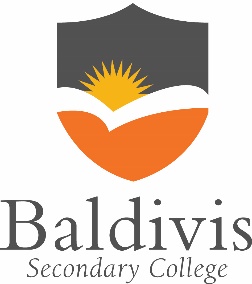
**Mathematics Specialist Unit 2**

# 2021 Investigation 3

 **Encryption using matrices**

**Weigthing 7% Due Date:** Thursday 10th September

The concepts and skills included in this investigation relate to the following dot points within the WA Mathematics Specialist syllabus:

2.2.1 apply matrix definition and notation

2.2.2 define and use addition and subtraction of matrices, scalar multiplication, matrix multiplication, multiplicative identity, and inverse

2.2.3 calculate the determinant and inverse of 2 × 2 matrices and solve matrix equations of the form *AX* = *B*, where *A* is a 2 × 2 matrix and *X* and *B* are column vectors

Security of information is of major interest to many corporations, and governments throughout the world, especially with respect to the military and economic information. You may be aware of security on your wireless connection where all transmissions are encrypted.

Many different ciphers have been developed over the years such as Four Square, Bifid, Trifid, Playfair and Hill to name a few.

The Playfair cipher was developed in 1854 by Charles Wheatstone but promoted by Lord Playfair after who it was named. The Playfair cipher is a symmetric encryption technique. It encodes pairs of characters (digraphs) using a 5 by 5 table and a set of 4 simple rules that are based on symmetry and the location of the digraphs within the table. The Playfair cipher was popularised in 2007 in the movie “National Treasure 2 - *The Book of Secrets*”. The Playfair cipher is no longer considered useful by military organisations due to the ease and speed in which it can be decoded by modern computers.

The Hill cipher was invented in 1929 by Lester S. Hill and was based on the principles of linear algebra.

In this. You will use the principals modelled to design and use your own encryption key. **It will be important to note the limitations of the simplified method of encryption.**

Matrix multiplication encryption steps are still used today in combination with nonlinear encryption steps to create secure ciphers.

This task has been split into 2 sections.

**Part A** is practice only. You may use the ideas and working you do in Part A as the mathematical working to support your submission for Part B. You should use Part A to investigate the method of coding you will use in the report you write for Part B.

**Part B** is a report to a company for which you have been asked to develop a method of encoding short SMS messages. Your response to Part B must be written as a report.

**Part A: Thinking about matrix coding**

**ENCODING**

Step 1: Character – Number encoding

Each character is encoded as a number.

*Table 1: Alpha numeric code*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| 0 | 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 |

e.g. the word ***code*** could be written as ***2, 14, 3, 4***

Step 2: Choice of an encryption matrix (also called the key)

e.g. Encryption matrix A =

Step 3: Write the message in a form that can be encrypted.

In this case 2 rows are needed, or a series of 2 x 2 matrices.

Matrix M = or we could have used

M =

The encryption matrix does not have to be a 2 x 2 matrix. One is used here for illustration purposes only.

Step 4: Encode the message using matrix addition

e.g. A+M =

Think about the way the message has been encoded and the kinds of SMS messages you send. Are extra characters needed (e.g., spaces, full stops, numbers)? Would spaces and full stops help to give away the code?

**SENDING THE MESSAGE**

**SECURITY LEVEL A**

The message could now be sent as a series of numbers. 7, 22, 5, -1

Separate to this, the code and instructions for decoding could be sent to the intended recipient.

For instance, in this case, we could send the instructions:

* Convert the series of numbers to a 2 x 2 matrix using the first half of the numbers for row 1 and the second half of the numbers for row 2
* Subtract the matrix
* Use Table 1 to convert your resulting numbers back to letters.

**SECURITY LEVEL B**

For greater security, the numbers could now be re-coded as letters. Before we can do this, the numbers must be converted to a number between 0 and 25 using Modulus 26 mathematics.

**Modulus 26 mathematics**

To understand mod 26 maths, consider the following.

As we have 26 characters a result not in the range 0 to 25 would be meaningless, mod 26 arithmetic keeps all results within our desired range. If a result lies outside of this range we just add or subtract multiples of 26 until the remainder is within our specified range.

e.g.. 30 (mod 26) = 30 – (1x26) = 4 and -59 (mod 26) = -59 + (3 x26) = 19

The coded matrix above would become

and the encoded message would become ***HWFZ***

Again instructions for decoding this message would now be sent to the recipient separately.

