

Cryptography

Introduction

Note: For a similar workshop, please refer to 'Cryptography', [Maths Sparks Volume I](#).

Cryptography is the art of producing or solving codes and has been used as a method of secure communication since as early as 1900 BCE. Whilst Cryptography initially concerned communication and linguistics, it has become an incredibly important area of mathematics given its roots in number theory and its relevance to internet security. One of the most well-known examples of Cryptography in ancient times was the 'Caesar cipher' which was first developed by Julius Caesar and reportedly used to communicate messages across the Roman Empire. The Caesar cipher is considered one of the most simplistic forms of encryption, given that it uses a substitution technique whereby each letter is replaced by another further on in the alphabet. However, frequency analysis can be used to decipher such codes and it is therefore considered a relatively weak and unreliable method of encryption. This being said, the 'Vigenère cipher', which is a variation of Caesar cipher, is a more secure form of communication given that a keyword is used to encrypt the message and thus each letter has a different shift. The 'Pigpen cipher' is a visual cipher, replacing letters with symbols. It was used throughout the American Civil war, as well as by the Freemasons.

Aim of Workshop

This workshop will introduce students to the basic concepts of Cryptography including ciphers, decrypting codes and the use of *modulo arithmetic* in Cryptography. Students will also be provided with the opportunity to create their own encrypted messages, which they can then give to their classmate to solve.

Learning Outcomes

By the end of this workshop, students will be able to:

- Describe historical decryption strategies
- Explain, in their own words, how modular arithmetic works.
- Encrypt and decrypt coded words using the Caesar, Vigenère and Pigpen ciphers

Materials and Resources

Vigenère grid, Pigpen cipher, encryption wheels, activity sheets, computer (optional)

KEY WORDS

Cipher

A way of making a word or message secret by changing or rearranging the letters in the message.

Shift

A value, X , which causes the letters to move X number of spaces up or down the alphabet line.

Cryptography: Workshop Outline

Suggested Time (Total mins)	Activity	Description
10 mins (00:10)	Introduction to Cryptography	<ul style="list-style-type: none"> · Introduce the concept of Cryptography and outline the history of Cryptography (see Workshop Introduction) · Explain what is meant by the term cipher (see Key Words)
35 mins (00:45)	Activity 1 The Caesar Cipher	<ul style="list-style-type: none"> · Introduce modular arithmetic using the example of a clock and the days of the week (see Appendix – Note 1) · Explain the Caesar cipher and demonstrate how to encrypt and decrypt words (see Appendix – Note 2) · Hand out Activity Sheet 1 and an encryption wheel to each student (Appendix – Note 4) · Activity Sheet 1: Students encrypt and decrypt various messages using the Caesar cipher (see Appendix – Note 3)
25 mins (01:10)	Activity 2 The Vigenère Cipher	<ul style="list-style-type: none"> · Mention that the Vigenère cipher is a variation of the Caesar cipher and explain how it works using an example on the board (see Appendix – Note 5) · Hand out Activity Sheet 2 and the Vigenère table to each student (see Appendix – Note 8) · Activity Sheet 2: Students encrypt and decrypt various messages using the Vigenère cipher (see Appendix – Note 6)
15 mins (01:25)	Activity 3 The Pigpen Cipher	<ul style="list-style-type: none"> · Explain how the Pigpen cipher works (see Appendix – Note 7) · Activity 3: Ask students to encrypt messages using the Pigpen cipher and give it to their partner to solve (see Appendix – Note 9)
15 mins (01:40)	Kahoot Quiz (Optional)	<ul style="list-style-type: none"> · Activity 4: Students answer questions relating to Cryptography using Kahoot (see Sources and Additional Resources for the link and Appendix – Note 10 for solutions)

Note 1: Modular Arithmetic

Modular arithmetic is a system of counting where we cycle back to the start upon reaching a fixed quantity known as the modulus. Once we reach 12 on a clock, for example, we start back at 1. Therefore, 15:00 on a clock corresponds to 3 modulo 12, denoted $3 \pmod{12}$.

