Danny Aburas

Year 12 Maths Studies
Investigation

Matrix Cryptography

Topic: Working with Linear Equations and Matrices
Subtopics: 3.3 Matrices
3.4 The Inverse of a Matrix

A completed investigation should include:

- an introduction that outlines the problem to be explored, including its significance, its features, and the context
- the method required to find a solution, in terms of the mathematical model or strategy to be used
- the appropriate application of the mathematical model or strategy, including
  - the generation or collection of relevant data and/or information, with details of the process of collection
  - mathematical calculations and results, and appropriate representations
  - the analysis and interpretation of results
  - reference to the limitations of the original problem
- a statement of the results and conclusions in the context of the original problem
- appendices and a bibliography, as appropriate.

Learning Requirements	*Assessment Design Criteria*	*Capabilities*
1. understand fundamental mathematical concepts, demonstrate mathematical skills, and apply routine mathematical procedures 2. use mathematics as a tool to analyse data and other information elicited from the study of situations taken from social, scientific, economic, or historical contexts 3. think mathematically by posing questions/problems, making and testing conjectures, and looking for reasons that explain the results 4. make informed and critical use of electronic technology to provide numerical results and graphical representations 5. communicate mathematically and present mathematical information in a variety of ways 6. work both individually and cooperatively in planning, organising, and carrying out mathematical activities.	**Mathematical Knowledge and Skills and Their Application** The specific features are as follows: MKSA1 Knowledge of content and understanding of mathematical concepts and relationships. MKSA2 Use of mathematical algorithms and techniques (implemented electronically where appropriate) to find solutions to routine and complex questions. MKSA3 Application of knowledge and skills to answer questions in applied and theoretical contexts. **Mathematical Modelling and Problem-solving** The specific features are as follows: MMP1 Application of mathematical models. MMP2 Development of solutions to mathematical problems set in applied and theoretical contexts. MMP3 Interpretation of the mathematical results in the context of the problem. MMP4 Understanding of the reasonableness and possible limitations of the interpreted results, and recognition of assumptions made. MMP5 Development and testing of conjectures, with some attempt at proof. MMP6 Contribution to group work. **Communication of Mathematical Information** The specific features are as follows: CMI1 Communication of mathematical ideas and reasoning to develop logical arguments. CMI2 Use of appropriate mathematical notation, representations, and terminology.	Communication Learning

Danny Aburas

Danny Aburas

Performance Standards for Stage 2 Mathematical Studies

	Mathematical Knowledge and Skills and Their Application	Mathematical Modelling and Problem-solving	Communication of Mathematical Information
A	Comprehensive knowledge of content and understanding of concepts and relationships. Appropriate selection and use of mathematical algorithms and techniques (implemented electronically where appropriate) to find efficient solutions to complex questions. Highly effective and accurate application of knowledge and skills to answer questions set in applied and theoretical contexts.	Development and effective application of mathematical models. Complete, concise, and accurate solutions to mathematical problems set in applied and theoretical contexts. Concise interpretation of the mathematical results in the context of the problem. In-depth understanding of the reasonableness and possible limitations of the interpreted results, and recognition of assumptions made. Development and testing of valid conjectures, with proof. Constructive and productive contribution to group work.	Highly effective communication of mathematical ideas and reasoning to develop logical arguments. Proficient and accurate use of appropriate notation, representations, and terminology.
B	Some depth of knowledge of content and understanding of concepts and relationships. Use of mathematical algorithms and techniques (implemented electronically where appropriate) to find some correct solutions to complex questions. Accurate application of knowledge and skills to answer questions set in applied and theoretical contexts.	Attempted development and appropriate application of mathematical models. Mostly accurate and complete solutions to mathematical problems set in applied and theoretical contexts. Complete interpretation of the mathematical results in the context of the problem. Some depth of understanding of the reasonableness and possible limitations of the interpreted results, and recognition of assumptions made. Development and testing of reasonable conjectures, with substantial attempt at proof. Productive contribution to group work.	Effective communication of mathematical ideas and reasoning to develop mostly logical arguments. Mostly accurate use of appropriate notation, representations, and terminology.
C	Generally competent knowledge of content and understanding of concepts and relationships. Use of mathematical algorithms and techniques (implemented electronically where appropriate) to find mostly correct solutions to routine questions. Generally accurate application of knowledge and skills to answer questions set in applied and theoretical contexts.	Appropriate application of mathematical models. Some accurate and generally complete solutions to mathematical problems set in applied and theoretical contexts. Generally appropriate interpretation of the mathematical results in the context of the problem. Some understanding of the reasonableness and possible limitations of the interpreted results, and some recognition of assumptions made. Development and testing of reasonable conjectures, with some attempt at proof. Some productive contribution to group work.	Appropriate communication of mathematical ideas and reasoning to develop some logical arguments. Use of generally appropriate notation, representations, and terminology, with some inaccuracies.
D	Basic knowledge of content and some understanding of concepts and relationships. Some use of mathematical algorithms and techniques (implemented electronically where appropriate) to find some correct solutions to routine questions. Sometimes accurate application of knowledge and skills to answer questions set in applied or theoretical contexts.	Application of a mathematical model, with partial effectiveness. Partly accurate and generally incomplete solutions to mathematical problems set in applied or theoretical contexts. Attempted interpretation of the mathematical results in the context of the problem. Some awareness of the reasonableness and possible limitations of the interpreted results. Attempted development or testing of a reasonable conjecture. Superficial contribution to group work.	Some appropriate communication of mathematical ideas and reasoning. Some attempt to use appropriate notation, representations, and terminology, with occasional accuracy.
E	Limited knowledge of content. Attempted use of mathematical algorithms and techniques (implemented electronically where appropriate) to find limited correct solutions to routine questions. Attempted application of knowledge and skills to answer questions set in applied or theoretical contexts with limited effectiveness.	Attempted application of a basic mathematical model. Limited accuracy in solutions to one or more mathematical problems set in applied or theoretical contexts. Limited attempt at interpretation of the mathematical results in the context of the problem. Limited awareness of the reasonableness and possible limitations of the results. Limited attempt to develop or test a conjecture. Attempted contribution to group work.	Attempted communication of emerging mathematical ideas and reasoning. Limited attempt to use appropriate notation, representations, or terminology, and with limited accuracy.

