Cyber DLA Read Me – This is a Lateral Stretch/Application DLA

Who: This DLA is designed for students who have completed the Matrix Algebra lessons MA103.

Emphasis: This DLA has an emphasis on Matrix Multiplication and the Inverse Matrix.

Stretch: This DLA asks students to explore the field of Cryptology without having been taught this material in class. It introduces students to the Simple Encryption Technique presented in section 3.4 of MRCW, as well as the Hill Cypher.

Timing: Individual – 17 Minutes; Team - 30 Minutes; Reflection - 6 Minutes

Grading: Focus is placed on matrix operations.

Technology: Students have full use of technology throughout this DLA. The intent of this technology use is to give students an opportunity to determine when and how to make appropriate use of technology as a tool for modeling.

General Overview:

- As a read ahead, students will see read section 3.4 of MRCW and should attempt the Do Problems presented there.
- As individuals, students will use a given original message and encryption to determine a transformation matrix using the Simple Encryption Technique from MRCW.
- As teams, students will compute the inverse of a matrix and discuss the implications of a matrix not being invertible in a cryptology application. They will then work to encrypt a matrix using the Hill Cypher.
- As individuals, students will reflect on why the Hill Cypher is a more powerful encryption technique and will begin to think about the challenge of reversing modular arithmetic.

When: This DLA is most appropriate in the first half of Block II of MA 103.

Component	Problem	Possible Points	Topic
Individual	1	5	Matrix Dimensions
	2	5	Develop Original Message Matrix
	3	10	Determine Transformation Matrix
Team	4	5	Inverse of Transformation Matrix
	5	5	Why Invertible is Necessary
	6	5	Matrix Multiplication
	7	10	Matrix Multiplication and Mod
Reflection	8	5	Why Hill Cypher More Secure
	Total	50	

READ AHEAD

7 October 2019

DLA 2A Cyber – MA103 50 Points

Congratulations! You have just been selected for an AIAD with Cyber Command. You were selected because of the exceptional work you have been doing in MA 103. The person running your AIAD at Cyber Command has reached out to you and she sounds excited about working with you. In her introductory email, she mentioned that while she graduated from USMA many years ago, she constantly leans on her mathematical modeling skills to solve real world problems every day.

Your new boss mentioned that she downloaded *Modeling in a Real and Complex World* from the MA 103 blackboard site and there was some excellent material in the text that you should revisit before you arrive at Cyber Command to ensure you hit the ground running. She specifically mentioned section 3.4: Cryptology.

Expectations for preparation: To be successful and make a good first impression with your boss and coworkers, make sure to review that section. What do you think you will be working on at Cyber Command? Will the types of problems you might see look like the Do Problems in section 3.4? What other topics that we have covered in MA 103 might be helpful to you while on this assignment?

Preparation techniques for DLAs include looking at lesson and block objectives, reviewing course material in this block, making connections to the course material covered thus far, doing additional problems that reinforce the connection made to the critical concepts in the block, and lastly make a sheet of notes as needed.

INDIVIDUAL

Cadet____ 7 October 2019

Section: _______________

DLA 2A Cyber – MA103 50 Points

GENERAL INSTRUCTIONS: Read all instructions carefully.

1. You have 55 minutes to complete the DLA. You will have 17 minutes for the first individual portion, 30 minutes for the team portion, and 6 minutes for the individual reflection portion.
2. Early departure from the individual reflection portion is authorized. Give the DLA to your instructor or place it on your instructor's desk when completed.
3. Authorized items: One sheet (normal 8"x11" paper, front and back) of hand-written notes, your laptop computer (only a blank worksheet of Microsoft Excel or blank Mathematica notebook is allowed) and a calculator (issued or graphing).
4. Items not authorized: any type of Microsoft Excel templates or worksheet already filled out, any type of Mathematica templates or notebooks already filled out, internet, any computer programs other than MS Excel or Mathematica, any type of phone, or other electronic device.
5. Including this cover sheet, there are 5 pages to the DLA.
6. Clearly indicate your answer by underlining or boxing your solution (e.g. $\underline{0 < x < 5}$, or $\boxed{0 < x < 5}$).
7. **Show your work**.
    a. Work done on your computer will not be graded. Therefore, you should describe your process when using technology. For example: if you use MS Excel to iterate, provide the first two terms of your iteration and the last two terms.
    b. Partial credit can only be awarded if you **show your work**. It is always best to show intermediate steps to illustrate your problem-solving process (i.e. $p_1 =$; $p_2 =$).
8. Use a blank continuation sheet if you need more space and clearly identify that the problem is continued both on the DLA and on the continuation sheet. Be sure to place your name on all continuation sheets.