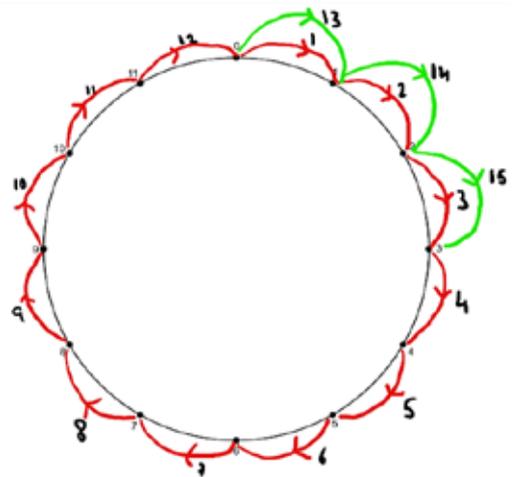
If we are working with mod n , we replace each of the numbers with its remainder when divided by n .

$$15 \equiv 12 + 3 \Rightarrow 15 \equiv 3 \pmod{12}$$

$$27 \equiv 2(12) + 3 \Rightarrow 27 \equiv 3 \pmod{12}$$

$$35 \equiv 2(12) + 11 \Rightarrow 35 \equiv 11 \pmod{12}$$

The same idea applies in Cryptography whereby once the letter Z is reached, we go back to A. This will be demonstrated in the example of Caesar cipher.



Note 2: Caesar Cipher

The Caesar cipher was used by Julius Caesar for military messages. This is a very simple cipher where each letter is shifted forward by a common number of places, known as the shift.

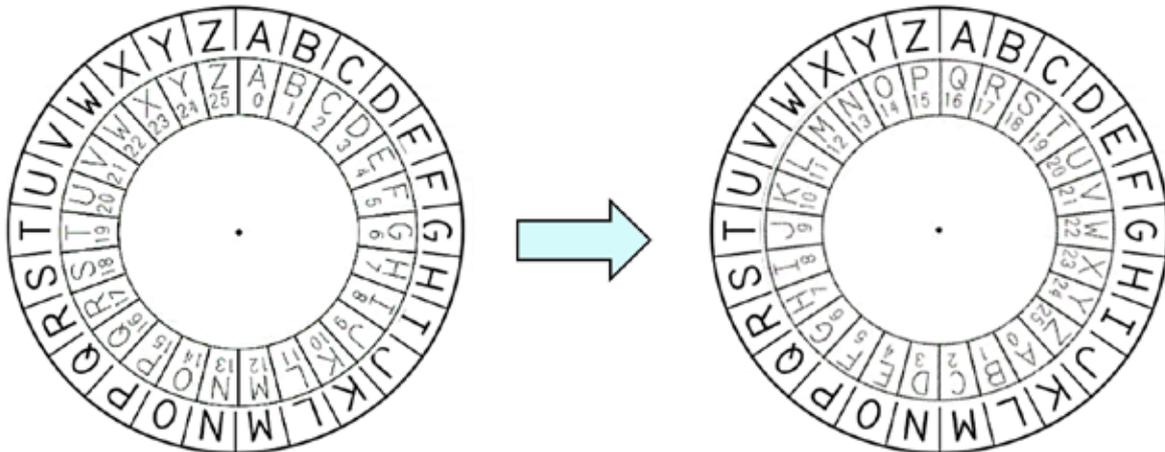
In the following example, we want to encrypt the message "Julius Caesar" using a shift of 10:

1. Write down the message to be coded
2. Fill in the number corresponding to the letter (A = 0 and Z = 25)
3. Add the shift to the numbers corresponding to the letters (which is 10 in this example)
4. Reduce your answer mod 26 (since there are 26 letters in the alphabet)
5. Translate these numbers back to letters to find the encrypted message (i.e. 19 = T etc.)

Original	J	U	L	I	U	S	C	A	E	S	A	R
Place no.	9	20	11	8	20	18	2	0	4	18	0	17
Add Shift	19	30	21	18	30	28	12	10	14	28	10	27
Mod 26	19	4	21	18	4	2	12	10	14	2	10	1
Final	T	E	V	S	E	C	M	K	O	C	K	B

To use an encryption wheel, we start off by aligning the inner and outer wheel. We then move the inner wheel n times, where n is the shift. In the example above, the shift is 10 so we rotate the inner wheel 10 places in a clockwise direction. The outer wheel represents the encrypted letter (e.g. the encrypted letter for A is now K, B is now L etc.)

