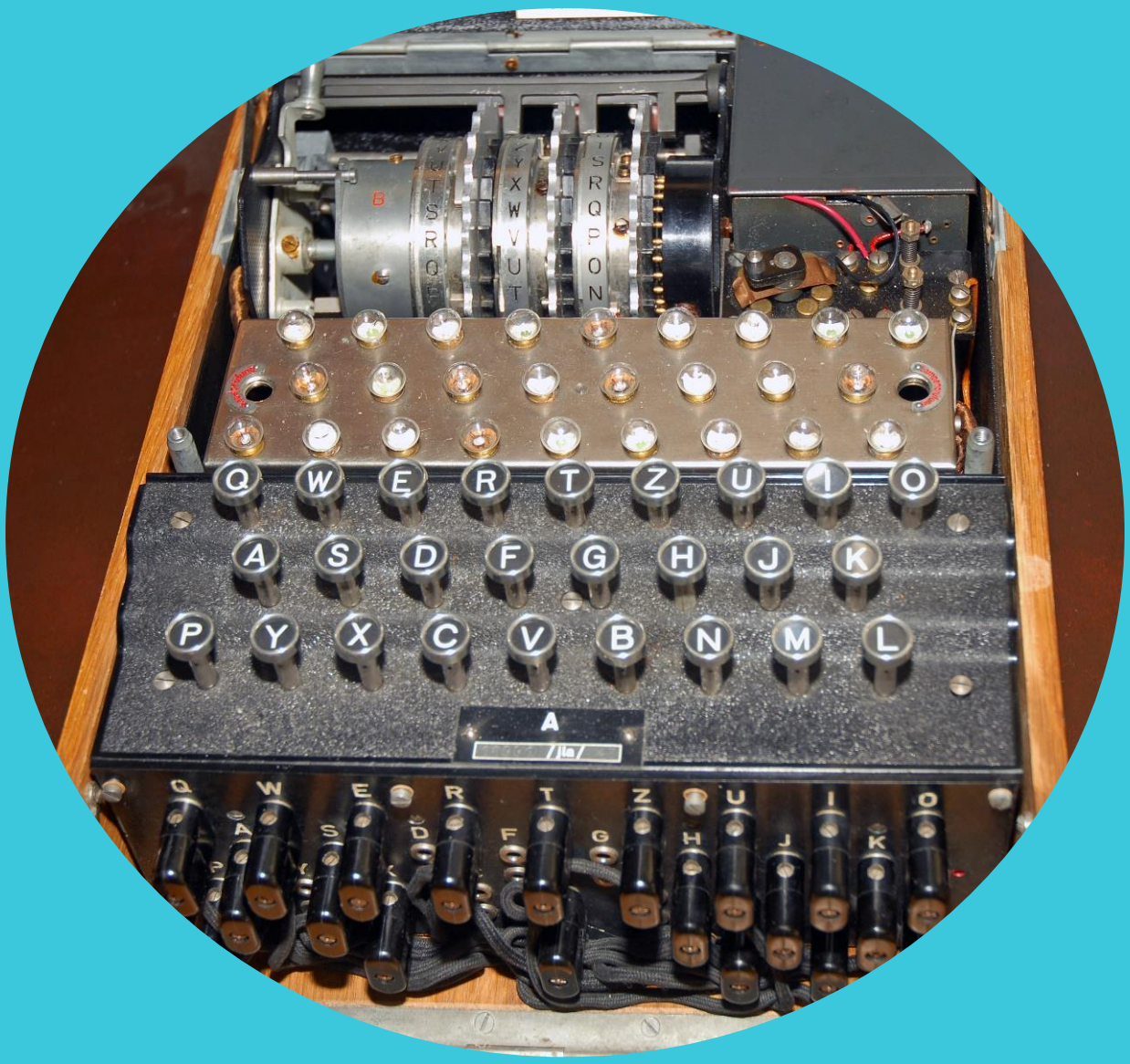
Researchers in Schools



Numbers and Codes:

Can Maths Help Keep Our Data Safe?

Key Stage 4 Programme

Pupil Name

Coursebook Designed by **Dr. P. Adrom**

Timetable and Assignment Submission

Timetable – Tutorials

Tutorial	Date	Time	Location
1	4 December 2019	12.45	The University of Manchester
2	17 January 2020	15.30	A15
3	24 January 2020	15.30	A15
4	31 January 2020	15.30	A15
5	7 February 2020	15.30	A15
6 (Feedback)	28 February 2020	15.30	A15
7 (Feedback)	13 March 2020	15.30	A15

