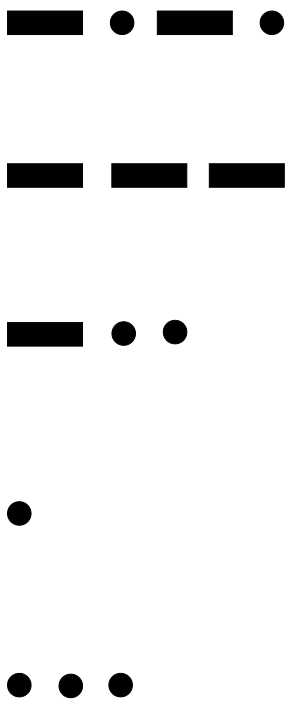
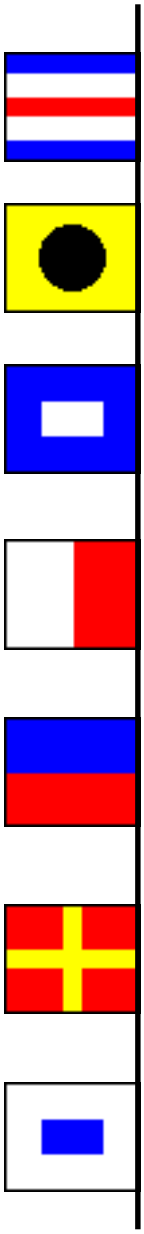
CRYPTOLOGY

Notes



&



Cryptology is the study of 'hidden writing', but is more generally thought of as being to do with codes and ciphers. It involves working with both language and mathematics. For that reason it is an excellent topic around which to base some work in the classroom, and the material offered here was developed with that purpose in mind.

These notes are intended to provide background and guidance to the various sections, worksheets and other support that make up the entire unit on cryptology.

Scrambled Messages

This simple device might be likened to treating the whole message as one big anagram. Technically it is an example of a transposition cipher.

Sheet1. The degree of difficulty experienced (from zero to impossible) will depend very much upon the reading skills of those attempting it. Exercise 1 could be read straight off the page.

Sheet 2. This method is known in the standard works as the "railfence method". Writing the message to be sent in groups of five letters is used without comment. It is, of course, done to make it easier to copy and to work with, rather than having a continuous stream. It is not sent with its original word divisions since that would betray too much of its possible contents.

Sheet 3. Exercise 2 will need some experiments to be tried on paper. It is interesting to see how such a small move on from the previous method makes for a considerable increase in difficulty in reading it.

Sheet 4. This is an extension of the previous method using more lines but organising it by use of a matrix.

Sheet 5. In Exercise 3 it is helpful if squared-paper is available. (Size to suit) The idea of *nulls* to make a message up to size is introduced.

Notice it does matter about the direction of writing the plain and the cipher texts. All that is needed is to know that the two texts are at right-angles to each other, and it is easier to read and look for words when going across than going down.

Buried Messages

The importance of this method is in disguising that there even is a secret message. It was originally devised by Girolamo Cardano in the 1500's and hence known as a "Cardano Grill".

Sheet 1. Contains only instructions on the use of the Window Reader (= Cardano Grill).

Sheet 2. Exercise 4 requires only straight-forward use of the Window Reader.

Sheet 3. Exercise 5 needs the way in which the Window Reader is to be used to be discovered by trial and error. It will be important that the Reader has the arrow (correctly placed) on the back.

Sheet 4. This merely presents the message in its usual 5-letter group format, and shows how it is placed in the grid. Exercise 6 is based on that and again requires the way in which the Window Reader is to be used to be discovered. Squared-paper (1 cm) needed.

Sheet 5. This provides an illustration of how the secret message might be further disguised, culminating in Exercise 7.

Sheet 6. Contains six copies of the Window Reader needed for the various exercises. Worth printing on card if they are to be kept for use another time. It reduces the preparation time as cutting out those square holes is a little fiddly.

Further Work.

The given Window Reader only exposes 24 squares out of the 36 possible on the complete grid. Design and make a grid that will reveal ALL 36 squares (and none twice!).

Improve the sent-message for 'Help me' at the top of Sheet 5.

Write a different set (or maybe just one) of message(s) to put in the 'newspaper' to hide the real messages to be found in Exercise 7.

Devise another set of exchanges that might have happened. The solution should show the real message, the message to be printed, and the grid filled in so that it can be checked easily.

Coded Messages

The difference between codes and ciphers is blurred. Definitions tend to indicate that ciphers operate on the separate letters of the plain text whereas codes work on complete words or even phrases. But it is not quite as simple as that and it is not important.

The code book referred to here is identified as The *Small* Code Book but the explanation given and Exercise 8 can be done using only the single sheet extract provided, but note this is convenient for decoding only.

Sheet 1. The backgound to code books is given. They were indeed much used once, but those days have long since passed and they have a much more limited use now, though they do still have some point.

Sheet 2. Exercise 8. Straight-forward decoding using either the book or the extract sheet.