Note: if students are decrypting a coded message, they use the outer wheel and read the corresponding letter on the inner wheel.



Note 3: Solutions for Activity Sheet 1

Q1. Chris wants to encrypt the phrase "ATTACK AT DAWN" using a Caesar cipher and a shift of 10.

	A	T	T	A	C	K	A	T	D	A	W	N
I	0	19	19	0	2	10	0	19	3	0	22	13
II	10	29	29	10	12	20	10	29	13	10	32	23
III	10	3	3	10	12	20	10	3	13	10	6	23
IV	K	D	D	K	M	U	K	D	N	K	G	X

Encrypted message: KDDKMU KD NKGX

Q2. Sally wants to encrypt the phrase "BRUTE FORCE ATTACK" by a shift of 5.

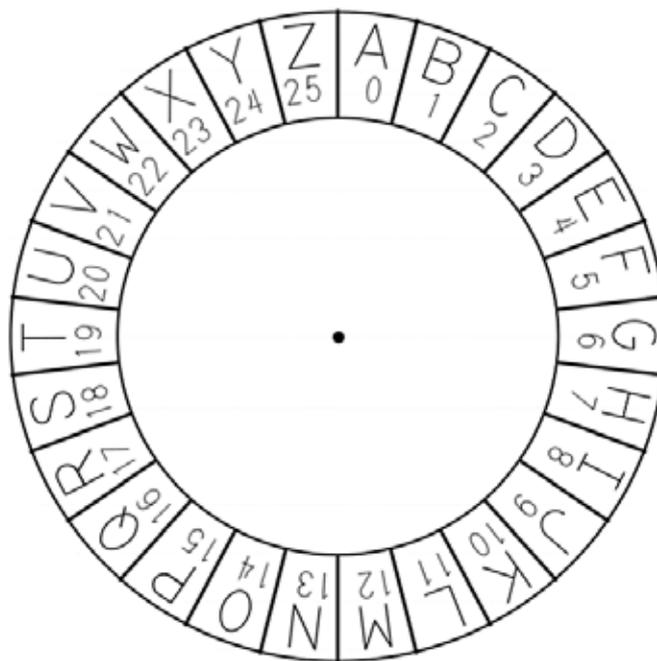
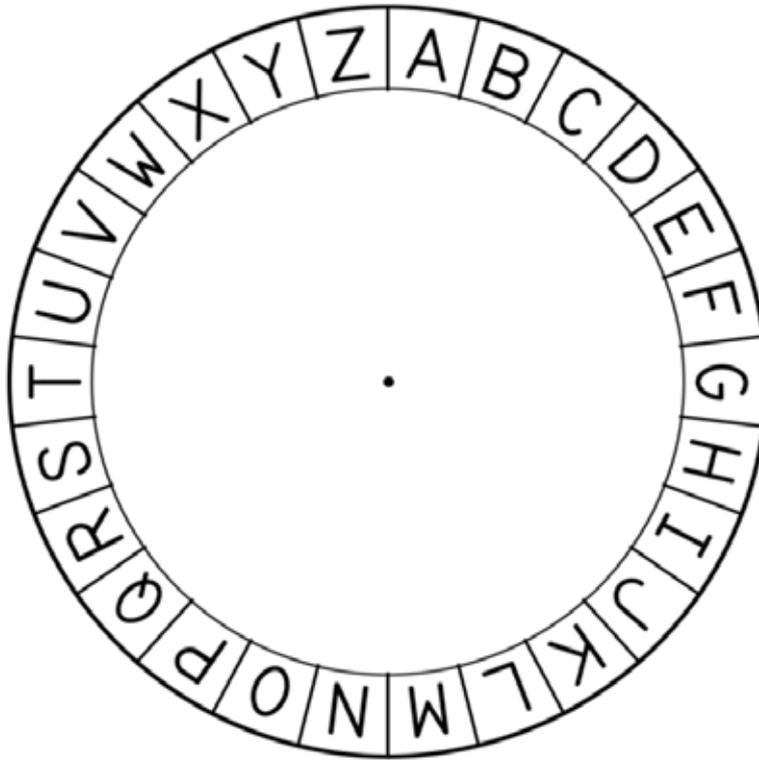
B	R	U	T	E	F	O	R	C	E	A	T	T	A	C	K
G	W	Z	Y	J	K	T	W	H	J	F	Y	Y	F	H	P

