Cryptography

Introduction

Cryptography is the art of producing or solving codes and has been used as a method of secure communication since as early as 1900 BC. 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. Text messages, emails and online banking, for example, are all secured with end–to–end encryption techniques to ensure the safety of our personal details. It is therefore evident that Cryptography still has modern day applications. One of 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 therefore it is considered a relatively weak and unreliable method of encryption. That 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.

Aim of Workshop

This workshop will introduce students to the basic concepts of Cryptography including ciphers, decrypting codes and the use of prime numbers in Cryptography. Students will also be provided with the opportunity to create their own encrypted messages, which they can then give to their partner to solve. By the end of this workshop students will have a better understanding of how Cryptography works and its relevance to internet security.

Learning Outcomes

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

- Encrypt and decrypt coded words using Caesar and VigenĐre ciphers
- Explain, in their own words, how 'modulus' works
- Produce their own ciphers
- Be familiar with historical decryption strategies

Materials and Resources

Alphabet line

Keywords

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 Workshop and Concept of Cryptography**	– Define what is meant by Cryptography (similar to workshop introduction) – Explain how modulus works (see **Appendix – Note 1**) – Mention applications of Cryptography such as internet banking, emailing, WhatsApp etc.
25 mins (00:30)	**Activity 1** **Caesar Ciphers**	– Brief introduction to the Caesar Cipher using a video clip (link included in **additional resources**) – Explain how to encrypt a word using an example on the board (see **Appendix – Note 2**) – **Activity Sheet 1**: In pairs, students attempt activity 1 using the alphabet line to guide them. Students are asked to pick a word and encrypt it using a particular shift value of the alphabet. Their partner must then attempt to break the code using the key shift.
5–10 mins (00:50)	**Activity 2** **Sentence Breaker**	– **Activity Sheet 2**: Students complete activity sheet 2 in pairs – Show students the encrypted sentence on **Activity Sheet 3** and ask them to try figure out how to solve it without given the key shift (looking at possible vowels etc.) – You can relate this activity back to the video clip shown at the start of the workshop
25 mins (01:15)	**Activity 3** **Vigenère Cipher**	– Introduce students to Vigenère Cipher and show how to encrypt using Vigenère by working through an example on the board (see **Appendix – Note 3**) – **Activity Sheet 3**: In pairs, students complete Activity Sheet 3 using Vigenère Cipher

Cryptography Workshop Appendix

Note 1: The Concept of 'modulus'

Modular arithmetic is a way of counting integers whereby numbers "wrap around" upon reaching a fixed quantity known as the **modulus**. For example, once we reach 12 on a clock, we start back at 1. The same applies in Cryptography whereby once the letter Z is reached, we go back to A.

Example 1: If we want to encrypt the letter 'T' using a shift of 8 on the alphabet line, then we will need to take the modulus into account. This is due to the fact that 'T' corresponds to the number 20 on the alphabet line and thus, by adding 8, we get a value of 28. However, there is no 28th letter in the alphabet so we get 26 remainder 2. The letter encoded by the number 2, in this case 'B', is therefore the encrypted letter for 'T'.

Note 2: How to Encrypt a Word using the Caesar Cipher

1. To encrypt a word using the Caesar Cipher, each pair of students will require two copies of the alphabet line (see appendix).
2. Students write down their word on a piece of paper and convert it to the relevant numbers on the alphabet line.
3. Students must then decide on a key shift **X** (a value between 1 and 26) to code their word and add this value to each of the numbers, taking the modulus into account where necessary.
4. Students then convert these new numbers back to letters. This is their encrypted word.
5. Students then hand their coded message and chosen shift to their partner so that they can decrypt it (by working backwards).

Example 1: Chris decides he wants to encrypt his name with a Caesar Cipher using a shift of 9.