Component	Problem	Possible Points	Points Earned
Individual	1	5	
	2	5	
	3	10	
Team	4	5	
	5	5	
	6	5	
	7	10	
Reflection	8	5	
	Total	50	

INDIVIDUAL

Cadet____ 7 October 2019

Section: _______________

DLA 2A Cyber – MA103 50 Points

Show your work

Welcome to Cyber Command! Here is your first assignment.

A specialist intercepted an encrypted message which read

$$53, 72, 88, 122, 72, 105, 84, 117, 29, 41, 121, 168, 73, 102, 64, 92, 60, 83, 95, 129.$$

After interrogating its sender, he reveals the original message read "Don't Forget Nothing" but was encoded with no punctuation by a 2 × 2 transformation matrix often used by insurgent forces with the equation $AO = E$. A coworker reminds you that A is the transformation matrix, O is the original message, and E is the encoded message. You notice that the message only contains 17 letters, but there are 20 numbers in the encrypted message. Therefore, the sender must have included spaces in their original message and followed the common practice of putting one or more extra spaces at the end of a message to finish filling out the matrix. Answer the following questions to aid Cyber Command in keeping our forces safe.

1. [5 Points] Since A is a 2×2 transformation matrix, what must be the dimensions of the matrix containing the original message, O?

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Number	1	2	3	4	5	6	7	8	9	10	11	12	13

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Space
Number	14	15	16	17	18	19	20	21	22	23	24	25	26	27

2. [5 Points] Assuming the alpha-numeric translation provided above, give the matrix O.

3. [10 Points] Using O and the provided values for E, determine the transformation matrix used to encrypt your enemy's messages, A.

TEAM

Cadet__________________________ Cadet__________________________

Cadet__________________________ Cadet__________________________

Section: _______________ 7 October 2019

DLA 2A Cyber – MA103 50 Points

Show your work

4. [5 Points] Given $A = \begin{bmatrix} 2 & 3 \\ 3 & 4 \end{bmatrix}$. What is A^{-1}? To receive full credit, show all necessary steps. Note that Mathematica code is not enough.

5. [5 Points] Why does A have to be invertible? (What would happen if it wasn't?)

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Number	1	2	3	4	5	6	7	8	9	10	11	12	13

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Space
Number	14	15	16	17	18	19	20	21	22	23	24	25	26	27

6. [5 Points] The following encrypted message has been intercepted recently on several occasions from the same enemy.

$$14, 19, 83, 114, 98, 137, 72, 105, 72, 99, 91, 123, 96, 133\ ,64, 87.$$

You can now decode its meaning! What does it say?

TEAM

Cadet__________________________ Cadet__________________________
Cadet__________________________ Cadet__________________________
Section: _______________ 7 October 2019

DLA 2A Cyber – MA103 50 Points

Show your work

Congratulations! You have completed your first assignment. Your boss is very happy and has decided you are ready to move on. She is not a fan of numeric codes. She thinks they are incredibly cumbersome because you must use commas and you get such unruly numbers to work with. She remembers reading about a way to relay messages entirely with alphabetic code in *Modeling in a Real and Complex World*. She wants you to work on encoding a message using this alphabetic alternative called the Hill Cypher.

You remember reading about it as you prepared for the AIAD and know that you will need to transform letters to numbers using the standard alpha-numeric coding from before, then multiply by a transformation matrix (also just like before), but then you will need to translate all of the encoded numbers back to letters using modular arithmetic – specifically mod26. Since your boss knows this is new to you, she provides you with the following table to get you started in figuring out the modular arithmetic with mod26.

Number	1	2	3	4	5	6	7	8	9	10
Equivalent Numbers	27	28	29	30	31	32	33	34	35	36
	53	54	55	56	57	58	59	60	61	62
	79	80	81	82	83	84	85	86	87	88
	105	106	107	108	109	110	111	112	113	114

Additionally, she provided you with a transformation matrix – $A = \begin{bmatrix} 2 & 5 \\ 1 & 2 \end{bmatrix}$, and a message with no spaces or punctuation to send back to your MA 103 course director – "GOARMYBEATNAVY".

7. [10 Points] Using the Hill Cypher method along with the transformation matrix provided, give the alphabetic encoded message for your MA 103 course director.

INDIVIDUAL REFLECTION

Cadet____ 7 October 2019

Section: _______________

DLA 2A Cyber – MA103 50 Points

Show your work

8. [5 Points] Besides not having large numbers or a need for commas, why is the Hill Cypher a more powerful encryption technique? (What would you need to do to decode the message you just encoded?)