Sheet 3. Extracts from The *Small* Code Book which allow the exercises to be done.

The *Small* Code Book

This is provided in a separate file and is to be found from the Cryptology Menu. It requires to be printed double-sided on 6 sheets of A4 paper. These are then folded in half, interleaved and stapled through the middle. Printing on coloured paper makes it look much more attractive. It can be a lot of work to make a class-set and is probably only worth doing if it is to be used on other occasions. However, at least a few should be made so that it can be made clear just what a code book is (in principle). The photo-copying, as always, requires a bit of care. Clearly both sides need to be the same way up, but also the page numbers must be correct. It may help to remember that backing numbers must be consecutive. So, starting with 1**:** 1 backs 2, 3 backs 4, and so on. The cover is easy, it is only a single sheet and single-sided!

Further Work

Writing and sending messages to each other is the obvious thing to be done. This is rather limited if only the extract sheet is available. Having and using the code book is much more realistic, apart from the necessarily limited vocabulary of such a small book. Perhaps insist that the message must contain no more than two words which are spelt out in full. Keep an eye on the content that is being exchanged, and every message should bear the name of the sender!

Simple Cipher Messages

This first type of encipherment is the one known to most people where each letter of the plain text is substituted by a letter from the cipher alphabet. These are substitution ciphers.

Sheet 1. How the cipher alphabet can be matched to that of the plain text, either by writing them out on two slips, or by making and using a St Cyr Slide. These can be cut from copies of Sheet 6 (4 to a sheet) printed on paper or card.

Sheet 2. This merely 'bends' the slips of Sheet 1 around into a circle to make two cipher wheels which does away with the doubled alphabet needed for the straight slips and is generally handier to use, besides being a more robust format. Pre-printed wheels are on Sheet 7. Exercise 9 is a straight-forward use of the method whichever aid is used. The last 4 questions require the sort perseverance that is very necessary in later work when attempting some cryptanalysis.

Sheet 3. Introduces the idea of using a mixed-up cipher alphabet and shows just one way of achieving it by using a 'scrambling key'. Exercise 10 uses this.

Sheet 4. Carries on from the previous sheet, only using a ready-made table of mixed-up cipher alphabets. Exercise 11 needs this table (on Sheet 8) to be available. It is also a familiarisation exercise for the use of this table which is built upon in the next sheet.

continued…

Simple Cipher Messages *continued…*

Sheet 5. The security of a given cipher system can be increased considerably, by using several different cipher alphabets over one message and this sheet shows how it can be organised. In fact there was a very long period when it was considered that messages enciphered by such a system were unbreakable. It was Friedrich Kasiski (1805-1881) a major in the Prussian army who published (in 1863) a small book containing an analysis of how such ciphers could be broken. The same analysis had been developed 9 years earlier by Charles Babbage but went unnoticed until very recent times, so Kasiski got the credit for it.

The table on Sheet 8 is needed for Exercise 12 which provides work in reading messages that use this system. The last two questions require a plain text message to be put into cipher.

Sheet 6. Has 4 *St Cyr Slides* for making up. Paper is adequate for these especially if they are not intended to be kept and reused. Cutting the slots can present difficulties. Try folding the wide strip slightly, without creasing it, and making a first cut at the middle. It is called a *St Cyr Slide* after the French Military Academy of St Cyr where students were introduced to it during their cryptology course in the 1800's.

Sheet 7. Cipher wheels for making up. Again, best done on card because they are then definitely easier to handle. So, make a set and make sure they are used again (and again). The centre fastening can present a difficulty, though there is a particular type of paper fastener for dealing with this. A quick fix is to use a drawing pin and push it through into a small piece of soft wood or a rubber. Make the necessary holes in the two wheels separately before putting them together to ensure alignment. The numbers on the inner (smaller) wheel are not needed at this stage.

Pupils could be required to make their own! Nice piece of practical geometry, dividing a circle into 26 equal parts. Sheet 9 could be used to help those who cannot otherwise cope.

Sheet 8. Polyalphabetic Cipher Table. More generally known as a *Vignère Tableau*.

Sheet 9. Circle divider (26) to provide help in the making of Cipher Wheels.

That is the end of what may justifiably be described as the 'simpler' work. It now becomes a little heavier on the mathematics. Modulo arithmetic is used, but no prior knowledge is assumed, the few rules needed are stated with little explanation. Matrix multiplication is also used. It might be an opportunity to do some formal work on these topics, before, during, or afterwards.

Addition Ciphers

Sheet 1. Explains how addition (modulo 26) generates the cipher message.

Sheet 2. Exercise 13 provides practice in doing the above. Note that the last two generate unbreakable messages. The key is as long as the message and so, any key that recovers a readable message will work. The real key is only needed to recover the correct message. So, even this simple system offers some security for short messages with long keys.

The method needed for deciphering such messages starts here and is continued on the next sheet. The relationship between the enciphering and deciphering keys is explained.

