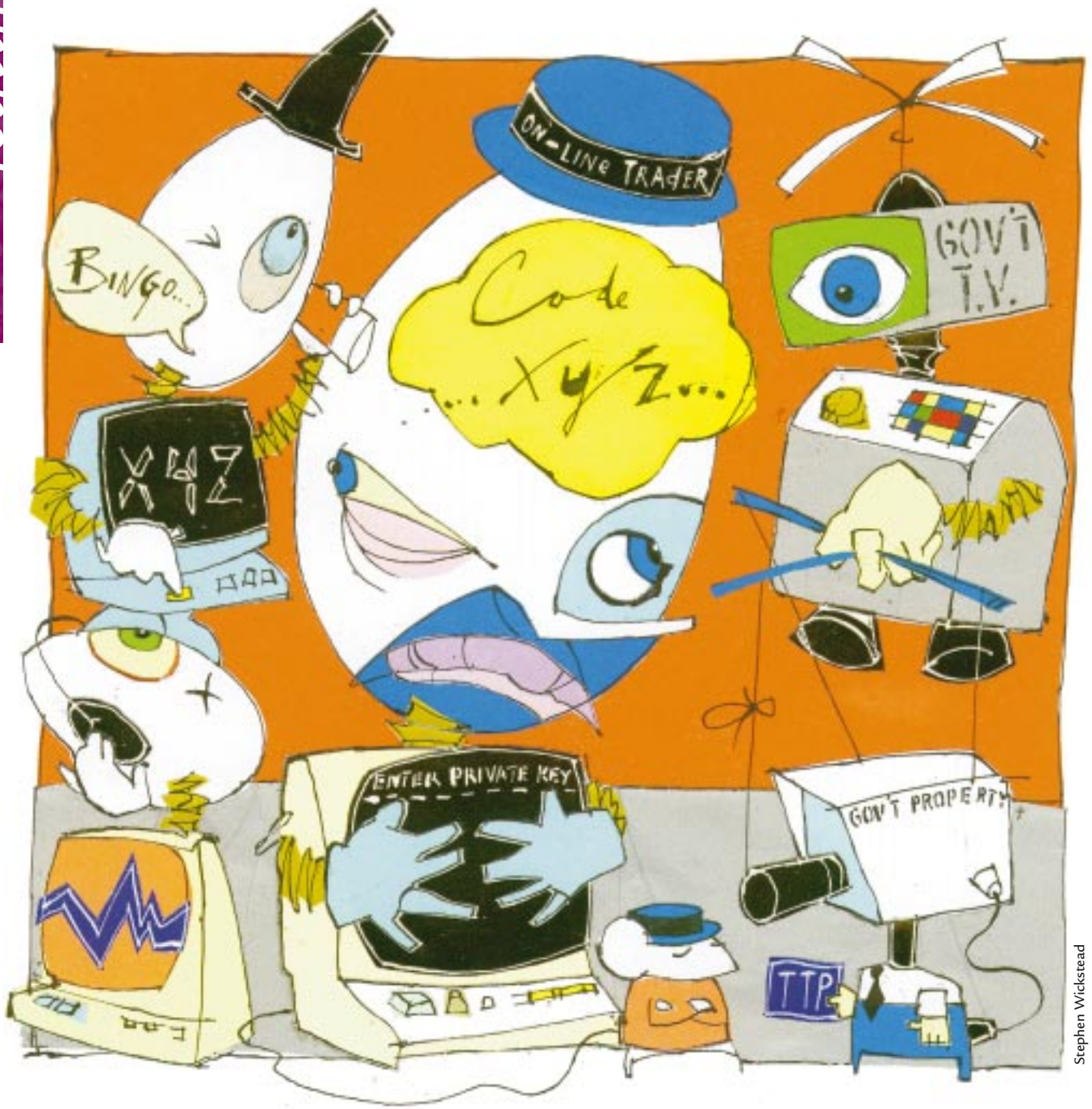


Stephen Wickstead

Spies, lies & the internet

AS THE GOVERNMENT PREPARES TO REGULATE E-COMMERCE, ENCRYPTION BECOMES THE SUBJECT OF THE MOST HEATED POLITICAL DEBATE OF THE CENTURY. JOHN LEYDEN EXAMINES THE PRINCIPLES BEHIND IT AND THE POTENTIAL THREAT TO CIVIL LIBERTIES.

ALONG WITH THE PROVINCE OF SPIES AND CYBERPUNKS, encryption is hitting the mainstream as government legislation, expected next year, sets up a next-generation model for e-commerce. As the Government sets a framework for online trade, small business users might at first well wonder why the software of espionage thrillers is dropping onto their desktop. The answer is a simple one: trust. Potentially, fraud is easier across the internet because it might be achieved without leaving any trace — and certainly no eyewitness. Without an environment of trust and privacy, customers are highly unlikely to provide confidential information.

Of course, it's possible for an internet user to buy a book from Amazon.com or even carry out online banking, today. However, these models of business depend on existing business relationships. To establish more complex contracts online (for instance setting up a small business or buying a house) requires legal recognition and a framework to build a public key infrastructure (PKI). For the user, a PKI means complex online transactions can be performed seamlessly, which isn't really possible today.

