

The History of Cryptography

How the history of codebreaking can be used in the mathematics classroom with resources on a new CD-ROM

by Simon Singh

The Code Book on CD-ROM

The Code Book on CD-ROM operates on PC computers and should be compatible with any version of Windows. It should start up as soon as it is inserted, or you can double-click on the open icon in your CD-ROM folder.

The CD-ROM largely follows the structure of *The Code Book* with chapters that focus on the birth of cryptography, Victorian ciphers, World Wars I and II, the Information Age and Quantum Cryptography. Each section includes history, interactive tools, explanations, animations and video clips from the Channel Four series *The Science of Secrecy*.

In this article, I will use underlined keywords to refer to particular pages from the CD-ROM. If you visit the CD-ROM index (by clicking on the ? box) and type the underlined keywords into the search box, then it will take you directly to the relevant page. I hope that this article will give you some ideas about how to use the CD-ROM in the classroom, but specific suggestions and worksheets are available on the CD-ROM in the Teacher section.

The CD-ROM could be used to prepare a lesson or in the course of a lesson. It could be used in connection with a whiteboard or networked to a room of PCs. Alternatively, you could copy the CD-ROM onto several PCs, which would allow pupils to indulge in some of the encrypting and codebreaking activities. Finally, you are welcome to copy the CD-ROMs for free distribution to your students, although you might find it cheaper to order more copies at www.simonsingh.net, where CD-ROMs are available at cost price.

Introduction

Since writing *The Code Book* (a history of codes and codebreaking), I have given several talks about cryptography to pupils ranging from 9 to 18 years. The subject is of obvious interest to young people as it includes spying, intrigue, secrecy, the Enigma cipher, mobile phones and the Internet. Furthermore, cryptography is built on mathematics so it can be used to illustrate several aspects of the topic and its applications in the real world. Because cryptography has such a long and rich history, there is the opportunity to pick up on aspects of the history syllabus, such as the Elizabethans or the Second World War.

New projects mean that I am not visiting schools for the foreseeable future, but I am still keen to encourage cryptography in the classroom, so this article includes some examples of how a lesson could be built around the history of codes and codebreaking. The different suggestions are appropriate for a range of ages and abilities. I should stress that my background is as a journalist rather than a teacher, so there may well be some missed opportunities, and I would appreciate any feedback on how my examples could be improved or suggestions for other ways of linking mathematics and cryptography in the classroom.

In addition to this article, teachers might find it helpful to read *The Code Book*. Also, Nick Mee of Virtual Image Ltd and I have developed an interactive CD-ROM to accompany *The Code Book* and to support cryptography in the classroom. A free copy of the first release of the CD-ROM accompanies this journal. Much of this article emphasizes how the CD-ROM can be used in the classroom.

The Birth of Cryptography

Ever since humans have been sending messages, there has been a need to protect them from prying eyes. There are two methods that can be used to encrypt a message. The *transposition* method moves the characters around. For example, letters can be written back to front. The CD-ROM contains examples of transposition, such as the railfence cipher or the scytale, but the alternative method, *substitution*, is of more mathematical interest. Substitution involves replacing each character with a difference character.

An elementary substitution cipher is the Caesar shift cipher, whereby each letter of the alphabet is substituted by the letter that is a fixed number of places further down the alphabet. If every letter is shifted 2 places, then A is encrypted as C, and B is encrypted as D, ... and Z is encrypted as B. Cryptographers deal in terms of the original or plain alphabet and the cipher alphabet. When they are placed next to each other, then the shift becomes apparent.

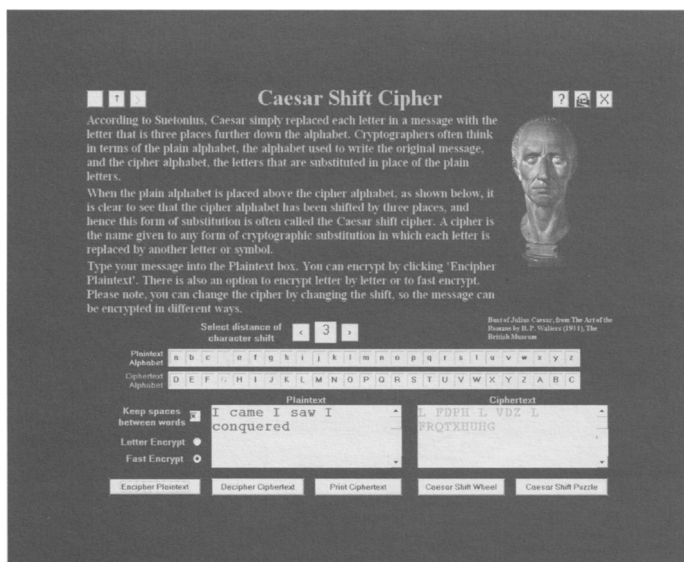
| Plain alphabet | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| Cipher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