Sheet 3. Shows the complete working for deciphering these messages, though it does not need to be set out in such detail. Exercise 14 is a good workout of these new skills.

Multiplication Ciphers

Sheet 1. Introduces the reduced alphabet ADEHILNORST of 11 letters. The reason for this is to keep the arithmetic, multiplication modulo 11, within as small a compass as possible, and these are the most commonly used letters in the English language. A table of results of multiplication modulo 11 is provided, and a demonstration of its use is given by enciphering a message.

Sheet 2. Shows how the deciphering key is formed, and Exercise 15 is a comprehensive set of questions on all of the above.

Sheet 3. Explains one of the important ideas behind modern cryptology, that the message itself should play a part in forming the cipher so that, in effect, the key is changing (or being modified) all the time. Not a new idea – cryptographers in the 1500's used the principle to devise what was known as an 'autokey' system.

Addition and multiplication are now combined to do matrix multiplication (mod 11) and this is explained in detail with the encipherment of a message.

Sheet 4. Shows the same matrix multiplication at work for the decipherment of a message. The necessary multiplication matrix is merely given. The forming of an inverse matrix under modulo arithmetic is not attempted, but is mentioned. Note that the enciphering and deciphering matrix multiplied together should (must!) produce the identity matrix, and that they are interchangeable in their functions.

Exercise 16 provides work on deciphering with the necessary matrix given. The last question is a challenge.

Rotor Ciphers

This section is probably only suitable for a more limited audience. It is an attempt to give a clear idea of the principles behind the famous Enigma machine. Many will have heard of this machine ciphering system and the important part it played in the Second World War.

Sheet 1. Explains the basic principles underlying rotor ciphers and how the model works, including the notation used to indicate how to set it up. This sheet could be omitted, and the whole explanation delivered orally (with some practical work), then only Sheet 2 would be needed if the Exercise 17 is to be done. Certainly some check that the model is being used correctly is needed before embarking on the next sheet.

Sheet 2. Contains a detailed explanation of how the decipherment of a message is carried out, a guide to organised working, and Exercise 17. No enciphering exercises are offered but could be set as an extension. Merely devising a message using only the 11-letter alphabet is an interesting exercise in itself.

Sheet 3. Is the master copy for making the models. Definitely better made on card rather than paper because of the way the rotors have to be manipulated.To allow the whole thing to be fitted into a reasonable space and be clearly legible the reduced alphabet ADEHILNORST of 11 letters, and used in previous work, has been used.

Much has been written about the Enigma machine (and Bletchley Park which was the centre for English cipher breaking in the Second World War and is now a museum). For further reading see the Book List in these notes. Briefly the Enigma machine was invented by Arthur Scherbius, a German inventor, in 1918. At about the same time, similar machines were also invented (independently) in the Netherlands, Sweden, and the USA. They were intended for commercial use mainly, and the military forces of nearly all major countries seemed to ignore their possibilities. The German forces took up the Enigma in 1926 and the rest is - history!

As an indication of the difficulties involved in trying to break the Enigma ciphers, it is worth noting that the machine could generate something like 10^{15} different ciphers.

Cryptanalysis

This is generally considered to be the most interesting part of cryptology: the breaking of an unknown cipher. At the level used here (single cipher-alphabet substitution) it is not difficult provided only that one's reading skills are adequate.

The basis of all cipher-breaking relies on a knowledge of the statistical distribution of the letter frequencies of the language used. So a good prior exercise here is to require a frequency count to be made of the letters found in the written form of the English language. The task can expressed in a form like this:-

> Select any 'ordinary' book. Open it at random. Mark a definite beginning and, starting out from there, copy out 100 (or 50 or 1000 or whatever) letters. Ignore all punctuation and spaces, writing it as one continuous stream. Record the book and page used. Now count how often each letter of the alphabet appears in that stream.
>
> Some sheets from 'Additional Materials' are useful here. The necessary number of letters can be copied on to a *Message Recording Sheet.* (1) will hold 925 letters and (2) will hold 1540 letters. The Letter Frequency Recording Sheet will help with the counting.
>
> Finally, all the separate results can be collated and compared with some 'standard' work on the expected frequencies of at least the more popular letters. There is a sheet on this in the 'Additional Materials' section.

Sheets 1 to 3 explain the method. This could be done as a class demonstration and, for that purpose, the message NJXE**…** is given in slide format in the section entitled 'Display Material'.

Sheet 4 Exercise 18. Given that the most frequent letters are ETA (in some order) in all the messages, these are not too difficult. To reduce the slog of copying out the messages, and to inculcate some organizational methods, the first four are spaced out on **Sheet 7** ready to be worked on. The alphabet underneath each is to record the frequencies of the cipher letters and also the matching plain letters as they are assumed or recovered.

Otherwise, one of the Message Recording Sheets in the 'Additional Materials' section can be used, remembering to leave adequate spacing between the lines. The use of pencil and rubber is almost essential, and should be encouraged – do try something!

Sheet 5 Exercise 19. Getting more difficult. Only the E is a given.

