KNOX GRAMMAR SCHOOL

STATE

DA VINCI DECATHLON 2021

CELEBRATING THE ACADEMIC GIFTS OF STUDENTS IN YEARS 7 & 8

Code Breaking - ANSWERS

TEAM NUMBER _____

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

PART 1

SPINNING WHEELS (7 MARKS EACH)

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's 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.

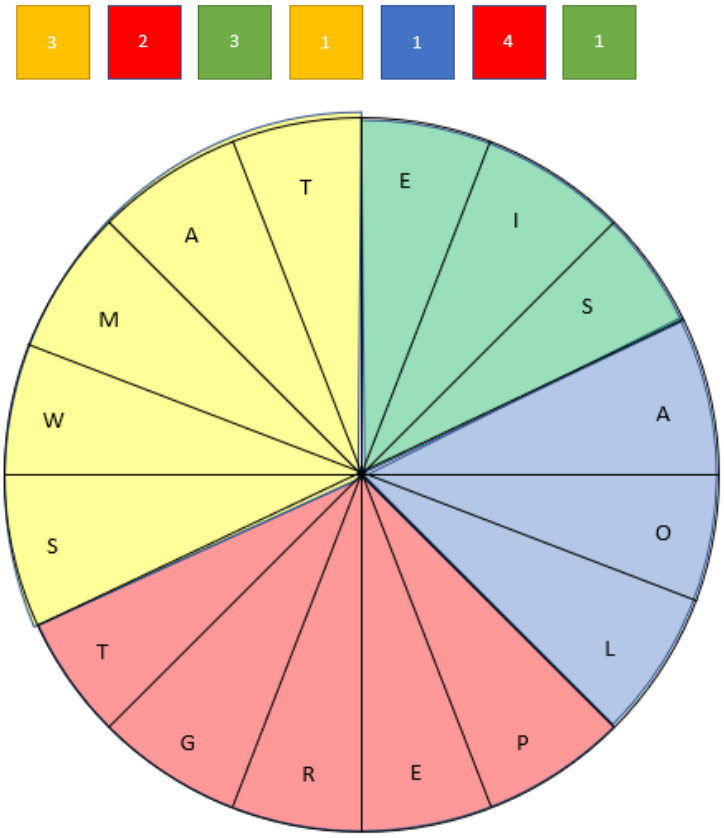
For a player to win they must be able to fill in the blanks of the following sentence where each blank word is encoded within one of the wheels/clocks below:

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

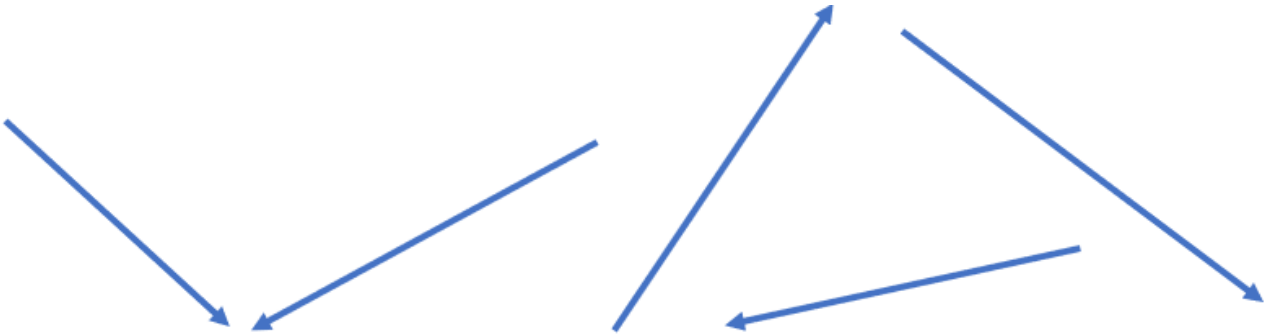


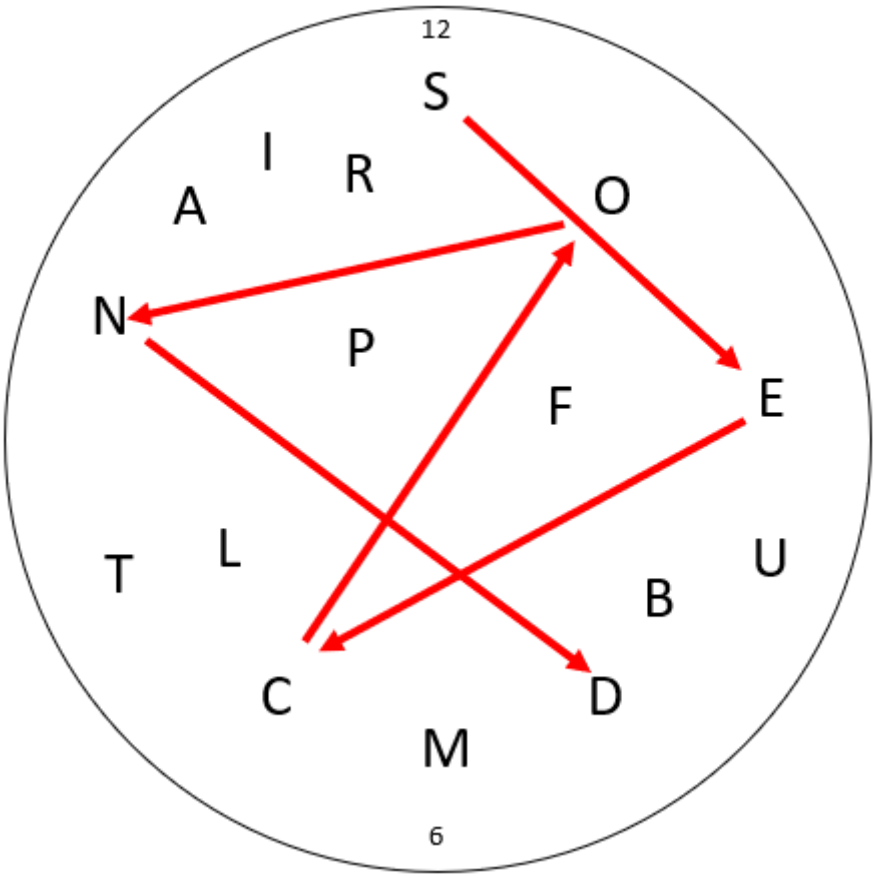
Encryption	MESSAGE

The box colour denotes which section of the spinning wheel and the number within the box denotes which specific bay/letter when going clockwise. E.g. the first letter is in the yellow section, then we move three bays in the clockwise direction and arrive at the letter M.

BLANK 2

Start this question at 12 O'clock



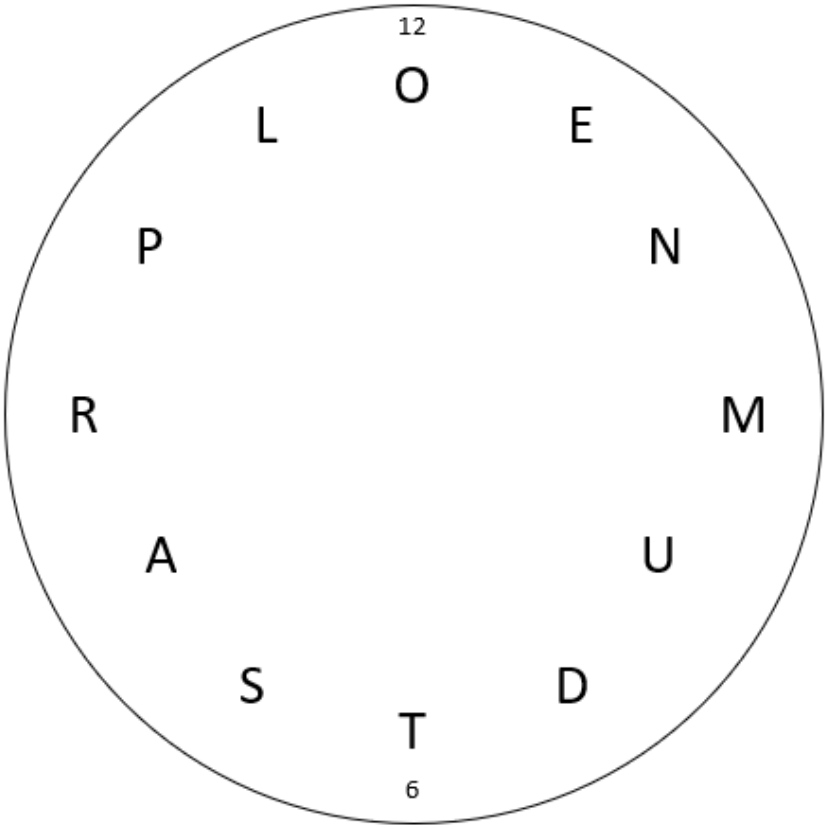


Overlay the arrows on the clock face with the first arrow starting at 12 O'clock.

