KNOX
GRAMMAR
SCHOOL

STATE

DA VINCI DECATHLON 2021

CELEBRATING THE ACADEMIC GIFTS OF STUDENTS IN YEARS 7 & 8

Code Breaking

TEAM NUMBER _____

1	2	3	Total
/28	/27	/25	/80

PART 1

SPINNING WHEELS

Tom works as part of the travelling carnival group and as the youngest member, he is in charge of cleaning all of the spinning wheels and clocks. He has noticed that people no longer seem to play the spinning wheel so using these and the large clocks he has devised a new game.

Using these items, he has devised a more intellectually challenging game where the player's success is predicated more on their code-breaking ability as opposed to luck and chance.

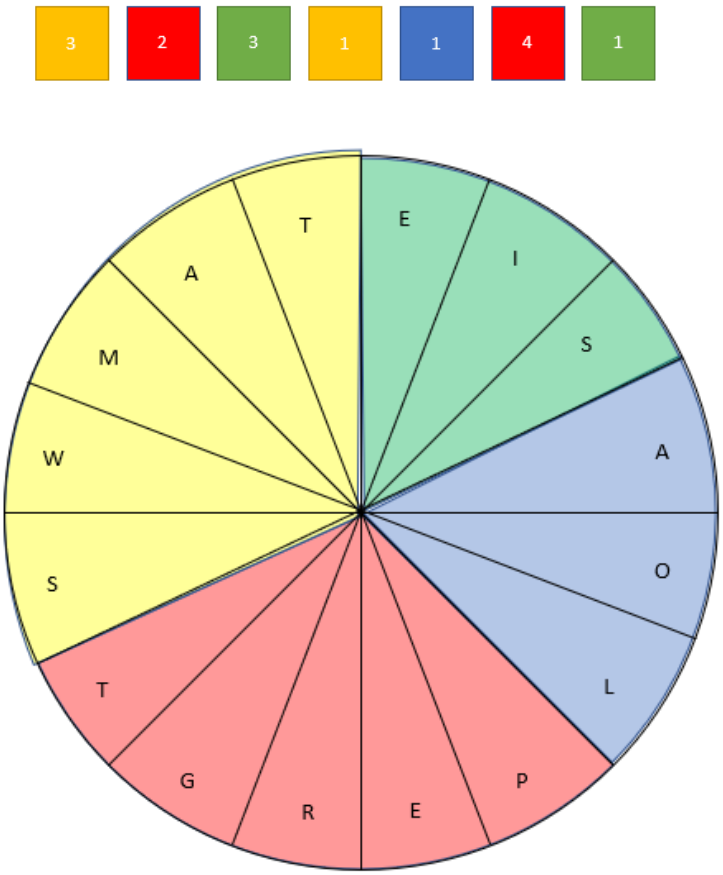
For a player to win they must be able to fill in the blanks of the following sentence where each blank word is encoded within one of the wheels/clocks below:

When you find the _____ wait for exactly one _____ it may seem _____ but the aim is for you to learn how to _____ well!

Note the encrypted message is above the clock/wheel for all the blanks

NOTE: Only your work in the answer boxes (orange/white) will be marked.