Sheet 6 Exercise 20. No helps. Though these are not, technically speaking, any harder than the previous ones, they do require a lot of work of the trial and error variety and that can prove to be too much for many. It is suggested that these are only given to those who would like something to get their teeth into!

Public Key Ciphers

But only for those who really want to know. The explanation of how the RSA system works is covered in 4 pages using some small numbers. The remaining (10) pages give help with some of the mathematical ideas involved – if needed.

Additional Materials

Some sheets that might come in useful at any time in this work.

Display Materials

A miscellany of some of the subject matter of the various sections, written large, so that it could be projected onto a screen if the work is being delivered from the front, or discussed.

Other Systems

This section gives a quick look at some other ideas for enciphering messages. There are 8 separate self-contained sheets. One way of using this in the classroom would be for pupils to work in pairs. Each pair would have a sheet and be required to study it, before they individually (successfully) wrote a message to each other using the method explained. Given that some other pair(s) could be using the same sheet then the exchange of messages could be widened.

The sheets are not all of equal difficulty and some thought should be given to the matter before they are given out. The 8 sheets are

1. Quick 'n' Easy

The hardest bit for many will be the task set in the 2nd line.

2. A Polybius Chequerboard

This shows another way in which the plain text letters of the alphabet can be identified by cipher. Notice how it doubles the length of the message.

3. A Self-referenced Chequerboard

This idea is very useful since it does allow letters to be enciphered in different ways which, with care, makes it much harder for the cipher to be broken.

4. The Playfair Cipher

Another use of the chequerboard. The strong point of this one is that since it is based on digraphs then, automatically, letter frequencies are not so obvious. It was a very good field cipher.

5. Hiding the Frequencies

This shows another way of hiding letter frequencies. Provided the messages were short enough then they would be unbreakable. But it must never be forgotten that if several messages were sent using the same chequerboard, the count could be aggregated over all those messages and the relative frequencies would eventually show. Technically, this is a homophonic cipher, and this format is not the most usable display. Better is a tabular form where the alternatives for each letter are shown in a list, so the user can readily see which ones are available.

6. The ADFGVX Cipher

A lovely example of a cipher that was actually used, and which led to a most dramatic result when it was broken. The real greatness of Painvin's work was the time scale within which he had to work, linked to the fact that the analysis of that type of cipher had not been done before. As a footnote, the German (Nebel) who invented it had wanted a second transposition (of the rows) but the commanders overruled him, saying it would make too much work of the whole thing. Painvin said, if they had done it, the cipher would have been unbreakable!

7. Book Ciphers

One obvious way for two correspondents who wish to communicate in private is to use identical books and give page/line/word positions to hide their messages. Try it. It can be very difficult finding the the word you need, and the use of a dictionary as the book is merely a gift to the experienced cipher breaker.

The method outlined here is entirely different. It uses the text to provide a very long key. As long as the message in fact. If the starting position is not known, then even having a copy of the book will not help - it is just about unbreakable. **Note:** 2 identical books are needed.

The letter addition idea is not referred to as modulo arithmetic, and it is left to the obvious pattern in the table to deal with what happens when the answer goes beyond 25.

8. Symbol Ciphers

The use of symbols always makes a message look much more formidable. It isn't of course, if it is just a simple substitution cipher. Set up an equivalence table and change all the symbols to letters as they are much easier to work with.

The Stories

Two stories are given in their entirety *The Gold Bug* and *The Dancing Men*. The first is by Edgar Allen Poe, the second is by Sir Arthur Conan Doyle. Both are recognised as classics of the genre.

These stories are worthwhile reading. They show the thinking that goes on when trying to solve a cipher, and that it is much more that just counting letters and making automatic substitutions. What the stories do not do, is to convey the enormous amount of work that usually goes into the trial and error necessary, and following all the false leads that go nowhere.

It is not suggested that class sets of these texts are needed (unless they are to be stored and used more widely) but there should be a few copies around for those who would like to see these classic works, especially perhaps after doing the actual cipher work

The Gold Bug *(1843)*

The full story covers 25 pages.

The actual cipher message is on page 19, and the analysis follows on pages 20 to 22.

Page 19 could be handed out for individual, paired, or group work.

The Dancing Men *(1905)*

The full story covers 10 pages.

The cipher messages are spread through the story, as Sherlock Holmes received them. However, that may not be the most convenient way for our purpose, so they have also been printed all together on a single sheet at the end, and that sheet could be given out, or possibly projected on a screen for discussion/work purposes. Perhaps it should be made clear at the outset that the flags are used only to indicate word-endings. If that is not done, the counting will be wrong and also the advantage of having an unknown message divided into words will be lost. After all, Holmes' analysis first assumes, and then makes use of, that fact. The messages are numbered 1 to 6, but remember that Holmes broke the cipher using only the first five, the sixth one he composed himself. However, he also knew the background and that is an undeniable help (particularly knowing that the name of the lady was Elsie) so, perhaps using all six messages to break the cipher is fair.

