Researchers in Schools

Sending Secrets and Cracking Codes

Key Stage 4 Programme

Pupil Name

Coursebook Designed by **Dr T Kirk**

Timetable and Assignment Submission

Timetable – Tutorials

Tutorial	Date	Time	Location
1	4th December 2019	13:00-14:00	University of Manchester
2	17th January 2020	15:00-16:00	RBHS – B6
3	24th January 2020	15:00-16:00	RBHS – B6
4	31st January 2020	15:00-16:00	RBHS – B6
5	7th February 2020	15:00-16:00	RBHS – B6
6 (Feedback)	28th February 2020	15:00-16:00	RBHS – B6
7 (Feedback)	13th March 2020	15:00-16:00	RBHS – B6

Timetable – Homework Assignments

Homework Assignment	Description	Due Date
Tutorial 1	Baseline Assignment.	13th December 2019
Tutorial 2	Modulo Arithmetic Practice Worksheet	15th January 2020
Tutorial 3	Choose a short song lyric or movie quote that you like. Encrypt that quote using the given private key.	22nd January 2020
Tutorial 4	Swap your homework from Tutorial 3 with a friend. Decrypt their ciphertext using the same private key and find out which song or movie their message comes from.	29th January 2020
Tutorial 5	Final Assignment	6th March 2020

Assignment Submission – Lateness and Plagiarism

Lateness	
Submission after midnight on 9th August	10 marks deducted
Plagiarism	
Some plagiarism	10 marks deducted
Moderate plagiarism	20 marks deducted
Extreme plagiarism	Automatic fail

Contents

Course Rationale	**4**
Mark Scheme	**5**
Glossary of Keywords	**9**
Tutorial 1	**10**
Activity 1	**11**
Activity 2	**12**
Tutorial 2	**14**
Activity 1	**14**
Activity 2	**16**
Activity 3	**17**
Tutorial 3	**18**
Activity 1	**18**
Activity 2	**19**
Tutorial 4	**21**
Activity 1	**21**
Activity 2	**22**
Tutorial 5	**24**
Activity 1	**24**
Tutorial 6	**26**
Reflection on feedback	**27**
Tutorial 7	**28**
Reflecting on the course	**29**
Appendices	**30**
Referencing correctly	**30**

Course Rationale

Every time you log in to Snapchat, Instagram or any other social media, your computer is doing complicated algebra with huge numbers to check that your password is correct.

But why do we need to make it so complicated? The reality is that there are people out there who want to steal passwords so they can access personal data, e-mails, or even bank accounts.

In this course, you will see an introduction to cryptography – an area of maths designed to keep important information secure. Cryptography was used in Roman times by Julius Caesar, in World War 2 to keep messages hidden from Nazi Germany, and is still used today by banks, companies and the government.

You will learn about a special kind of algebra that you will never see in the school curriculum. You will see how it can be used to create codes and use it yourself to send secret messages to your classmates.

You will finally see a real answer to a question you have probably heard a thousand times.

"But Sir, when will we ever use algebra in real life?"

Uni Pathways Mark Scheme 2019 – problem-set assignments

	Skills	1st (70-100)	2:1 (60-69)	2:2 (50-59)	3rd (40-49)	Mark /100
Subject knowledge	Knowledge and understanding	○ All content included and materials used are relevant to the general topic and to the specific question/title ○ Good understanding of all the relevant topics. ○ Technical terms are defined and used accurately throughout ○ Clear justification of how the material and content included is related to the specific issues that are the focus of the assignment	○ Most of the content included is relevant to the general topic and to the specific question/title ○ Good understanding of most the relevant topics ○ Technical terms are used accurately but not always clearly defined. ○ Adequate justification of how the content included is related to the specific issues that are the focus of the assignment	○ Some of the content included is relevant to the general topic and to the specific question/title ○ Good understanding on some of the relevant topics but occasional confusion on others. ○ Scientific terms are used mostly accurately with occasional confusion and often not defined. ○ Some justification on how the content included is related to the specific issues that are the focus of the assignment	○ The content included and materials used are not applied to the question/title in a relevant manner ○ There is confusion in how understanding of the topics is expressed	
Critical thinking	Research and evidence	○ Uses evidence/calculations to support claims/assertions/ideas, consistently clearly and convincingly ○ Data is effectively analysed, and appropriate assumptions/conclusions are reached ○ Includes rich sources of research findings, data, quotations or other sourced material as evidence for the claims/ideas	○ Uses evidence/calculations to support claims/assertions/ideas, mostly clearly and convincingly ○ Data is analysed and the assumptions/conclusions that are reached are mostly appropriate ○ Includes adequate sources of research findings, data, quotations or other sourced material as evidence for the claims/ideas	○ Uses evidence/calculations to support claims/assertions/ideas, at times clearly and convincingly ○ There is an attempt to analyse data is and draw assumptions/conclusions ○ Includes some sources of research findings, data, quotations or other sourced material as evidence for the claims/ ideas	○ Data is presented largely without analysis	
	Developing an argument	○ Argument/proof is <u>exceptionally</u> well-developed and well-justified ○ Uses content from the tutorials in an unfamiliar context and does so accurately and confidently.	○ Argument/proof is <u>clear and well-developed,</u> and position is justified ○ Uses some content from the tutorials in an unfamiliar context, but not always accurately	○ Argument/proof is <u>clear but not well-developed</u> ○ Limited use of content from the tutorials in other contexts	○ Sometimes the argument/proof is not clearly established ○ Limited use of content from the tutorial and often inaccurately	
	Critical evaluation	○ Effectively critiques the problem set and effectively establishes a thorough response to it	○ Some evidence of critiquing the problem set and establishes a reasonable response to it	○ Limited evidence of critiquing the problem set and establishes a response to it that has some coherence	○ The problem is explored in the work but without explanation	