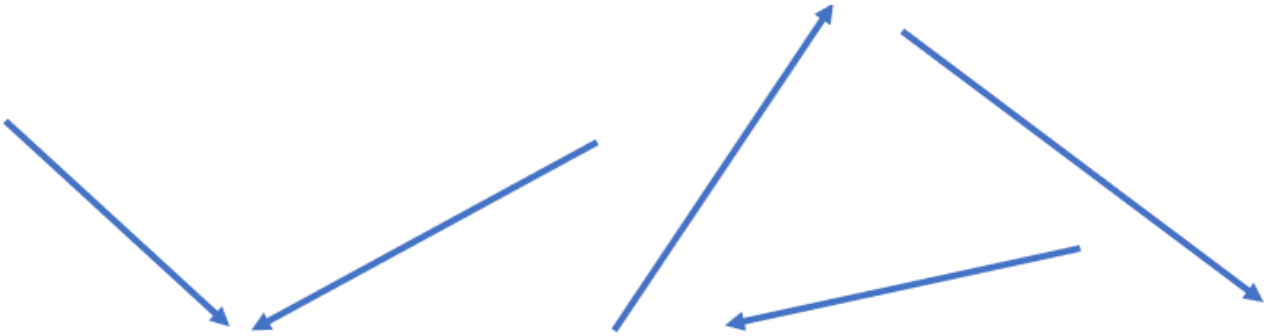
BLANK 1

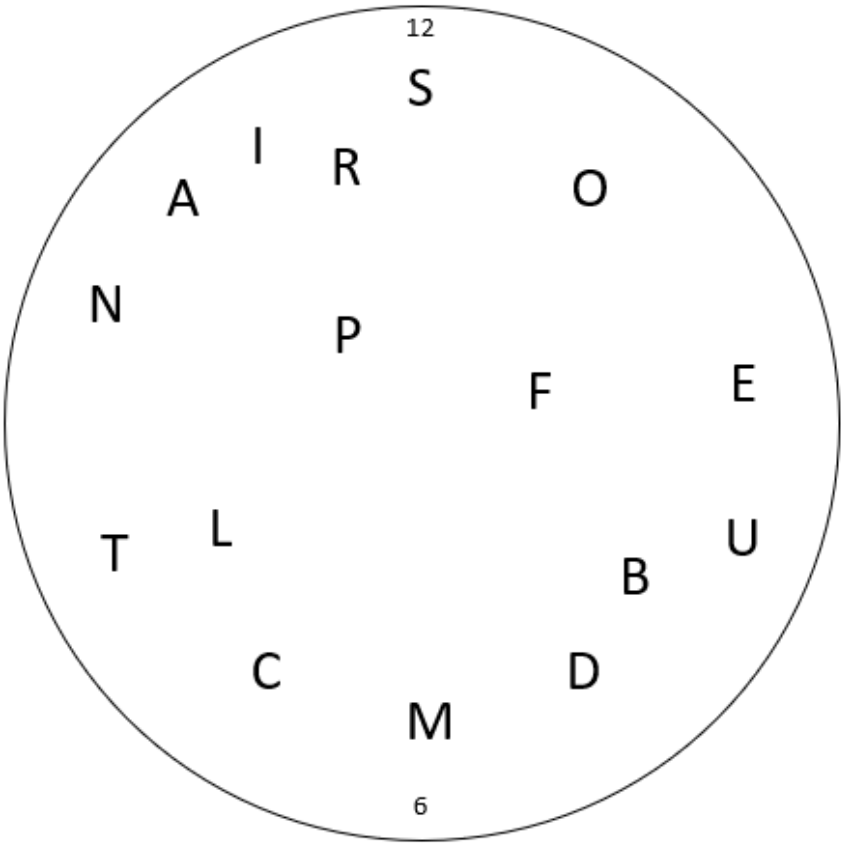


Encryption	

BLANK 2

Start this question at 12pm

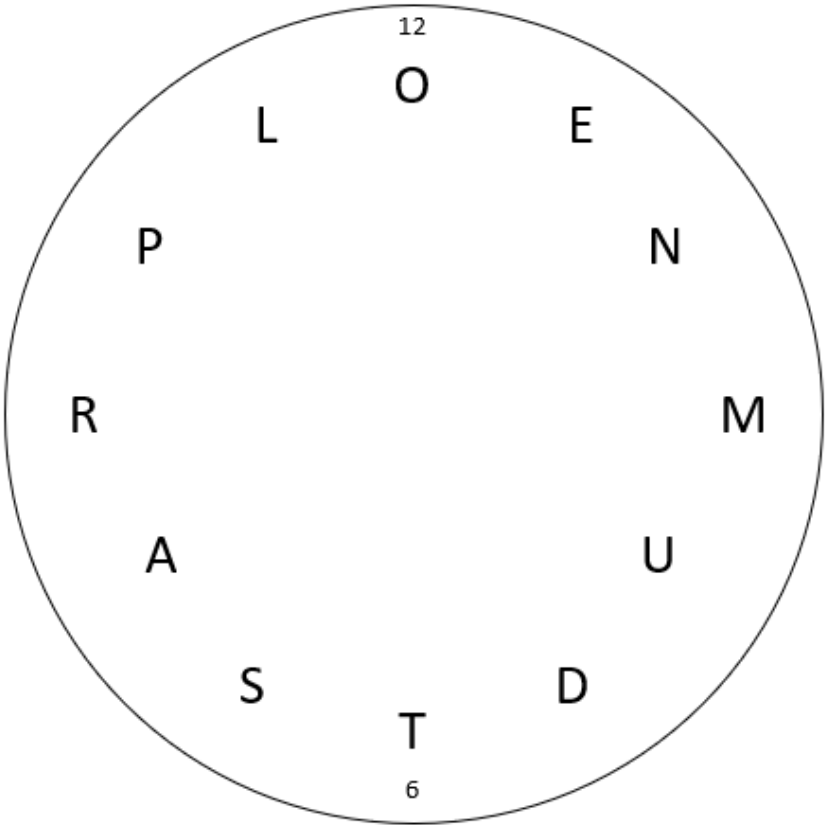




Encryption	

BLANK 3