> Jules Verne also wrote some stories involving ciphers: *Journey to the Centre of the Earth (1864), The Cryptogram (1882)*, and *Mathias Sandorff (1885)*.
> The second involves a polyalphabetic cipher, the last uses a Cardano Grill.
> All of Jules Verne's books are available for downloading/reading on line.

Further Work

That will be more than enough for most!

A link could be made to science by reference to invisible inks. They are generally good fun, and it is interesting to see how very simple, ordinary materials can be used.

For those who would like to look a little further, there is masses of material on the Web. Just do a search on 'cryptology' – and keep going.

The list of 'Other Sources' given later in these notes also gives some guidance.

For the computer buffs, especially embryo programmers, there is no end of things that can be done. For starters, what about a program that analyses a message and gives frequency counts? And then another one that allows you to try substituting for various letters. And then another one which counts digraphs. And then **…** and then **…** and then its a job for life!

The history of cryptology is quite complex and full of deviations and duplicities as befits such a subject. Only a few highlights along the way are given here

Whilst there are many isolated incidents known about the sending of secret messages in early times there is little evidence of a coherent attempt to regularise cryptography. Also, most of the early work concerned **steganography** (hiding the actual message) rather than **cryptography** (putting the message into cipher).

The first use, of any significance, of a cipher, must be attributed to Julius **Caesar** in about **50 BC**. It was a shift cipher, where each plain letter was simply replaced by another some (fixed) distance away from it in the alphabet.

In the **1300's nomenclators** were introduced and used for many centuries, mainly by diplomats. It was the breaking of one of these that led directly to the exposure of the Babington Plot and the subsequent execution of Mary, Queen of Scots (in **1587**).

Alberti wrote a treatise on cryptology in the **1400's** which is generally accepted as marking the start of modern cryptology. Though his work did not attract much attention at the time he introduced all the basics that would later be used. He is the 'father' of cryptology.

Trithemius wrote the first *published* book on cryptology which appeared in **1518** two years after his death. (Another of his writings on steganography and religious matters, was proscribed by the Catholic church for over 200 years.)

However, the best-known work was that by **Vigenère** which was published in **1585**. Though his ideas were not new they were well-explained, especially regarding the use of polyalphabetic ciphers and keywords. Unfortunately, it appears to have influenced later workers only very slowly.

In France in the **1600's** Louis XIV employed the **Rossignols** (father and son) very successfully as cryptanalysts. They also invented the Great Cipher which was not broken for over 200 years (by **Bazeries**)

By the **1700's** most countries had their **Black Chamber** which is the generic name for centres employed in cipher breaking and intelligence gathering.

The **1800's** were a time of much invention and one of the more important of these was that of the telegraph. Now, using the Morse Code, messages could be sent vast distances very quickly and a means of enciphering those messages was needed. The names of **Wheatstone** and **Playfair** were prominent here. While on the cryptanalysis front, both **Kasiski** and **Babbage** (independently) described how a polyalphabetic cipher could be broken.

In the early **1900's** wireless became available which increased the capacity for sending messages. Then the First World War inevitably encouraged a need for better ciphers and the associated requirement for better cipher breaking. Many interesting stories come from this period. Some prominent 'names' to watch out for are **ADFGVX**, **Painvin**, **Zimmermann**, **Montgomery** & **de Grey**, **Room 40**, **Magdeburg**.

In the **1920's Mauborgne** developed the idea of a **one-time pad** and **Scherbius** invented the **Enigma** machine. In the US, **Yardley** showed how reading the other side's ciphers could play a major part in diplomatic conferences, and the Japanese learnt an important lesson. The US learnt nothing and shut down their Black Chambers!

The **Friedmans** (husband and wife) in the US were employed privately to work on ciphers and even, sometimes, to help out the military. In the run-up to WW2 and and also during the war, he played a major part in breaking the Japanese ciphers, especially **Purple**.

In the **1930's** the Polish cryptanalyst **Rejewski** first broke the early **Enigma** ciphers. This work was continued in WW2 when 'names' like **Bletchley**, **Turing**, **Welchman**, and many others became known, but not until about 30 years after.

During the later years of the **1900's**, with the rise of the internet, the need for the highest possible security became acute. From that need came **asymmetric** and **Public Key** ciphers. Coincidentally, the major names associated with this work, come in three's.

In the UK (at GCHQ) **Ellis**, **Cocks**, and **Williamson**, got all the principles sorted out (by 1975) but were forbidden to publish anything (until 1997).

Meanwhile, in the USA, **Diffie**, **Hellman**, and **Merkle**, had (independently) done very much the same thing but were allowed to publish!

So it was that **Rivest**, **Shamir**, and **Adleman**, got to develop the idea and create the system now known as **RSA**. It was not the only implementation of the idea, but it was the one that became a commercial success.

Now that system is beginning to look as though might be flawed, and the search is on for something better to replace it!

The history of cryptology has one consistent pattern running through it. A new cipher is invented, then it is broken. The period between the two events may be a short one, it may be a long one, but it has always happened that way so far, and there is no reason to believe it will not continue.