Danny Aburas

FOLIO TASK: MATRIX CRYPTOGRAPHY

Introduction

Many communications that are transmitted between and within countries need to be secure. Coding the messages can provide that security. One method of encoding involves using an alpha numeric code that is then encrypted by matrix multiplication. To decode the message the recipient needs to be sent separately the message and the decoding technique.

A simple alpha numeric code is one where A = 1, B = 2 etc and a 'space' = 0

Mathematical Procedures, Discussion and Analysis

- Write a message of at least 12 characters.
- Develop a coding technique that involves an alpha numeric code and matrix multiplication.
- Code the message and prepare a set of instructions to allow someone else to decode the message.
- Decode the message. You will be required to work in pairs to decoding each other's message and discussing possible refinements.
- Discuss the limitations of the original problem and your solution as well as appropriate refinements and/or extensions

Conclusion

Summarise your methods of solution and state your findings.

Introduction

The purpose of this investigation is to explore the various properties and concepts of matrix cryptography. Specifically, this investigation requires the use of matrix algebra to encode a message of 12 characters or more using a developed encryption technique. The method involves

an alphanumeric code and a form of matrix multiplication to scramble this message. The code must be "decodable", meaning readers can decipher the scrambled words when given the appropriate "keys" and precise instructions.

The first task is to develop an effective technique of encoding a message. The 26 letters of the alphabetic are to be allocated corresponding digits. To complicate the system, the first half of the alphabetic are to be allocated even numbers, while the rest of the alphabet was allocated odd numbers.
Next, the message of choice, "IONCANNONREADY" is to be translated to a numeric code using the alphanumeric system. This numeric code will then be broken up into packets of matrices with dimensions 4x1. The numeric values will be placed into the elements of the matrices systematically and blank elements remaining in excess will be replaced with the letter Z (digit number 25) purely to just fill all the matrices completely. Now the message matrices are all cipher shifted using an algorithm and all code matrices undergo the same cipher shift.
A 4x4 scramble matrix with a determinant of 1 is then to be created by using properties of "upper triangular matrices" and "transpose matrices". The scramble matrix is then multiplied by each packet of code and an encoded message is achieved.

After encoding the message, instructions for decoding the message must be prepared. Using matrix algebra, a method of decoding is given to the partner along with other required information such as the cipher shift, scramble matrix and alphanumeric system. The partner must use information given and follow instructions presented to decode the message.