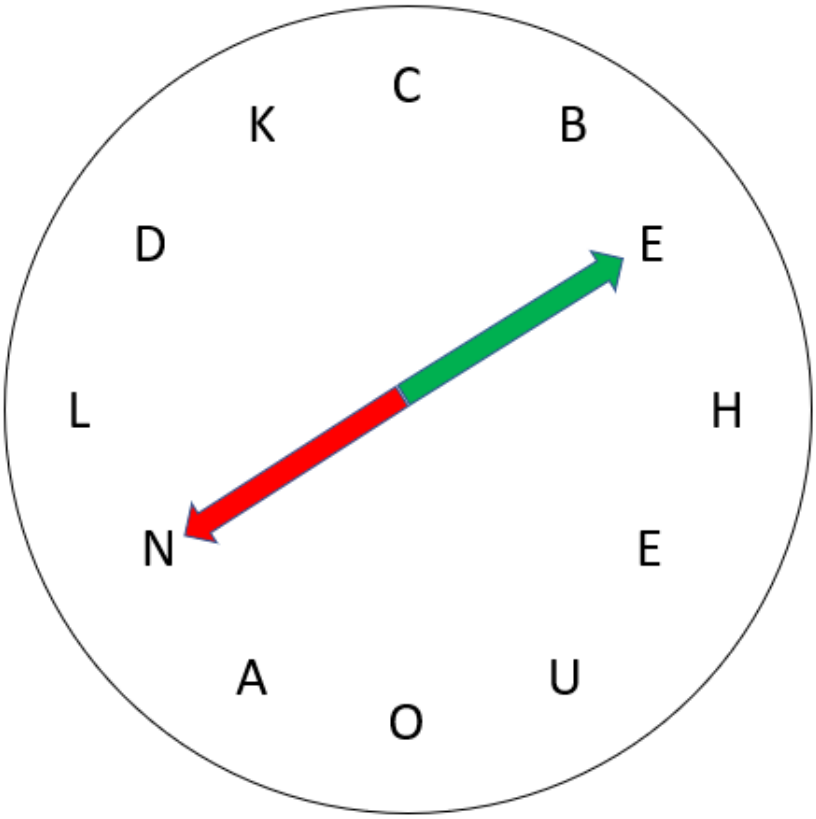
45′ – 40′ – 10′ – 25′ – 00′ – 15′



Encryption	

BLANK 4

When you're driving the lights FIRST turn green and SECOND turn red. Once you pass the first set of lights, make two equal turns left.