Encryption	SECOND

BLANK 3

45’ – 40’ – 10’ – 25’ – 00’ – 15’

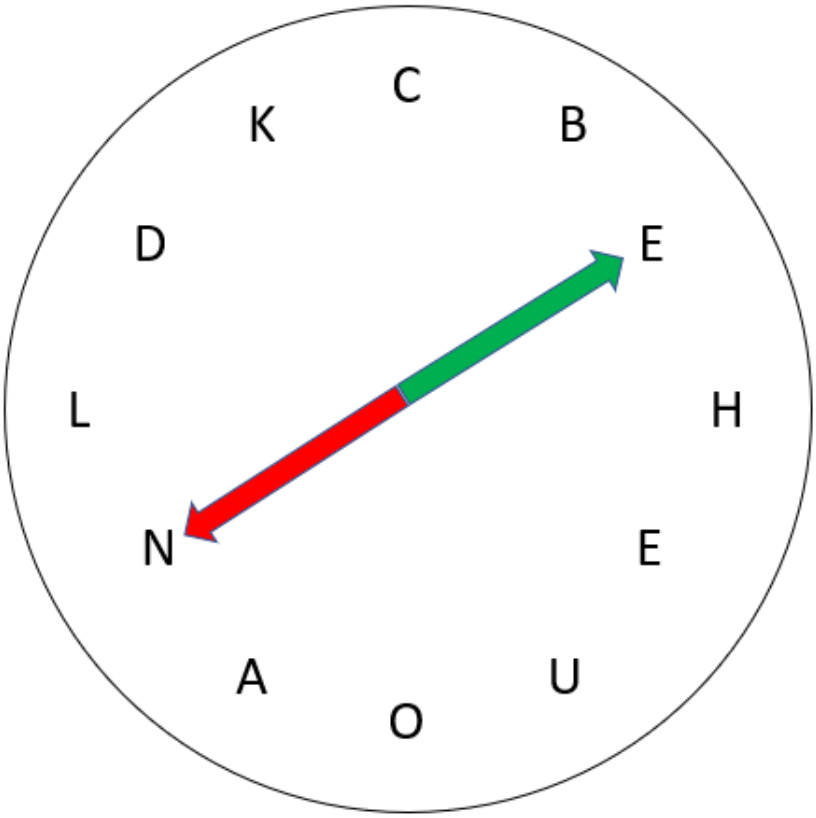


The word is encrypted as minutes. i.e. the first letter is 45’ so this would correspond to R.

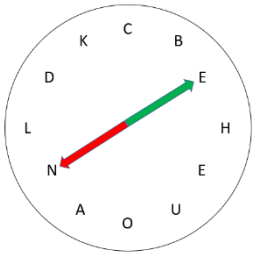
Encryption	RANDOM

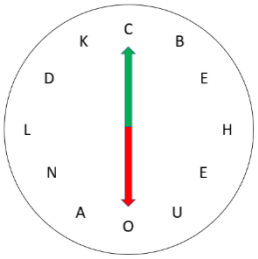
BLANK 4

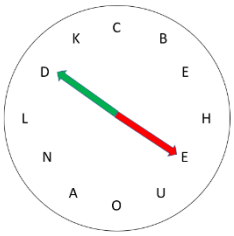
When you're driving the lights FIRST turn green and SECOND turn red. Once you pass the first set of lights, make two equal turns left.



The starting point is given to the students. We first read the green arrow (E) and then the Red (N) (as per the instructions). Then turn the arrows 2 letters counter clockwise (relative to the green arrow). Now the green arrow points at (C) and the red at (O) and again repeat once more and thus two equal turns have been made.







Encryption	ENCODE

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 are 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?

NO! if the same input is provided then the output will be the same also due to the fact the algorithm does not actually change.

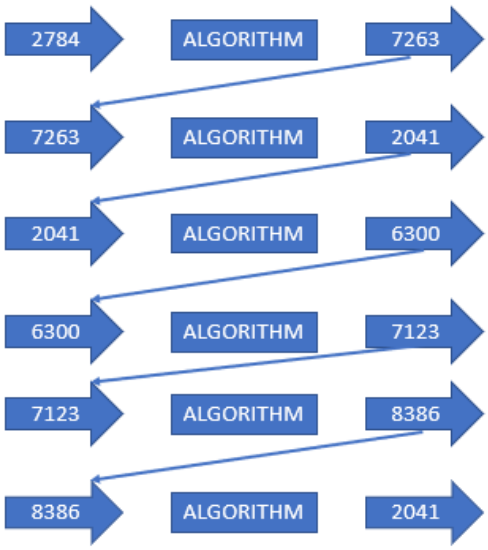
In order to have a changing algorithm this also needs an algorithm of its own and, therefore, that secondary algorithm would also be fixed, meaning that we again don't achieve absolute randomness. (Note this second line is not needed but is used as justification in the case students say that assuming the algorithm evolves/changes.)

