Math Investigation: Cryptography

### Introduction: background info, aim/purpose, description of investigation

The term cryptography originated from two Greek words, ‘kryptós’, which means hidden, and ‘graphein’ which means writing. As civilisations evolved, human beings got organised in tribes, groups, and kingdoms, which fuelled the natural need for people to communicate secretly, and thus ensuring the continuous evolution of cryptography. (tutorialspoint.com, 2018)

Cryptography has been used as far back as 4000 years ago, when Egyptians would communicate through messages written in hieroglyph, which were pictorial symbols used to represent words. This illustrative code would evolve to mono-alphabetic ciphers during 500 – 600 BC, which involved replacing shifting the letters of a message by an agreed number. This sort of cypher is famously known as the Caesar Shift Cypher, which Julius Caesar’s messengers would use to deliver secret messages. Nowadays, cyphers are used mainly to transfer information within businesses, and hiding secrets from other companies.

Cryptography, or the study of encoding and decoding messages, is of major interest to large corporations and governments, due to them needing to securely transmit confidential information. The aim of this investigation is to firstly explore how messages can be decoded through matrix subtraction and modulo 26. Then, a cypher will be created in order to send a short, coded message and have instructions on how to decode the message. The difficulties and limitations encountered whilst using the chosen method of encryption will be discussed, as well as the reasoning behind selecting this type of cypher.

Thinkswap Document

### Mathematical Investigations and Analysis

#### Coding matrices using addition

For the following task, a simple cypher, as seen in Figure 1, will be given, and the ciphertext below will be decoded to find the original message.

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

*Fig. 1: Table representing integer values which have been assigned letters of the alphabet.*

The word SEND is written as 19 5 14 4, which can be written using a 2 x 2 matrix:

19 5

[ ]

14 4

2 7

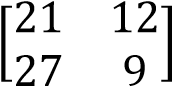
To encrypt the message, the matrix [ ] is added onto it.

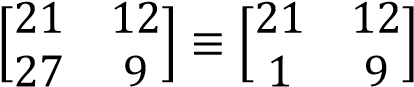
13 5

19 5 + [ 2 7 ] = [ 21 12]

[ ]

14 4 13 5 27 9

Finally, this is converted into modulo 26, which is done by adding or subtracting multiples of 26 to any number not in the range 0 to 25. For example, 27 is not in the range 0 to 25. Using modulo 26, 27 is written as: 27 – (26 x 1) = 1. After conversion,  is written as:

 (𝑚𝑜𝑑 26)

21 12 2 7

To decode [ ] , [ ] must be subtracted from it.

1 9 13 5

21 12 2 7 19 5

[ ] − [ ] = [ ]

1 9 13 5 −12 4

Since the numbers need to be in the range 0 to 25, -12 is converted to modulo 26.

-12 + (26 x 1) = 14

19 5

Thus, the fully decrypted matrix is [ ], values which correspond to the letters SEND using the

14 4

cypher in Figure 1.

For decryption of the full message, SEND MONEY PLEASE, refer to appendix 1.

After the decryption of the message, the result was SEND MONE YPLE ASEE, which forms the phrase, ‘SEND MONEY PLEASE’. When the last few letters of a message are repeated, they are not actually part of the message, and are dummy letters used to fill up spaces in the matrix.

Thinkswap Document

The encryption matrix given will be used to decode the following message:

21 12 1 9 22 15 18 25 20 22 2 21 21 1 2

25 10 12 0 20 23 1 21 20 8 1 21 10 15 2

5 23 3 6 12 4

Firstly, these values must be written into 2 x 2 matrices:

21 12 22 15 20 22 21 1 10 12 23 1 8 1 15 2 3 6

[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

1. 9 18 25 2 21 2 25 0 20 21 20 21 10 5 23 12 4
2. 7 2 7

The matrix [ ] was added onto each matrix during the encryption process, so [ ] must

13 5 13 5

therefore be subtracted from each matrix when decrypting.

21 12 2 7 19 5

[ ] − [ ] = [ ]

1 9 13 5 −12 4

19 5 19 5

After converting [ ] into modulo 26, the resulting matrix is [ ] , which was translated

−12 4 14 4

to mean SEND using Figure 1. For the decryption of the rest of the matrices, refer to appendix 2.

The rest of the message was decrypted to be:

SEND THET ROOP STOT HEMO UTHO FTHE MURR AYYY. This forms the phrase SEND THE TROOPS TO THE MURRAY, as the last two letters were dummy letters.