But it does not matter. A good cipher will always take time to be broken, and if the incident, the battle, the war, or whatever, is over by the time the real message has been recovered by the 'enemy' then the cipher will have achieved its purpose.

No (genuine) cipher will endure for all time! Will it?

A

ABC code was the earliest of the many code books which became available to commercial users after the laying of the trans-atlantic cable in 1866. The main purpose of such codes was to reduce the cost of sending cable-grams (which were very expensive) by reducing several words to a group of letters which counted as only one word. Secrecy was not paramount.

ADFVGX cipher was a very good German cipher used in WW1 which proved difficult to break. It was a mixture of substitution and transposition.

ASCII is the American Standard Code for Information Interchange and is used internationally to identify 256 different characters (in binary notation) so that they can be sent electronically.

asymmetric keys used in ciphering, mean that the key used to **de**cipher the message is different to the one used to **en**cipher it.

autokey was a method, first suggested in the 1500's, where the message became part of the ciphering system. But often it meant that one error could render the whole message unreadable. It was improved upon later, but did not find general favour.

B

Black Chamber was the term used to describe those offices or departments which dealt with the 'black' art of looking for and breaking cipher messages.

Bletchley Park is an estate in Buckinghamshire, UK, which was acquired by the government to house its Code and Cipher School, where all the cipher-breaking work in WW2 was centred. It is now a museum.

bombe was a machine (electrical/mechanical and not electronic) which could test many variations of a key on a given message much more quickly than could be done by human hand.

C

Caesar cipher was one of the earliest substitution ciphers used (by Julius Caesar, about 60 BC) in which each plain text letter was changed into cipher by using another letter a fixed distance away in the alphabet. It is a simple additive cipher.

cipher text is the form in which an original message, having been suitably 'disguised', is sent.

code is often used as having the same meaning as cipher. Strictly, a code should mean that words or phrases are being substituted, usually by use of a code-book.

Colossus was a major step forward from the **bombe** in that it used electronic valves which made it much faster, and also it could be more easily programmed to deal with different situations. It is often described as the 'first' modern digital computer. (1943).

crib A crib is when a piece of the original plain text is known (or can be reasonably guessed at) and can be used as an aid in breaking into the cipher message.

crypt- comes from the Greek word for 'hidden'.

cryptanalysis is the means by which a cipher message is analysed and broken without knowing the key.

cryptography is the practice of devising and writing hidden messages.

cryptology is the general term to cover the study of all the work dealing with hidden messages.

D

Data Encryption Standard or **DES** was the system adopted by the US government in 1976 as being the official standard. It is, in effect, a transposition cipher, but the necessary moving around is done on the binary digits of the message and not the individual letters or words. It is extremely complicated and can only be done by a computer.

decipher, **decrypt**, **decode** all refer to the work of recovering the plain text of a message which has been hidden by use of a cipher or code.

digraph, **bigram** is a group of two adjacent letters.

E

encipher, **encrypt**, **encode** all describe the business of hiding a plain text message by putting it into cipher or code.

Enigma was the name of an enciphering machine made in 1918 by the German inventor Arthur Scherbius, and was employed with devasting effect by the Germans in World War 2.

G

G C H Q is the Government Communications Headquarters, which is the main centre in the UK for all matters dealing with communications (including ciphers). It is located near Cheltenham.

K

key is used in cryptology in the sense of an object that is used to lock (or unlock) something. It is the element which controls the variables that set up the cipher or the system. More than one key may be used.

M

magic was the code-name of the USA operation dealing with the breaking of the Japanese top-level ciphers.

microdot is the business of so miniaturising a message, even the size of a whole page, that it is no bigger than a full stop which can then be 'hidden' by simply sticking it in place on an innocuous piece of writing. The actual message could be in cipher. First used in 1941.

monoalphabetic means that only a single cipher alphabet was used to encipher the plain text message.

N

N S A is the National Security Agency which is the main centre in the USA for all matters dealing with communications (including ciphers). It is located at Fort Meade, Maryland.

nomenclator is the name for a book (or a system) which uses a combination of cipher and code to encrypt a message. This method gained some favour in the 1500's.

nulls have no meaning. They are put in either to confuse those trying to break into the cipher (by altering the frequency of the letter-count) or to make a message up to some specified length

O

one-time pads are randomly produced sets of keys, made up into pads, which are used for messages between individuals. Each key is destroyed as it is used, so it is a one-time system, and very secure.

P

P G P Pretty Good Privacy is the name of a system, devised by Phil Zimmermann, based on the **RSA** system but with additions, and which is freely available to private individuals for their own use.

plain text is the original message in readable form.

polyalphabetic means that more than one cipher alphabet was used to encipher the plain text message.

public key cryptography is an **asymmetric** cipher system. That is, it uses two different keys, one to **en**cipher the message and a different one to **de**cipher it. This means that one of the keys can be published openly for anyone to use, but only the person who owns (and created) the key has the other key to decipher the message.

