MATHEMATICS MATTERS

Internet shopping: stopping the scammers

With ever more people purchasing things online, there is a greater potential reward for internet fraudsters. Mathematics helps make sure your money doesn't end up in the wrong hands.

The internet has revolutionised the way we shop. Customers can order goods and services without the need to leave the house. Weekly shopping no longer requires an actual visit to the supermarket, films can arrive through your letterbox, you can even send a birthday card without ever seeing it.

Such flexibility, along with online companies often able to offer more competitive prices, has seen online internet sales sky-rocket; UK shoppers spent a combined total of £10 billion online in the first two months of 2011 alone. However, online transactions have a dark side: scammers out to defraud. One particular method of online fraud is known as 'phishing'. This is where emails or instant messages attempt to direct you to a website which has been designed to trick you into believing it is legitimate.

One of the most common examples of this practice is with online banking. Fraudsters send out emails claiming to be from your bank. When you click on the link you are directed to a website which looks identical to the bank's real website, before being asked to enter sensitive information such as credit card details. And the practice is on the increase. There were 1,700 recorded phishing attacks in 2005; by 2010 the number had soared to 51,000. In 2009, UK online banking losses due to phishing hit £60 million.

In the fight against this online fraud, mathematics plays a crucial role in helping you to know the site is genuine. When you log on to shop.com or bank.co.uk, your browser will display a symbol to tell you the site is genuine: it could be a green strip to the left hand side of the address bar or a locked padlock on the right hand side. Clicking on these symbols will say something along the lines of "this website has been identified by Company XYZ" or "Verified by: Company XYZ". The key to this verification is cryptography - the ancient practice of sending coded messages.

> "In 2009 UK online banking losses due to phishing hit £60 million."

One of the oldest and simplest ways of encoding a message is to use a "Caesar Cipher", named after the Roman emperor. In this method each letter is shifted by a set amount, for example by two letters. "This is a code" becomes "Vjku ku c eqfg".

Knowing the secret, or "key" allows you to encipher and decipher messages. However, Caesar Ciphers are easy to crack and not up to the job for internet security. Instead, the type of encryption used online is Public Key (PK) encryption, devised in secret by mathematician Clifford Cocks at the UK Government Communications Headquarters (GCHQ) in 1973. It was only revealed that PK encryption was formulated first at GCHQ in 1997.

The danger with conventional ciphers is that, at some point, you have to send the key – the secret of how to decipher the message. Imagine that, rather than encoding the message, you locked it in a padlocked box. At some point you need to send the recipient the key to that box. If that key is intercepted then the interceptor can read all your messages and all future messages sent the same way. It is much safer to have one key that locks the box and a different key to unlock it. PK encryption works in just this way: it's a system that uses two separate kinds of key, one public one private.

The keys are generated by multiplying two large prime numbers – a number only divisible by one and itself – together to get a bigger number. The trick is that if you are only given the bigger number it is very hard to guess what the two prime numbers were.

Institute of mathematics & its applications

National HE STEM Programme

The larger number is the basis of the public key, the two original prime numbers are kept a secret and so are the basis of the private key. A simplified example that doesn't use prime numbers would be to imagine the public key was 256. There are many possible numbers that could have been multiplied together to reach this number. For example, it could have been 256 x 1, 4 x 64 or 16 x 16. The prime numbers used in PK encryption are each at least 1024 digits long. This is referred to as a one-way trap door. It is very easy to go one way, but very hard to go the other.

The only additional component needed for online security is a certificate authority (CA). This is a trusted entity that provides a website with a certificate that says it has seen and checked its public key. The CA is the Company XYZ that appears next to the green strip or padlock next to the address bar.

When a browser logs onto shop.com it asks that site to identify itself. Shop.com sends the browser its certificate, which has been encoded – or digitally signed - with the CA's private key, along with a message encoded with its own private key. The public key

of the CA is hard-wired into the browser and so it can decipher the certificate. As the certificate contains the website's public key, the browser should be able to use it to decipher the additional message the website has sent. If the message is successfully deciphered then the website is genuine.

Then, when you submit your credit card's details to shop.com, the browser can encrypt this information using the website's newly authenticated public key, which only the website can decipher using its private key.

With £250 billion spent online by UK shoppers in the first decade of the 21st century, and with internet purchases set to account for half of all retail sales by 2020, it is mathematics that is helping to protect arm-chair shoppers from would-be scammers.

TECHNICAL SUPPLEMENT

Public and Private keys

The two original prime numbers used in PK encryption are at least 1024 bits long and known as p and q. The product of multiplying p and q together is a much larger number, N. Another number is then generated known as φ such that $\varphi = (p-1)(q-1)$.

A number is then selected that lies between 1 and φ that shares no common multiples with φ other than 1. This is called e and is then used to calculate a second number, d which satisfies the equation $e.d \equiv 1 \bmod \varphi$. The number e is the "encryption exponent" and d is the "decryption exponent".

N and e then form the public key which can be widely published to allow anyone to encode a message. The remaining numbers, d, p and q are kept secret and form the private key which allows only you to decipher the message.

Encryption

If Alice wants to send a message to Bob using PK encryption, she must first obtain his authentic public key. This could be authenticated using a similar certificate authority as used in internet security. This would give her N and e. She would then represent her unencrypted message as a number, m, between 0 and N. She must then work out her encrypted message, c, where $c = m^e \bmod N$. The result, c, is what she would send to Bob.

Decryption

Once Bob has received the encrypted message, c, from Alice he can decipher it using his private key. Using d, which Bob kept secret, he can work out m from the equation $m = c^d \bmod N$. He then has Alice's original message.

Authentication

Bob can use prove that he knows the secret d without revealing anything useful by a challenge-response exchange. Alice sends Bob the encryption of a message m^e and challenges Bob to reveal m. Bob can do this since he knows d but does not reveal anything about his secret useful to a would-be imposter.

.

References

http://www.cesg.gov.uk/publications/Pages/categorylist.aspx?cat=History

The IMA would like to thank the staff of GCHQ for their help in the preparation of this document.