A message was encrypted using matrix addition. The message was ‘OPEN THE DOOR’. The

* 1. 3 encryption matrix used to secure the message was [ ].
  2. 2

The message was firstly converted to numbers using Figure 1:

15 16 5 14 2 12 21 5 4 15 15 18

The numbers were put into three 2 x 2 matrices:

15 16 2 12 4 15

[ ] [ ] [ ]

5 14 21 5 15 18

8 4

And finally, they were encrypted using the encryption code [ ] by adding the code to each of the

5 7

matrices:

15 16 + [8 4] = [23 20]

[ ]

5 14 5 7 10 21

As all the values are already in modulus 26, no alterations will be made. For the encryption of the remaining matrices, refer to appendix 3.

#### Coding matrices using multiplication

Matrix multiplication is can also be used to encrypt messages and is actually more secure than codes made using matrix addition. Two matrices can only be multiplied together if matrix A has the same number of columns as the number of rows in matrix B. Eg. If matrix A is a 2 x 2 and matrix B is a 2 x 3, then they can be multiplied together.

Thinkswap Document

2 3

The message ‘SEND MONEY PLEASE’ will be encrypted using the encryption matrix [ ].

1 2

The message is first converted into numbers using Figure 1, and then written into 2 x 2 matrices:

19 5 13 15 25 16 1 19

[ ] [ ] [ ] [ ]

14 4 14 5 12 5 5 5

2 3

The next step in the encryption process is to multiply the matrices by the encryption matrix, [ ].

1 2

[19 5] [2 3] = [43 67]

14 4 1 2 32 50

As none of the numbers are in modulo 26, they need to be adjusted:

43 – (26 x 1) = 17

67 – (26 x 2) = 15

32 – (26 x 1) = 6

50 – (26 x 1) = 24

17 15

After converting to modulo 26, the final encrypted matrix was [ ].

6 24

For encryption of the other 3 matrices, refer to appendix 4.

After encrypting all of the matrices, the message was SEND MONEY PLEASE, which was converted from:

17 15 6 24 15 17 0 14 3 3 20 21 15 15 25

To decrypt a message encrypted through matrix multiplication, the inverse of the encryption

a b message is needed. For example, the inverse of matrix [ ] is:

c d

1. d −b

[ ] (det A = ad – bc) detA −c a

1. 3

The encryption matrix used to encrypt SEND MONEY PLEASE was [ ] , and the determinant of

1 2

the matrix was calculated as:

det A = ad – bc

∴det A = (2 × 2) – (3× 1) det A = 4 – 3

det A = 1 Therefore, the inverse of the encryption matrix was:

2

1

det

A

[

d

−

b

−

c

a

]

=

1

1

[

2

−

3

−

1

2

]

=

[

2

−

3

−

1

2

]

−

3

2

]

was given to the receiver to ensure the code

functioned properly

.

SEND =

[

19

5

14

4

]

∴

[

19

5

14

4

]

[

2

−

3

−

1

2

]

=

[

19

−

21

−

12

30

]

As the numbers

-

21

,

-

, and 30 are not

12

between 0

-

26:

, so they were converted to mod

25

-

+ 26 =

21

5

-

12

+ 26 =

14

30

–

4

=

26

The final resulting matrix was

[

19

5

14

4

]

, proving that the decryption matrix was correct.

Thinkswap Document

The decryption matrix [

−1

A decryption of the word SEND was made to do this:

When using matrix multiplication to encrypt messages, when ad – bc ≠ 1, the value outside the inverse matrix becomes a fraction. The letters in the investigation were assigned values intentionally so there would be no need to deal with fractions when working out the inverse of a matrix. This was done so it would be less difficult to decrypt the messages.

This issue can be resolved by using encryption and decryption software built to decipher more complex messages. This reduces the chance for human error and also requires less time. An alternative method would be to simply create a code where ad – bc does equal 1.

#### Creating a code

A cipher has been created to encrypt a short message which will be sent between separate offices of a company via SMS. Instructions have been provided which explain how to encode and decode messages.

To encrypt a message using the cypher made, please follow these steps:

1. Convert the message into numbers using the table below.

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

*Fig. 2*

1. Put the numbers into 2 x 2 matrices, adding a dummy letter(s) at the end of the message if they do not form a 2 x 2 matrix.
2. Add the encryption matrix [4 1] to each of the matrices.

