Name: Solutions Date: _____

Baldivis Secondary College

Year 11 Mathematics: Applications

Investigation 1, 2015

Topic – Encoding and Decoding using Matrices

Take home component

Important Information:
Although the take-home component is not worth any marks, it is essential in preparation for the in-class component. Knowledge and skills gained will be extended in the in-class validation component. This in-class validation will be completed under test conditions on the day in which this take-home component is due. The take-home component may be used when completing the in-class component. Contact may be made to parent(s) if the take-home component is not available for submission (at the start of the lesson).

Date out:	*Week____* *Date_____*	**Date Due:**	*Week____* *Date_____*		
Take home component weighting:	*0% of the year*	**In-class component weighting:**	*10% of the Semester, 5% of the Year*		

AIM: *In this assessment, you will be investigating how matrices are used in encoding and decoding messages. You will be using your CAS ClassPad for this investigation.*

A security sensitive message (e.g. war time intelligence or email message) may be disguised by sending it in code. An alphabet code may be disguised by representing the letters of each word by numbers and then scrambling the numbers using an encoding matrix. The message is later interpreted by the receiver and by applying a decoding matrix we are able to return the numbers to their original value. The message can then be deciphered.

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	-
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	26	27

The numbers 1 to 26 are chosen to represent the letters A to Z.

To send the message: **"SEND IN THE SUBS"**

S	E	N	D	-	I	N	-	T	H	E	-	S	U	B	S
19	5	14	4	27	9	14	27	20	8	5	27	19	21	2	19

the numbers representing the letters in the message are grouped in fours and expressed in square matrix form.

$\begin{bmatrix} 19 & 5 \\ 14 & 4 \end{bmatrix}$ $\begin{bmatrix} 27 & 9 \\ 14 & 27 \end{bmatrix}$ $\begin{bmatrix} 20 & 8 \\ 5 & 27 \end{bmatrix}$ $\begin{bmatrix} 19 & 21 \\ 2 & 19 \end{bmatrix}$

1. Complete the last two matrices above.

The message is coded by using an encoding matrix such as $\begin{bmatrix} 4 & 1 \\ 3 & 1 \end{bmatrix}$

Each matrix is multiplied by this matrix: $\begin{bmatrix} 4 & 1 \\ 3 & 1 \end{bmatrix} \times \begin{bmatrix} 19 & 5 \\ 14 & 4 \end{bmatrix} = \begin{bmatrix} 90 & 24 \\ 71 & 19 \end{bmatrix}$

(4 x 19) + (1 x 14) = 90 (4 x 5) + (1 x 4) = 24

(3 x 19) + (1 x 14) = 71 (3 x 5) + (1 x 4) = 19

Encoding

2. Code the rest of the message.
Note: The encoding matrix must be the left matrix when multiplying, as shown on the previous page.

$\begin{bmatrix} 4 & 1 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 27 & 9 \\ 14 & 27 \end{bmatrix} = \begin{bmatrix} (4\times27)+(1\times14) & (4\times9)+(1\times27) \\ (3\times27)+(1\times14) & (3\times9)+(1\times27) \end{bmatrix} = \begin{bmatrix} 122 & 63 \\ 95 & 54 \end{bmatrix}$

$\begin{bmatrix} 4 & 1 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 20 & 8 \\ 5 & 27 \end{bmatrix} = \begin{bmatrix} (4\times20)+(1\times5) & (4\times8)+(1\times27) \\ (3\times20)+(1\times5) & (3\times8)+(1\times27) \end{bmatrix} = \begin{bmatrix} 85 & 59 \\ 65 & 51 \end{bmatrix}$

$\begin{bmatrix} 4 & 1 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 19 & 21 \\ 2 & 19 \end{bmatrix} = \begin{bmatrix} (4\times19)+(1\times2) & (4\times21)+(1\times19) \\ (3\times19)+(1\times2) & (3\times21)+(1\times19) \end{bmatrix} = \begin{bmatrix} 78 & 103 \\ 59 & 82 \end{bmatrix}$

3. Fill in the table to show what set of numbers the message now comprises of.

S	E	N	D	-	I	N	-	T	H	E	-	S	U	B	S
90	24	71	19	122	63	95	54	85	59	65	51	78	103	59	82

4. Numbers greater than 27 are reduced by repeatedly **subtracting 27** until a number between 1 and 27 is obtained.

90 – **27** – **27** – **27** = 9

24

71 – **27** – **27** = 17

19

Fill in the table to complete the message.