Q3. Mohammed wants to decode "VJCQB RB ODW" using a shift of 9. Using your wheel, can you decrypt the message?

V	J	C	Q	B	R	B	O	D	W
M	A	T	H	S	I	S	F	U	N

Decrypted message: Maths is fun

Note 4: Encryption Wheel Template



Note 5: Vigenère Cipher

The Vigenère cipher, also referred to as 'le chiffre indechiffable', is a variation of the Caesar cipher which uses a keyword to encrypt the message and thus, each letter has a different shift. In the following example, we want to encrypt the message: "Vigener" using the keyword "Key":

1. Write down the message to be coded
2. Include the corresponding numbers beside the letters to be coded (A = 0 and Z = 25)
3. Write in the keyword underneath, repeating the keyword if necessary
4. Include the corresponding numbers beside the letters in the keyword (A = 0 and Z = 25)
5. Add the value of the keyword letters to the original letters (each letter will have a different shift)
6. Reduce your answer mod 26
7. Translate these numbers back to letters to find the encrypted message (i.e. 5 = F etc.)

Original	V (21)	I (8)	G (6)	E (4)	N (13)	E (4)	R (17)	E (4)
Keyword	K (10)	E (4)	Y (24)	K (10)	E (4)	Y (24)	K (10)	E (4)
Add Shift	31	12	30	14	17	28	27	8
Mod 26	5	12	4	14	17	2	1	8
Final	F	M	E	O	R	C	B	I

Original	V	I	G	E	N	E	R	E
Keyword	K	E	Y	K	E	Y	K	E
Final	F	M	E	O	R	C	B	I

Alternatively, you can use the Vigenère square to encrypt messages using a keyword:

1. Write down the original message
2. Fill in the keyword underneath
3. Using the Vigenère table, find the first letter of the keyword along the top row (in this case K)
4. Find the letter in this column that is also in the row associated with the corresponding letter of the original phrase (in this case V). This gives us our first encoded letter (i.e. F)
5. Continue for each of the letters in the message.

Keyword

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Original

Note: To decrypt a message, we find the letter of the keyword in the first row and identify the encrypted letter in the same column (in this case F). Now read across to find the original letter.

Note 6: Solutions for Activity 2

Q1. Using the keyword "CIPHER", encrypt the phrase "OVER AND OUT".

	O	V	E	R	A	N	D	O	U	T
I	C	I	P	H	E	R	C	I	P	H
II	Q	D	T	Y	E	E	F	W	J	A

Encrypted message: GWZYJ KTWHJ FYYFHP

Q2. Decrypt the phrase "FIEQ BYOY FROL" using the keyword "MONDAY".

	F	I	E	Q	B	Y	O	Y	F	R	O	L
I	M	O	N	D	A	Y	M	O	N	D	A	Y
II	T	U	R	N	B	A	C	K	S	O	O	N

Decrypted message is: Turn back soon

Q3. Decrypt the phrase "UT BZ JMIGPFS" using the keyword "MATHS".

	U	T	B	Z	J	M	I	G	P	F	S
I	M	A	T	H	S	M	A	T	H	S	M
II	I	T	I	S	R	A	I	N	I	N	G

Decrypted message is: It is raining

Note 7: Pigpen Cipher

In order to encrypt a message using the Pigpen cipher, the alphabet is written in grids as shown below and each letter is then encrypted by replacing it with a symbol that corresponds to the portion of the grid containing the letter (i.e. the borders for each letter).