Written communication	Structure and presentation	○ Ideas are presented in paragraphs and arranged in a logical structure that is appropriate for the assignment ○ The introduction clearly outlines how the essay/report will deal with the issues ○ The conclusion summarises all the main points clearly and concisely ○ All calculations, formulas and methods are clearly structured, clear to follow and correct ○ Tables and graphs are effectively constructed including appropriate headings, units and scales. ○ All sources are referenced correctly in an agreed format	○ Ideas are presented in paragraphs and arranged in a structure that is mostly appropriate for the assignment ○ The introduction adequately describes how the essay/report will deal with the issues ○ The conclusion summarises most of the main points clearly ○ Calculations, formulas and methods are mostly structured, clear to follow and correct ○ Most tables and graphs are well constructed ○ Most sources are referenced correctly in an agreed format	○ Ideas are presented in paragraphs and arranged in a structure ○ The introduction mentions how the essay/report will deal with the issues ○ The conclusion summarises some of the main points clearly ○ Calculations, formulas and methods are not always structured, clear to follow and correct. ○ Some tables and graphs are well constructed but contains some errors ○ Some sources are referenced correctly in the agreed format with occasional errors	○ Ideas are presented in paragraphs but there is a lack of structure in how the work is presented ○ The work lacks an introduction that establishes the scope of the question ○ The work lacks a conclusion that summarise the main points raised ○ Work is not referenced accurately	
	Language and style	○ No spelling, grammar or punctuation errors ○ Writing style consistently clear, tone appropriate and easy to follow ○ Accurate and consistent use of technical language and vocabulary	○ Minimal spelling, grammar or punctuation errors ○ Writing style mostly clear, tone appropriate and easy to follow ○ Some attempts of using technical language and vocab alary, but not always accurate	○ Some spelling, grammar or punctuation errors ○ Writing style moderately clear, tone appropriate and easy to follow ○ Use of simple language and vocabulary effectively but struggles to use technical language	○ There are a significant number of spelling, grammar and punctuation errors ○ Use of simple language and vocabulary effectively but a lack of technical language	
					Overall Mark for written element (average of the 6 marks from the criteria above)/100	
						+
					Problem Set mark/100	
						÷ 2
					Final mark/100	

Baseline Assignment (problem-set): Pupil Feedback Report

Name of Pupil	
Name of School	
Name of RIS teacher	
Title of Assignment	

How your assignment is graded:

Grade	Marks	What this means
1st	70+	Performing to an excellent standard at A-level
2:1	60-69	Performing to a good standard at A-level
2:2	50-59	Performing to an excellent standard at GCSE
3rd	40-49	Performing to a good standard at GCSE
Working towards a pass	0-39	Performing below a good standard at GCSE
Did not submit	DNS	No assignment received by The Brilliant Club

Lateness	
Any lateness	10 marks deducted
Plagiarism	
Some plagiarism	10 marks deducted
Moderate plagiarism	20 marks deducted
Extreme plagiarism	Automatic fail

Marks

OVERALL MARK / 100		FINAL MARK / 100 (including any deductions)	
DEDUCTED MARKS		FINAL GRADE	

If marks have been deducted (e.g. late submission, plagiarism) the teacher should give an explanation in this section:

Mark Breakdown and Feedback

Knowledge and Understanding		Research and Evidence	
	mark		*mark*
Developing an Argument		**Critical Evaluation**	
	mark		*mark*
Structure and Presentation		**Language and Style**	
	mark		*mark*

Problem Set	
Comment	*mark*

Final Assignment (problem-set): Pupil Feedback Report

Name of Pupil	
Name of School	
Name of RIS teacher	
Title of Assignment	

How your assignment is graded:

Grade	Marks	What this means
1st	70+	Performing to an excellent standard at A-level
2:1	60-69	Performing to a good standard at A-level
2:2	50-59	Performing to an excellent standard at GCSE
3rd	40-49	Performing to a good standard at GCSE
Working towards a pass	0-39	Performing below a good standard at GCSE
Did not submit	DNS	No assignment received by The Brilliant Club

Lateness	
Any lateness	10 marks deducted
Plagiarism	
Some plagiarism	10 marks deducted
Moderate plagiarism	20 marks deducted
Extreme plagiarism	Automatic fail

Marks

OVERALL MARK / 100		FINAL MARK / 100 (including any deductions)	
DEDUCTED MARKS		FINAL GRADE	

If marks have been deducted (e.g. late submission, plagiarism) the teacher should give an explanation in this section:

Mark Breakdown and Feedback

Knowledge and Understanding		Research and Evidence	
	mark		*mark*
Developing an Argument		**Critical Evaluation**	
	mark		*mark*
Structure and Presentation		**Language and Style**	
	mark		*mark*
Problem Set			
			mark

Subject Vocabulary

Word	Definition	In a sentence
Encrypt	The process of putting raw information through a code to make that information difficult to read.	Alice will encrypt the password before storing it, so that nobody can steal her information.
Decrypt	The opposite of "Encrypt", this is the process of returning encrypted code back to readable information.	David is trying to decrypt Alice's password so he can access her e-mail account.
Algorithm	An ordered list of instructions, sometimes intended to be repeated.	If you follow the algorithm you will eventually break the code.
Plaintext	The raw data or information that you want to keep secure but has not yet been encrypted.	The plaintext is "Meet me in secret tonight at midnight".
Ciphertext	The encrypted plaintext which is now secure and impossible to read.	The ciphertext is "SKWE OK DL KSOEMN JAOENTD SD SOPLWNFU".
Private Key	A piece of information that you need to encrypt or decrypt your information but is only shared with people you trust.	I gave the private key to Sophie so she can read the message I send her.
Public Key	A piece of information that you need to encrypt or decrypt your information but is made publicly available so anybody can use it.	The public key is "a=5 and b=8", please share it online so others can solve our puzzle.
Symmetric	A type of encryption where only 1 key is needed to encrypt and decrypt the message, and everybody uses the same key.	AES-128 is a modern symmetric encryption type, but the key is kept very private to stop people from stealing our information.
Asymmetric	A type of encryption that usually uses multiple keys. Some of these keys are public, and some are kept private.	RSA is a modern asymmetric type of encryption that uses three different keys.
Modulo Arithmetic	A special type of algebra used in almost all modern encryption.	Using modulo arithmetic, can you evaluate the following expressions?
Computational Complexity	A measure of how easy or hard it is for a computer to do a task.	The computational complexity of RSA encryption is very high, meaning it would take computers a very long time to break the code.
Crib	A short piece of plaintext which you think is contained in the ciphertext.	We think that this e-mail starts with the word "dear", so we can use this to try and break the code.

Tutorial 1 – Introduction to Cryptography

Tutorial Objectives

By the end of this tutorial I will be able to…

- Encrypt and Decrypt short messages using Ciphers.
- Define specialist terminology and use it correctly in the context of cryptography.
- Explain why, when and where we use cryptography in the real world.

