

## Matrix Encryption ©Trujillo

Data encryption has become a necessity with the rise of sensitive data being stored and transmitted via computers. The methods included in this section provide a good introduction to the ideas of encryption.

A common way to send coded messages is to assign each letter of the alphabet to a number **1–26** and send the message as a string of integers. For example, if we encode the message “Daredevil is a B list hero” according to the chart(KEY) below,

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

Using the number 0 = Space, we get the string of numbers:

4 1 18 5 4 5 22 9 12 0 9 19 0 1 0 2 0 12 9 19 20 0 8 5 18 15

Now this type of coding is not very secure as there are simple methods to break this code. A more secure method is to use matrices to further encode a message. For this lesson, we will continue to use the chart above that assigns an integer between 1 – 26 to a letter in the alphabet. We will also continue to use the number 0 to represent a space between words.

### Steps to code a message:

1. Convert the message into integers using the chart above.
2. Create an invertible, square coding matrix  $C_{n \times n}$ . Depending on the dimensions of  $C_{n \times n}$  break up the string of numbers into  $n$  number of rows of equal length, adding zeros at the end of the  $n$ th row as needed.
3. Create the message matrix  $M$  using the rows you have just created.
4. Multiply  $CM$  to encode the message. The product of  $CM$  is a matrix that represents the encoded message.

### Example 1: “Daredevil is a B list hero”

Using a coding matrix  $C_{5 \times 5}$ ,

$$C_{5 \times 5} = \begin{pmatrix} -1 & 2 & -2 & 1 & 1 \\ 0 & 3 & 0 & 0 & -1 \\ -2 & 2 & 1 & -2 & 4 \\ -2 & -1 & -1 & -1 & 1 \\ 3 & 1 & 1 & 4 & -5 \end{pmatrix}$$

Using the string of numbers already determined above, the message has been coded into integers:

4 1 18 5 4 5 22 9 12 0 9 19 0 1 0 2 0 12 9 19 20 0 8 5 18 15

$$M = \begin{pmatrix} 4 & 1 & 18 & 5 & 4 & 5 \\ 22 & 9 & 12 & 0 & 9 & 19 \\ 0 & 1 & 0 & 2 & 0 & 12 \\ 9 & 19 & 20 & 0 & 8 & 0 \\ 5 & 18 & 15 & 0 & 0 & 0 \end{pmatrix}$$

Multiply  $CM$  to get the encoded matrix

$$CM = \begin{pmatrix} 54 & 52 & 41 & -9 & 22 & 9 \\ 61 & 9 & 21 & 0 & 27 & 57 \\ 47 & 70 & 28 & -8 & 2 & 40 \\ -34 & -13 & -53 & -12 & -25 & -41 \\ 45 & -1 & 71 & 17 & 53 & 46 \end{pmatrix}$$

The message "Daredevil is a B list hero" has now been encoded to the following string of numbers:  
54 52 41 -9 22 9 61 9 21 0 27 57 47 70 28 -8 2 40 -34 -13 -53 -12 -25 -41 45 -1 71 17 53 46

Example 1 is a bit EXTRA, however, you should be able to see that this method of using matrices to encode can get extremely complicated. Complicacy is the goal since we wish to keep the message confidential and intended for our target audience only.

To un-code the message we need to use  $C^{-1}$  since  $C^{-1}CM = IM = M$ .  
Once we get the matrix  $M$ , we can then use the KEY.

First find  $C^{-1} = \begin{pmatrix} \frac{12}{89} & \frac{-19}{178} & \frac{-39}{178} & \frac{-137}{178} & \frac{-25}{89} \\ \frac{5}{89} & \frac{22}{89} & \frac{3}{89} & \frac{-10}{89} & \frac{-3}{89} \\ -30 & 3 & 53 & 31 & 18 \\ \frac{16}{89} & \frac{-55}{178} & \frac{37}{178} & \frac{25}{178} & \frac{26}{89} \\ \frac{15}{89} & \frac{-23}{89} & \frac{9}{89} & \frac{-30}{89} & \frac{-9}{89} \end{pmatrix}$  \*\*found using calculator methods

Then multiply  $C^{-1}CM = \begin{pmatrix} \frac{12}{89} & \frac{-19}{178} & \frac{-39}{178} & \frac{-137}{178} & \frac{-25}{89} \\ \frac{5}{89} & \frac{22}{89} & \frac{3}{89} & \frac{-10}{89} & \frac{-3}{89} \\ -30 & 3 & 53 & 31 & 18 \\ \frac{16}{89} & \frac{-55}{178} & \frac{37}{178} & \frac{25}{178} & \frac{26}{89} \\ \frac{15}{89} & \frac{-23}{89} & \frac{9}{89} & \frac{-30}{89} & \frac{-9}{89} \end{pmatrix} \begin{pmatrix} 54 & 52 & 41 & -9 & 22 & 9 \\ 61 & 9 & 21 & 0 & 27 & 57 \\ 47 & 70 & 28 & -8 & 2 & 40 \\ -34 & -13 & -53 & -12 & -25 & -41 \\ 45 & -1 & 71 & 17 & 53 & 46 \end{pmatrix}$

Again , using calculator we get,

$$M = \begin{pmatrix} 4 & 1 & 18 & 5 & 4 & 5 \\ 22 & 9 & 12 & 0 & 9 & 19 \\ 0 & 1 & 0 & 2 & 0 & 12 \\ 9 & 19 & 20 & 0 & 8 & 0 \\ 5 & 18 & 15 & 0 & 0 & 0 \end{pmatrix}$$

Writing the numbers in a string, we get:

4 1 18 5 4 5 22 9 12 0 9 19 0 1 0 2 0 12 9 19 20 0 8 5 18 15

then using the KEY

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

And the fact that the number 0 represents a space we get the coded message:

Daredevil is a B list hero

As was stated before, Example 1 was a bit EXTRA. Here's another example: Example 2 if you will...

**Example 2:** Find a matrix to decipher the secure message represented by the following string of numbers.

29 -13 16 15 8 19 -18 93 85 24 105 133 56 72

The matrix used to encode the original message is  $C = \begin{pmatrix} 2 & -1 \\ 3 & 4 \end{pmatrix}$

*Solution:*

If  $C$  was used to encode then  $C^{-1}$  will be the matrix to decipher the message. So using the formula from

class  $C^{-1} = \frac{1}{11} \begin{pmatrix} 4 & 1 \\ -3 & 2 \end{pmatrix} = \begin{pmatrix} \frac{4}{11} & \frac{1}{11} \\ -\frac{3}{11} & \frac{2}{11} \end{pmatrix}$  also writing the string of numbers into a matrix we get the

matrix  $CM = \begin{pmatrix} 29 & -13 & 16 & 15 & 8 & 19 & -18 \\ 93 & 85 & 24 & 105 & 133 & 56 & 72 \end{pmatrix}$

Now multiply  $C^{-1} \cdot CM$  using a calculator to get the matrix  $M = \begin{pmatrix} 19 & 3 & 8 & 15 & 15 & 12 & 0 \\ 9 & 19 & 0 & 15 & 22 & 2 & 18 \end{pmatrix}$

Write the string of numbers out:

19 3 8 15 15 12 0 9 19 0 15 22 2 18

using the KEY we get the message: " **SCHOOL IS OVER**"