Parabola Volume 42, Issue 3 (2006)

Unbreakable Cyber-Secrets

Nuno Crato[1]

The safety of electronic commerce is secured by an innovative mathematical method: a public key that allows you to lock messages in a safe, but a safe that can only be open with another device—a secret key!

Are you afraid to send your credit card number through the Internet? Did you ever abstain from buying a CD or a book because the seller asked you to use your Visa or MasterCard? Well, you are not alone in this distrust. There are many Portuguese and many people around the world who do not benefit from e-commerce because they fear security breaks. Yet, the circulation of confidential data through the Internet is based on one of the most secure information systems created to date. By following some basic rules, such as avoiding unknown commercial sites and not sending confidential information by direct mail (not ciphered), the world of e-commerce is at your fingertips.

The Internet opened many possibilities, unthinkable only a few years ago. It became a giant public library and it made it possible for ordinary citizens to access international commerce in a safe and speedy fashion. Do you wish to buy that technical manual you cannot find in bookstores and whose exact title you cannot remember? Do you want that Bob Dylan CD you cannot find? Are you a collector and would like to get a nineteenth century compass? You can do all that through the Internet for it even gives you access to several international networks where, for a good bargain, you can even find that Max Planck autobiography you would love to read but is sold out. Who knows? Maybe, as it happened to this writer, there is one bookstore in New Zealand that is willing to sell it to you through the Internet.

[1]Nuno Crato is Professor of Mathematics, Technical Univeristy of Lisbon, Portugal, and is also President of the Portugese Mathematical Society.

But is it safe to send our credit card number through those bits and bytes that circulate God knows where? How can Amazon and other e-commerce corporations guarantee that your information does not reach less scrupulous hands that manipulate some computer keyboard, somewhere in the world? It may be true that information is ciphered, but even if the message is coded with a key that is sent to my computer, can't some crooks discover that secret key?

This question makes sense. For million of years now, secret communications have relied on cipher systems based on a so-called symmetrical key that allows people to code and decode messages. People would agree on a given key by saying, for example, A stands for B, B stands for C, and so on. This way, when they wanted to say GOOD MORNING, they would write, HPPE NPSOJOH. This type of key that serves to code the message is the same one that, once reversed, is used to decode the message. The safety of communication systems was based on the assumption that this key could be kept secret.

Ciphered communication through the Internet is based on an innovative principal called the asymmetrical key. It is a real revolution in cryptography; perhaps the most important since the beginning of coded messages. The system, which is incorporated in different browsers, in some electronic mail systems, and, of course, in banking communications, is based on a method proposed by Ronald Rivest, Adi Shamir and Leonard Adleman. In 1977, these MIT researchers proposed a coding method that became known for their initials: RSA.

(a) *Ronald Rivest*

(b) Adi Shamir

(c) Leonard Adleman

MIT researchers Ronald Rivest, Adi Shamir and Leonard Adleman, conceived in 1977 the RSA coding system. As it was recently discovered, British Intelligence researchers James Ellis and Clifford Cocks had previously created a system based on the same principles. They had, however, kept their ideas secret.

Using this system, the message recipient or the Internet seller constructs a key composed of two large numbers (N, e). He then sends these two numbers to the client's computer and does not worry about safety—if he so wishes, he can even publish them in the newspaper. The client's computer rewrites the message in numerical form (usually according to ASCII computer codes), gets a third number (M), and applies a sim-

ple formula: it raises M to e, divides the result by N, and computes the remainder, obtaining the number C it then sends through the Internet.

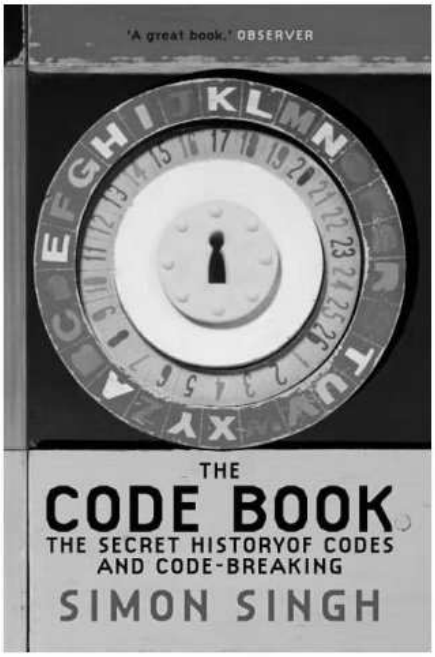
What is amazing is that this number C, which constitutes the coded message–for example, a credit card number—can be seen by anyone. Even if one knows the public key (the numbers N, e) the message is not decodable.

So, how can the message receptor decode the message? Well ... since he was the one who produced the public key, he knows how it was created: he picked N as the product of two prime numbers (whole numbers larger than 1 and only divisible by themselves and by 1), say p and q, and did not reveal them. Knowing them, he creates another number d, such that $(ed - 1)$ is divisible by $(p - 1)(q - 1)$. He then raises the coded number C to d, divides it by N and gets the division remainder. This remainder is the original message M. Does it sounds like a miracle? Not really. It is simply the ingenious application of an important number theory result known as the Euler theorem.

What makes this system virtually unbreakable is a simple fact: the factorization of a number as the product of its prime factors is extraordinarily time consuming when we are dealing with large numbers. To obtain the product of two numbers is easy. However, even if we know that a given number N is the product of two prime numbers, finding these two factors is not trivial; and without knowing them the message is unbreakable.

Indeed, we have to make sure two things happen: that the number N is really large and that p and q are well chosen, in order to increase the factorization time to such an extent that it becomes practically impossible for an Internet crook to attempt to do it.

As always, with any advance in cryptography techniques a related advance in decoding techniques follows. The RSA system has been subject to different threats from various mathematicians who search for algorithms to decipher the private key d, with or without factoring the public key N in its prime factors. Albeit the limited success of these attempts, they have forced experts to restrict the components of the system to ensure its safety, namely by ensuring the use of large numbers in RSA keys. To date, mathematics has not yet offered any decoding method that can function against RSA. E-commerce continues to be safer than to hide your money under the mattress.



Simon Singh is an author known to Portuguese readers through his book, *Fermat's Enigma*. His recent work, *The Code Book*, is a fascinating voyage through the world of cryptography. In it you can find a detailed explanation of the RSA system. To know more, you may also browse through www.rsa.com/rsalabs