Preamble

Cryptography is the act of concealing information from being understood by anyone unintended to do so, usually, this is done by transformation of a message, or any data, into some incomprehensible scrambled form. Humans have always had the need to conceal information from people who may wish to cause harm by the use of that information, and for that purpose many forms of Cryptography have been used extensively for a very long time. To most people, it is merely a matter of privacy. Keeping communications private and away from unintended listeners gives peace in the minds on many people.
However, for some people, the encryption of messages is far more essential. For example, when a country is under attack, the enemy is looking desperately for strategies exploit of the country's weaknesses, however, for the enemy to recognize a country's weaknesses, knowledge of that particular country must be obtained. For example, information about the locations of bases, airfields and populated areas, may be gathered and used to the enemy's advantage. To render this gathering of secrets harder for the enemy, encryption of classified documents , messages and other data now becomes very important to any country's government.

Results.

Encoding Method

A	B	C	D	E	F	G	H	I	J	K	L	M
2	4	6	8	10	12	14	16	18	20	22	24	26

Danny Aburas

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	3	5	7	9	11	13	15	17	19	21	23	25

First, the following alphanumeric system was chosen. Note that the corresponding digits are not merely a direct substitution in order of letters, but instead, we can rearrange the corresponding digits in some pattern or random order. In this case, the first half of the alphabet is allocated even numbers, while the remaining half is allocated odd numbers. This renders the code tougher to break without the alphanumeric system being provided to the intended reader.

Now, a message, written in English, was created. The message chosen is "**IONCANNONREADY**", a quote from the Command and Conquer game series, the ion cannon fires charged particles and causes devastating damage to the enemy base. This message translates to the corresponding numeric code using the system above :
18,3,1 ,6,2,1,1,3,1, 9,10,2,8,23.

This code must now be broken into uniform packets or "chunks" to be coded. It is decided that the chunks will consist of 4x1 matrices. This is as the encoding matrix is a 4x4 and to be multipliable by each packet, the number of columns of matrix A must equal the number of rows of matrix B by definition.

Notice that the two elements are blank*. To fix this, "dummy" letters will be placed into the packets at random only to complete all packets to 4x1 matrices.

Z, digit 25*, was positioned in places of empty elements at random. All packets are now 4x1 and the message matrices and are ready for encoding.

18, 3, 1, 6, 2, 1,1,3,1, 9,10,2,8,23 now becomes,18316 211319102823**

*18, 3, 1, **25**, 6, 2, 1,1,3,1, 9, 10,2,8,23,**25***
183125* 621131910282325*
Now the message is in a form that may be encoded, however, the message code at the present state is very straight forward as the digits directly represent the corresponding letters. A disguise of some kind must be used to give this code additional security by shifting all the values by some scalar quantity. This technique is well known as a "Cypher Shift". A cypher shift refers to the process in which, an algorithm or scalar quantity is applied to all elements in each of the packet matrices so that the digits no longer directly represent the corresponding letters. To find the real values, the cypher shift must be known by the decoder and the reverse of this mathematical process must be applied. Without the cypher shift process being known, the original values remain shifted and concealed.
The cypher shift algorithm chosen is 3x +6**.** The algorithm (3x + 6) is applied to all elements in all matrices as shown to produce a cypher shift. This process is demonstrated below.

3x +6183125 6015981 3x +66211 241299

3x +631910 1593336 3x +6282325 12307581

The new cypher shifted matrix Code is as follows, 6015981241299 157333618307581
The reverse of this process to obtain the original value can be performed by algebraic methods. As the cypher shift is 3x +6 = new value, the original value can be obtained by using for formula,
x= new value -63**.** This "key" is required if one wishes to reverse the cypher shift and decode the message.

This message code is now ready to be encoded using matrix methods. The following method of Encoding is performed by creating a scramble matrix and multiplying it with each of the elements in the

column matrices to generate a new matrix with encoded value.
As the digits corresponding to the letters are integers and do not contain any fractions, consequently, when encrypted, digits must also be integers to correspond to a specific letter. To make sure this occurs, the decided scramble matrix should have a determinant of one to ensure no fractions are obtained in the answer. This is done by using upper triangular matrix method, which states, the determinant of any square matrix of upper triangular matrix form is the product of the leading diagonals, as shown below.

Det p000lk00hgf0dcba = p× k× f× a

If matrix A is an upper triangular matrix, the determinant of the matrix can be found by multiplying the leading diagonals. If these diagonals multiply to give a value of 1, then this method can be used to construct a scramble matrix with a determinant of 1, as shown below.