Because messages are usually composed of letters, the link to mathematics is not obvious. However, in this case, we can think of the Caesar cipher in terms of addition. If each letter is labelled 0–25, then encryption involves adding a fixed value to each number, and the result is converted back to a letter. For example, if the shift is two, then A = 0, and $0 + 2 = 2$, and 2 = C, so A would be encrypted as C. If encryption is addition, then decryption is subtraction.

Interpreting the Caesar cipher mathematically also involves an understanding of modular arithmetic. For example,

$Z = 25$, and $25 + 2 = 27$, and $27 = 1 \pmod{26}$, and $1 = B$, so Z would be encrypted as B.

The CD-ROM has some history about the Caesar cipher and an interactive tool that can be used to encrypt and decrypt messages. There is also a video clip that shows a Caesar wheel, a device composed of two discs with alphabets drawn around the edge of each one. The discs can be placed on top of each other and rotated to correspond to a particular shift. The CD-ROM provides a printout that pupils can use to build their own Caesar wheel. Other exercises might involve pupils encrypting their own names using a shift of their own choice. Or encrypted words might be given to pupils. If codebreaking is done in teams, then each member of the group could check a different shift.



The Caesar Shift Cipher page from the CD-ROM, which enables you to type in a message and encrypt it according to a shift of your choice. You can also decrypt messages, including a puzzle message, which would require checking various shifts. It is also possible to cut and paste the encrypted text, which could then be e-mailed to somebody. Alternatively, the encrypted message could be texted via a mobile phone

As well as additive ciphers, there are also multiplicative ciphers, or a combination of the two, which is known as an affine cipher. The multiplicative cipher has an interesting mathematical quirk that pupils can explore. Although it is alright to multiply by 3, it is not alright to multiply by 2. This is because if every letter is multiplied by 2, then pairs of letters are encrypted in the same way. For example, both A and N are encrypted as A, because 2×0 and 2×13 are both equivalent to zero (mod 26). In fact, you can only multiply by a number that does share a factor with 26.

Before concluding this section, it is worth noting that each cipher has an inherent flexibility, which is technically known as the key. The Caesar cipher is flexible because it allows any shift between 1 and 25, so it has 25 possible keys (or 26 keys if you allow the zero shift). The most general form of substitution allows the cipher alphabet to be any rearrangement of the alphabet, so it has $26!$ or 400 million billion billion keys. Pupils could work out the number of keys for these two ciphers and various other ciphers, such as the multiplicative and the affine ciphers.