6 2

1. Then, multiply each individual matrix by the encryption matrix [2 1].

1 1

1. Ensure each matrix is written in modulus 26.
2. Finally, write all values as cipher text. (e.g. not in 2 x 2 matrix form)

To decrypt a message using the cypher made, please follow these steps:

1. Multiply each matrix by the inverse of the encryption matrix [2 1].

1 1

2. Then, subtract the encryption matrix [4 1] from each matrix.

6 2

1. Ensure each matrix is written in modulus 26.
2. Convert the values in the matrices into letters using the table above.

The message ‘DESTROY BOXES’ was encoded using the cypher created. The letters were firstly converted to numbers using Figure 2:

Thinkswap Document

1 2 16 17 15 12 22 25 12 21 2 16 Then, these numbers were arranged into three 2 x 2 matrices as shown:

1 2 15 12 12 21

[ ] [ ] [ ]

16 17 22 25 2 16

The first matrix was encrypted as follows:

1 2 4 1 5 3

[ ] + [ ]=[ ]

16 17 6 2 22 19

5 3 2 1 10 + 3 5 + 3

[ ] [ ]= [ ]

22 19 1 1 44 + 19 22 + 19

13 8

= [ ]

63 41

As 63 and 41 are not in the range 0 – 25, they need to be converted to modulus 26:

63 – (26 x 2) = 11

41 – (26 x 1) = 15

13 8

Therefore, the final resulting matrix is [ ]. For the encryption of the remaining matrices, refer

11 15

to appendix 5.

Finally, the encrypted matrices were written as cypher text:

13 8 11 15 25 6 5 3 2 12 8 0

The first encrypted matrix was then decrypted, firstly by arranging the values into a 2 x 2 matrix:

13 8

Matrix 1: [ ]

11 15

2 1

Then, it was multiplied together with the inverse of the encryption matrix [ ].

]

1

1

1

𝑎𝑑

−

𝑏𝑐

[

1

−

1

−

1

2

]

=

1

1

[

1

−

1

−

1

2

]

=

[

1

−

1

−

1

2

]

[

13

8

11

15

]

[

1

−

1

−

1

2

]

=

[

13

−

8

−

13

+

16

11

−

15

−

11

+

30

=

[

5

3

−

4

19

]

The

next

step of decryption is to subtract the encryption matrix

[

4

1

6

2

]

from this matrix:

[

5

3

−

4

19

]

−

[

4

1

6

2

]

=

[

1

2

−

10

17

]

As

-

10

is not in the range 0

–

25

, it needs to be adjusted to modulus 26 form

:

-

10

+ (26 x 1) =

16

Therefore, the final decrypted matrix is now:

Thinkswap Document

1 2

[ ]

16 17

The final step of decryption would be to rearrange the numbers into cyphertext and convert each value into letters using the table above, like so:

1 2 16 17 = D E S T For the decryption of the remaining matrices, refer to appendix 6.

The decrypted matrices were:

1 2 15 12 12 21

[ ] [ ] [ ]

16 17 22 25 2 16

These values correspond to the original message, DESTROY BOXES. Therefore, the decryption process was successful.

#### Other codes

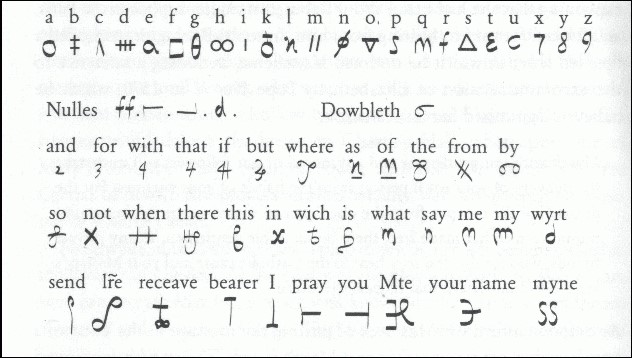
Throughout history, there have been hundreds upon thousands of cyphers created, many of them deciphered by mathematicians. A famous example is the Enigma machine, a Nazi coding device that looked like a typewriter and had one of the most intricate cryptographic systems of the time. This machine required the user to type in a message which it would then scramble using three to five notched wheels or rotors. In order to decode the message, the receiver would need to know the exact settings of the rotors. Incredibly, some brilliant British mathematicians were able to crack the code and read the messages sent by the Germans in World War II.