Det A = Det1000l100hg10dcb1= 1

A scramble matrix in this form may be used as it produces a determinant of 1. However, let us see what happens when we multiply this scramble matrix with the first packet from our code.

From this, we can see that the first row remains unchanged by the multiplication as the first value is 1 and all other values are zero. The second and third row's elements, also, were not multiplied by all elements in the scramble matrix due to the multiplication by zero.

1000l100hg10dcb1×6015981 = 60+0+0+060l+15+0+060 h+15g+9+060d+15 c+9b+81

Instead of using this flawed method, an improvement to the process should be made.
According to the transpose rule, the scramble matrix A, multiplied by its transpose should produce a new scramble matrix with a determinant of 1. The general case is shown below.

Det(A x A^T)= 1

As Det1bcd01gh001l0001x1000l100hg10dcb1 = 1

Note: l, h, g, d , c & b are generated at random, as these values do not alter the determinant value of 1. The matrix and its transpose generated as follows by multiplication of a triangular matrix and it's transpose, this calculation is performed by the use of graphic calculator.

This scramble matrix will be used to encode the message code by multiplication.
1656014700150001x1000510074106561 = 10256416755246737293156561

This scramble matrix will be tested in order see what happens when we multiply this scramble matrix with the packets of code. The multiplication process is carried out by graphic calculator and the results are shown below.

10256416755246737293156561×6015981 = 781562613339570
10256416755246737293156561 ×241299 = 354329011560267

10256416755246737293156561 ×1593336 = 360333632019369
10256416755246737293156561 ×12307581 = 646564774044753

IT is apparent that this process has completely scrambled the code, also note that using this scramble matrix does not seem to inflict the flaws of using a triangular matrix such as the values remaining the identical, this is due to the fact that none of the elements in this scramble matrix are zeros. So therefore, a matrix (A X A^T) is most appropriate to be used as the scramble matrix.
Now, after being scrambled, the message code has developed as shown below.
7733616932775583543290115602673603336320193696465647740447 53

Danny Aburas

This is the final scrambled code. This code is virtually unbreakable, unless the decoder is provided with the inverse of the scramble matrix, the cypher shift and the alphanumeric system or using a very powerful computer program. It is assumed the security is sufficient for our purposes, no further processes will be carried out to scramble this matrix, however, for extreme security, it is possible to display the scrambled code in alphabetical format instead of a numerical code.

26 units are subtracted from each value from the scrambled code , until a value of 1 to 26 is achieved.

The resulting digits are displayed to the left.

Converting the numerical codes to alphabetical characters will be done by taking each scrambled element from the final scrambled matrix and continually subtracting 26 (number of characters used) by the use of a calculator until a digit between or equal to 1 and 26 is reached. That value will then correspond to an alphabetical character. By using this method, it is completely impossible to break unless the decoder knows the original scrambled matrix. So using this method ensures the code is unbreakable. The mathematical calculations and method are shown below.

781562613339570354329011560267360333632019369646564774044753
117112715267159175173142 5

Matrices are removed and the following liner code remains:
11, 7, 1, 12, 7,15,26,7, 15,9,17,5,17,3,14,25

The directly above code will now be converted to a character set as a replacement for numbers. The code bellow is fully converted and the process cannot be reversed without precise knowledge of the steps performed in earlier processes of subtracting 26 units, consequently, this code cannot be given to a member to decode.
Converted code: **SQNFUZMQURVPVOGZ**

This extension to the method is useful if the message was to never be decoded by anyone, for example, bank pin numbers, passwords and other personal information could be encoded in this manner right after being typed into a computer. Unless the computer records the amount of times 26 units were subtracted from the original digits in the scrambled matrix to obtain a value between 1 -26, this yields even the original encrypted matrix highly secure.

Decoding tutorial

This tutorial will demonstrate how the encrypted message can be decoded. The decoding can only be performed if given the scramble matrix, the cipher shift algorithm and the alphanumeric code. The 4 matrices shown below have been cipher shifted, then scrambled using matrix multiplication to conceal the true message.

781562613339570354329011560267360333632019369646564774044753

Using matrix algebra, it can be seen that the original code matrix, A, can be obtained by multiplying the scrambled matrix ,B, by the inverse of the scramble matrix used, X^{-1}

To decode the message, the last step performed to encode this message must be performed first. The last process performed to the matrices was multiplication with a scramble matrix.