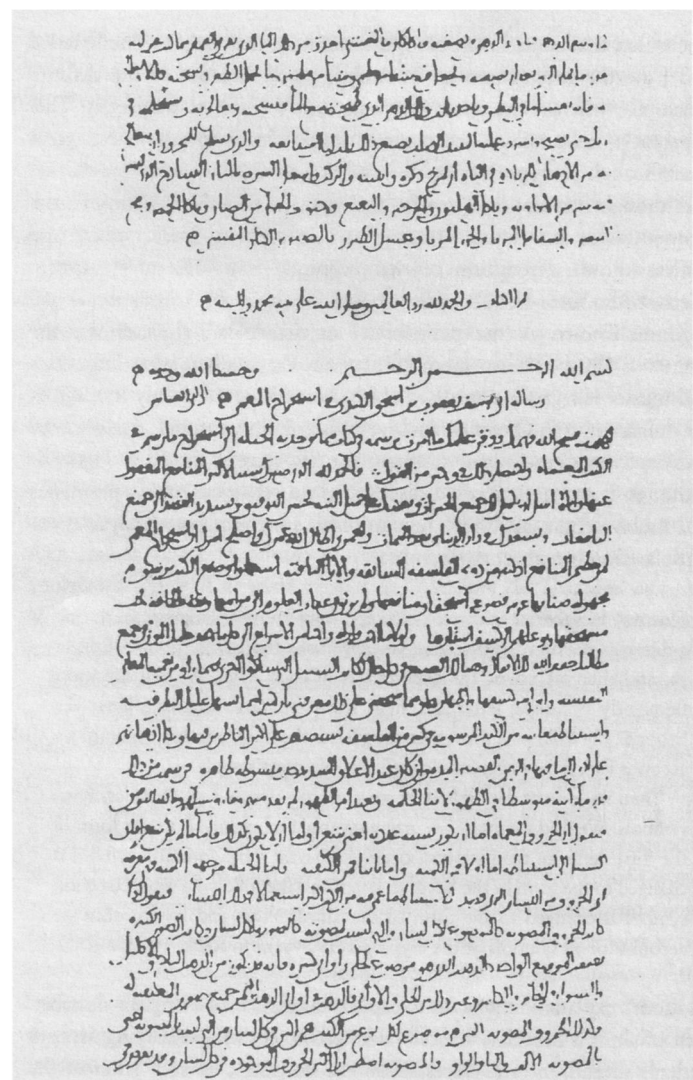
Along the way they would learn about the mathematics of permutations. Pupils are often surprised at the huge number of keys that arise out of rearranging just 26 letters, and are

further shocked at the amount of time it would take to crack an encrypted message by brute force. If everybody on the planet worked night and day checking one key per second, how long would it take to crack the general substitution cipher?

Codebreaking

The history of cryptography has two sides. There are those who develop ciphers and those who crack them. The sender and receiver both know the recipe for encryption and decryption (i.e. the key), but potential eavesdroppers are kept in the dark. If the encrypted message is captured by an eavesdropper, then it is passed to the codebreaker, who has the job of deciphering the message without any prior knowledge of the key.

It is not known who pioneered codebreaking (or cryptanalysis), but the earliest essay on the subject is by the 9th century scientist al-Kindi, who was working in Baghdad. Known as the philosopher of the Arabs, al-Kindi was the author of 290 books about medicine, astronomy, mathematics, linguistics and music but his greatest treatise, which was only rediscovered in 1987 in Istanbul, is entitled *'A Manuscript on Deciphering Cryptographic Messages'*.



The first page of al-Kindi's manuscript *On Deciphering Cryptographic Messages*

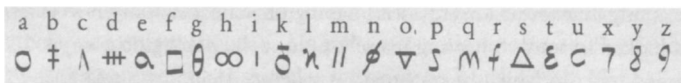
Al-Kindi noticed that if a letter is replaced with a different letter (or symbol), then the new letter will take on all the characteristics of the original. A letter might be disguised, but it can still be recognized because its traits have been passed onto its substitute. The most obvious trait is

frequency. The letter E is the most common letter in English, accounting for 13% of all letters, so if E is replaced by W, then W will account for 13% of letters in the encrypted message, so a codebreaker can work out that W actually represents E.

Cracking the substitution cipher by so-called frequency analysis offers plenty of opportunity for learning about mathematics. Pupils can gather data and plot bar graphs showing the frequency distribution of letters, which is fairly universal for any English text, but which varies from language to language. They can use this to crack real messages. Also, pupils can see how the distribution tends towards the average distribution as the sample text increases in size. Another interesting exercise is to plot the inverse of the number of points attributed to scrabble letters and compare this to the previous frequency distribution.

The CD-ROM can contribute to a lesson in several ways. There is a video clip relating to the invention in Baghdad of codebreaking, and another that shows how frequency analysis works by comparing the frequency distributions of Shakespeare's *Hamlet* and *The Sun*. They use the same proportion of letters but just put them in a different order. There is also a frequency analysis tool which will help pupils to crack codes by plotting frequency charts. There is even a page that will generate a puzzle message for pupils to crack. In addition to counting letter frequencies, the code-breaking tool gathers letter pair (digraph) frequencies and other useful statistics.

One of the advantages with cryptography is that it is cross-curricular and the CD-ROM has a section devoted to Mary Queen of Scots, who plotted against Elizabeth I and sent coded messages. The CD-ROM contains video clips, details of Mary's cipher, and describes the execution that was a consequence of her broken cipher. Pupils can write messages using Mary's cipher or even decipher a message encrypted using her cipher alphabet.