Encryption and Decryption

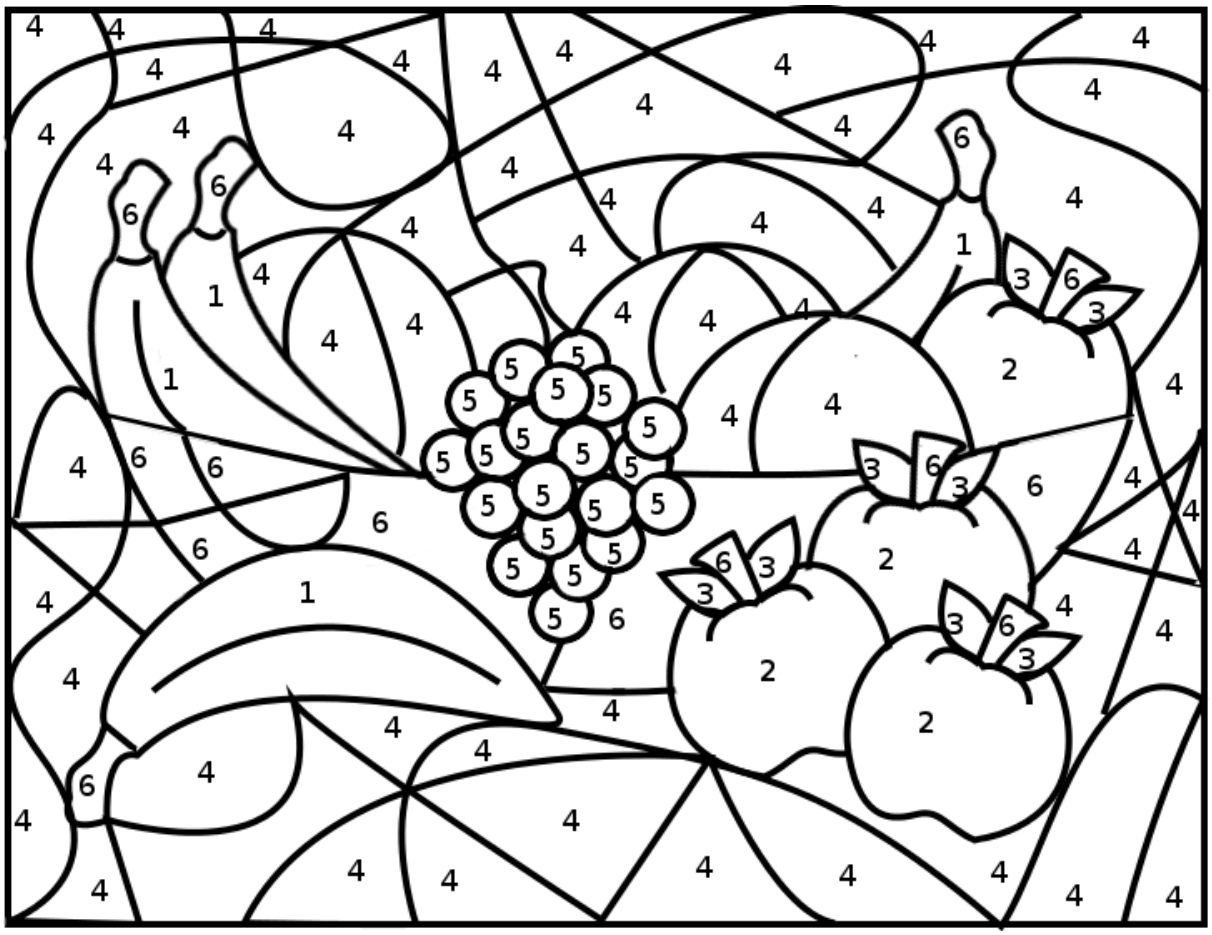
Cryptography is about obscuring information in such a way that the only way to see that information is to know the rule used to hide it. We want to keep that rule very secret and very hard to figure out, otherwise somebody clever enough could break our code and see our information.

Definition: Encryption is the process of hiding information using a rule.

Definition: Decryption is the opposite of Encryption. It is the process of retrieving the original information using the rule. Sometimes you may need to break or steal the rule first if you do not know it.

Activity 1 – Decryption-by-Numbers

Look at the following picture which has been obscured. Normally, we would tell the rule to children, and have them colour the image to reveal the picture. However, you could do this without us even telling you the rule. Complete the table at the bottom of the page.



Number	Colour
1.	
2.	
3.	
4.	
5.	
6.	

What we see is that not every rule is secure, even if we keep it secret. We can look for patterns, use some existing knowledge, and apply logic and reasoning to try and guess the rule. In reality, things will be much more complicated than the above image, but the same ideas can be applied. We can find patterns in even the most complex of messages and apply what we know about language to try and break a code!

Discussion Time: Do you think the above idea is a good way to hide a picture? If not, what could we do better? How could we make the image or the rule more complex so that the next person to try and figure out the colours would find it much harder?

Public and Private Keys

When we create the rules for encryption and decryption, we may need to share those rules with certain people so that they can easily see the information we have hidden.

If the rule is shared with others, we know they will be able to read any message we send them. This means we can make that rule a lot more complicated since we don't need them to be able to solve anything – we have already told them how to solve it!

This means people without the rule trying to break our code will have a much harder time.

Definition: A rule which we only share with a few people is called a Private Key. A rule which anybody can see is called a Public Key.

Activity 2 – Decryption-by-Numbers Extreme

The following task will require you to use a Private Key that I will share with you and only you.

Use the private key I will give you to evaluate the following list of equations, then use those values to complete the large group activity in front of you.

$3x + 2$ Evaluated using your private key equals White.

x^2 Evaluated using your private key equals Light Red.

$37 - x$ Evaluated using your private key equals Dark Red.

$\frac{x}{4} + 1$ Evaluated using your private key equals Black.

Discussion Time: What information might we want to keep safe? Who would want to steal that information?

Baseline Assignment

Please read the instructions below for both the written component and the problem set. Your assignment is to complete the questions below. You may use a calculator. Pay close attention to the success criteria given.

Written Component (250 Words)

Think about all the times you have had to make an account for things like school, Facebook, Instagram, Snapchat, etc. They will usually ask you to make passwords that have a certain length, use capital letters, numbers, or special symbols. Using the ideas we discussed in Tutorial 1, write a few paragraphs (250 words) on why you think passwords are made this way and discuss what you think might be the strengths and weaknesses of using these passwords.

Success Criteria

- Identify correctly and discuss some of the strengths and weaknesses of creating and using passwords with these restrictions.
- Work is presented neatly with proper spelling, grammar and punctuation.
- Correct terminology used in context.

