KNOX
GRAMMAR
SCHOOL

STATE

DA VINCI DECATHLON 2022

CELEBRATING THE ACADEMIC GIFTS OF STUDENTS IN YEARS 7 & 8

CODE-BREAKING

TEAM NUMBER _____

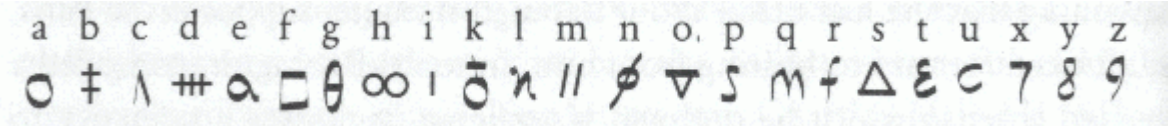
1	2	3	Total	Rank
/15	/15	/20	/50	

QUESTION 1

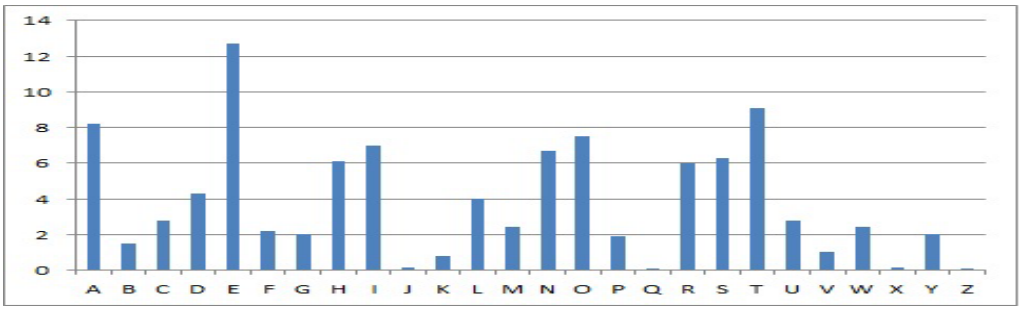
CRYPTOGRAPHY AND ITS PATTERNS 15 MARKS

Cryptography is full of patterns. Patterns are evident in code-making and code-breaking. Patterns must be used as a means of encryption and the detection of patterns can be useful in the decryption of ciphers.

It is time now to recreate history and explore some patterns already broken. In the 16th century during what has come to be known as the *Babington Plot* Mary Queen of Scots had her plans foiled by the expertise of the codebreakers in Queen Elizabeth's palace. The following was the cipher used by Mary:



At face value it might seem as if the code is unbreakable given that there are random characters used to make up the letters, however a rather simple tool was used by Elizabeth's code breakers to crack the cipher known as ***Frequency Analysis***



1) Given the above table outline what frequency analysis is and how it was used to break Mary's cipher.

4 MARKS

Answer	

The simple substitution cipher was quickly broken due to frequency analysis, or the analysis of patterns. Ciphers are constantly under attack from codebreakers once a pattern is identified it becomes the cipher's weakness.

2) Decode the following ciphers and identify the pattern that allowed you to do so.

a.

W a p t e n d y u e ?
h t a t r s o o s e

3 MARKS

Answer	

b. Key Word: CHANGE

DOW NFN YOU NGAFPDGR TDFS?

4 MARKS

Answer	

c. Key: 18

QGM ZSNW VGFW OWDD LG YWL LZAK XSJ

4 MARKS

Answer	

QUESTION 2

PATTERNS AND LANGUAGE 15 MARKS

In 1822 the Rosetta stone was translated which gave unprecedented insight into the workings of the Egyptian Hieroglyphic language. This was only achieved through the recognition of patterns. The Rosetta stone featured a section in Ancient Greek, a long since understood language which enabled a reading into the hieroglyphs.

In 2022 we have contacted a small civilisation in an undiscovered Mediterranean island. To best understand their culture, we first need to understand their language. From their writing and limited interactions, we know they write using a variation of the Latin alphabet as well as a few simple words.

Much like German and French the language uses gendered articles but there seems to be no discernible way of figuring out the message. Below are the words we know:

I – ce

You – de

He – cë

She – cé

The - ke

Woman – é Larnya

Man – ë Gramma

Ocean – Wammy

Oceans – Wammye

Swim – Wamlon

Paper – Mira

Papers - Mirae

Write – Mirlon

Train – Zud

Trains – Zude

Law – Goyo

Laws – Goyoe

Tren – with

1) There are believed to be discernible patterns present in the limited amount of language that we understand. Given the two below sentences

   Cë Wamlën tren kë Wammy

   Cé Mirlén tren ké Mira

   What seems to be the rule regarding the way sentences are formed and using this rule write a sentence with a translation?