Encryption	

PART 2

PRNG: PSUEDO RANDOM NUMBER GENERATORS

Chance and probability are powerful notions when it comes to the realms of cryptography and the encoding of data and messages. Ultimately the best form of encoding is that which is random since inherent to the notion of randomness is an inability to precisely predict outcomes and be able to intercept and decode data. One such tool that can be applied, especially in the realms of computer science, is the use of random number generators (or in this case pseudo).

In a simplistic way we can consider a computer and the way it encodes/processes information to be in three parts. An input signal/information flows through an algorithm, which then produces an output.

PRNG 1 – RANDOMISED INPUT (3 MARKS)

One way of generating 'random' outputs is through randomising the input. A common method to achieve this is through the use of sensors that collect external data such as:

- Light intensity
- Sound
- Humidity
- Photoreception

Obviously since these environmental factors are random then the input data is also random and, therefore, the output should be random.

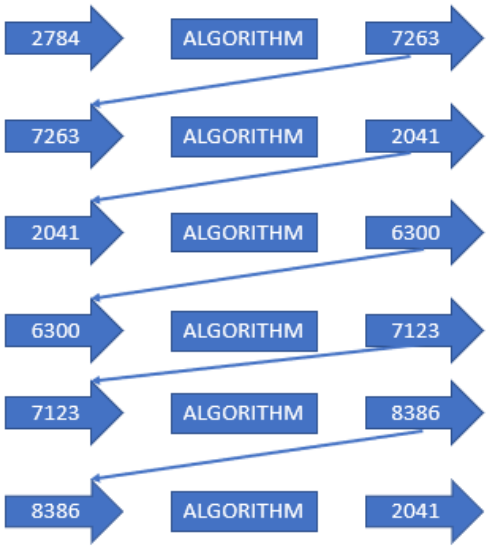
- Is the output completely random because the input is random?

Is it completely random? (Y/N) (1 mark)	
Explain your answer (2 marks)	

PRNG 2 - ITERATIVE SEED RANDOM NUMBER GENERATOR (4 MARKS)

For this style of PRNG the output number is used as the input/seed for the subsequent stage.

Briefly explain the problem with the example given below (answers longer than 3 sentences won't be marked):



Explanation of the problem:

PREM – PSUEDO RANDOM ENCODING MODEL INSPIRED ENCODING

PREM is a form of random data encryption, which uses different and often adjacent data values in the encryption process.

Assume the following matrix $\boldsymbol{B}$ of binary data is to be encoded representing a 16 bit block

The input data matrix **B**

Columns correspond to i

Rows correspond to j	1	2	3	4
1	1	0	1	1
2	0	1	1	0
3	1	0	0	0
4	0	1	0	0

For the context of this question subscript 'i' refers to the column index and subscript 'j' refers to the row index (as alluded to above) (e.g.$b_{3,2} = 1$)

Additionally, we will define:

$$a \oplus b$$

As a binary function with inputs a,b which are either 0 or 1, with outputs:

$$true = 1$$
$$false = 0$$

The function requires two inputs, if they are both the same it has an output of 1 (true) and if they differ then it has an output of 0 (false) ~~0 (+) 0 = 1~~

