write a program that will display the actual message as opposed to the string of vectors (that still need to be translated). For example, in the discussion example, you would want to output "LINEAR_ALGEBRA_RULES" instead of

[12	9	14]	[5	1	18]	[0	1	12]	[7	5	2]	[18	1	0]	[18	21	12]	[5	19	0]