A is the original code,
X is the scramble matrix
B is the scrambled code matrix.
$AX=B$
$AXX^{-1}=BX^{-1}$.
$AI=BX^{-1}$.
$A=BX^{-1}$

Therefore each one of the matrices must be multiplied with the inverse of the scramble matrix used to encode. To find the inverse of the scramble matrix a graphic calculator was used. Results are shown below.

X = 102564167252467372931565 61

X-1=1-619-59-531-9930813-82264-824-59373-12033759

Each packet of the encoded messages matrices will now be multiplied by the inverse of the scramble matrix, X^{-1} , to obtain the original message code.

1-619-59-531-9930813-82264-824-59373-12033759 × 781562613339570= 6015981

1-619-59-531-9930813-82264-824-59373-12033759×354329011560267 = 241299

1-619-59-531-9930813-82264-824-59373-12033759×360333632019369=1593336

1-619-59-531-9930813-82264-824-59373-12033759× 646564774044753=12307581

The following codes have now been decoded:
6015981241299 157333618307581

However, the elements in the matrix code are still cipher shifted. In order for this code to be readable, the cipher shift process must be reversed. The following algorithm was used to cipher shift the elements of the matrices

3x +6 = C,

where x is the original element value, and C is the cipher shifted value. The original value can be obtained by rearranging the cypher shift equation, using algebraic methods, to:

C -63=x

The above equation can now be used to obtain the original values by inputting the cipher-shifted values given in each element into C, and X, the original values, are obtained.

C -636015981 183125 C -63241299 6211

C -631573336 31910 C -6318307581 282325

The cipher shift has now been removed and the original message code is shown below.

183125 621131910282325

The elements can now be read systematically from top to bottom. The Matrices are removed and the bare code remains.

18, 3, 1, 25, 6, 2, 1,1,3,1, 9, 10,2,8,23,25

Now, for the sake of reading this message, the following alphanumeric system is used to convert the numeric code to alphabetical form.

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

18, 3, 1, ***25****, 6, 2, 1,1,3,1, 9, 10,2,8,23,****25 translates to*** **IONZCANNONREADYZ**

Now, the code has been cracked and is readable. Ignoring the letters Z in the message, the reader can now understand from this message that the powerful ion cannon is ready to be fired.

Summary

Both cipher shift algorithms and matrix multiplication methods of encryption were made use of in the encoding process. Results obtained from both these methods provided reasonable outcomes. Comparison between the cipher shift technique and matrix multiplication approaches of encoding showed that the use of a cipher shift was less time consuming and quite simple, while matrix multiplication methods were a little more complex as the scramble matrix needed to produce a determinate of 1. Technology was used for all matrix algebra calculations such as multiplication and finding the inverse.

Analysis/Discussion

Assumptions were made that the calculations performed in the encoding method are correct and do not contain any mathematical errors. In addition, it is assumed that the person who wishes to decode the message has a basic understanding of matrix algebra, and is able to follow mathematical instructions. Another assumption being made is that the graphic calculator settings used are correct and the does not contain any errors or glitches and that the equations entered into the program are correct.

The limitations faced in this investigation include the following. Firstly, The alphanumeric code chosen does not contain the character for a space, capital letters, or any punctuation marks such as comer, full stop etc. Due to the lack of punctuation, the decoder may poorly or incorrectly understand the true meaning of the message. In addition, the letter Z, (25) was used to fill in empty elements in the "chucking process". This could render the message even harder to read as sometimes new words can be formed by addition of letters. As this message is short and consists of 3 words, it does not pose huge problem to decode and read, but if this method was used to decode a large script, the intended reader would take a very long time to decode the message and more essentially, have a very hard time understanding what the message means due to the grammar. To tackle this issue, additions of capital letters, punctuation marks, and a space character to the alphanumeric system will need to be considered. Another limitation is that the scramble matrix has to be multipliable by the packets of data and so both have to contain dimensions of corresponding rows to columns or vice versa to satisfy this.