1. What will his name look like after he encrypts it?

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
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	26

2. Convert the word "**Chris**" to the corresponding numbers using the alphabet line

c	h	r	i	s
3	8	18	9	19

3. Add 9 (the shift) to each number shown in blue above
4. Check the alphabet line to see what each of these new numbers now translates to

12	17	27	18	28
L	q	a	r	b

The encrypted message for "**Chris**" is thus "**Lqarb**"

Example 2: Alternatively, students can use their second alphabet line to find the new "secret" letters for their encrypted word. For example, if the shift is 3, students place the second alphabet number line in such a way that 1 now corresponds with 4 on the second alphabet line.
Notice how each letter has now shifted 3 places (which is the same as adding the shift to each number as in the example above). The letter "a", for example, has now become "d"– hence the word "apple" on the top line will correspond to the coded message "dssoh" on the bottom line. Using this method, students can directly read their coded message from the alphabet line.

Note: The overhang at the end of the alphabet line will, in theory, loop around such that x, y, z now become a, b, c respectively. This is the same idea behind the modulus.

			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
			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	26
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			
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	26			

Note 3: How to Encrypt a Word using the Vigenère Cipher

1. Write out the words you want to encrypt.
2. Find the corresponding number for each letter of your message from the number line and also the corresponding number for each letter of the keyword.
3. Write and match up the keyword with your message.
4. Replace the letters with the numbers.
5. Add the numbers together.
6. Locate the numbers on the alphabet line to give you your encrypted message.

Example 1: Maria wants to encrypt the message "See you later" using a VigenĐre Cipher and the keyword "maths". What will her message look like after she encrypts it?

1. Message to encrypt = **See you later**

   Keyword = **maths**

2. Find the corresponding number for each letter

s	e	e	y	o	u	l	a	t	e	r
19	5	5	25	15	21	12	1	20	5	18

m	a	t	h	s
13	1	20	8	19

3. Match the keyword with the message by repeating it until all letters of the message are accounted for

s	e	e	y	o	u	l	a	t	e	r
m	a	t	h	s	m	a	t	h	s	m

4. Now replace the letters above with the numbers

19	5	5	25	15	21	12	1	20	5	18
13	1	20	8	19	13	1	20	8	19	13

5. Add the numbers on the top with those on the bottom

32	6	25	33	34	34	13	21	28	24	31

6. Locate the numbers (in yellow) on the number line to give the encrypted message, taking the modulus into account

f	f	y	g	h	h	m	u	b	x	e

Encrypted message is thus: **ffy ghh mubxe**

Sources and Additional Resources

https://www.youtube.com/watch?v=sMOZf4GN3oc (Caesar Cipher video link)

http://www.furthermaths.org.uk/files/Encryption.pdf

http://practicalcryptography.com/ciphers

Activity 1 – Caesar's Cipher

You can use the alphabet line to help you encrypt or decrypt the messages.

1	a	1	a	1	a	1	a	1	a	1	a
2	b	2	b	2	b	2	b	2	b	2	b
3	c	3	c	3	c	3	c	3	c	3	c
4	d	4	d	4	d	4	d	4	d	4	d
5	e	5	e	5	e	5	e	5	e	5	e
6	f	6	f	6	f	6	f	6	f	6	f
7	g	7	g	7	g	7	g	7	g	7	g
8	h	8	h	8	h	8	h	8	h	8	h
9	i	9	i	9	i	9	i	9	i	9	i
10	j	10	j	10	j	10	j	10	j	10	j
11	k	11	k	11	k	11	k	11	k	11	k
12	l	12	l	12	l	12	l	12	l	12	l
13	m	13	m	13	m	13	m	13	m	13	m
14	n	14	n	14	n	14	n	14	n	14	n
15	o	15	o	15	o	15	o	15	o	15	o
16	p	16	p	16	p	16	p	16	p	16	p
17	q	17	q	17	q	17	q	17	q	17	q
18	r	18	r	18	r	18	r	18	r	18	r
19	s	19	s	19	s	19	s	19	s	19	s
20	t	20	t	20	t	20	t	20	t	20	t
21	u	21	u	21	u	21	u	21	u	21	u
22	v	22	v	22	v	22	v	22	v	22	v
23	w	23	w	23	w	23	w	23	w	23	w
24	x	24	x	24	x	24	x	24	x	24	x
25	y	25	y	25	y	25	y	25	y	25	y
26	z	26	z	26	z	26	z	26	z	26	z