PURPLE was the code-name given to one of the top-level Japanese ciphers.

R

Room 40 in the Old Admiralty Building in London was the centre for the UK's cipher-breaking efforts in World War 1.

rotor ciphers are those generated by machines containing their wiring in a system of wheels (or rotors) which are continually being moved so as to make up many different cipher alphabets. Examples are Enigma, Sigaba, Typex.

R S A is the name given to an **asymmetric** cipher system devised by Rivest, Shamir and Adleman. It is used in **public key** ciphers.

S

SIGABA a top-level machine used by the US military, which used a form of **rotor** ciphering.

sigint means Signals Intelligence. This refers to the gathering of messages from many sources, but mainly radio and cable, and the information that can be derived (before any cipher breaking is done) from knowing the positions of its sender and its destination, and possibly, who they were. Useful **cribs** can be derived in this way.

steganography means 'hidden writing'. In this, the aim is that the message itself is hidden so it is not apparent there even is a message. The most obvious example is when invisible ink is used or, in more recent times, the use of **microdots**. The hidden message could still be in cipher.

substitution cipher is a ciphering system which changes every letter in the original plain text message into another (usually different) letter in the cipher message.

super-encipherment means that (at least) two enciphering processes have been used in succession in changing a message from plain text to cipher text. Often, one will be of the substitution type, the other, transposition.

super-imposition is the method used to break a cipher when several messages have been found which are known to have been enciphered by the same system and key

T

transposition cipher is one in which the real message is disguised by re-arranging its letters in some systematic way, rather like an anagram on a large scale.

trigraph, **trigram** both mean a group of three adjacent letters.

TYPEX a top-level machine used by the UK military, which used a form of **rotor** ciphering.

U

ultra was the code-name of the UK operation dealing with the breaking of the German Enigma ciphers.

V

Vernam key was one of the early attempts (1920's) to utilise a key which was extremely long. Ideally, it should be at least as long as the message itself. It was implemented on the punched-tape systems in use at that time.

Vigenère tableau is a set of a pre-prepared cipher alphabets, laid out in the form of a table.

Z

Zimmermann telegram a famous instance in World War I where the breaking of a German cipher was a direct influence on the USA in entering into the war.

Adleman Leonard *(-)* US mathematician who put the 'A' into the public key system known as RSA.

Alberti Leone Batista *(1404-1472)* Italian architect and polymath who wrote the first treatise on cryptology.

Babbage Charles *(1791-1871)* Professor of mathematics at Cambridge, UK. Noted as an inventor, especially of an early form of mechanical computer. Was a formidable cryptanalyst.

Bacon Roger *(1214-1294)* English philosopher who produced the first known European work on cryptography.

Bazeries Etienne *(1846-1931)* Commandant in the French Army who was a master cryptanalyst in the period, roughly, 1890 to 1920

Cardano Girolamo *(1501 -1576)* Italian mathematician. A prolific writer on all manner of things, he invented the Cardano grill for hiding messages.

Childs J. Rives *(1893-1987)* US Army lieutenant in WW1 who did excellent work on cipher-breaking. Later became a politician and ambassador.

Cocks Clifford *(-)* English cryptographer. Worked with **Ellis**.

Diffie Whitfield *(1944-)* US mathematician and cryptographer. In early 1970's, with Hellman and Merkle, developed the asymmetric key principle.

Ellis James *(-1997)* English cryptographer. Worked at GCHQ and (with others) devised a public key system in the 1970's, but was not allowed to publish it, so it did not become generally known until 1997.

Friedman William *(1891-1969)* US Army colonel. One of the greatest of cryptanalysts, he was very successful over a 40-year period. His work culminated with the breaking of the Japanese Purple cipher at the beginning of WW2.

Friedman Elizebeth *(1892-1975)* Wife of, and co-worker with, William. Also aided the Authorities by breaking the ciphers of the bootleggers in the 1920's and 30's.

Hagelin Boris *(1892-)* Swedish engineer who invented a successful mechanical enciphering machine, used in the US as M209 version, which made him a millionaire.

Heburn Edward *(1869-1952)* developed and built rotor ciphering machines in the USA from 1921 onwards.

Hellman Martin *(1946 -)* US cryptographer who worked with **Diffie**.

Hitt Parker *(-)* US Army colonel. Cryptanalyst in WW1.

Kasiski Friedrich *(1805-1881)* Prussian Army major. Wrote first analytical solution of a polyalphabetic cipher .

Kerckhoffs Auguste *(1835-1903)* Dutch professor of languages published, in 1883, the first explicit set of principles governing all cryptological process.

Mauborgne Joseph *(1882-)* US Army major. Chief Signals Officer who developed the 'one-time pad'.

Merkle Ralph *(1954-)* US cryptographer who worked with **Diffie**. Later worked in nanotechnology.

Painvin Georges *(-)* French Army lieutenant. Credited with breaking the ADFVGX cipher in World War I.

