
September 2002
Features

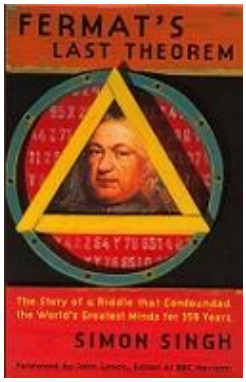
Safety in numbers

by Rachel Thomas

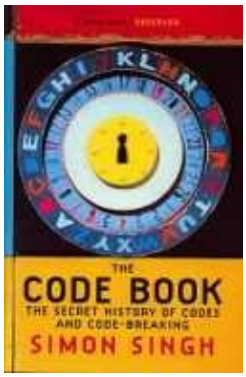
Encryption, codes and ciphers were once associated only with spies, espionage and illicit letters between lovers. But cryptography − the science of secrecy − is now a part of our everyday lives, and we use it whenever we send an e−mail or shop online. It is the mathematics behind cryptography that has enabled the e−commerce revolution and information age.

Simon Singh speaking at the IMECT conference in July

Plus met Simon Singh to talk about the science of secrecy in the art deco monolith of Senate House, part of the University of London... an appropriate meeting place, since Senate House is thought to be the inspiration behind the "Ministry of Truth" in George Orwell's *1984*! Singh is the author of *Fermat's Last Theorem*, the first book about mathematics to make it to number one in Britain's best−seller lists. His second book *The Code Book*, also a bestseller, follows cryptography from its use by the Spartan armies of the 5th century BC all the way to its crucial role in electronic commerce and communications today. A CD−ROM based on *The Code Book* is soon to appear in which Singh aims to emphasise the application of mathematics to cryptography. "You write coded messages with letters, so it seems that is more to do with linguistics. Or you write codes with invisible ink and that's more to do with chemistry. So what I have tried to do is to more explicitly point out the mathematics."



Mathematics has always been central to cryptography. Julius Caesar used a substitution cipher, now known as the Caesar Shift Cipher, where messages were encoded by replacing each letter in the alphabet with the letter three places along. So an A would be replaced by D, B with E and so on. When looked at mathematically, representing each letter by the number of its position in the alphabet − A = 0, B = 1, ..., Z = 25 − the Caesar Shift Cipher uses modular arithmetic. You add 3 modulo 26 to each letter (actually the number representing the letter) to get the encoded message. "You can see that this is modular arithmetic modulo 26," Singh explains. "So mathematics comes into the most elementary cipher."

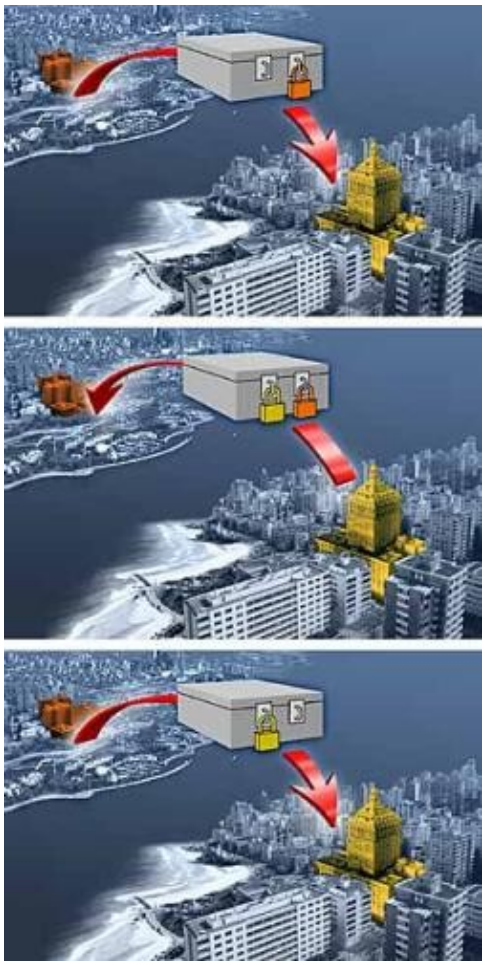


Key distribution

More recently, mathematics provided the solution to the *key distribution problem*, one of the biggest problems in cryptography for over 2,000 years. Suppose you wanted to buy something over the internet, say the latest Madonna CD from Amazon. At some point you will be asked to type in your credit card details and send them to Amazon. As Singh explains, that's the dangerous point. "If someone intercepted your message to Amazon, they could steal your credit card number and buy things in your name. So you would encode your credit card number according to some special recipe which scrambles it up, moves it around, substitutes it and does all those good things that codes do.

"Now the problem is, when it gets to the other end somebody has to decode it, but they don't have the recipe because you have the recipe. Amazon are a good example because they are in Seattle, so how do you get the recipe to Seattle so they can unscramble your code? The recipe is what we call the key, and getting the key between the receiver and the sender is called the Key Distribution Problem."

It had been thought that the only way around this problem was for the sender and receiver to meet in person, or have a courier deliver the key. Singh says that this is what people did in the Second World War. "People would deliver keys across deserts and U−boats would come back to base to pick them up, and so on."