For example:

A =  E =  Y = 

A	B	C	J	K	L
D	E	F	M	N	O
G	H	I	P	Q	R

The following shows the word "Pigpen cipher" encrypted using the Pigpen cipher:



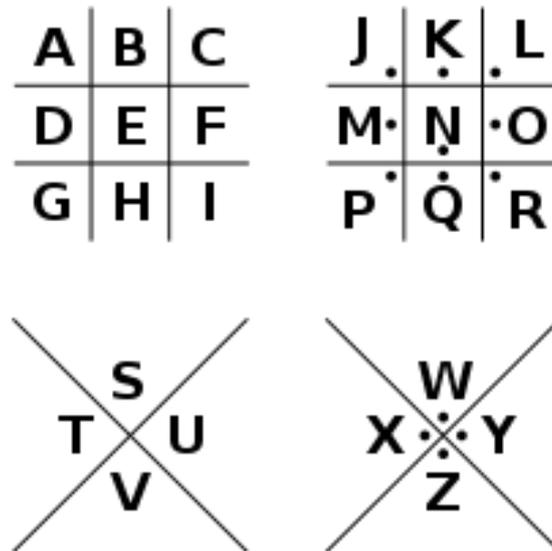
	S	
T		U
	V	

	W	
X		Y
	Z	

Note 8: Vigenère Table Printout

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	D
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	C
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	B
Z	Z	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

Note 9: Pigpen Cipher Printout



Note 10: Solutions for the Kahoot Quiz (link available in additional resources)

Q1. Decode this message using a Caesar cipher (link available in additional resources"=) with a shift of 3: "U JXOHP QEB PMLQ"

X marks the spot

Q2. Using the keyword "KEY" encode this message using the Vigenère cipher: "HEADS UP"

RIYNW SZ

Q3. Which cipher was described as "le chiffre indechiffable"?

The Vigenère cipher

Q4. Encode this message using a Caesar cipher with a shift of 10: "See You Later"

COO IYE VKDOB

Q5. Decode this message using the Pigpen cipher:



Mexican Wave

Cryptography: Activity 1

Q1. Chris decides he wants to encrypt the phrase "ATTACK AT DAWN" using a Caesar cipher and a shift of 10. Follow the steps labelled 1 to 4 below to encrypt this message. One letter has been completed for you.

1. Fill in the numbers corresponding to each letter.
2. Add the shift (here it's 10) to each number.
3. Reduce each number modulo 26.
4. Read off the letters corresponding to the reduced numbers.

	A	T	T	A	C	K	A	T	D	A	W	N
I		19										
II		29										
III		3										
IV		D										

Q2. Sally wants to encrypt the phrase "BRUTE FORCE ATTACK" by a shift of 5.

1. Match the inner and outer wheels to begin (make sure A corresponds to A).
2. Turn the inner wheel clockwise by your shift (in this case 5).
3. For each letter in your message, find it on the inner wheel and write the corresponding letter on the outer wheel in the box below.

B	R	U	T	E	F	O	R	C	E	A	T	T	A	C	K

Q3. Mohammed wants to decode "VJCQB RB ODW" using a shift of 9. Using your wheel, can you decrypt the message?

V	J	C	Q	B	R	B	O	D	W

Cryptography: Activity 2

Q1. Using the keyword "CIPHER", encrypt the phrase "OVER AND OUT" by following the steps below:

- I. Fill in the keyword letter by letter under the phrase, repeating if necessary.
- II. Using the Vigenère table, find the letter where the two letters above meet (for the first letter, for example, we need to find where column O and row C coincide).

	O	V	E	R	A	N	D	O	U	T
I	C	I								
II	Q			Y						

Q2. Decrypt the phrase "FIEQ BYOY FROL" using the keyword "MONDAY" by following the steps below:

- I. Fill in the keyword letter by letter under the phrase, repeating if necessary.
- II. Find the letter of the keyword you are looking for along the top row of the Vigenère table. Then, follow down the column until you find the corresponding letter of the coded phrase. Read across to the first column to find the original letter.

	F	I	E	Q	B	Y	O	Y	F	R	O	L
I	M											
II	T											

Q3. Decrypt the phrase "UT BZ JMIGPFS" using the keyword "MATHS".

	U	T	B	Z	J	M	I	G	P	F	S
I											
II											