Playfair Lyon *(1818-1898)* 1st Baron. Professor of Chemistry at Edinburgh, Scotland. MP. Helped to devise the cipher system bearing his name.

Polybius *(201 - 120 BC)* Greek historian. One of the earliest writers on a practical cipher system, based on the 'chequerboard' idea.

Porta Giovanni Battista Della *(1535-1615)* Italian scientist. The earliest cryptologist to show how polyalphabetic ciphers might be broken.

Rejewski Marian *(1906-1980)* Polish cryptanalyst who was the first to break the Enigma ciphers in 1932

Rivest Ronald *(-)* US computer scientist who took up the work of Diffie, Hellman, Merkle and, with Shamir and Adleman, created the public key system known as RSA.

Rowlett Frank *(1908-1998)* US Army colonel. First government-appointed cryptanalyst. Was responsible for breaking many top-level ciphers in WW2.

Shamir Adi *(-)* US mathematician who put the 'S' into the public key system known as RSA.

Trithemius Johannes *(1462-1516)* Benedictine abbot in Germany, who wrote the first book on cryptology.

Turing Alan *(1912-1954)* English mathematician and cryptanalyst. Did major work first in breaking the Enigma ciphers, and later into developing one of earliest electronic computers.

Wheatstone Sir Charles *(1802-1875)* English physicist who invented many instruments for telecommunications and also helped devise the Playfair cipher.

Williamson Malcolm *(-)* English cryptographer who worked with **Ellis**.

Vernam Gilbert *(1890-1960)* US Electrical engineer who devised the idea of a one-time tape which enciphered messages as they were keyed in.

Vigenère Blaise de *(1523-1596)* French diplomat and writer, who wrote a major work on cryptology in 1585.

Walsingham Sir Francis *(1530-1590)* English diplomat. Credited with reforming the "Intelligence Service", he did a lot to keep Elizabeth I secure, including the cipher-breaking which resulted in the execution of Mary, Queen of Scots.

Yardley Herbert *(1889-1958)* US crytanalyst in WW1 and afterwards. Wrote book which raised public awareness of cipher work. Unpopular with government! Very 'colourful' character.

Zimmermann Arthur *(1859-1940)* German Foreign Secretary. His ciphered message to Mexico in 1917 was broken and helped decide the USA to go to war.

Zimmermann Phil *(-)* US computer scientist who devised the cipher system PGP (Pretty Good Privacy) especially for the 'ordinary' user of the Internet.

BOOKS

Only titles, author(s) and date of first publication are given which should be sufficient to locate it – if it is still in print, and many are not, but should be obtainable through libraries.

The Code Breakers by David Kahn, 1967

This major work which covers over 2,000 years of cryptology, and runs to nearly1200 pages, is a must for all who have a strong interest in the subject. There are shorter versions which omit much of the technical detail. Its date of publication precludes it from being topical over things like Enigma and Public Key ciphers.

The Code Book by Simon Singh, 1999

Has a much shortened version of the history of cryptology but gives very good coverage to the second half of the 20th century.

Code Breakers: The Inside story of Bletchley Park by Hinsley & Stripp, 1993

A collection of accounts of the many aspects of Bletchley Park, written by those who served there in the different sections.

Enigma: The Battle for the Code by Hugh Sebag-Montefiore, 2000

Very full account of the Enigma ciphers, and the people involved from 1930 to 1945.

The Hut Six Story by Gordon Welchman, 1982

An account of the breaking of the Enigma ciphers by one of those who did it.

Ultra Goes to War by Ronald Lewin, 1978

The Enigma story, told (by an historian) without too much technical detail

The Emperor's Code by Michael Smith, 2000

On the breaking of the Japanese ciphers by the Allies.

Code Breaker in the Far East by Alan Stripp, 1995

The British contribution to breaking Japanese ciphers by one in the middle of it.

The American Black Chamber by Herbert Yardley, 1931

Very good read on all aspects by a master cryptanalyst. This was the one the US government did not want published. Read it, and it will be clear why.

Elementary Cryptanalysis by Abraham Sinkov, 1966

All fully explained by a professional mathematician and cryptanalyst

Elementary Cryptanalysis by Helen Fouché Gaines, 1939

Detailed explanations of methods of solving all the classic forms of ciphers.

On the WEB

There is much. Go to any search engine (www.google.com) and give it 'cryptology' and you will be offered about 100,000 documents! Be more specific, like 'cryptology + transposition' to cut it down. 'Cryptology + museum' is very good.

Search on 'lanaki' which is the pseudonym of Randy Nichols, a former president of the American Cryptogram Association. He ran a course for some students which was delivered entirely on line, but the lessons (all 21 of them) are available for anyone to look at. Very heavy stuff this, but could be useful for filling in some detail. (Like how to do a Kasiski analysis for example.)

Try www.simonsingh.net. This is the home page of the author of *The Code Book* mentioned above. Amongst another things it offers a chance to purchase (at little more than cost price) a CD-ROM which contains a wide variety of information, activities and material.