For instance, in this case, we could send the instructions:

* Use Table 1 to convert the message to a series of numbers
* Write the numbers in two rows, using the first half of them for the top row and the second half for the bottom row. Fill any remaining spaces with a zero.
* Subtract the matrix
* Use mod 26 maths to convert the elements of this product to numbers between 0 and 25.
* Decode the letters using Table 1.

**Are there other ways to use matrices?**

Could you send longer messages using matrix addition?

Show how matrix **multiplication** can be used to encode a message.

Develop your own coding system for encoding letters to numbers.

The encoding matrix should not be limited to a 2 x 2 matrix.

Not all matrices will work as encoding and decoding matrices. Find at least one example of a matrix that does not work.

Try to find out which of the encoding matrices don’t work for **both levels** of security. What is important when choosing an encoding matrix?

Practise coding and decoding at least one message using both levels of security and writing instructions that someone else can follow to use your coding and decoding method.

**Get someone else in the class to use your method to decode a message you have sent them.** In an appendix at the end of your report, acknowledge the person who helped you to refine your instructions.

**INTERNET RESEARCH**

Conduct some research into an aspect of cryptology and cyphers. Some suggestions for areas include:

* Banking details
* Emails
* Types of encoding

Try to find out how some methods of encryption work and in what sort of environment they might be used.

Think about whether or not they might be suitable to encrypt SMS messages sent from a mobile phone and why this would be so.

**Part B: The Task**

You have been tasked with writing a report on encrypting short messages that are to be sent between separate offices of your company by SMS texts. There is some concern that the messages will be intercepted by competitors. As the messages are so short and on their own may not provide the competitors with vital information, they may be encrypted with relatively low security such as is provided by the above encryption methods. Your report

should contain the following features:

* An introduction to the task
* A short summary one of the different types of encryption in use today.
* A **brief** indication of why these current methods are unsuited to a small enterprise requiring only low level security.
* An explanation of your proposal for encoding and decoding messages **for each of security levels A and B as described above.**
* A worked example of the encoding and decoding of a short message (10 – 20 characters) using **two** methods ***similar to*** Security Level A and Security Level B described above**.   
  You may not use the encoding method used in the example for part A.**
* An explanation of any difficulties that might be encountered when using either method.
* A recommendation of the method you would choose with explanation of why you recommended it.
* An appendix to your report acknowledging the help of the person who helped you to refine your instructions.

**The format of the investigation report must be a typed report to include double spacing and 12 point font, but hand written calculations can be embeded into the document. Reports should be submitted electronically via Connect.**

# Appendix 1 – Grade descriptions Year 11

|  |  |
| --- | --- |
| **A** | **Identifies and organises relevant information**  Identifies and organises relevant information from complex sources, for example descriptive passages, labelled diagrams or tables of data. Recognises various vector and trigonometric functions and their domain and range. Identifies key elements in ambiguous data, such as how the domain of an angle affects the sign of the trigonometric ratios. Identifies key information from scattered sources such as interpreting the physical contexts involving combinations or permutations and solving related problems. |
| **Chooses effective models and methods and carries the methods through correctly**  Chooses and uses the correct technique or model in unpractised situations. Carries deductive reasoning and extended responses through clearly. Simplifies complicated fractions and works efficiently with algebraic expressions in fraction form. Translates fluently between representations, such as geometric vector diagrams to algebraic expressions. Uses a calculator appropriately for calculation, algebra and graphing, and highlights less obvious features of graphs, such as asymptotes or end points. |
| **Follows mathematical conventions and attends to accuracy**  Uses correct notation with vectors, matrices, combinatorics and complex numbers. Defines variables and parameters to suit the context. Draws clear geometric and vector diagrams with appropriate scales and labels. Works well with exact values such as surds, radian values or factorial notation, and recognises the difference between open and closed intervals. Uses appropriate logical operators and geometric notation when setting out geometric proofs. |
| **Links mathematical results to data and contexts to reach reasonable conclusions**  Pays attention to units in all tasks, giving answers to the correct degree of accuracy, and uses radian measure when appropriate. Takes account of the domain with time as the independent variable defined in vector problems, or by the context of the question, and excludes any results outside the domain. |
| **Communicates mathematical reasoning, results and conclusions**  Shows the main steps in mathematical reasoning in a logical sequence. Sets out geometric proofs in a logical and clear manner. Draws diagrams and defines appropriate vertices and angles to use in the working of a problem. Relates the result of a problem to the context of the question by using the correct units and any related notation, such as vector notation. |