In relation to the method, a number of proofs were done to demonstrate thoroughly the process of finding a scramble matrix with a determinant of 1 and so the method of generating scramble matrix used was reasonable. The amount of characters that can be encoded is unlimited; however, as mentioned above, the major limitation is the lack of punctuation which could render the decoded message incomprehensible by the intended reader. Therefore, this method is reasonable to be used for the encryption of small messages of 1-4 words but the alphanumeric system will need to be improved to accommodate larger passages of script. In relation to the results obtained, all calculations of matrix algebra were performed on the Casio fx-9860G AU PLUS graphics calculator. This calculator was presumed to be suitable for this investigation. The calculated results were decoded and results proved that calculations were accurate therefore the results obtained are correct. In addition, the method of cryptography used is virtually unbreakable without the scramble matrix and cipher shift unless a powerful program is used, therefore this method of encryption reliable. In conclusion, this method of encryption used is more than reasonable for our purposes.

Conclusion

The purpose of this investigation has been to generate and encrypt a message that can be decoded by the use of matrix algebra properties. From the investigation, it was found that:

- An alpha-numeric code consisting of 26 different letters was required to encode the message in a numeric manner.

- For the message to be encoded by matrix methods, it was necessary to convert the massage into matrix form by allocating the letters in the message systematically into four 4x1 "packet" matrices. Fake or decoy letters were also introduced into the matrices to complete the dimensions required.

- The fundamental point to decoding any matrix coding process is to find the inverse of the matrix used to encode it and multiply the code by this inverse matrix.

- It was discovered that, as fractions do not represent any letters in the alpha-numeric code, in order to decode the message properly, avoiding fractions being produced is crucial. When decoding the message by multiplication with the inverse of the scramble matrix, the scramble matrix needs to have a determinant of 1 so that no fractions are obtained.
- The encoding matrix with a determinant of 1 was generated by multiplying a lower triangular matrix with its transpose.
- By completing this investigation and obtaining good results, matrix cryptology demonstrated to be a reasonable and reliable method of coding and decoding message matrices.

Bibliography

Wikipedia , 'Caesar cipher', wiki article, accessed 12 may 2012, available at: http://en.wikipedia.org/wiki/Caesar_cipher

Khan Academy, 2012, 'Linear Algebra: Upper Triangular Determinant ', *Khan Academy*, Available at: http://www.khanacademy.org/video/linear-algebra--upper-triangular-determinant?playlist=Linear+Algebra

Haese, R, Haese, S, Van Dulken, T, Harris, K & Thompson, A 2006, *Mathematical Studies*, 2nd edition, Haese & Harris, Adelaide.

khoury, J. (). *Matrices-Application to Cryptography.* Available: http://aix1.uottawa.ca/~jkhoury/cryptography.htm. Last accessed 5/14/2012.

Decoding Instructions

The four matrices shown have undergone encryption by being cipher shifted, and then scrambled using matrix multiplication to conceal the true message.

781562613339570354329011560267360333632019369646564774044753

Danny Aburas

To decode the message, the last step performed to encode this message must be performed first. The last process performed to the matrices was multiplication with a scramble matrix.

A is the original code.
X is the scramble matrix
B is the scrambled code matrix.

Using matrix algebra, it can be seen that the original code matrix, A, can be obtained by multiplying the scrambled matrix, B, by the inverse of the scramble matrix used, X^{-1}.

$AX=B$
$AXX^{-1}=BX^{-1}$.
$AI=BX^{-1}$.
$A=BX^{-1}$

To simplify things a little, the inverse of the scramble matrix is provided instead of giving the scramble matrix and having the inverse found by the reader as this could help prevent errors.

The inverse of the scramble matrix is given. This is the key to decoding the code.

X^{-1}= 1-619-59-531-9930813-82264-824-59373-12033759

1. **Multiply each of the four encrypted matrices above with X^{-1} (given above).** graphic calculator should be used for this multiplication process. This process should result in with four packets of data that have been decoded.

2. Even though the code has been decoded, the elements in the matrix code are cipher shifted and the process must be reversed. The following algorithm was used to cipher shift the elements of the matrices: $3x + 6 = C$,
where x is the original element value, and C is the cipher shifted value. The original value can be obtained by algebraically rearranging the cypher shift equation, using algebraic methods, to: $C - 63 = x$. **Apply this algorithim to <u>each element</u> in the four matrices obtained in the previous step by inputing each element to the placeholder C and replace each value with X value obtained.**

3. **Using the set of matrices obtained in the last step, starting with the first matrix, read the elements of each matrix systematically from top to bottom and list them in a line from right to left**

4. **The alpha numeric code is provided bellow, to read this message, just replace each of the numbers with the corresponding letters of the alphabet. HAVE FUN!**

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

Decoding.

Danny Aburas

Using the decoding instructions, the code was decoded by a member of the class, Jordan Maguire.