Timetable – Homework Assignments

Homework Assignment	Description	Due Date
Tutorial 1	Baseline assignment: Cryptosystems	13 December 2019
Tutorial 2	Relations and congruence classes	24 January 2020
Tutorial 3	'Inversion' of congruence classes	31 January 2020
Tutorial 4	Leonhard Euler	7 February 2020
Tutorial 5	Final assignment: Modular arithmetic and the RSA cryptosystem	Draft: 14 February 2020 Final: 6 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**
Baseline Assignment	**15**
Tutorial 2	**16**
Homework	**20**
Tutorial 3	**21**
Homework	**26**
Tutorial 4	**27**
Homework	**30**
Tutorial 5	**31**
Final Assignment	**36**
Tutorial 6	**37**
Reflection on feedback	**38**
Tutorial 7	**39**
Reflecting on the course	**40**
Appendices	
Referencing correctly	**41**

Course Rationale

We live in an increasingly interconnected world where communication and data underlie many aspects of our lives, from the ways we have personal relationships (e.g. social networks) to national and international infrastructure and industries (e.g. medical records in the NHS, or GPS). This expansion of information storage and exchange highlights the necessity of protecting privacy and confidentiality as unauthorised access to data can have important consequences.

Cryptography is an area of mathematics that studies methods of encrypting messages, which means changing a message so that its meaning cannot be easily discovered, and decrypting to recover the original. Cryptography considers how complex this problem can be, and what makes some encryption systems stronger (less easily attacked) or weaker than others.

In this course we will learn about some ideas that are the basis of a common cryptographic method, the RSA system. As well as enabling us to understand why RSA is a strong system, the concepts we learn will show how mathematics can describe and explain similar patterns and structures in different contexts.

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	○ 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	○ 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	○ 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	
Wri tte	Structure and presentation	○ Ideas are presented in paragraphs and arranged in a logical structure that is appropriate for the	○ Ideas are presented in paragraphs and arranged in a structure that is mostly appropriate for the	○ Ideas are presented in paragraphs and arranged in a structure ○ The introduction mentions how the	○ Ideas are presented in paragraphs but there is a lack of structure in	

		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	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	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	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
Algorithm	A clearly-defined sequence of operations for solving a problem	
Encryption	Transforming a message into a coded message	
Decryption	Recovering an original message from a coded message	
Cryptosystem	A set of ciphers and keys used for encrypting and decrypting messages	
Cipher	An algorithm that performs encryption or decryption	
Key	The information required for using a cipher	
Coprime	Two integers are coprime if their highest common factor is 1	
Congruence modulo n	This is a relation that two integers a and b have if they leave the same remainder when divided by n	
Congruence class modulo n	A set of all the integers that leave the same remainder when divided by n	
Euler's function	Denoted by ϕ, this function counts for each positive integer n the number of smaller positive integers that are coprime to it	

Tutorial 1 – Cryptosystems

By the end of this tutorial I will be able to

- explain what is a cryptosystem
- describe the difference between public key and private key systems
- use the Euclidean algorithm to decide whether two numbers are coprime

Starter

Starter: Imagine you are investigating a spy network and discover a coded message from one of its agents, containing information about her location. You suspect the message has been sent from either Italy or Spain. If the message states the location is URCKP, from where do you think it has been sent?

Think of a short message, for example a single word or sentence. Can you find a way of encrypting it? How would the decryption process work? What are the strengths or weaknesses of the method?

Ciphers and keys

Example: The monoalphabetic cipher

The monoalphabetic cipher is a private key and symmetric cipher.

What is a problem with using a private key cipher?

Prime numbers, coprime pairs

The Euclidean algorithm

Are 45 and 28 coprime?

Baseline assignment:
Cryptosystems

Use the Euclidean algorithm to decide which of the pairs $(16,25)$ and $(24,40)$ are coprime.

Find out about an (simple!) encryption method which we have not discussed in the tutorial. Briefly describe how it works, and what are its weaknesses.

Baseline assignment success criteria:

- Correct application of the Euclidean algorithm
- Reference to suitable sources and clear explanation of research findings
- Justification of claims, using appropriate technical vocabulary

Tutorial 2 – Congruence classes

By the end of this tutorial I will be able to

- define what congruence means
- state what congruence classes are
- use the correct notation for congruence classes

Starter

When a number is divided by 5, what can the remainder be? What can we say about the numbers which leave the same remainder?

How about division by 9?

Congruence modulo n

Is it true that $3 \equiv 6 \bmod 4$? What about $8 \equiv 14 \bmod 6$?

Congruence classes

Example

Discussion: distinguishing '=' and '≡ '

Homework:

Relations and congruence classes

Pick a number that is coprime to 8. Use the Euclidean algorithm to show that it is coprime.

Now pick another number that is congruent modulo 8 to the first number. Is it also coprime to 8?

Can you generalise this?

Success criteria:

- Correct calculation using the Euclidean algorithm
- Clear conclusion to the problem
- An attempt at generaliation of the conclusion

Tutorial 3 – Modular Arithmetic

By the end of this tutorial I will be able to

- explain the meaning of operations on congruence classes
- define addition and multiplication in modular arithmetic
- do calculations in modular arithmetic efficiently

Starter

Pick two numbers, add them and divide the result by 5. What is the remainder? Is it related to the remainders when each of the numbers is divided by 5?