Problem Set

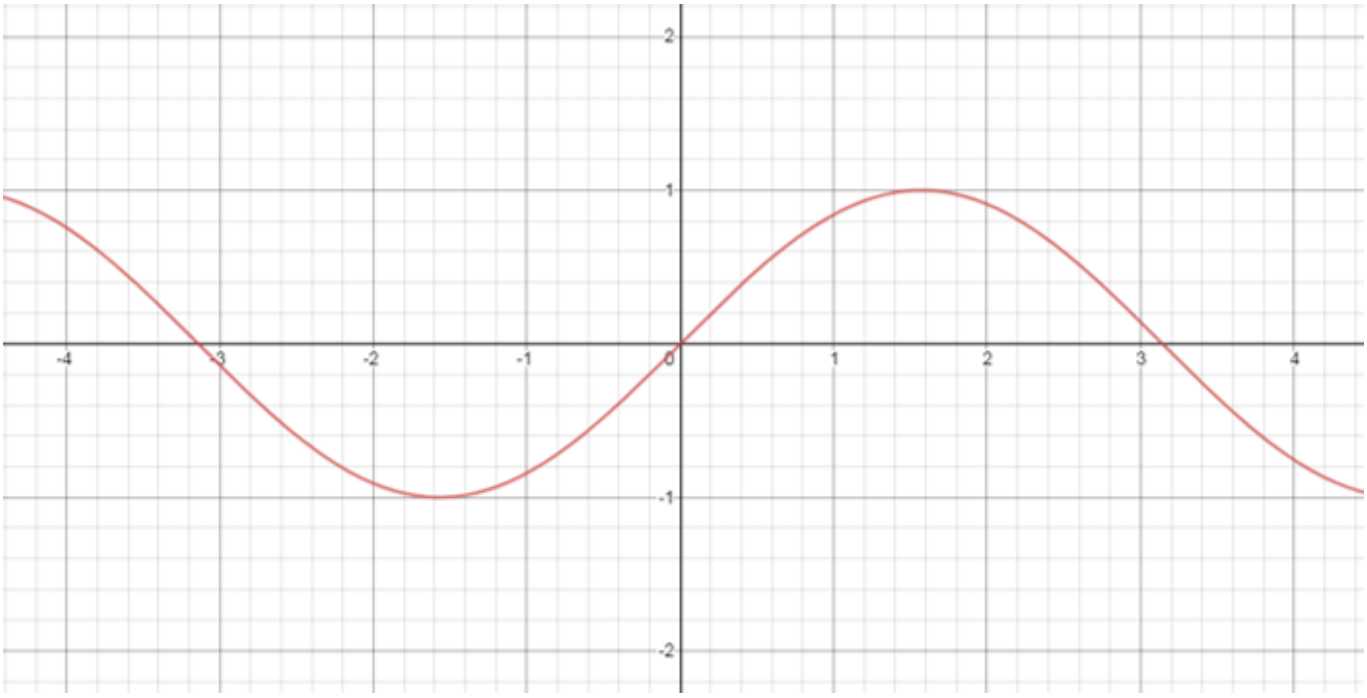
Question 1: Expand the brackets in the equation $(xy + 2x^2)(y^2 + 3) = a$.

Question 2: Use your answer to Question 1 to find a when $x = 1$ and $y = 2$.

Question 3: $zy = \frac{x}{3} + \frac{z^2}{3}$

Using the above equation, find x when $z = 1$ and $y = 4$.

Question 4: On the graph below, estimate the possible values for x when $y = 0.5$



Success Criteria

- All problems answered correctly with all working shown.
- All work is well structured and neatly presented.

Tutorial 2 – Modulo Arithmetic

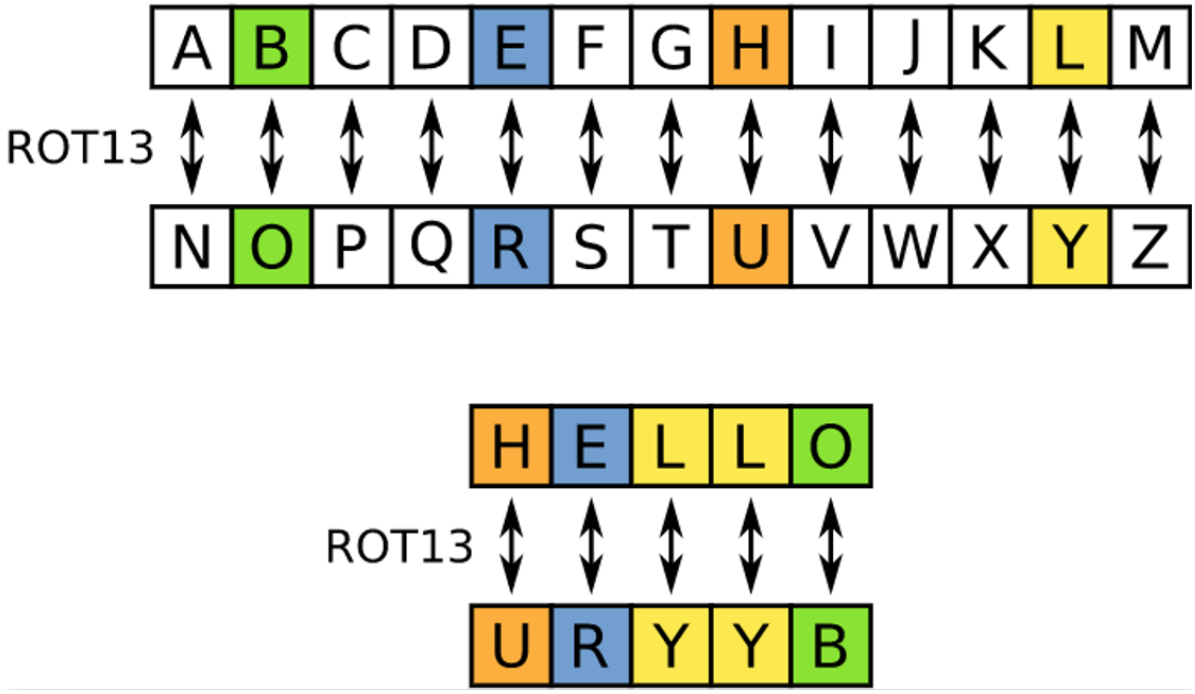
Tutorial Objectives

By the end of this tutorial I will be able to…

- Perform addition and multiplication using modulo arithmetic with various bases.
- Find the set of solutions to linear equations in modulo arithmetic.
- Explain why modulo arithmetic is useful for both computers and mathematicians.

Activity 1 - ROT13

ROT13 (meaning rotated 13 places) is a type of encryption that swaps letters using the rule shown in the image below, together with an example using the word "Hello".