The Cipher of Mary Queen of Scots

The Enigma Cipher Machine

As each cipher is broken, cryptographers set about designing stronger systems for encryption. For example, instead of substituting individual letters, the sender might substitute pairs of letters, which is known as digraph substitution. Better still, there is the book cipher, which allows any book to be the key, and which provides multiple substitutions for the same letter. This type of cipher was used to encrypt the notorious Beale papers, which apparently contain the location of a multi-million dollar treasure.

One of the pivotal breakthroughs in cryptography was the invention of the Enigma cipher machine which mechanized encryption and foiled frequency analysis. The machine looks like a typewriter and essentially has three components. First, there is an input keyboard. Second, there is an output lampboard. Third, in between the keyboard and lampboard, there is a scrambling device, which means that typing A might cause the letter M to light up on the lampboard. Crucially, the scrambling part of the Enigma has a dynamic element, which means that the scrambling mode changes after each letter is typed, so inputting A several times will



Second World War Enigma Cipher Machine

result in a pseudorandom output on the lampboard. In summary, this electromechanical machine connected the input to the output via an electrical circuit, and the circuit was constantly changing.

The Enigma machine was invented by Arthur Scherbius after the First World War and it was then used by Germany prior to and throughout the Second World War. Army units, the Luftwaffe, the Navy, railway stations, the civil service and anybody else who was sending secret messages would use the machine to encrypt and decrypt.

The CD-ROM has a video clip which allows users to meet the machine and see it being used. It also explains the basic principle behind the machine with an animation. Other animations become increasingly complex as new elements of the machine are introduced. Finally, there is a complete Enigma emulator, which behaves just like a real Enigma machine, and which allows pupils to encrypt and decrypt messages and send them via e-mail. The emulator also makes it possible to see the complete internal wiring of the machine and how this determines encryption. To ensure that this part of the CD-ROM loads properly, please access it via *Mechanisation of Secrecy*, then click on 'Using the Enigma', then click on 'Enigma emulator'.

It is important to appreciate that the strength of the Enigma machine did not depend on preventing it falling into Allied hands. Instead, it was the machine setting or key

that had to be concealed. The machine has billions of possible settings. If the sender and receiver have the same setting, then encryption and decryption are simple, but the eavesdropper who has not been told the key has to somehow deduce it. Nazi cryptographers believed that it was impossible to work out the key, and checking every key was impractical, so they assumed that German communications were safe. As we know now, they were wrong and Allied codebreakers at Bletchley Park routinely cracked the Enigma cipher.

Exercises for pupils might involve working out how many keys the Enigma machine has. For example, one feature of the Enigma key setting is a set of three rotors, each of which can be placed in 26 orientations. How many settings is this? These rotors can be swapped around – how many ways are there to put three different objects in three positions? How many more permutations are there if you can choose three rotors from a selection of five and put them in three positions? The Germans, however, decided that no rotor could remain in the same position two days running, so how many permutations are available on any particular day?

Another aspect of the key was a plugboard setting, which enabled pairs of letters to be swapped. So a plug cable connecting A and W meant that typing the letter A resulted in the signal following the path that would have been followed if W had been typed, and vice versa. Both sender and receiver must have the same plugboard setting. A question for pupils might be to work out the number of keys available if there are two plugboard cables to be placed in any 4 of the 26 letter sockets. The first cable can be placed anywhere, the other end can be placed in one of the remaining 25 sockets, and the first plug of the second cable can be placed in any one of the remaining 24 sockets, and the last plug has 23 potential sockets. So we have $26 \times 25 \times 24 \times 23$ possibilities. But if we had placed the first cable in letters A and J, and the second cable in V and D, then this would be the same as having placed first cable in V and D, and the second one in A and J. So we have to divide by 2!. Furthermore, plugging the first cable into A and J is the same as plugging it into J and A, and V and D is the same as D and V. So we have to divide by 2^2 . So the result is $26 \times 25 \times 24 \times 23 / (2! \times 2^2)$.