5 MARKS

Answer	

2) While it appeared that the plural of words was done merely by adding an e onto the end of the word i.e., Book would be **Stal** and its plural Books would be **Stale**, however the following sentence

   Da Stala tran secta

   Which we believe means ‘Your books are old’ does not conform to this rule. Why?

3 MARKS

Answer	

3) Given the current rules are dominated so heavily by the genderisation of phrases create a rule for the past tense of this language, write two sentences using that rule

7 MARKS

Answer	

QUESTION 3

THE DATA MATRIX 20 MARKS

With the advent of the modern computing age, data protection has become increasingly reliant on multi-step encryption as a means of ensuring data can change hands safely and securely. This has meant an uptake in the use of mathematics in cryptography. While more complex in theory once a pattern to encoding messages becomes clear, an individual can encrypt and decrypt at will.

Data matrices are an example of the use of mathematics in modern cryptography.

We first convert the secret message into a string of numbers by arbitrarily assigning a number to each letter of the message. Next, we convert this string of numbers into a new set of numbers by multiplying the string by a square matrix of our choice that has an inverse. This new set of numbers represents the coded message.

To decode the message, we take the string of coded numbers and multiply it by the inverse of the matrix to get the original string of numbers. Finally, by associating the numbers with their corresponding letters, we obtain the original message.

In Question 3 A to Z will correspond to the numbers 1 to 26, a space is represented by the number 27, and punctuation is ignored.

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

An example of encoding using a data Matrix for the message: CHARGE

Here we use the matrix A = $\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$ this is known as the data matrix key.

The first step is dividing the numbers into groups of 2

CH AR GE

Then numbers are assigned to the letters and converted into 2 x 1 matrices (as the original is a 4 x 2)

$\begin{bmatrix} C \\ H \end{bmatrix} = \begin{bmatrix} 19 \\ 27 \end{bmatrix}$ etc

To encode the 2x1 is then multiplied by the original matrix A

$$\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 8 \end{bmatrix} = \begin{bmatrix} 19 \\ 27 \end{bmatrix}$$

This is what CH is encoded as, this is repeated for each pair of letters

1) Using the same data matrix key encode the message ATTACK NOW (note spaces are coded as 27 they come after Z)

5 MARKS

Answer	

2) A message has now been encrypted using the data matrix A.

$$\begin{bmatrix}21\\26\end{bmatrix}\begin{bmatrix}37\\53\end{bmatrix}\begin{bmatrix}45\\54\end{bmatrix}\begin{bmatrix}74\\101\end{bmatrix}\begin{bmatrix}53\\69\end{bmatrix}$$

In order for this to be decoded the inverse of matrix A must be applied thus using

$A^{-1} = \begin{bmatrix}3 & -2\\-1 & 1\end{bmatrix}$ decode the message (here 27 will be used again for spaces)

5 MARKS

Answer	

3) Now using matrix B $\begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix}$ encode a 12-character message of your choice showing all relevant working, note this is now a 3x3 matrix.

10 MARKS

Answer	

END OF PAPER

KNOX
GRAMMAR
SCHOOL

STATE

DA VINCI DECATHLON 2022

CELEBRATING THE ACADEMIC GIFTS OF STUDENTS IN YEARS 7 & 8

CODE-BREAKING SOLUTIONS

TEAM NUMBER _____

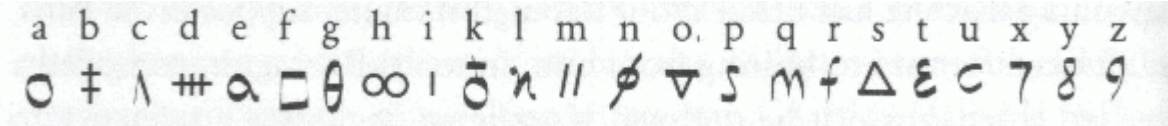
1	2	3	Total	Rank
/15	/15	/20	/50	

QUESTION 1

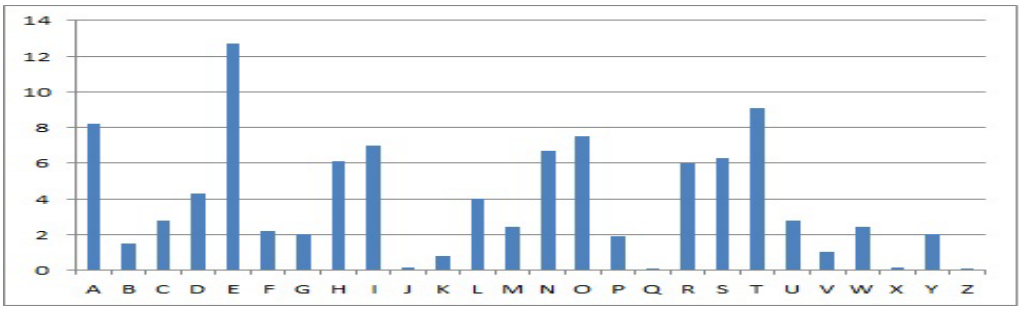
CRYPTOGRAPHY AND ITS PATTERNS 15 MARKS

Cryptography is full of patterns. Patterns are evident in code-making and code-breaking. Patterns must be used as a means of encryption and the detection of patterns can be useful in the decryption of ciphers.