No exchanging of keys is necessary

But thankfully, mathematicians weren't about to give up that easily. "The great thing about mathematics is that something might look impossible, but unless somebody has proved it is, then mathematicians say 'well, let's try and find a solution.'" And that is just what they did. This is how Singh explains the solution.

"I put a message in a box, I close the lid, turn the key and send it to you. But you can't open it because I've still got the key. Some mathematicians, Diffie, Hellman and Merkle thought of another way to think about it.

"How about I put the message in the box, I close the lid and I *padlock* it and then send it to you. Now you still can't open it. What you do is you put *your* padlock on it and send it back to me. Then I take my padlock off, send it back to you. You take your padlock off and you open the box."

So theoretically a message could be communicated secretly without ever exchanging a key. "Suddenly that example blows away what for 2,000 years people thought was impossible. There is no key being exchanged."

Mathematical padlocks

Then they thought more about how padlocks work. Anyone can snap shut an open padlock − you don't need a key to lock it − but opening it again is really tough. In this way, when you buy something from Amazon you just need a single padlock. "You say, 'hey Amazon can you send me your padlock?', and they send you their *open* padlock", says Singh. " You snap it shut on the box containing your credit card details as you don't need

their key, send it to Amazon and they've already got the key as it was their padlock in the first place." So by sending you their open padlock, Amazon can then open it again and retrieve your payment information.

"That breakthrough really transformed security on the internet. It has created thousands of jobs and it's made the mathematicians who invented it millionaires. It's an extraordinary breakthrough. But the question is, how do you make a mathematical padlock? Obviously you don't use real padlocks on the internet, you need to have some kind of software or digital one.

"The way you do this is you say to a mathematician, what is special about a padlock? And what is special is that it is very easy to lock up but very hard to open − what is called a one−way operation in maths, something that is very easy in one direction but very hard in the other. Multiplication is a classic one. It is very easy to multiply two numbers and get a result, but it is hard to take a result and get back the two numbers. That is what is at the heart of a mathematical padlock." For example, 17 multiplied by 7 is fairly easy to work out, but can you quickly calculate what two number multiply together to get 143?

Maths is the key... Image from www.freeimages.co.uk

The type of mathematical padlock used today on the internet is called the RSA public key cryptosystem, named after its inventors Ronald Rivest, Adi Shamir and Leonard Adleman. An RSA padlock consists of two numbers: the encryption key, e, and the modulus the mathematics will be based on, N. For example, let's use the padlock with encryption key $e = 3$ and modulus $N = 55$. Before you encrypt the message, it is first turned into a number by using a standard method such as ASCII where the characters are replaced by binary digits. Then to securely encrypt the digital message m, say $m = 14$, it is changed into a different number, c, called the ciphertext, by performing the following calculation:

$$\begin{aligned} c &= m^e \bmod N \\ &= 14^3 \bmod 55 \\ &= 2744 \bmod 55 \\ &= 49 \bmod 55 \end{aligned}$$

since 49 is the remainder when 2744 is divided by 55. Therefore, the ciphertext c is 49.

This ciphertext can then be decrypted using a key, in this case, $d = 27$, in the following way:

$$c^d \bmod N = 49^{27} \bmod 55$$

which after some work ...

$=14 \bmod 55$

And we see that the ciphertext is decrypted to the original message of 14 using the key *d*. For this system to work it is necessary to find numbers *e, N* and *d* such that this process of decrypting the ciphertext *c* is successful for any message. So for any message *m*:

$$\begin{aligned} m &= c^d \bmod N \\ &= (m^e)^d \bmod N \\ &= m^{ed} \bmod N \end{aligned}$$

So for the RSA system to work you need to find numbers *e*, *N* and *d* such that raising any message *m* to the power of *ed* modulo *N* is equivalent to raising a number to the power of 1 in our normal arithmetic.

Hmmm...

The RSA system provides a method of calculating these numbers in such a way that it is possible to find the key *d*, using the padlock *e* and *N*, only if you know the factors of *N*. This is where the security of the system lies. The padlock is chosen such that *N* is the product of two giant prime numbers. In August 1999 a large team of mathematicians took over 35 computing years to factorise a 155 digit number, and according to the RSA site, current technology cannot factorise numbers of 230 digits. So if you choose two big enough prime numbers so that *N*, the product of these primes, is more that 230 digits long, it is not feasible to crack the key by factoring *N* given available computing resources. As long as the two primes are kept secret, the padlock − *e* and *N* − can be published secure in the knowledge that the key *d* cannot be calculated from that information.

Calculating the RSA padlock and key is not straightforward, but it is interesting to note that it uses some very old maths. One stage of the process uses Euler's phi function that he developed in the eighteenth century and another uses an extension of the Euclidean algorithm recorded in *The Elements* in 300BC.