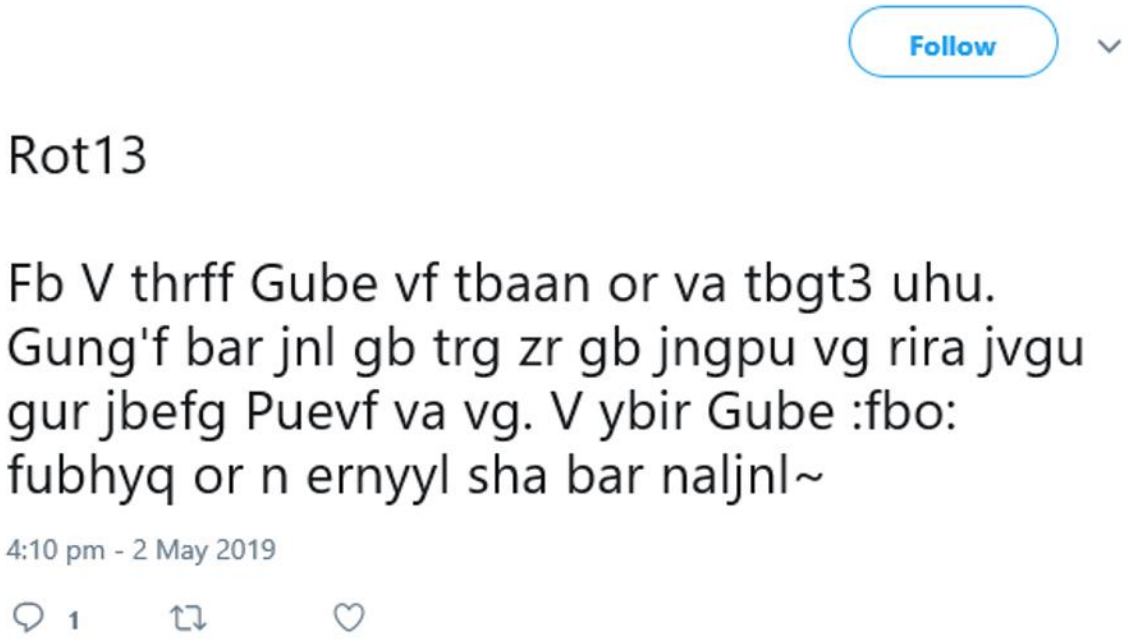


ROT13 is a special case of something called a Caesar Cipher, named after the Roman Emperor who used the cipher to make all his letters impossible to read.

A Caesar Cipher shifts the alphabet so that each letter is swapped with another, and in the above cipher we are shifting 13 places.

Discussion Time: Do you think this is a good way to keep information secret? Could you figure out how to decrypt it? How many guesses would it take you?

People on social media recently who did not want to spoil a recent popular movie for other fans used ROT13 to encrypt their posts. Because the Cipher is so easy to encrypt and decrypt, it meant that fans who had seen the movie could decrypt it easily and discuss it, but people who didn't decrypt it would just see a mess of letters.



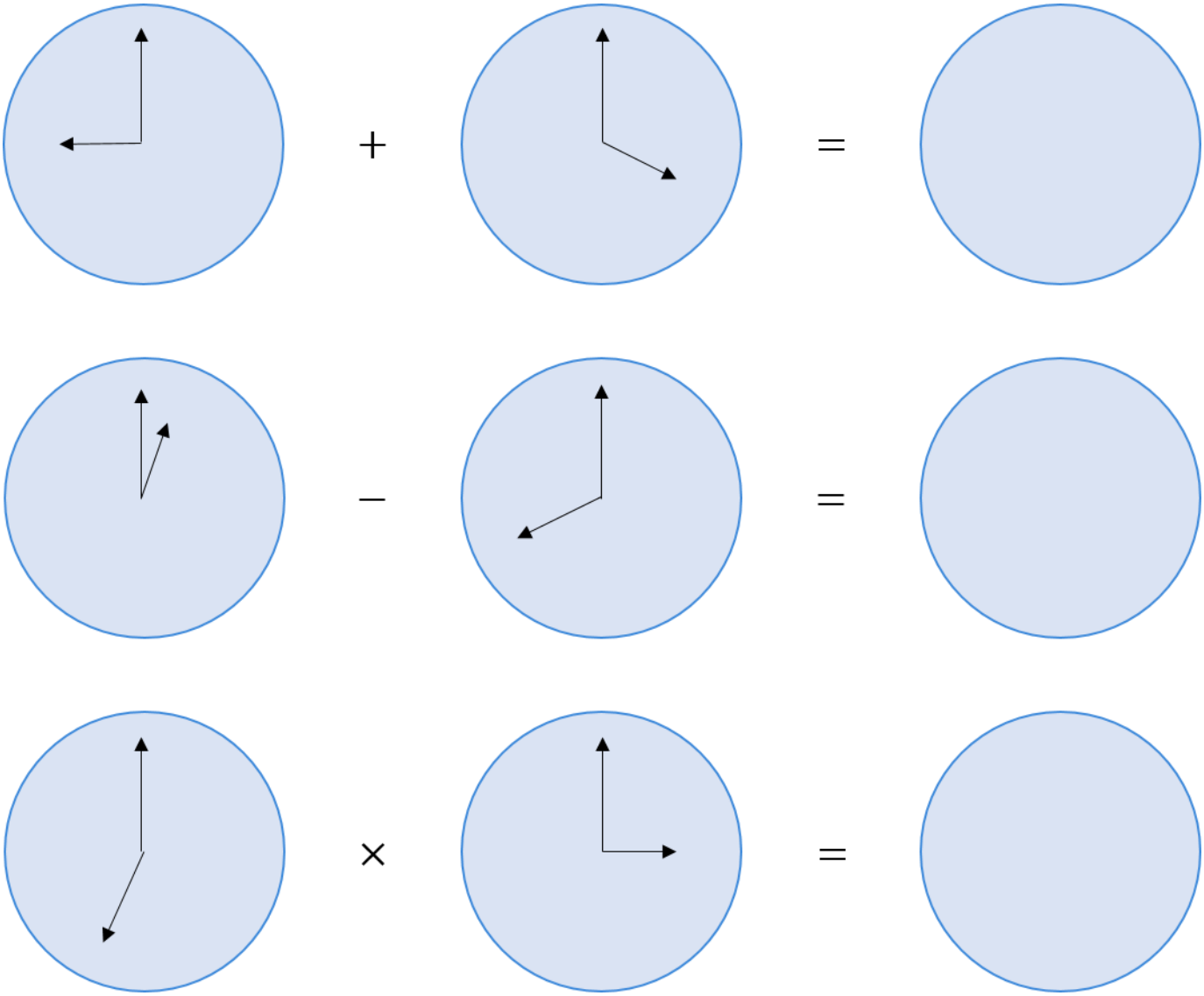
Use ROT13 to decrypt the social media post above and tell me what movie they were trying to avoid spoiling.

Movie Name: _____

Activity 2 – Clock Arithmetic

Modulo Arithmetic is sometimes called "Clock Arithmetic". This is because we could think of a clock as being "mod 12" arithmetic. When we add hours, we don't just keep going up forever – the clock only goes up to 12.

Draw the hands on the clocks in the following equations.



The skills you used here are fundamentally the same as you will use in the next activity. Whenever you found yourself with an answer outside the range of 1 to 12, you added or subtracted 12 hours until you were within the right range.

This is because you know that a clock at 1pm on Tuesday will look the same as a clock at 1am on Friday. This would work for any time or any day – all we need is that the time between them is a multiple of 12 hours.

That is modulo arithmetic!