It is time now to recreate history and explore some patterns already broken. In the 16th century during what has come to be known as the *Babington Plot* Mary Queen of Scots had her plans foiled by the expertise of the codebreakers in Queen Elizabeth's palace. The following was the cipher used by Mary:



At face value it might seem as if the code is unbreakable given that there are random characters used to make up the letters, however a rather simple tool was used by Elizabeth's code breakers to crack the cipher known as ***Frequency Analysis***



1) Given the above table outline what frequency analysis is and how it was used to break Mary's cipher. (4 Marks)

Answer	The table shows the average frequency of letters in words (1 mark). So the letter 'e' is the most commonly used in the English alphabet, appearing around 12.6% of times in messages (1 mark). We can use this information to help us break a code given by a Monoalphabetic substitution cipher. This works because if "e" has been encrypted to a square (as done in the above cipher) then every"square" was an "e". Hence, the most common letter in the cipher should be "square". (2 Marks)

The simple substitution cipher was quickly broken due to frequency analysis, or the analysis of patterns. Ciphers are constantly under attack from codebreakers once a pattern is identified it becomes the cipher's weakness.

1) Decode the following ciphers and identify the pattern that allowed you to do so.

a. (3 Marks)

W a p t e n d y u e ?
h t a t r s o o s e

Answer	What patterns do you see (2 marks) Identifies as a rail fence cipher (1 Mark)

b. (4 Marks) Key Word: CHANGE

DOW NFN YOU NGAFPDGR TDFS?

Answer	How did you decipher this? (2 Marks) Identifies this as a key word cipher using CHANGE to form the ciphertext

c. (4 Marks) Key: 18

QGM ZSNW VGFW OWDD LG YWL LZAK XSJ

Answer	You have done well to get this far. (2 Marks) Identifies as a Caesar cipher with 18 shifts (2 Marks)

QUESTION 2

PATTERNS AND LANGUAGE

In 1822 the Rosetta stone was translated which gave unprecedented insight into the workings of the Egyptian Hieroglyphic language. This was only achieved through the recognition of patterns. The Rosetta stone featured a section in Ancient Greek a long since understood language which enabled a reading into the hieroglyphs.

In 2022 we have made contact with a small civilisation in an undiscovered Mediterranean island. In order to best understand their culture, we first need to understand their language. From their writing and limited interactions, we know they write using a variation of the Latin alphabet as well as a few simple words.

Much like German and French the language seems to use gendered articles but there seems to be no discernible way of figuring out what's what. Below are the words we know:

I – ce

You – de

He – cë

She – cé

The - ke

Woman – é Larnya

Man – ë Gramma

Ocean – Wammy

Oceans – Wammye

Swim – Wamlon

Paper – Mira

Papers - Mirae

Write – Mirlon

Train – Zud

Trains – Zude

Law – Goyo

Laws – Goyoe

Tren – with

1) There are believed to be discernible patterns present in the limited amount of language that we understand. Given the two below sentences

   Cë Wamlën tren kë Wammy

   Cé Mirlén tren ké Mira

   What seems to be the rule regarding the way sentences are formed and using this rule write a sentence with a translation? (5 Marks)

Answer	3 Marks – Verbs and their conjugations are formed based on whether the object of the sentence is male or female. 2 Marks any new sentence that is correct in its conjugation if they use feminine then 'e' must have an accent and an umlaut for male. I.e Cë Mirlën Goyoe – He writes laws

2) While it appeared that the plural of words was done merely by adding an e onto the end of the word i.e., Book would be **Stal** and its plural Books would be **Stale**, however the following sentence

   Da Stala tran secta

   Which we believe means 'Your books are old' does not conform to this rule. Why? (3 Marks)

Answer	2 Marks: Notes that before sentences were formed off of whether the object was a male or femle i.e. he or she. 2 Marks: Identifies and elaborates on how in this sentence the object is a thing (genderless) meaning that it cannot be conjugated that same was as in the previous question. 1 Mark: Identifies that a is used in place of e when there is no gender

3) Given the current rules are dominated so heavily by the genderisation of phrases create a rule for the past tense of this language, write two sentences using that rule (7 marks)

Answer	Designed to test the ingenuity of students: Award 3 Marks for creating a rule that makes sense and can be used to turn any of the above phrases into the past tense. Given the explanation satisfies a coherent past sentence structure award the three marks 2 Marks – Per sentence written that conforms to their created past tense.