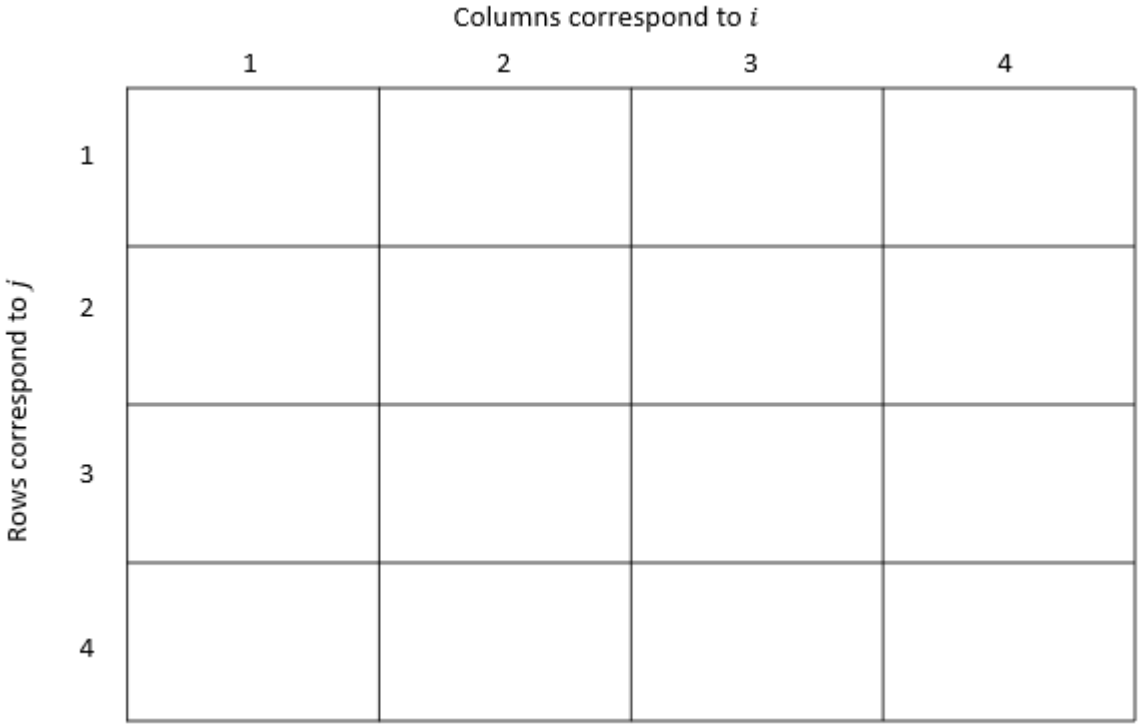
e.g.

$$1 \oplus 1 = 1$$
$$0 \oplus 1 = 0$$
$$0 \oplus 0 = 1$$

ENCODING 1 (7 MARKS)

Your task is to encode the previous data matrix $\boldsymbol{B}$ into a new encoded matrix $\boldsymbol{P1}$ according to the following cipher.

