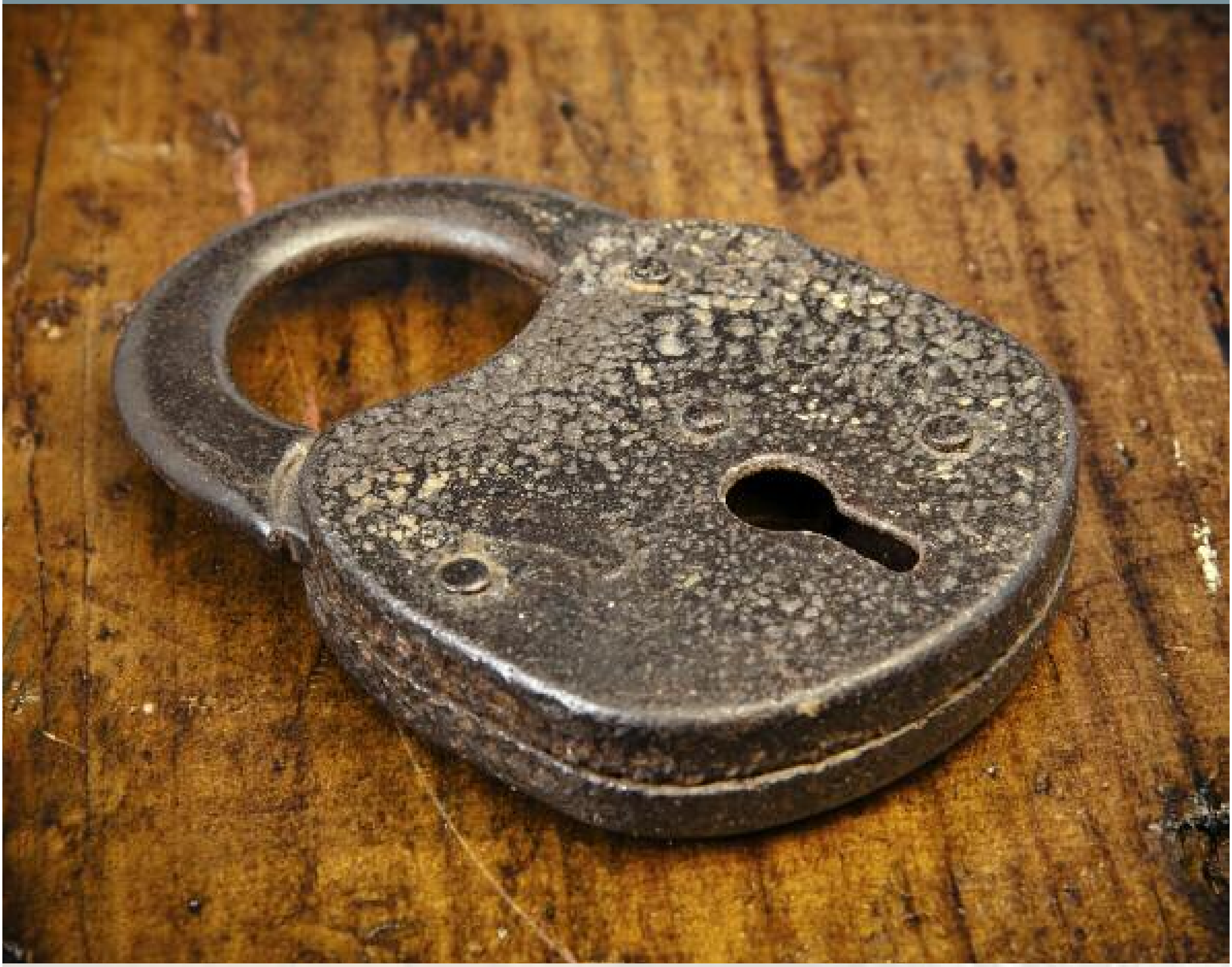

Keeping secrets on the Internet

How do modern codes keep your data safe online? **Ben Stephenson** of the University of Calgary explains.

When Alan Turing was breaking codes, the world was a pretty dangerous place. Turing's work helped uncover secrets about air raids, submarine locations and desert attacks. Daily life in Europe might be safer now, but there are still threats out there. You've probably heard about the dangers that lurk online – scams, identity theft, viruses and malware, among many others. Shady characters want to know your secrets, and we need ways of keeping them safe and secure to make the Internet work. How is it possible that a network with so many threats can also be used to securely communicate a credit card number, allowing you to buy everything from songs to holidays online?