Activity 3 – Modulo Arithmetic

How To:
Modulo Arithmetic will always be done using a given base. For now, we will use **base n**. We do maths just like we're used to, except if we get an answer that is **equal to or bigger than n** or **smaller than 0**, we add or subtract **n** until we are within the range.
You could also think of it as taking the **remainder when dividing by n.** Below is an example where **n is 7**.

$$3 \times 5 \ (mod\ 7) = 15 \ (mod\ 7)$$

15 is bigger than 7, so we subtract 7.

$$15 - 7 = 8$$

8 is bigger than 7, so we subtract 7.

$$8 - 7 = 1$$

1 is bigger than 0 and smaller than 7.

Therefore we are done, and so..

$$3 \times 5 \ (mod\ 7) = 15 \ (mod\ 7) = 1 \ (\mathrm{mod}\ 7)$$

Below are some questions. Use modulo arithmetic like in the example above to calculate the answers in the given bases.

1. $4 + 8 \ (mod\ 9) =$
2. $7 \times 6 \ (mod\ 11) =$
3. $72 \div 12 \ (mod\ 5) =$
4. $12 - 45 \ (mod\ 7) =$
5. $9 \times 6 \ (mod\ 53) =$
6. $9 \times 6 \ (mod\ 54) =$
7. $-5 \times 6 \ (mod\ 7) =$
8. $-30 \div -6 \ (mod\ 3) =$

Extension

1. $3x \ (mod\ 4) \quad when\ x = 6$
2. $5x + 2 \ (mod\ 7) \quad when\ x = 5$
3. $2x \ (mod\ x)$

Tutorial 3 – The Affine Cipher 1

Tutorial Objectives

By the end of this tutorial I will be able to…

- Encrypt a message using the Affine Cipher.
- Understand cryptographic vocabulary in the context of the Affine Cipher.
- Define what it means for numbers to be coprime and explain what this means in the context of the Affine Cipher.

Activity 1 – Alphanumeric Replacement

Before we can use maths to encrypt our messages, we need a way to relate a number with a letter of the alphabet.

We do this using the following alphanumeric replacement cipher.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

To use the Alphanumeric Replacement Cipher, simply replace each letter in a message with the number. Note that we go from 0 to 25, not from 1 to 26. It doesn't really make a difference, but it does make the maths a little bit easier.

For example, "Hello" would become "7 4 11 11 14".

Use the Cipher to convert the following numbers back to plaintext.

1. **12 0 19 7 18**

2. **18 4 13 3 18**

3. **18 4 2 17 4 19**

4. **12 4 18 18 0 6 4 18**

Activity 2 – The Affine Cipher: Encryption

We now use modulo arithmetic, together with alphanumeric replacement, to make a much stronger cipher than we've used so far.

We will use a private key consisting of two numbers **a** and **b**, and we will always be working **(mod 26)**.

The Affine Cipher Encryption Algorithm

Step 1: Convert your plaintext into numbers using the Alphanumeric Cipher.

Step 2: For each number $\boldsymbol{x}$ in your converted plaintext, do the following calculation:

$$ax + b \ (mod\ 26)$$

Step 3: Convert each number back to a letter using the Alphanumeric Cipher.

Example:

Below is an example using the private key **a = 5** and **b = 8**. Remember we always work **(mod 26).**

Plaintext	**U**	**N**	**I**	**V**	**E**	**R**	**S**	**I**	**T**	**Y**
$\boldsymbol{x}$	20	13	8	21	4	17	18	8	19	24
$\mathbf{5}\boldsymbol{x} + \mathbf{8}$	108	73	48	113	28	93	98	48	103	128
$\mathbf{5}\boldsymbol{x} + \mathbf{8}\ (\boldsymbol{mod}\ \mathbf{26})$	4	21	22	9	2	15	20	22	25	24
Ciphertext	**D**	**V**	**W**	**J**	**C**	**P**	**U**	**W**	**Z**	**Y**

Using the affine Cipher with private key **a = 5** and **b = 8**, we see that the word "UNIVERSITY" is encrypted as "DVWJCPUWZY".

You should notice that unlike the ROT13 cipher, this is a lot more complex than simply shifting the alphabet. Every letter moves to a different place in the alphabet.

Your Turn!

First try with a different private key.
Complete the following table with private key **a = 3** and **b = 4**

Plaintext	U	N	I	V	E	R	S	I	T	Y
x										
$3x + 4$										
$3x + 4 \ (mod\ 26)$										
Ciphertext										

Now do another example and choose your own word to encrypt.
This time use the private key **a = 7** and **b = 2**.

Plaintext										
x										
$ax + b$										
$ax + b \ (mod\ 26)$										
Ciphertext										

Finally, choose both your own word, and your own private key.

Plaintext										
x										
$ax + b$										
$ax + b \ (mod\ 26)$										
Ciphertext										

Discussion Time: Did your final encryption work? There are some choices for **a** which will not give you a unique encryption.

Tutorial 4 – The Affine Cipher 2

Tutorial Objectives

By the end of this tutorial I will be able to…

- Decrypt a message using the Affine Cipher.
- Explain the strengths and weaknesses of the Affine Cipher using the correct terminology.

Activity 1 – Multiplicative Inverses

We now need to know how to reverse the Affine Cipher so that we can read the messages we want to send to each other. The decryption algorithm is mostly the same, but we first need to do something with the private key.

For an Affine Cipher with private key **a** and **b**, we need to find the **multiplicative inverse** of **a (mod 26)**.

Definition: The multiplicative inverse of **a (mod 26)** is a number **c** such that **a** × **c = 1 (mod 26)**.

Example: The multiplicative inverse of **5 (mod 26)** is **21.**
This is because **5** × **21 = 105 = 1 (mod 26).**

Calculating the multiplicative inverse of a number is best done using something called the **Euclidean Algorithm**. However, this is quite a long process to do by hand, so we will instead use calculators to do it for us. In fact, for numbers this small, it is usually quicker to try every number between 0 and 25 until we find the inverse **c.**

Complete the table below until you find the multiplicative inverse of **3 (mod 26).**

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$3x\ (mod\ 26)$																			

The multiplicative inverse of 3 (mod 26) is _____.

Activity 2 – Decrypting an Affine Cipher

We now see the algorithm for decrypting an Affine Cipher. We use a private key **a** and **b**, but this time we need to first calculate the multiplicative inverse of **a (mod 26)**. We will label this inverse **c**.

The Affine Cipher Decryption Algorithm

Step 1: Convert your ciphertext into numbers using the Alphanumeric Cipher.

Step 2: For each number $\boldsymbol{x}$ in your converted ciphertext, do the following calculation:

$$c(x - b)\ (mod\ 26)$$

Where **c** is the multiplicative inverse of **a (mod 26)**.