For N cables, the result is:

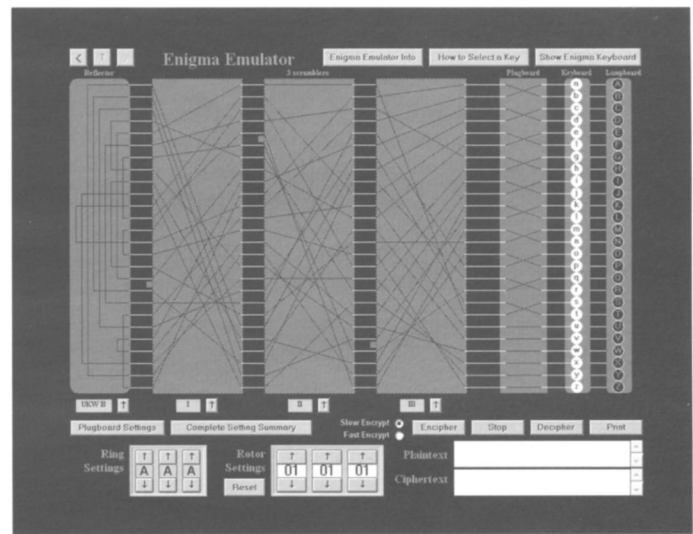
$$26 \times 25 \times \dots [(26 - (2N - 1))] / (N! \times 2^N).$$

An interesting question is to work out the number of cables that gives the biggest number of permutations. The answer is not 13. Alternatively, pupils can examine a simpler plugboard by looking at the permutations within a plugboard of 4 sockets and 2 cables, or 6 sockets and 2 cables, etc. A full and adequate description of the Enigma is not possible in the space available, but ten minutes with the CD-ROM should give you a decent idea of the inner workings of the Enigma cipher.

Again, here is an aspect of cryptography that ties in with the history syllabus, namely the Second World War. Furthermore, Alan Turing and the other mathematicians who cracked the Enigma cipher show the application of mathematics and how it can change the course of history. One of the reasons that I enjoy talking to teenagers about cryptography is that it demonstrates that mathematics is not just fascinating for its own sake but can also be a matter of life and death. Mathematicians can be heroes too.

Modern Cryptography

Now that we live in the Information Age, cryptography is more important than ever before and the mathematics



The Enigma emulator on the CD-ROM has all the features of a genuine Enigma machine and enables you to encrypt and decrypt messages

involved plays an integral part in our daily lives. Mobile phones, pay-TV, encrypted e-mails and e-commerce would not be possible without the mathematics of cryptography. I have not properly explored how this area of mathematics can be used in the classroom, so I would appreciate any ideas. In the meantime, here are a few initial thoughts.

Computer cryptography also involves substitution and transposition, but first letters have to be turned into binary numbers via ASCII code. These numbers can then be encrypted by entering them into mathematical functions. The receiver takes the encrypted number and reverses the function to obtain the original number. Pupils can experiment with binary numbers and manipulating them, and can even invent their own encryption functions.

Ciphers such as the Data Encryption Standard (DES) use this principle. Again, this is a cipher that has different settings or keys. The number of possible keys is 2^{56} . When the DES cipher was developed in the mid-1970s, it was impossible to check every key and crack the cipher by brute force. Today, however, there are modern computers that are fast enough to crack the DES cipher within a day. A task for pupils might be to work out how long it would take to crack DES using a standard home PC, assuming a certain number of operations per second. Or, if computers double in speed every 18 months (Moore's Law), how long will it be before a home computer can crack DES within a day. Or, how long would it take to crack other modern ciphers, such as the new Advanced Encryption Standard, which has 2^{128} keys.

So far, all the ciphers that have been discussed have been traditional (or symmetric) ciphers, which means that decryption is the opposite of encryption and the sender and receiver have the same knowledge, namely the key. How the sender and receiver agree the key in the first place has always been a thorny issue known as the key distribution problem. For centuries the sender and receiver had to meet to agree the key or a trusted courier had to deliver the key.

However, in the 1970s cryptographers developed the concept of public key cryptography which allowed two people who have never met to send each other secret messages. This is why it is possible to send your encrypted credit card details to a company that you have not dealt with before but they (and nobody else) can still decrypt the details.

We can compare traditional and public key ciphers in the following way. If I want to send you a precious jewel, then I can put it in a box and lock it with a key. But when the box is delivered to you, you cannot open it because you do not have the key. This is an analogy for traditional encryption. In contrast, what would happen if you (the receiver) send me an open padlock and kept the key to the padlock. I could then use the padlock to lock the jewel in a box, because I do not need the key to snap the padlock shut. When you receive the box, you can open the padlock, because you retained the key.