1. **Daniel decides he wants to encrypt his name with a Caesar Cipher using a shift of 10.**

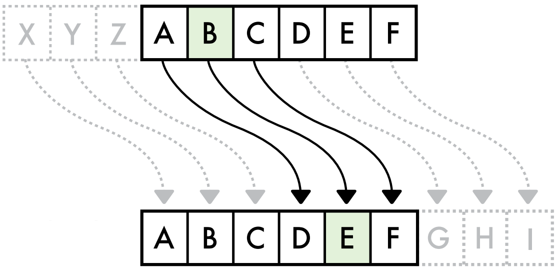
   Which of the following represents his encrypted name?

   □ a. nkxsqv

   □ b. ncpkgn

   □ c. nkxsov

   □ d. none of the above



2. **Jessica decides she wants to encrypt her name with a Caesar Cipher using a shift of 22.**

   Which of the following represents her encrypted name?

   □ a. faggwqo

   □ b. faoqgay

   □ c. faooeyw

   □ d. none of the above

3. **Thomas wants to encrypt his name with a Caesar Cipher using a shift of 15.**

   What will his name look like after he encrypts it?

   □

4. **Ishaan is expecting to receive an encrypted message with the name of one of his classmates. He knows the message will be encrypted with a Caesar cipher using a shift of 10. When he returns to his desk, he finds a piece of paper with the following message on it:**

   l b k x n y x

   Help Ishaan crack the code by writing the decrypted message in the answer box

   □

5 **Tiffany receives an encrypted message with the name of one of her classmates. She knows the message is encrypted with a Caesar cipher using a shift of 11. The piece of paper has the following code on it:**

x t n s l p w

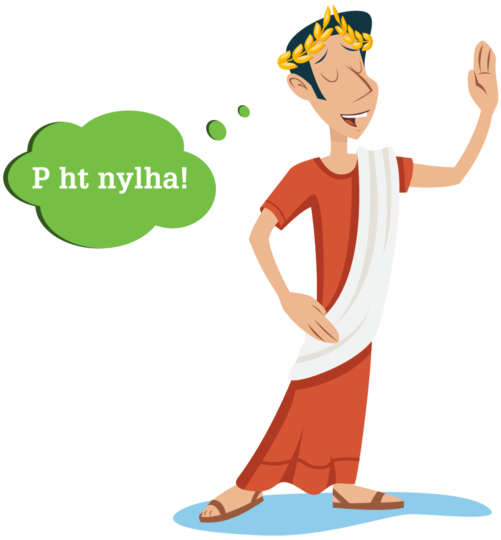
Help Tiffany crack the code by writing the decrypted message in the answer box

6. **Gabriela decides she wants to encrypt her name with a Caesar Cipher using a shift of 17.**

What will her name look like after she encrypts it?

Additional Questions

1. **Using a shift of 7, crack what Caesar is thinking.**



2. **In pairs, come up with a word, encrypt it using Caesar's Cipher and then give it to your partner to decrypt. The key shift must also be given to your partner.**

Activity 2– Sentence Breaker

Figure out the shift for an encrypted sentence.

Hap ia pwga w oahbea

UCD Maths Sparks Facilitators, 2015

Activity 3 – Vigenère's Cipher

1. **Emily wants to encode the following cryptic message:**

Uptown funk

In an effort to increase security, **Emily** decides to encrypt it with a VigenĐre cipher using her own name as the keyword. What will the secret message look like once it is encrypted? Use extra paper to figure out the encryption and write your coded answer in the box below.

2 **Using the word Vigenère as the shift, encrypt the sentence below and place in the speech bubble to code what Vigenère is saying.**

I'm smarter than Caesar