Step 3: Convert each number back to a letter using the Alphanumeric Cipher.

Example: We will decrypt the ciphertext from Tutorial 3. The private key was **a = 5** and **b = 8**.
We convert the ciphertext into numbers, and then calculate the multiplicative inverse of **a (mod 26).**

The multiplicative inverse of **5 (mod 26)** is **21**.

Ciphertext	**D**	**V**	**W**	**J**	**C**	**P**	**U**	**W**	**Z**	**Y**
$\boldsymbol{x}$	4	21	22	9	2	15	20	22	25	24
$\mathbf{21}(\boldsymbol{x} - \mathbf{8})$	-84	273	294	21	-126	147	252	294	357	336
$\mathbf{21}(\boldsymbol{x} - \mathbf{8})\ (\boldsymbol{mod}\ \mathbf{26})$	20	13	8	21	8	17	18	8	19	24
Plaintext	**U**	**N**	**I**	**V**	**E**	**R**	**S**	**I**	**T**	**Y**

As expected, when we decrypted "DVWJCPUWZY" using the same private key that was used to encrypt it, we get back to our original word "UNIVERSITY".

Your turn!

The following message was encrypted using private key **a = 3** and **b = 2**.

Use the multiplicative inverse you found in Activity 1 to decrypt the following ciphertext.

Ciphertext	**Q**	**O**	**J**	**J**		**L**	**S**	**P**	**O**	
x										
$c(x-b)$										
$c(x-b)\ (mod\ 26)$										
Plaintext										

The decrypted message is: _____

Ask your partner for their ciphertext from Page 19, Question 2.

Try to decrypt their message.

Remember the private key was **a = 7** and **b = 2**.
The multiplicative inverse of **7 (mod 26)** is **15.**

Ciphertext										
x										
$15(x-2)$										
$15(x-2)\ (mod\ 26)$										
Plaintext										

The decrypted message is: _____

Discussion Time: What strengths and weaknesses of the Affine Cipher can you think of? Do you think it is hard for people to guess the key? What about for a computer to guess the key? Discuss with your partner and then we will feed back to the group.

Tutorial 5 – Cribs and Modern Encryption

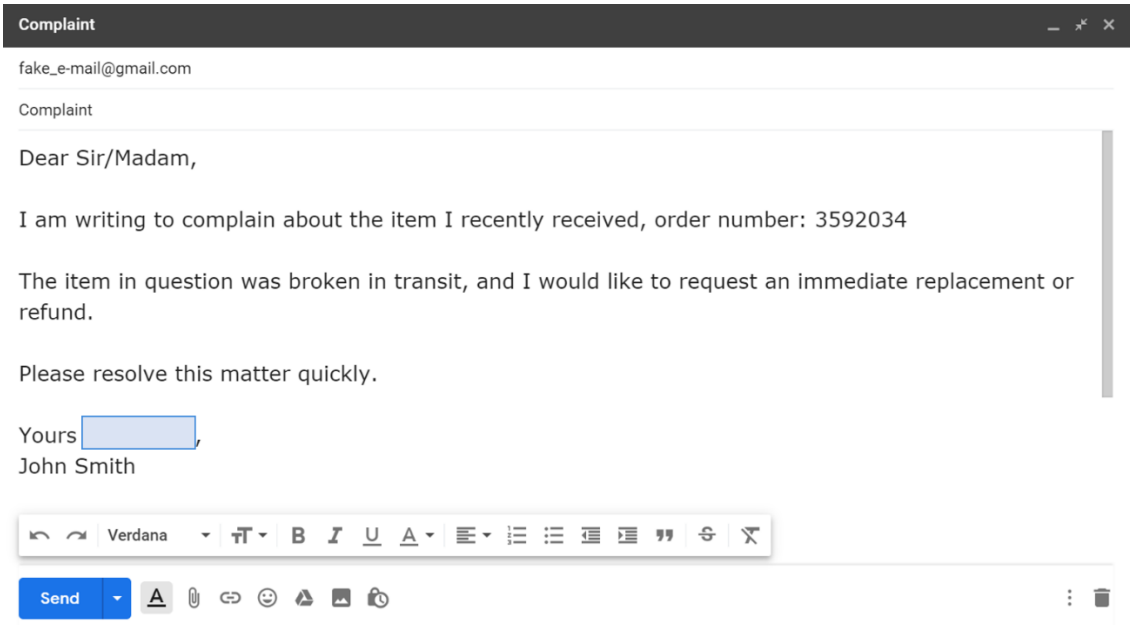
Tutorial Objectives

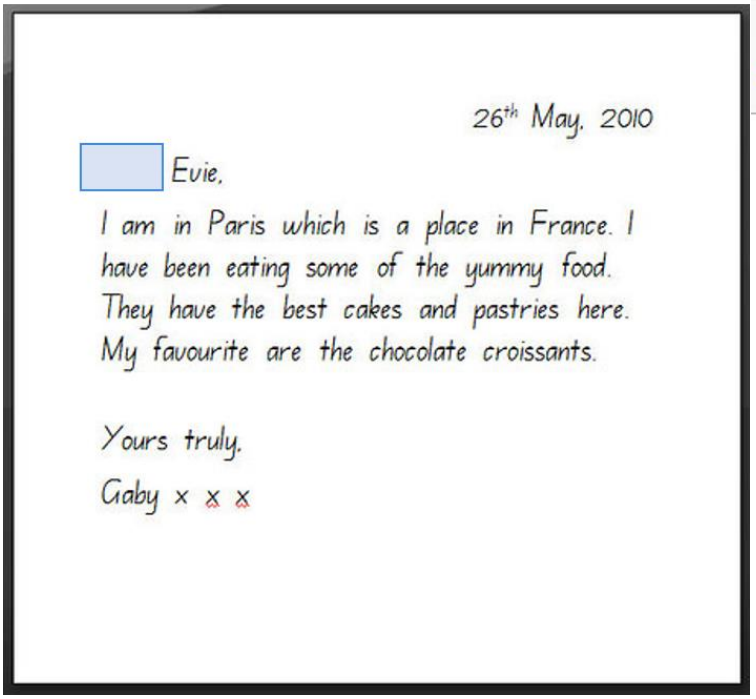
By the end of this tutorial I will be able to…