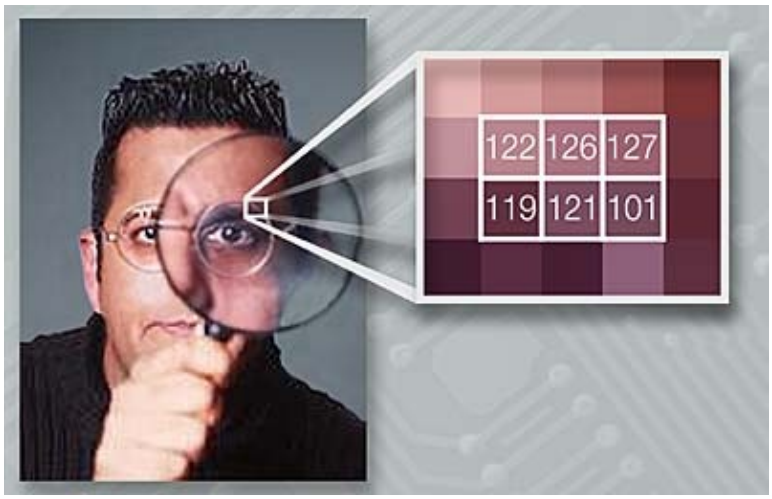
In practice, RSA isn't used to encrypt actual messages, but instead used to encrypt the key of another coding system, such as DES or triple DES. "The thing is that RSA is very slow," says Singh. "So if I was sending you a huge long message it would take a long time for me to encrypt it with RSA. So what I could say is you send me your RSA open padlock. Instead of locking up the message, I encrypt the message using DES with another key, send it to you and you can't read it because you don't have the DES key yet. The DES key is quite small so I can lock that up with your RSA padlock which is much quicker and send it to you. So it is a two−stage process."

So at the moment, RSA has put the code−makers ahead, but will the code−breakers find a way of cracking RSA padlocks? Singh guesses that RSA will be pretty much unbreakable. "Nobody has proved it is impossible, and somebody tomorrow might come up with a really clever way to break it but I don't think that

will happen." Factoring is one of a class of difficult problems, called NP problems, that many mathematicians believe are fundamentally hard, though they have not yet proved this.

A picture is worth a thousand words...

So RSA will remain secure as long as large enough keys are used, a benchmark that changes with each advance in computing power. However, in some instances it is not adequate just to have large enough keys to make your encryption unbreakable. Sometimes it is necessary to hide the fact that you are using cryptography, or indeed that you are sending a message at all. *Steganography*, the practice of hiding messages, is an area within the science of secrecy running parallel to cryptography. It has progressed from swallowing messages concealed in wax balls and using invisible inks, to methods that can be used on the internet today. "I could send you send you a JPEG, a picture of my trip to Australia on holiday, but hidden in that picture, hidden in the digital information, would be a message," Singh explains. If you blow up that digital picture, each pixel of the image actually has a number associated with it. For example, with a black and white image, each pixel contains the measure of brightness between, say, 1 and 128.



Steganography in action − a message can be encoded in the numerical values of the pixels

"Say I want to send you SOS, which is ...−−−... in Morse code, but I am going to call it 111000111," Singh says. But instead of writing the message in 0's and 1's, Singh can use whether the pixels are even or odd to represent the message: odd for 1, even for 0. "So before I send the image I need to make the first number odd, so 123, the second number odd, so 127, the third number odd, so I leave it. Then the next three numbers need to be even, so I get the following":

123 127 127
120 120 102

"When you get the picture all you need to do is just read it off − odd odd odd even even even... But the picture looks the same because the human eye couldn't detect such small changes, say 1%, in the individual pixels of the picture". In this way people can send messages over the internet hidden in image files, or perhaps posting them on web sites, without others even being aware there is a message to intercept.

Last year changes to US export laws meant that strong encryption, that is, encryption software using suitably large keys, could be exported legally to most countries. But, given recent events and the ensuing war on terror, will governments crack down on cryptography again? Singh feels that this is where maths and politics meet.

"It is something people are going to be voting on. The government in five or ten years time might say we want to ban all cryptography because the threat to national security from terrorism is too great. And the opposition party might say, no because if you ban cryptography the economy and e−commerce will collapse. And another political party might say no you can't ban cryptography because then nobody will have any privacy. So it is very difficult to know which fear is bigger. Are you more worried about losing your privacy, about terrorism, about losing your job if your dotcom goes bust? It is just not clear but maybe there is a balance, a compromise there."

About this article

Rachel Thomas is news editor on *Plus*. For this article Rachel interviewed author, journalist and TV producer Simon Singh.

Simon Singh

Simon Singh is the author of two best selling books: Fermat's Last Theorem and The Code Book. He has directed television versions of both books and is currently producing a CD−ROM version of the Code Book. Details for the CD−ROM are available at his website, where you can also buy signed copies of his books.

You can try your hand at cryptography in the new interactive section of Simon's website − the Black Chamber.

Download PDF version | Printer friendly version

Return to article

- contact
- copyright info
- sponsors
- privacy info

Plus is part of the family of activities in the Millennium Mathematics Project, which also includes the NRICH and MOTIVATE sites.