Parabola Volume 42, Issue 3 (2006)

Alice and Bob

Nuno Crato

Illustrations by Fernando Guerreiro Martins

Internet communication is based on coding mechanisms that guarantee privacy in the exchange of messages. Mathematics makes this possible without having the people involved agree on a secret key.

Alice and Bob live in isolation and can only communicate by mail. But they know the mail carrier reads their letters. Alice has a message for Bob and she does not want it to be read. What can she do? She thought of sending Bob a message in a safe with a lock, but how would she send him the key to open the safe? After giving it much thought, she decided to send him the safe with the lock. She knows Bob is smart and will eventually understand her idea.

The mail follows its course. With a few back and forth turns and without any exchange of keys, Bob opens the safe and reads the message. How do you think they solved the problem? If you like riddles, stop here and think about it.

How am I going to tell Bob I love him?

It is simple . . . after you figure it out . . . Bob gets the safe and closes it with another lock for which he has the key. He then sends Alice the safe by mail, this time locked with two locks. She removes her lock, for which she has the key, and sends the safe by mail again. When Bob gets it, he only needs to use his key, open the safe and read the message. Thus, the mail carrier has no opportunity to read it.

This story is a retelling of an old riddle and of one of its solutions. It inspired three young Americans, Whitefield Diffie, Martin Hellman and Ralph Merkle, to create a cryptography system according to which secret communication is secured by the use of two keys that the two involved parties never exchange. It was this invention that propelled the RSA system discussed in the first of these three articles.

Alice and Bob are fictitious characters, but cryptologists systematically use these names. It makes for a more interesting story than to talk about sender and receptor,

or merely A and B. Also, a third character is usually added to these two. Represented in the story by the mail carrier, it is customary to call this character "Eve" which, in English, stands for the one who eavesdrops.

I can't wait to read Alice's letter !!!

Until Diffie, Hellman and Merkle invented their two-key system, communication of ciphered messages required the exchange of one key. It would be imperative for Alice and Bob to meet before the exchange of messages and to agree on using a key that no one else, other than the two of them, knew. Only thus could they exchange secret messages from a distance without having Eve intercept them. It was in this way that secret messages worked, from the time of the Roman Empire to modern times, from spies, government agents, and generals to simple lovers. It would be necessary for Alice and Bob to agree from the beginning on how to code and decode the messages.

Diffie, Hellman and Merkle's idea is indeed revolutionary. According to their plan, Alice and Bob start by agreeing on two numbers. And these can be publicly known. Then, each of them picks another number that is kept secret. Next, after some calculations they reach the same result: a number that no one else knows and that is the key to decode their messages. Although ingenious, this process is quite simple and is briefly explained in the box. Everything is similar to the story of the two locks. There is no exchange of keys but, except for Eve, the persons involved are eventually able to open the safe.

Using a most appropriate analogy, Simon Singh, in his work *The Code Book*, to which we made reference in the first article in this series, tells the story as if Alice and Bob wanted to create a secret kind of paint without making its ingredients known. The first step is to pick a certain base color and have each person take one liter home. Next, Alice adds a liter of a secret color to that paint, but she does not tell anyone what color she is adding—not even her partner. Bob does the same thing with another secret color he chooses. Then, they exchange the cans with the paint mixtures and could not care less whether Eve is observing them.

Back at home, Alice adds one liter of her secret color to the can Bob gave her. She now has three liters of paint: one-third is the original color, one-third is Bob's secret color, and one-third is her own secret color. At home, Bob does the same corresponding thing with the can Alice gave him. He gets the exact same result Alice got, because the color components are the same. They never revealed their secret colors to one another, but they both ended up with the same final color and no one, not even Eve who was

always eavesdropping and knew about the exchange of paint in the cans, could find out the final color.

In cipher systems there are numbers instead of paints and there is an ingenious application of a branch of mathematics known as number theory. Without the advances in cryptography it would not be possible for Internet commerce and communication to be as secure as it is.

The creation of public keys

The procedure created by Diffie, Hellman and Merkle marks the birth of the public key cryptography, used in conjunction with secret keys that are not exchanged. It is based on modular arithmetic, which essentially consists of working with the remainders of the integer division by a number, the modulo. A good example is given by our 12 hour system. If a running clock shows 10 o'clock, what time will it show 5 hours later? The result is obviously 3 o'clock, which is the remainder of the integer division of $10 + 5 = 15$ by 12. In mathematics we write $10 + 5 = 3 \pmod{12}$, since $15 = 3$ in the congruence modulo 12 of our common analog clocks. With this notation we describe below the procedure followed by Alice and Bob, following closely an example supplied by Simon Singh. Our two friends are able to agree on a common cryptographic key without ever exchanging it and without any one else being able to discover it.

Alice and Bob agree on the numbers 7 and 11, and they compute the result of 7^X (mod 11)
(they don't even care to hide this information).

Alice chooses 3 as her secret number.
Alice computes $7^3 = 343 = 2$ (mod 11).
Alice sends the result 2 to Bob.
Bob chooses 6 as his secret number.
Bob computes $7^6 = 117649 = 4$ (mod 11).
Bob sends the result 4 to Alice.

(Usually, this is a crucial moment the message exchangers want to keep secret. This concern, however, does not exist here. Even if this information exchange is public, no one can find the secret key).

Alice takes Bob's result 4 and her secret number 3 and computes $4^3 = 64 = 9$ (mod 11).
Bob takes Alice's result 2 and his secret number 6 and computes $2^6 = 64 = 9$ (mod 11).

Alice and Bob find the same number 9, without having told one another their secret numbers.