The relay race on the Internet

When data travels over the Internet it is passed from computer to computer, much like a baton is passed from runner to runner in a relay race. In a relay race, you know who the other runners will be. The runners train together as a team, and they trust each other. On the Internet, you really don't know much about the computers that will be handling your data. Some may be owned by companies that you trust, but others may be owned by companies you have never heard of. Would you trust your credit card number to a company that you didn't even know existed?

The way we solve this problem is by using encryption to disguise the data with a code. Encrypting data makes it meaningless to others, so it is safe to transfer the data over the Internet. You can think of it as though each message is locked in a chest with a combination lock. If you don't have the combination you can't read the message. While any computer between us and the merchant can still view or copy what we send, they won't be able to gain access to our credit card number because it is hidden by the encryption. But the company receiving the data still needs to decrypt it and open the lock. How can we give them a way to do it without risking the whole secret?
If we have to send them the code a spy might intercept it and take a copy.

One-way keys

The solution to our problem is to use a relatively new encryption technique known as public key cryptography. (It's actually about 40 years old, but as the history of encryption goes back thousands of years, a technique that's only as old as Victoria Beckham counts as new!) With this technique the code used to encrypt the message (lock the chest) is not able to decrypt it (unlock it). Similarly, the key used to decrypt the message is not able to encrypt it. This may sound a little bit odd. Most of the time when we think about locking a physical object like a door, we use the same key to lock it that we will use to unlock it later. Encryption techniques have also followed this pattern for centuries, with the same key used to encrypt and decrypt the data. However, we don't always use the same key for encrypting (locking) and decrypting (unlocking) doors. Some doors can be locked by simply closing them, and then they are later unlocked with a key, access card, or numeric code. Trying to shut the door a second time won't open it, and similarly, using the key or access code a second time won't shut it. With our chest, the person we want to communicate with can send us a lock only they know the code for. We can encrypt by snapping the lock shut, but we don't know the code to open it. Only the person who sent it can do that.

We can use a similar concept to secure electronic communications. Anyone that wants to communicate something securely creates two keys. The keys will be selected so that one can only be used for encryption (the lock), and the other can only be used for decryption (the code that opens it).
The encryption key will be made publicly available – anyone that asks for it can have one of our locks. However, the decryption key will remain private, which means we don't tell anyone the code to our lock. We will have our own public encryption key and private decryption key, and the merchant will have their own set of keys too. We use one of their locks, not ours, to send a message to them.

Turning a code into real stuff

So how do we use this technique to buy stuff? Let's say you want to buy a book. You begin by requesting the merchant's encryption key. The merchant is happy to give it to you since the encryption key isn't a secret. Once you have it, you use it to encrypt your credit card number. Then you send the encrypted version of your credit card number to the merchant. Other computers listening in might know the merchant's public encryption key, but this key won't help them decrypt your credit card number. To do that they would need the private decryption key, which is only known to the merchant. Once your encrypted credit card number arrives at the merchant, they use the private key to decrypt it, and then charge you for the goods that you are purchasing. The merchant can then securely send a confirmation back to you by encrypting it with your public encryption key. A few days later your book turns up in the post.

This encryption technique is used many millions of times every day. You have probably used it yourself without knowing it – it is built into web browsers. You may not imagine that there are huts full of codebreakers out there, like Alan Turing seventy years ago, trying to crack the codes in your browser. But hackers do try to break in. Keeping your browsing secure is a constant battle, and vulnerabilities have to be patched up quickly once they're discovered. You might not have to worry about air raids, but codes still play a big role behind the scenes in your daily life.

A big brain, big number trick

A Turing machine manipulates long sequences of 1s and 0s, made of anything from electronics to chocolates, to make calculations (see page 10). Let's do it bigger. Get a friend to set their phone to calculator mode, and then multiply together any ten single digits. This will create a really, really big number. The friend should keep this big number a secret so you have no idea what it is. But even though you don't know the big number, your big brain will be able to spot something missing.

Get your friend to read out nine digits of their number, in random order, and to hold one of those digits back. That's the number you have to figure out. Oh, and to make it more difficult, that number shouldn't be zero; it's too easy to predict nothing. Your friend reads out their numbers, and after a dramatic pause you correctly reveal the secret digit they have held back. Your brain's like a Turing machine, only clearly bigger and better, as it was able to crack the hidden digit code. Or is it all a trick? (Hint: yes it is.)

Find out how it's done in the magazine+ section of our website, **www.cs4fn.org.**