Web Encryption 101

At some point everyone worries how safe it is to send credit card details over the internet. Isn't there a risk that baddies will somehow intercept your data in transit and steal your information?

Computer scientists back in the seventies puzzled over how data could be encrypted in such a way that a user could send data from their browser, have it transit over the internet from router to router and country to country, then arrive safe and sound at the recipients website. In particular, with a guarantee that that if the data was intercepted in transit it could not be read by a third party (Confidentiality) and also not changed or tampered with in any way (Integrity).

What they came up with was masterfully clever, and involves creating two very, very large numbers which are mathematically related. The first number is called the Private Key, and the second the Public key. Each of these two numbers are huge – up in the zillions of billions.

For example:
Private Key: 384657301836454583928345663466465686058463267346560239456712309345672 34
Public Key: 234578091456718923478234565876234709812346587964536987263456743522345 56

Now let's take the example that you want to buy a some books using your credit card from the Amazon website.

Both the Amazon Private Key and Public Key are stored on the Amazon webserver. The Private Key is held as a very closely guarded secret. No-one else has access to the Private Key except the Amazon webserver.

Now from your home or office or internet café you connect to the Amazon website and order some books. When you have finished adding items to your shopping cart and click through to the pay now page (where you will enter your credit card details), the Amazon website automatically sends a copy of its Public Key to your browser. Now your browser does something very clever. It takes your credit card details and the Amazon Public Key and feeds them both into an encryption program which is built-in to the browser. The output of this encryption program is an enormous stream of encrypted gobbledygook that is then sent over the public internet and back to the Amazon website.

Your credit card and order details end up looking something like this:

FH%Ih+&Y8fc\+v32k086';Ht68Fg56F%68g1!23k3^987hkk(J@f_=hu56}hD#76^6^\7tjkl34576543#3l;*5^

So how on earth does that encrypted gobbledygook get decrypted once it arrives at the Amazon web server? Remember that the Private Key and the Public Key are mathematically related. The only number known to man that will decrypt your order details is the Private Key!

The only way a hacker could try and guess that Private Key is by brute force, but because the Private Key is such a ridiculously large number with current computing power it would take hundreds of thousands of years to try and guess it!

An easy way to know if this encryption system is being used when you are browsing a particular website is to look for a small padlock symbol near where the website address is displayed in your browser, and/or the letters https:// at the start of the website address.

Of course this article is only looking at how the Private Key/Public Key encryption works. This technology, whilst in itself really secure, is unfortunately not enough to guarantee the safety of your data on the internet, as other forms of viruses and malware may also be present on your computer – for instance a keyboard logger Trojan which sneakily records your keystrokes as you type on the keyboard. To safeguard against these types of attacks, you will still need to have up to date anti-virus software installed on your computer.