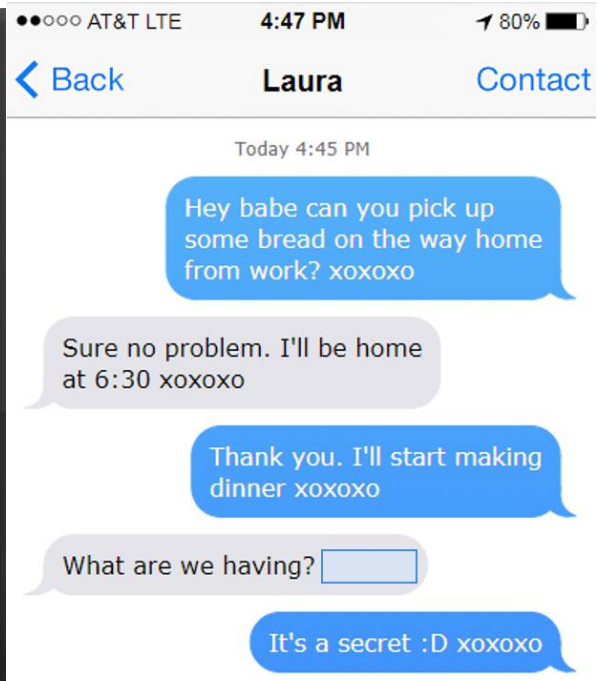
- Break the Affine Cipher using a Crib.
- Explain what is meant by Symmetric and Asymmetric Encryption.
- Understand modern cryptography and computational complexity.
- Describe the strengths and weaknesses of modern cryptography.

Activity 1 – Cribs

In cryptography, a Crib is a piece of the plaintext which you suspect is contained in the original message. By comparing the ciphertext with the crib, you can obtain a system of equations that can allow you to solve the private key and break the encryption. The images below all contain words which have been blanked out. Try to guess what the word is likely to be.







Final Assignment

Please read the instructions below for both the written component and the problem set. Your final assignment is to complete the questions below. You may use a calculator. Pay close attention to the success criteria given.

Written Component (1000 Words)

Question:

Research the RSA encryption method and write an essay discussing the strengths and weaknesses of this encryption.

Success Criteria:

- Discuss using Point, Evidence and Explain both the strengths and weaknesses of RSA Encryption.
- Use terminology correctly and in context.
- Provide sources for your evidence and explanations, and properly reference where these sources are used.
- All writing should be coherent with correct grammar, punctuation and spelling.

Problem Set

Question 1:

Encrypt the plaintext "UNI PATHWAYS" using an Affine Cipher with private key **a = 15** and **b = 9**

Question 2:

The ciphertext "WMRHO KO MWMJKZE" was encrypted using private key **a = 3** and **b = 12**. Decrypt this ciphertext.

Question 3:

You suspect that the ciphertext "C VIORRE OLLVIYCOFI EGK XIRLCBS WI GKF EIAFIVDOE FXOBM EGK " is a text message which ends with the words "Thank you" and was encrypted using an Affine Cipher.

Find the private key used to encrypt the message.

Success Criteria:

- Solutions are correct and all working is shown.
- Good Presentation: All work should be well structured and neatly written.

Tutorial 6 – Feedback tutorial

What is the Purpose of Tutorial 6?

- To receive feedback on your final assignment
- To respond to the feedback from your Uni Pathways teacher
- To write targets for improvement on your final assignment

Final assignment feedback from your Uni Pathways Teacher

(Remember to look at the mark scheme to help you understand what you have done well so far, and how you can do even better in your final assignment)

Here are three things that my Uni Pathways Teacher thought I did well in my draft assignment
•   •   •

Here are three things that my Uni Pathways Teacher thinks that I could do to get a higher mark in my final assignment
•   •   •

Tasks from my Uni Pathways Teacher to do during the feedback tutorial to help me improve
•   •   •
My response:

Actions I will take to improve my final assignment after this tutorial…
•   •   •

Hand in date for my final assignment:	

Tutorial 7 – Final tutorial

What is the Purpose of Tutorial 7?

- To receive feedback and a grade on your final assignment.
- To reflect on the programme including what you enjoyed and what was challenging.
- To ask any questions you may have about university.

Final assignment feedback from my Uni Pathways Teacher

Final mark:	University style grade:
Feedback: Here are three things that my Uni Pathways teacher thought I did well in my final assignment • • •	

Here are three things that my Uni Pathways teacher thinks I should remember for when I am doing this kind of study in the future
• • •

University

What questions do you still have about University after taking part in Uni Pathways?
•   •   •

Reflecting on Uni Pathways

What did you most enjoy about Uni Pathways?
•   •   •

What did you find challenging about the programme?	How did you overcome these challenges?
• • •	• • •

Appendix 1 – Referencing correctly

When you get to university, you will need to include references in the assignments that you write, so we would like you to start getting into the habit of referencing in your Brilliant Club assignment. This is really important, because it will help you to avoid plagiarism. Plagiarism is when you take someone else's work or ideas and pass them off as your own. Whether plagiarism is deliberate or accidental, the consequences can be severe. In order to avoid losing marks in your final assignment, or even failing, you must be careful to reference your sources correctly.

What is a reference?

A reference is just a note in your assignment which says if you have referred to or been influenced by another source such as book, website or article. For example, if you use the internet to research a particular subject, and you want to include a specific piece of information from this website, you will need to reference it.

Why should I reference?

Referencing is important in your work for the following reasons:

- It gives credit to the authors of any sources you have referred to or been influenced by.
- It supports the arguments you make in your assignments.
- It demonstrates the variety of sources you have used.
- It helps to prevent you losing marks, or failing, due to plagiarism.

When should I use a reference?

You should use a reference when you:

- Quote directly from another source.
- Summarise or rephrase another piece of work.
- Include a specific statistic or fact from a source.

How do I reference?

There are a number of different ways of referencing, and these often vary depending on what subject you are studying. The most important to thing is to be consistent. This means that you need to stick to the same system throughout your whole assignment. Here is a basic system of referencing that you can use, which consists of the following two parts:

1. **A marker in your assignment**: After you have used a reference in your assignment (you have read something and included it in your work as a quote, or re-written it your own words) you should mark this is in your text with a number, e.g. [1]. The next time you use a reference you should use the next number, e.g. [2].
2. **Bibliography**: This is just a list of the references you have used in your assignment. In the bibliography, you list your references by the numbers you have used, and include as much information as you have about the reference. The list below gives what should be included for different sources.

    a. **Websites** – Author (if possible), title of the web page, website address, [date you accessed it, in square brackets].

    E.g. Dan Snow, 'How did so many soldiers survive the trenches?', http://www.bbc.co.uk/guides/z3kgjxs#zg2dtfr [11 July 2014].

    b. **Books** – Author, date published, title of book (in italics), pages where the information came from.

    E.g. S. Dubner and S. Levitt, (2006) *Freakonomics*, 7-9.

    c. **Articles** – Author, 'title of the article' (with quotation marks), *where the article comes from* (newspaper, journal etc.), date of the article.

    E.g. Maev Kennedy, 'The lights to go out across the UK to mark First World War's centenary', Guardian, 10 July 2014.

Notes

Notes

Notes

Notes

UNI PATHWAYS

UNI PATHWAYS

researchersinschools.org