In essence, this is what happens when you buy something on-line. Your browser automatically asks the retailer to send its padlock to you, which is then used to lock up your credit card details. The card details can be unlocked by the retailer, who retains the key to the padlock.

A full explanation of public key cryptography is outside the scope of this article, but it is described in detail on the CD-ROM. At the heart of public key cryptography is a one-way function that involves exponentials, modular arithmetic, prime numbers and the difficulty of factoring compared to multiplication. In other words, here is an excellent opportunity to discuss these topics in a context that involves real world applications.

Again, cryptography shows that mathematics is relevant to the real world. Without the mathematics of cryptography, the financial landscape would look very different and the dot.com revolution would never have happened.

To show that mathematics and politics sometimes encounter each other, teachers could point out that modern ciphers are effectively unbreakable, bringing unparalleled levels of security to everybody from businesses to MI5. This, however, leaves us with some difficult problems because these ciphers can also be used by criminals and terrorists. Mathematical cipher algorithms are at the centre of a debate about the politics of encryption. Civil libertarians believe that we all have a right to the encryption that enables privacy, while law enforcers are concerned that criminals and terrorists will use unbreakable ciphers to evade surveillance.

In conclusion, cryptography is a topic that can be used to illustrate the principles of mathematics and its applications. Furthermore, it mixes mathematics with history and brings to light those mathematicians who have influenced history, from the execution of Mary Queen of Scots to the Second World War. Finally, it shows how mathematics and politics can mix in relation to the issue of privacy. All in all, codes and codebreaking is a rich topic that can be brought into the classroom in many different ways.


Using the CD-ROM

I hope that the CD-ROM will encourage the discussion of cryptography in classroom. In addition to being used in mainstream teaching, I also hope that it will be used in maths clubs, maths masterclasses and summer schools. I am also wondering whether it can be used as part of the data gathering exercise that is part of the GCSE mathematics course. Cryptography and the CD-ROM could also be used at the start of a lesson as a quick warm-up exercise or it could be the basis for more detailed project work.

If you would like to see the notes and worksheets that have already been developed for teachers, then you can visit the teacher section of the CD-ROM, where you can download some documents. A shortcut to these documents will appear on your desktop, but this may not work, in which case you

will probably find the documents in a folder marked **Codebook** on your main drive. For the latest material, please visit the Crypto Corner section of my web site: www.simonsingh.net where you can also keep up to date by signing up to the newsletter. Furthermore, the web site has a section where you can obtain further copies of the CD-ROM at cost price.

If you have developed a document relating to cryptography or the CD-ROM in the classroom and you would like to share it with other teachers, then please e-mail it to my assistant Claire Ellis (enigmaproject@hotmail.com) who will publicize it via my web site. Also, this CD-ROM is a brand new resource and Ms Ellis would be very interested to know the reaction of teachers and how the CD-ROM is being used. Furthermore, Ms Ellis is currently visiting schools in SE England, demonstrating a genuine Enigma cipher machine and talking to pupils about cryptography. Please e-mail her for more information and to arrange a visit.

Good luck and ibqzdsbdljoh. 

Keywords: Cryptography; Codes; History.

Author

Simon Singh, contact via: www.simonsingh.net

Simon Singh has a PhD in physics and is the author of *The Code Book* and *Fermat's Last Theorem*. He has also presented radio and television programmes about science and mathematics. For more information about his work and forthcoming projects, you can visit his web site www.simonsingh.net and he can be contacted via his assistant Claire Ellis (enigmaproject@hotmail.com).

The History and Use of Proof in Mathematics

Saturday 20 & Sunday 21
September 2003

A joint meeting between Oxford University
Department for Continuing Education
and

The British Society for the History of Mathematics
held at
Rewley House, Wellington Square, Oxford

The programme for this two-day conference will cover a variety of aspects of the history and use of proof. Issues addressed will include early examples of proof in mathematics, developments in proof, famous problems and the search for proof, software correctness and proof in the school mathematics curriculum.

This conference will appeal to those working in mathematics and mathematics education as well as those with a general interest in the subject.

For further details when available please contact Administrator, Day and Weekend Schools, OUDCE, 1 Wellington Square, Oxford OX1 2JA 01865 270368 or visit the BSHM website <http://www.dcs.warwick.ac.uk/bshm/index.html>