S	E	N	D	-	I	N	-	T	H	E	-	S	U	B	S
9	24	17	19	14	9	14	27	4	5	11	24	24	22	5	1

122 - 27 - 27 - 27 - 27 = 14
63 - 27 - 27 = 9
95 - 27 - 27 - 27 = 14
54 - 27 = 27
85 - 27 - 27 - 27 = 4
59 - 27 - 27 = 5

65 - 27 - 27 = 11
51 - 27 = 24
78 - 27 - 27 = 24
103 - 27 - 27 - 27 = 22
59 - 27 - 27 = 5
82 - 27 - 27 - 27 = 1

5. The numbers are then changed to letters by looking at the original alphabet and the message sent.

9	24	17	19
↓	↓	↓	↓
I	X	Q	S

Complete the coded message to be sent.

I	X	Q	S	N	I	N	–	D	E	K	X	X	V	E	A

Decoding

6. To decode the message the receiver needs to know the encoding matrix i.e. $\begin{bmatrix} 4 & 1 \\ 3 & 1 \end{bmatrix}$

The decoding matrix is the **inverse** of the encoding matrix $\begin{bmatrix} 1 & -1 \\ -3 & 4 \end{bmatrix}$

(Swap the diagonal values (4 and 1) around and multiply the other diagonals (1 and 3) by -1.)

Now each letter from the coded message can be decoded.
(The decoding matrix must be first.)

$$\begin{bmatrix} 1 & -1 \\ -3 & 4 \end{bmatrix} \times \begin{bmatrix} 9 & 24 \\ 17 & 19 \end{bmatrix} = \begin{bmatrix} -8 & 5 \\ 41 & 4 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -1 \\ -3 & 4 \end{bmatrix} \begin{bmatrix} 14 & 9 \\ 14 & 27 \end{bmatrix} = \begin{bmatrix} (1\times14)+(-1\times14) & (1\times9)+(-1\times27) \\ (-3\times14)+(4\times14) & (-3\times9)+(4\times27) \end{bmatrix} = \begin{bmatrix} 0 & -18 \\ 14 & 81 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -1 \\ -3 & 4 \end{bmatrix} \begin{bmatrix} 4 & 5 \\ 11 & 24 \end{bmatrix} = \begin{bmatrix} (1\times4)+(-1\times11) & (1\times5)+(-1\times24) \\ (-3\times4)+(4\times11) & (-3\times5)+(4\times24) \end{bmatrix} = \begin{bmatrix} -7 & -19 \\ 32 & 81 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -1 \\ -3 & 4 \end{bmatrix} \begin{bmatrix} 24 & 22 \\ 5 & 1 \end{bmatrix} = \begin{bmatrix} (1\times24)+(-1\times5) & (1\times22)+(-1\times1) \\ (-3\times24)+(4\times5) & (-3\times22)+(4\times1) \end{bmatrix} = \begin{bmatrix} 19 & 21 \\ -52 & -62 \end{bmatrix}$$

The message is then written as:

-8	5	41	4	0	-18	14	81	-7	-19	32	81	19	21	-52	-62

These numbers are finally adjusted by **adding or subtracting 27** if necessary. Complete the decoding.

-8	5	41	4	0	-18	14	81	-7	-19	32	81	19	21	-52	-62
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
19	5	14	4	27	9	14	27	20	8	5	27	19	21	2	19
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
S	E	N	D	–	I	N	–	T	H	E	–	S	U	B	S

[-8 + 27 = 19] [41-27 = 14]

$0+27=27$

$-18+27=9$

$81-27-27=27$

$-7+27=20$

$-19+27=8$

$32-27=5$

$-52+27+27=2$

$-62+27+27+27=19$

END OF TAKE HOME