Another well-known code involved replacing letters with symbols or a picture, such as the code was used by Mary Queen of Scots in an attempt to kill Elizabeth the First, as pictured beside. However, this code is quite easily decoded using trial and error and knowledge of the English language. In English, ‘E’ is the most common letter, and is used about 13% of the time, followed by ‘T’ and ‘A’. There are also only two one-letter words in English, ‘A’ and ‘I’, so a symbol by itself would need to stand for those two letters. A method called

‘frequency analysis’ is used to crack codes like these and was what was responsible for Mary’s eventual execution.

### Conclusion

This investigation studied how information could be encrypted through matrix addition, subtraction, multiplication, division, using the mod 26 structure. It was discovered that when using matrix multiplication for encryption purposes, the encryption matrix should be such that ad – bc = 1. If not, then encrypting using matrix multiplication would require the use of fractions, heavily complicating the encryption and decryption process. The chosen method of encryption, matrix addition paired with matrix multiplication, proved to be successful as it was relatively easy to use for the receivers of the message, but still complicated enough for enemies to not immediately decode.



Thinkswap Document

There were no difficulties encountered when using this code, likely because of how simple it is to use. However, this investigation did not require a high level of security, as the message was short and would likely not reveal much to any competitors. Codes which correspond letters to numbers are amongst the most common, as well as easy to solve, codes. The addition of having the numbers be multiplied and subtracted by matrices would definitely decrease the chance of the message being decoded, but with technology being so advanced these days, there is still a possibility that a computer could crack the cypher within seconds. The low level of security would be the only drawback from using this code, but as explained previously, the cypher was not meant to be very advanced anyways.

This investigation could be further extended by encoding a longer message or having to create a completely original cypher. Matrices of different forms could also be used, for example 3 x 3

matrices, of 4 x 3. Matrices where ad – bc  1 or 0 would result in fractions, which were avoided in this task but would be a good extension activity. Future investigations could solely focus on other ways of using matrices in real life.

### Bibliography

www.tutorialspoint.com. (2018). *Origin of Cryptography*. [online] Available at:

https://www.tutorialspoint.com/cryptography/origin\_of\_cryptography.htm [Accessed 27 Apr. 2018].

www.tutorialspoint.com. (2018). *Modern Cryptography*. [online] Available at: https://www.tutorialspoint.com/cryptography/modern\_cryptography.htm [Accessed 27 Apr.

2018].

Thinkswap.com. (2018). *Folio Investigation: Matrix Cryptography | Year 12 SACE - Mathematical Studies | Thinkswap*. [online] Available at: https://www.thinkswap.com/au/sace/mathematicalstudies/year-12/folio-investigation-matrix-cryptography [Accessed 27 Apr. 2018].

Thinkswap Document

Nrich.maths.org. (2018). *The Secret World of Codes and Code Breaking*. [online] Available at:

https://nrich.maths.org/2197 [Accessed 27 Apr. 2018].

# Appendix 1

15 22

## Matrix 2: [ ]

1 10

15 22 2 7 13 15

[ ] − [ ] = [ ] 1 10 13 5 −12 5

As -12 is not in the range 0 to 25, mod 26 is used:

-12 + 26 = 14

13

The resulting matrix is [

14

letters ‘MONE’.

1 23

Matrix 3: [ ]

25 10

As -1 is not in the range 0 to 25, mod 26 is used:

15

5

]

, which has values 13 15 14 5 and

(

using Figure

1)

correspond to the

[

1

23

25

10

]

−

[

2

7

13

5

]

=

[

−

1

16

12

5

]

16

5

]

, which has values 25 16 12 5 and

(

using Figure

1)

correspond to the

Thinkswap Document

-1 + 26 = 25

25

The resulting matrix is [

12

letters ‘YPLE’.

3 0

Matrix 4: [ ]

18 10

3 0 2 7 1 −7

[ ] − [ ] = [ ] 18 10 13 5 5 5

As -7 is not in the range 0 to 25, mod 26 is used:

-7 + 26 = 19

## 1 19

Hence, the resulting matrix is [ ], which has values 1 19 5 5 and (using Figure 1) correspond to

5 5

the letters ‘ASEE’.

#### Appendix 2

22 15

Matrix 2: [ ] 18 25

22 15 2 7 20 8

[ ] − [ ] = [ ]

18 25 13 5 5 20

The resulting matrix had values 20 8 5 20 and using Microsoft Excel, corresponded to the letters

‘THET’.