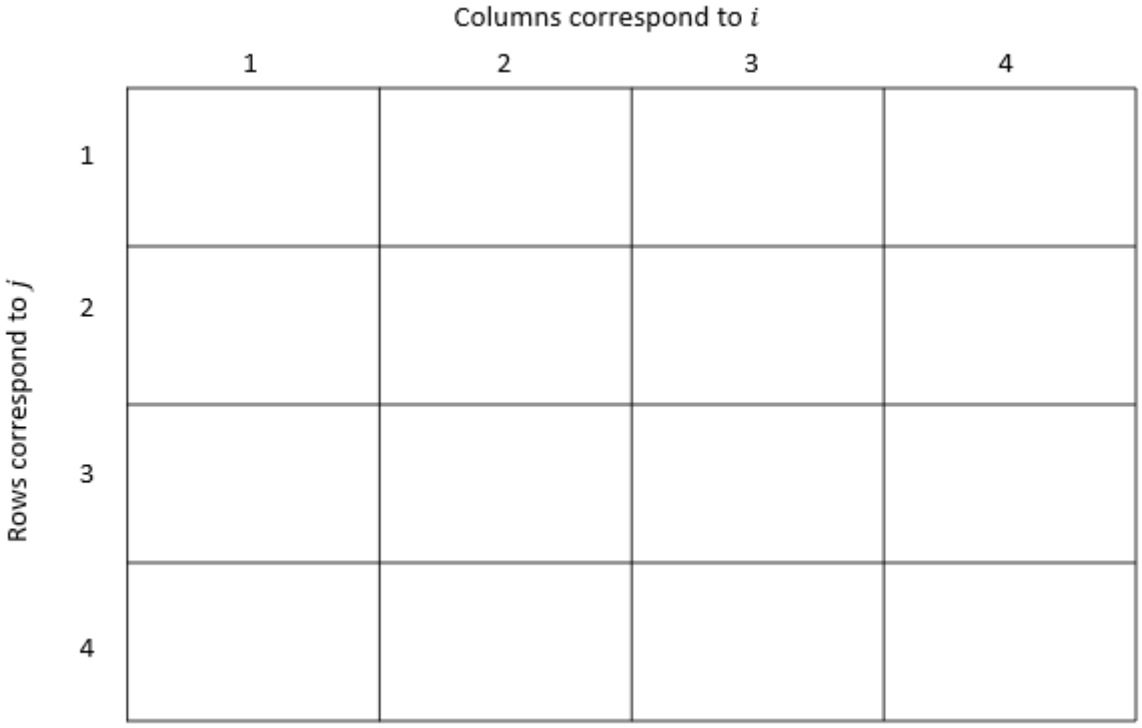
$$\boldsymbol{P1}: P_{i,j} = \begin{cases} b_{i,j} \oplus b_{i,j+1}, & j \in [1,2,3] \\ b_{i,j} \oplus b_{i,j-2}, & j = 4 \end{cases}$$



ENCODING 2 (5 MARKS)

With the same initial data matrix $\boldsymbol{B}$ encode into a new matrix $\boldsymbol{P2}$ according to the following cipher.
Hint: Consider why this specific cipher is inherently flawed!

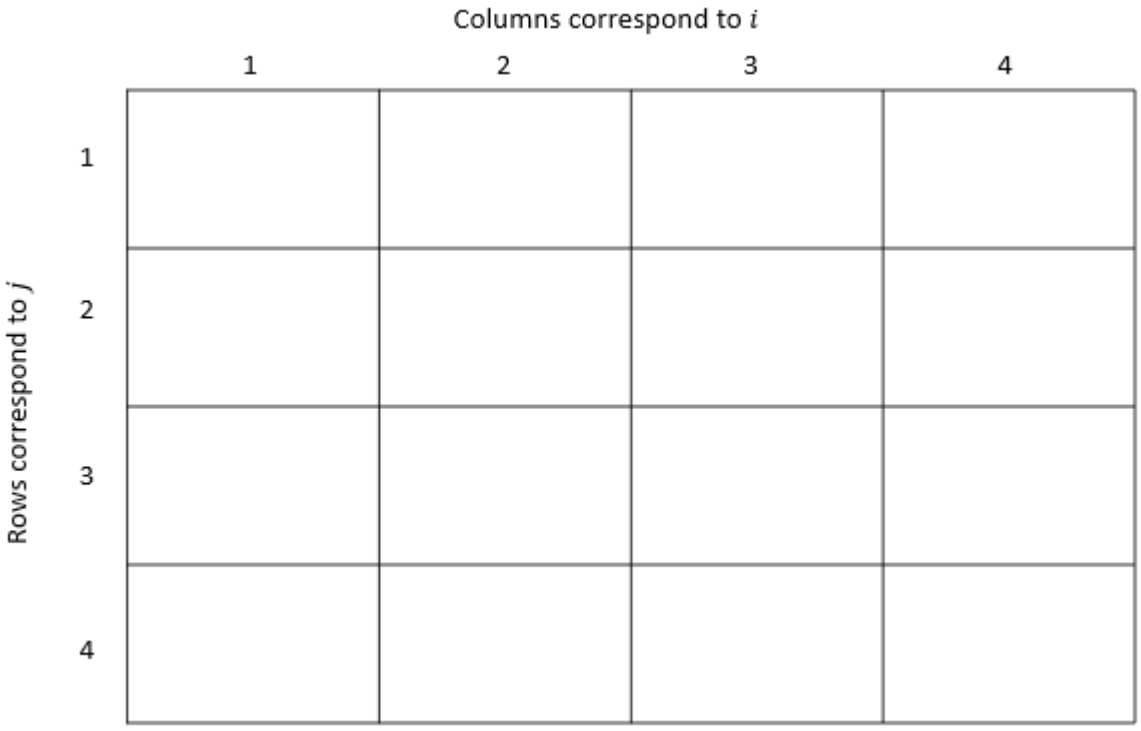
$$\boldsymbol{P2}: P_{i,j} = \begin{cases} (b_{i,j} \oplus b_{i,j+1}) \oplus p_{i,j}, & j \in [1,2,3] \\ (b_{i,j} \oplus b_{i,j-2}) \oplus p_{i,j}, & j = 4 \end{cases}$$