Try this with another pair of numbers.

Addition of congruence classes

Examples

$[2] + [3] \bmod 5$

$[6] + [7] \bmod 10$

Multiplication of congruence classes

Examples

$[4] \times [4] \bmod 6$

$[5] \times [5] \bmod 10$

$[2]^3 \bmod 5$

$[3]^4 \bmod 20$

<u>Doing calculations in modular arithmetic efficiently</u>

Do the following calculations with and then without using the simplifying technique discussed above. Compare how long it takes each way.

$7^3 \bmod 9$

$6^4 \bmod 4$

Homework:

‘Inversion’ of congruence classes

Pick a number less than 9. Is it possible to multiply it by another number so that the result is in $[1] \bmod 9$? (This is what it means to say that the number is invertible modulo 9.) For which of the numbers $\{1,2,\ldots,8\}$ is this possible? Do you see a common property?

Do the same exercise with calculations mod 15 too.

(Optional challenge problem: Recall that the Euclidean algorithm can show whether two numbers are coprime. Can you use this fact in answering the above problem?)

Success criteria:

- Understanding of modular arithmetic and how to calculate with congruence classes
- Correct identification of the numbers which can be inverted mod 8 and mod 15
- Clear statement of the conclusion reached
- (Optional problem: Providing an argument, using the Euclidean algorithm, to prove the property is correctly identified)

Tutorial 4 – Euler's theorem

By the end of this tutorial I will be able to

- define Euler's phi function ϕ
- calculate $\phi(n)$ for small values of n
- state Euler's theorem about the function ϕ

Starter

Work out how many natural numbers less than 15 are coprime to it. Next, factorise 15 as a product of primes. Do you see a connection between these answers?

Try the same calculations for 30.

Euler's phi function ϕ

Calculate $\phi(14)$ and $\phi(36)$ directly from the definition. Does the relation with prime factorisation noted earlier always obtain?

Euler's Theorem

Calculate the following and verify that Euler's Theorem in each case.

$2^8 \bmod 15$

$3^6 \bmod 14$

Homework:

Leonhard Euler

The function ϕ is named after Leonhard Euler. He was one of the most prolific mathematicians in history. You can read more about him and his work at

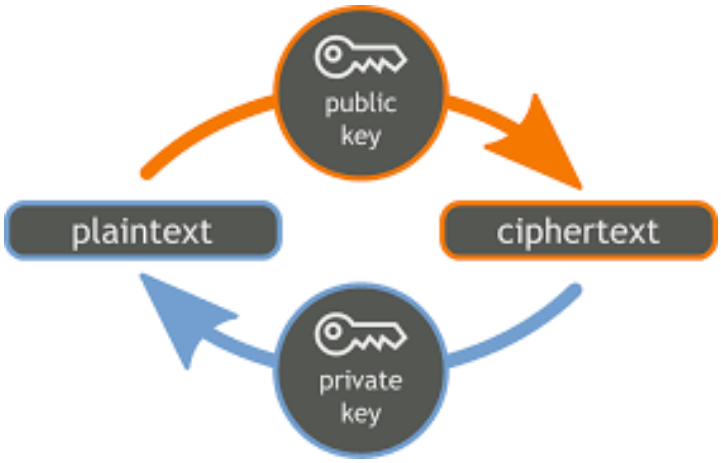
http://www-history.mcs.st-and.ac.uk/Biographies/Euler

Briefly describe one of his other discoveries or ideas, using your own research to provide some explanation of the concepts.

Baseline assignment success criteria:

- Evidence of research, including appropriate referencing of sources consulted
- Own writing of findings in a clear and self-contained summary

Tutorial 5 – The RSA system



By the end of this tutorial I will be able to

- describe, in a simple case, the operation of the RSA cryptosystem
- explain why RSA is a public key system
- understand the final assignment task

Starter: Review of cryptosystems

The RSA system

Some properties of the RSA system

Final assignment:

Modular arithmetic and the RSA cryptosystem

1. Use the Euclidean algorithm to determine whether 126 and 105 are coprime or not.

   Calculate
   $$([3] + [4])^5 \; mod \; 11$$
   simplifying the steps in the calculation where possible.

   Calculate
   $$5^5 \; mod \; 11$$
   using any results applicable.

2. Describe the operation of the RSA cryptosystem, using as examples calculations in mod 21 arithmetic.

   Explain the reasons for the strength of the RSA cipher.

   Find out about the authentication problem for cryptosystems, and briefly describe how it is solved in the RSA system.

Final assignment success criteria:

- Correct calculations in modular arithmetic, applying techniques learnt in the course
- Lucid explanation of RSA cryptosystem and its properties
- Reference to suitable sources, and clear presentation of research findings
- Justification of claims using appropriate technical vocabulary and logical structuring of argument

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

UNI PATHWAYS

UNI PATHWAYS

researchersinschools.org