QUESTION 3

THE DATA MATRIX 20 MARKS

With the advent of the modern computing age data protection has become increasingly reliant on multi-step encryption as a means of ensuring data can change hands safely and securely. This has meant an uptake in the use of mathematics in cryptography. While more complex in theory once a theory is understood a pattern to encoding messages becomes clear meaning that individual can encrypt and decrypt at will.

Data matrices are an example of the use of mathematics in modern cryptography the use of which is relatively simple:

We first convert the secret message into a string of numbers by arbitrarily assigning a number to each letter of the message. Next, we convert this string of numbers into a new set of numbers by multiplying the string by a square matrix of our choice that has an inverse. This new set of numbers represents the coded message.

To decode the message, we take the string of coded numbers and multiply it by the inverse of the matrix to get the original string of numbers. Finally, by associating the numbers with their corresponding letters, we obtain the original message.

In Question 3 A to Z will correspond to the numbers 1 to 26, a space is represented by the number 27, and punctuation is ignored.

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

An example of encoding using a data Matrix for the message: CHARGE

Here we use the matrix A = $\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$ this is known as the data matrix key.

The first step is dividing the numbers into groups of 2

CH AR GE

Then numbers are assigned to the letters and converted into 2 x 1 matrices (as the original is a 4 x 2)

$\begin{bmatrix} C \\ H \end{bmatrix} = \begin{bmatrix} 19 \\ 27 \end{bmatrix}$ etc

To encode the 2x1 is then multiplied by the original matrix A

$$\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 3 \\ 8 \end{bmatrix} = \begin{bmatrix} 19 \\ 27 \end{bmatrix}$$

This is what CH is encoded as, this is repeated for each pair of letters

1) Using the same data matrix key encode the message ATTACK NOW (5 Marks) (note spaces are coded as 27 they come after Z)

Answer

$$\begin{bmatrix}41\\61\end{bmatrix}\begin{bmatrix}22\\23\end{bmatrix}\begin{bmatrix}25\\36\end{bmatrix}\begin{bmatrix}55\\69\end{bmatrix}\begin{bmatrix}61\\84\end{bmatrix}$$

3 Marks awarded for the correct answer

1 mark awarded for showing knowledge of converting letters into unmultiplied data matrices i.e., AT becomes $\begin{bmatrix}1\\20\end{bmatrix}$

1 mark awarded for working regarding the multiplication of data matrices

AT becomes $\begin{bmatrix}(1x1)+(1x2)=3\\(20x1)+(20x3)=80\end{bmatrix}$

2) A message has now been encrypted using the data matrix A.

$$\begin{bmatrix}21\\26\end{bmatrix}\begin{bmatrix}37\\53\end{bmatrix}\begin{bmatrix}45\\54\end{bmatrix}\begin{bmatrix}74\\101\end{bmatrix}\begin{bmatrix}53\\69\end{bmatrix}$$

In order for this to be decoded the inverse of matrix A must be applied thus using

$A^{-1} = \begin{bmatrix}3 & -2\\-1 & 1\end{bmatrix}$ decode the message (here 27 will be used again for spaces) (5 Marks)

Answer

2 Marks awarded for identifying that the encoded message must be multiplied by the inverse data matrix i.e.

$\begin{bmatrix}21\\26\end{bmatrix} x \begin{bmatrix}3 & -2\\-1 & 1\end{bmatrix} = \begin{bmatrix}11\\5\end{bmatrix}$

Original matrices found 1 mark $\begin{bmatrix}11\\5\end{bmatrix}\begin{bmatrix}5\\16\end{bmatrix}\begin{bmatrix}27\\9\end{bmatrix}\begin{bmatrix}20\\27\end{bmatrix}\begin{bmatrix}21\\16\end{bmatrix}$

Message: Keep it up (2 Marks)

3) Now using matrix B $\begin{bmatrix}1 & 1 & -1\\1 & 0 & 1\\2 & 1 & 1\end{bmatrix}$ encode a 12-character message of your choice showing all relevant working, note this is now a 3x3 matrix. (10 Marks)

Answer	1 Mark: Creates a 12-character message (Can include spaces) i.e. Please Leave 3 Marks – Identifies that unlike a 2x2 a 3x3 requires letters to be split into groups of three. I.e. PLE / ASE / -LE / AVE 2 Marks – Encodes these based on the numeric letters to numbers system used in the previous two question eg. A=1 2 Marks – Places each set of now encoded numbers into a 3x1 matrix and multiplies each 3x1 with the 3x3 provided 2 Marks- Final answer properly encoded (markers will need to check the multiplication of student's matrices to confirm).