|  |  |
| --- | --- |
| **B** | **Identifies and organises relevant information**  Identifies and organises relevant information from concentrated or scattered sources. Draws and labels diagrams from written instructions. Identifies key elements in ambiguous data, for example distinguishing the time required as the time of day rather than the time elapsed. |
| **Chooses effective models and methods and carries the methods through correctly**  Carries deductive reasoning and extended responses through and applies various rules, for example the Distributive Law or Commutative Law to simplify vector dot products. Generalises mathematical structures when determining the transformational effects of the parameters *a*, *b*, *c* and *d*, in trigonometric equations, for example,. Moves between representations in unpractised ways, such as drawing vectors in the Cartesian plane to determine the resultant. Converts multi-dimensional units such as kilometres per hour to meters per second. Uses a calculator appropriately for vectors, geometry and graphing and pays attention to features of graphs, such as amplitude and phase shift. Carries through accurately with vector algebra. |
| **Follows mathematical conventions and attends to accuracy.**  Rounds to suit contexts, specified accuracies and boundary values on occasions, for example rounds  3.70 hours to 3 hours 42 minutes (i.e. to the nearest minute). Takes note of the laws used when dealing with matrix algebra. Interprets the information on diagrams by using the various geometric symbols such as parallel lines or congruent sides. |
| **Links mathematical results to data and contexts to reach reasonable conclusions**  Attends to units in extended tasks, such as determining the distance travelled in a set time given the vector equation of motion. Can switch logical statements, for example to their converse or contrapositive. |
| **Communicates mathematical reasoning, results and conclusions**  Shows main steps in reasoning when setting out a geometric proof. Identifies the period and scale factor of a tangent graph  from a given graph. |
| **C** | **Identifies and organises relevant information**  Identifies and organises relevant information that is relatively narrow in scope, for example, uses the information in diagrams supplied with the problem. Identifies the correct trigonometric formulas in straightforward situations. Writes the component form of vectors from a Cartesian diagram. |
| **Chooses effective models and methods and carries the methods through correctly**  Answers structured questions that require short responses, such as solving simple vector diagrams or composing functions. Makes common sense connections in practical diagrams involving navigation or simple bearings. Translates between representations in practised ways, for example matches trigonometric graphs to their stated equation, draws vector diagrams on a Cartesian plane from a given simple component form. Uses a calculator appropriately for calculation, combinatorics or straightforward graphing. Shows basic features on sketches of graphs located using a calculator. |
| **Follows mathematical conventions and attends to accuracy**  Defines introduced variables, for example, labels a diagram and allocates a variable to the length of an unknown side or the size of angle. Applies conventions for diagrams and graphs by labelling points with upper case letters, for example A, B and using arrows to convey the direction of a vector. Rounds to suit contexts and specified accuracies in short responses, for example, rounding angles to the nearest degree in navigation problems. |
| **Links mathematical results to data and contexts to reach reasonable conclusions**  Recognises specified conditions in short responses and includes the SI units with an answer when required, for example, velocity (ms-1) x time (s) = distance (m). Attends to radian measure or degrees as is appropriate in trigonometry problems. |
| **Communicates mathematical reasoning, results and conclusions**  Shows working and sets out algebraic solutions correctly in short response questions. Makes clear sketches of simple functions, including some detail. Draws simple diagrams to help with solving problems of space and measurement. |

|  |  |
| --- | --- |
| **D** | **Identifies and organises relevant information**  Identifies and organises relevant information that is narrow in scope. Converts degrees to radians and vice versa. |
| **Chooses effective models and methods and carries the methods through correctly**  Answers familiar, structured questions that require short responses, for example locating the intersection of two graphs. Reads the components of vectors from a diagram. Applies mathematics in practised ways to calculate magnitude of vectors. Simplifies fractions such as . |
| **Follows mathematical conventions and attends to accuracy**  Applies conventions for graphs to label axes, set up a scale, and label different graphs on the same axes with some errors. Rounds to suit contexts and specified accuracies in short responses, such as rounding to a stated degree of accuracy, for example *x* = 30.86 km(two decimal places). |
| **Links mathematical results to data and contexts to reach reasonable conclusions**  Does not recognise specified conditions to identify the need to give exact value answers with conversions of radian measure to degrees. Attends to units in short responses when prompted, for example, the unit measure when calculating the magnitude of a vector. |
| **Communicates mathematical reasoning, results and conclusions**  Uses correct vector notation most of the time. Expresses the component parts **i** and **j** of a vector during calculations and in manipulations of terms or expressions. Obeys conventions for vector diagrams. Labels simple geometry diagrams and expands combination and permutation expressions with some errors. |

|  |  |
| --- | --- |
| **E** | Does not meet the requirements of a D grade and/or has completed insufficient assessment tasks to be assigned a higher grade. |