ENCODING 3 (8 MARKS)

Encode the original data matrix $\boldsymbol{B}$ into a new matrix $\boldsymbol{P3}$ according to the following cipher:

$$\boldsymbol{P2}: P_{i,j} = \begin{cases} \left(b_{i,j} \oplus b_{i,j+1}\right) \oplus b_{i+3,j} & i = 1 \\ & j \in [1,2,3] \\ \blacksquare & \\ \left(b_{i,j} \oplus b_{i,j+1}\right) \oplus b_{i-1,j}, & i \in [2,3,4] \\ & j \in [1,2,3] \\ \blacksquare & \\ \left(b_{i,j} \oplus b_{i,j-2}\right) \oplus b_{i-1,j}, & i \in [2,3,4] \\ & j = 4 \\ \blacksquare & \\ \left(b_{i,j} \oplus b_{i,j-2}\right) \oplus b_{1,1} & i = 1 \\ & j = 4 \end{cases}$$



PART 3

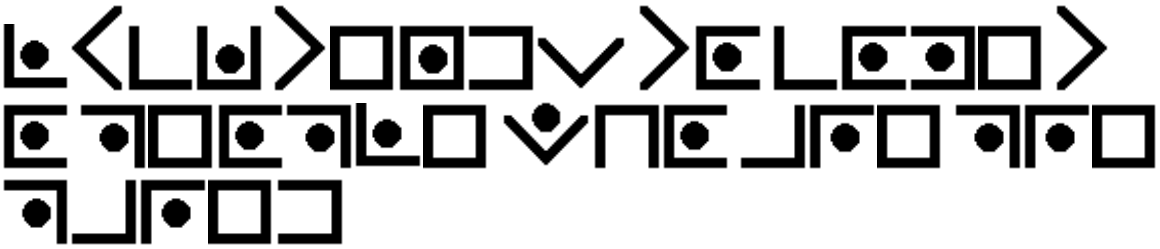
DECIPHER THE QUOTES:

QUOTE 1:

ZKHQ LW FRPHV WR OXFN PDNH BRXU RZQ – Bruce Springsteen

Encryption	

QUOTE 2:



- Colin Powell

Encryption	

QUOTE 3:

India Whiskey India Lima Lima Papa Romeo Echo Papa Alpha Romeo Echo Alpa November Delta Sierra Oscar Mike Echo Delta Alpha Yankee Mike Yankee Charlie Hotel Alpha November Charlie Echo Whiskey India Lima Lima Charlie Oscar Mike Echo – Abraham Lincoln

Encryption	

QUOTE 4:

os ylrettu ta ecnairav si ynitsed htiw lla eht elttil snalp fo nem – H.G. Wells

Encryption	

QUOTE 5:

The grid is given as an aid to help with the decoding of the cipher.

PHLAC RULTE INEV DGVA EEER ARRI NWBA DIEN – Jonathan Swift

Encryption	