Is it completely random? (Y/N) (1 mark)	NO
Explain your answer (2 marks)	Award marks for any mention of the fact that the algorithm doesn't change. i.e. if the same input is provided the output is the same … thus not random.

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!):



The last iteration produces an output of 2041, which has already occurred. This will result in an inescapable loop occurring and, thus, undermines the whole point of a random number generator since the outputs are no longer random but rather pre-determined.

Award marks for any mention of a loop occurring.

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**

Rows correspond to j \ Columns correspond to i	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.

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

Columns correspond to i

Rows correspond to j

	1	2	3	4
1	0	0	1	0
2	0	0	0	1
3	0	0	1	1
4	1	1	0	1

Deduct one mark for every mistake.

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!
NOTE:$p1_{i,j}$ refers to an element within the $\boldsymbol{P1}$ matrix (the one you just completed), however you can still complete this part if you haven't done the above question.

$$\boldsymbol{P2}: P_{i,j} = \begin{cases} (b_{i,j} \oplus b_{i,j+1}) \oplus p1_{i,j}, & j \in [1,2,3] \\ (b_{i,j} \oplus b_{i,j-2}) \oplus p1_{i,j}, & j = 4 \end{cases}$$

Columns correspond to i

Rows correspond to j

	1	2	3	4
1	1	1	1	1
2	1	1	1	1
3	1	1	1	1
4	1	1	1	1

Deduct one mark for every mistake.

ENCODING 3 (8 MARKS)

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

$$\boldsymbol{PP2}: P_{i,j} = \begin{cases} (b_{i,j} \oplus b_{i,j+1}) \oplus b_{i+3,j} & i = 1 \\ & j \in [1,2,3] \\ \blacksquare & \\ (b_{i,j} \oplus b_{i,j+1}) \oplus b_{i-1,j}, & i \in [2,3,4] \\ & j \in [1,2,3] \\ \blacksquare & \\ (b_{i,j} \oplus b_{i,j-2}) \oplus b_{i-1,j}, & i \in [2,3,4] \\ & j = 4 \\ \blacksquare & \\ (b_{i,j} \oplus b_{i,j-2}) \oplus b_{1,1} & i = 1 \\ & j = 4 \end{cases}$$

Columns correspond to i

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

Deduct one mark for every mistake.

PART 3

DECIPHER THE QUOTES: (5 MARKS EACH)

Award 5 marks for complete decryption, award 2 for partial decryption (at markers discretion).

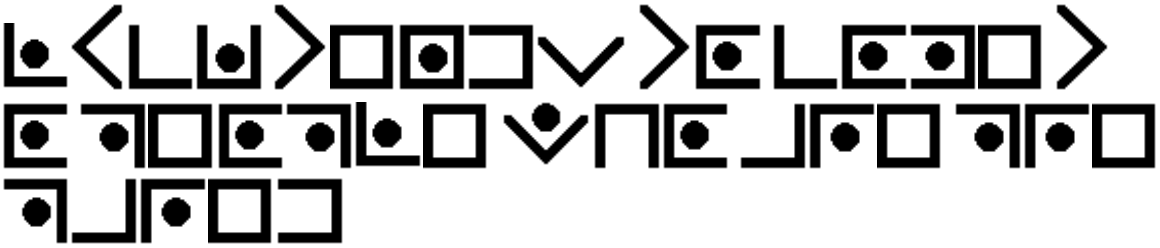
QUOTE 1:

ZKHQ LW FRPHV WR OXFN PDNH BRXU RZQ – Bruce Springsteen

Caesar shift (Shifted 3 units. i.e. a→c etc.)

Encryption	When it comes to luck make your own – Bruce Springsteen

QUOTE 2:



- Colin Powell

Standard pig pen cipher

Encryption	Luck tends to come to people who are prepared – Colin Powell

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

Phonetic Alphabet

Encryption	I will prepare and someday my chance will come – Abraham Lincoln

QUOTE 4:

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

Each word is reversed

Encryption	So utterly at variance is destiny with all the little plans of men – H.G. Wells

QUOTE 5:

PHLAC RULTE INEV DGVA EEER ARRI NWBA DIEN – Jonathan Swift

Block cipher, arrange each 'word' vertically in the grid and then read horizontally.

P	R	I	D	E	A	N	D
H	U	N	G	E	R	W	I
L	L	E	V	E	R	B	E
A	T	V	A	R	I	A	N
C	E						

Encryption	Pride and Hunger will ever be at variance – Jonathan Swift