20 22

Matrix 3: [ ]

2 21

20 22 2 7 18 15

[ ] − [ ] = [ ] 2 21 13 5 −11 16

As -11 is not in the range 0 to 25, mod 26 was used:

-11 + 26 = 15

The resulting matrix had values 18 15 15 16 and using Microsoft Excel, corresponded to the letters ‘ROOP’.

[

21

1

2

25

]

−

[

2

7

13

5

]

=

[

19

−

6

−

11

20

]

As

-

6

and

-

11

are not in the range 0 to 25, mod 26 was used:

Thinkswap Document

21 1

Matrix 4: [ ]

2 25

-6 + 26 = 20

-11 + 26 = 15

The resulting matrix had values 19 20 15 20 and using Microsoft Excel, corresponded to the letters ‘STOT’.

10 12

Matrix 5: [ ]

0 20

10 12 2 7 8 5

[ ] − [ ] = [ ] 0 20 13 5 −13 15

As -13 is not in the range 0 to 25, mod 26 was used:

-13 + 26 = 13

The resulting matrix had values 8 5 13 15 and using Microsoft Excel, corresponded to the letters ‘HEMO’.

23 1

Matrix 6: [ ]

21 20

23 1 2 7 21 −6

[ ] − [ ] = [ ] 21 20 13 5 8 15

As -6 is not in the range 0 to 25, mod 26 was used:

-6 + 26 = 20

The resulting matrix had values 21 20 8 15 using Microsoft Excel, corresponded to the letters ‘UTHO’.

8 1

Matrix 7: [ ]

21 10

8 1 2 7 6 −6

[ ] − [ ] = [ ] 21 10 13 5 8 5

As -6 is not in the range 0 to 25, mod 26 was used:

-6 + 26 = 20

The resulting matrix had values 6 20 8 5 and using Microsoft Excel, corresponded to the letters ‘FTHE’.

15 2

[

15

2

5

23

]

−

[

2

7

13

5

]

=

[

13

−

5

−

8

18

]

As

-

5

and

-

8

are not in the range 0 to 25, mod 26 was used:

Thinkswap Document

Matrix 8: [ ]

5 23

-5 + 26 = 21

-8 + 26 = 18

The resulting matrix had values 13 21 18 18 and using Microsoft Excel, they corresponded to the letters ‘MURR’.

3 6

Matrix 9: [ ]

12 4

3 6 2 7 1 −1

[ ] − [ ] = [ ] 12 4 13 5 −1 −1

As -1 is not in the range 0 to 25, mod 26 was used:

-1 + 26 = 25

The resulting matrix had values 1 25 25 25 and using Microsoft Excel, they corresponded to the letters ‘AYYY’.

[Appendix 3](#_Toc35199)

[13Matrix 2: [ ] 5](#_Toc35200)

[19 15](#_Toc35201)

13 5 ] + [5 3] = [18 8 ]

[

19 15 6 2 25 17

18 8

The resulting encrypted matrix was [ ], which had values 18 8 25 17.

25 17

1. 5

Matrix 3: [ ]

13 15

* 1. 5 5 3 18 8

[ ] + [ ] = [ ]

13 15 6 2 19 17

* 1. 8

The resulting encrypted matrix was [ ], which had values 18 8 19 17.

* 1. 17

1. 5

Matrix 4: [ ]

25 25

* 1. 5 5 3 19 8

[ ] + [ ] = [ ] 25 25 6 2 31 27

As 31 and 27 are not in the range 0 to 25, mod 26 was used as follows:

19

8

5

1

]

, which had values 19 8 5 1.

[

2

21

12

5

]

+

[

8

4

5

7

]

=

[

10

25

17

12

]

Thinkswap Document

31 – 26 = 5

27 – 26 = 1

Hence, the resulting encrypted matrix was [

#### Appendix 3

2 21

Matrix 2: [ ]

12 5

10 25

The resulting matrix was [ ], which has values 10 25 17 12.

17 12

4 15]

Matrix 3: [

15 18

4 15 ] + [ 8 4] = [ 12 19]

[

15 18 5 7 20 25

12 19

The resulting matrix was [ ], which has values 12 19 20 25.

20 25

Appendix 4

1. 15]

Matrix 2: [

1. 5

13 15 2 3 41 69

[ ] [ ] = [ ] 14 5 1 2 33 52 As none of the numbers are in the range 0 to 25, mod 26 was used:

41 – 26 = 15

69 – (26 × 2) = 17

33 – 26 = 7

52 – (26 × 2) = 0

15 17

The resulting encrypted matrix was [ ], which has values 15 17 7 0.

7 0

25 16

Matrix 3: [ ]

12 5

25 16 2 3 66 107

[ ] [ ] = [ ] 12 5 1 2 29 46

As

none

of the numbers are in the range 0 to 25, mod 26 was used:

29

–

26

= 3

46

–

26

=

20

14

3

3

20

]

, which ha

s

values 14 3 3 20.

[

1

19

5

5

]

[

2

3

1

2

]

=

[

21

41

15

25

]

Thinkswap Document

66 – (26 × 2) = 14

107 – (26 × 4) = 3

The resulting encrypted matrix was [

1 19

Matrix 4: [ ]

5 5

As 41 is not in the range 0 to 25, mod 26 was used:

41 – 26 = 15

21 15

The resulting encrypted matrix was [ ], which has values 21 15 15 25.

15 25

#### Appendix 5

15 12

Matrix 2: = [ ]

22 25

15 12 4 1 19 13

[ ] + [ ] = [ ]

22 25 6 2 28 27

19 13 2 1 38 + 13 19 + 13

[ ] [ ] = [ ]

28 27 1 1 56 + 27 28 + 27

51 32

= [ ]

83 55

As none of the numbers are in the range 0 – 25, they need to be converted into modulus 26:

51 – (26 x 1) = 25 32 – (26 x 1) = 6

83 – (26 x 3) = 5 55 – (26 x 2) = 3

25 6

The resulting final matrix is [ ]. These values are finally written in cypher text:

5 3

25 6 5 3

12 21

Matrix 3: [ ]

2 16

12 21 4 1 16 22

[ ] + [ ] = [ ]

2 16 6 2 8 18

16 22 2 1 32 + 22 16 + 22

[ ] [ ] = [ ]

8 18 1 1 16 + 18 8 + 18

54 38

= [ ]

34 26

As none of the numbers are in the range 0 – 25, they need to be converted into modulus 26:

54 – (26 x 2) = 2

34

–

(26

x 1) =

8

26

–

(26

x 1) =

0

2

12

8

0

]

.

These values are finally written in cypher text.

2

12 8

0

Then, it was multiplied together with the inverse of the encryption matrix

[

Thinkswap Document

38 – (26 x 1) = 12

The resulting final matrix is [

#### Appendix 6

The second encrypted matrix was decrypted, firstly by arranging the values into a 2 x 2 matrix:

25 6

Matrix 2: [ ]

1. 3

2 1

].

1 1

25 6 1 −1 25 − 6 −25 + 12

[ ] [ ] = [ ]

5 3 −1 2 5 − 3 −5 + 6

19 −13

= [ ]

2 1

4 1

The next step of decryption is to subtract the encryption matrix [ ] from this matrix:

1. 2

19 −13 4 1 15 −14

[ ] − [ ] = [ ] 2 1 6 2 −4 −1

As -14, -4, and -1 are not in the range 0 – 25, they need to be adjusted to modulus 26 form:

-14 + (26 x 1) = 12

-4 + (26 x 1) = 22

-1 + (26 x 1) = 25

Therefore, the final decrypted matrix is now:

15 12

[ ]

22 25

The final step of decryption would be to rearrange the numbers into cyphertext and convert each value into letters using the table above, like so:

15 12 22 25 = R O Y B

The third encrypted matrix was decrypted, firstly by arranging the values into a 2 x 2 matrix:

12 21

Matrix 3: [ ]

2 16

2 1

Then, it was multiplied together with the inverse of the encryption matrix [ ].

1 1

12 21 1 −1 12 − 21 −12 + 42

[ ] [ ] = [ ]

2 16 2 − 16 −2 + 32

−

1

2

=

[

−

9

30

−

14

30

]

The next step of decryption is to subtract the encryption matrix

[

4

1

6

2

[

−

9

30

−

14

30

]

−

[

4

1

6

2

]

=

[

−

13

29

−

20

28

]

Thinkswap Document

] from this matrix:

As none of the numbers are in the range 0 – 25, they need to be adjusted to modulus 26 form:

-13 + (26 x 1) = 13

29 - (26 x 1) = 3

-14 + (26 x 1) = 12

28 - (26 x 1) = 2

Therefore, the final decrypted matrix is now:

13 3

[ ]

2 12

The final step of decryption would be to rearrange the numbers into cyphertext and convert each value into letters using the table above, like so:

13 3 2 12 = OXES