There are four requisites for trusted communication: authentication, non-repudiation, integrity and encryption.

- **Authentication** means you can be certain who you are doing business with.
- **Non-repudiation** means no-one can deny having sent or received transaction data, establishing confidence that a contract entered into will be honoured. It's also important to know that a transmission hasn't been altered — and that's where integrity comes into play.
- **Integrity,** which goes without saying, is trust in fair and reputable business practices.
- **Encryption** is the process of scrambling a message in order to hide its content, thus providing confidentiality. Strong encryption is needed to prevent hacking but also frustrates law enforcement agencies when they seek to unscramble messages.

The British Government and the Clinton administration are concerned that the increasing availability of strong encryption techniques has important implications for the fight against serious crime, drug trafficking and terrorism. US encryption regulations, enshrined in the Arms Export Control Act, classify strong encryption as "munitions", making it an offence for a US company to export it without a licence. The US has recently increased the strength of encryption allowed for export, from 40-key (relatively easy for a determined and skilled hacker to break) to 56-key, which is still breakable but would take longer. For e-commerce to gain the confidence of users, nothing less than 128-bit encryption will do.

The Government's Strategic Export Controls White Paper would make British restrictions on cryptography exportation even more restrictive than those in place in the US. The White Paper extends current regulations on exporting encrypted information, from printed and physical media, to encompass the spoken word and electronic media such as email.

BANNING THE EXPORT OF STRONG encryption is one of the routes government takes to control encryption. Some countries, like France and Israel, go further and ban the use of cryptography entirely. The other is establishing the ability to "steam open" its citizens' electronic mail. This is where the spectre of the state as Big Brother enters the door and a branch of applied mathematics becomes the subject of the most heated political debate of the late 20th century. To understand what all the fuss is about, it's first necessary to understand how encryption works.

With most commonly used forms of encryption, individuals would have two keys; one public and the other private. A message is signed with the author's own private key, resulting in a digital signature. This email message, attachment and the digital signature are encrypted with an algorithm using the recipient's public key. On receipt, this message can only be decrypted with the recipient's private key. By using the author's public key, the recipient can verify the sender's digital signature, proving the message is authentic and has not been tampered with.

In a public key infrastructure environment, digital certificates are used in combination with private and public keys to certify the identity of the sender of electronic communications such as email and web-based forms. The certificates are generated and managed by bodies called Certificate Authorities (CAs).

Privacy advocates, human rights activists and software vendors OPPOSE KEY-ESCROW AS A COSTLY MECHANISM that threatens civil liberties

To implement a framework for electronic commerce, the Government propose legislation on encryption giving legal recognition to these digital signatures for the first time. It will also implement a voluntary licensing scheme for CAs or other providers of cryptographic services. Licensed organisations would have to deposit copies of scrambling keys with bodies called Trusted Third Parties (TTPs). Those so-called "escrowed" spare keys will be available under warrant for covert use by police and security agencies.

Privacy advocates, human rights activists and software vendors, oppose key-escrow as a costly mechanism that threatens civil liberties. Encryption guru Phil Zimmermann, the inventor of Pretty Good Privacy (PGP) said: "If you build an infrastructure where you hand keys to government, you tempt good government to do bad. We feared this kind of regulation so we made PGP resistant to key-escrow."

"Voluntary licensing does not necessarily mean you can go the way you want and do without licensing," warned Zimmermann who went on to say that the global nature of electronic commerce meant that other countries (some of which practice torture and persecution) would follow Britain's lead.

PGP is used by human rights organisations, including Amnesty International. In testimony to the US Senate, Zimmermann quoted from a letter he received in October 1993 from a Latvian, on the day that Boris Yeltsin was shelling his Parliament building. "Phil, I wish you to know: let it never be, but if dictatorship takes over in Russia your PGP is widespread from Baltic to Far East now and will help democratic people if necessary. Thanks."

IT'S NOT JUST PRIVACY ACTIVISTS AND software vendors overseas who are concerned about the Government's policy. The British Medical Association fear the Government's proposals for regulating the use of encryption will allow widespread tapping of personal medical information. The BMA is pushing to make sure medical data is exempt from the covert access to private electronic communications by law enforcement agencies. For its part, the Law Society is also warning its members to protect themselves against government spying by avoiding escrowed encryption. Despite arguments like these, the Government has not altered its plans substantially. Nigel Hickson, head of the DTI's Information Security Policy Group, said that the use of TTPs holding the keys for encryption is the best way to balance the conflicting needs of individual privacy and law enforcement, which

ENCRYPTION PROGRAMS

Setting the code

Algorithms

The most common forms of public key encryption programs rely on the fact that it is mathematically difficult to factor the product of two extremely large prime numbers. Using schemes like RSA a pair of keys (public and private), which are mathematically related to these two large prime numbers, can be produced.

To derive one key from the other, except by blind chance, relies on solving an almost impossible problem. Even stronger encryption could come in the future, based on the maths of elliptic curves.

Programs

- PGP (Pretty Good Privacy) is the cipher of choice for net-citizens. It uses several scrambling mechanisms, long key-lengths and is freely available on the internet.
- SSL (Secure Socket Layer) involves the secure wrapping of messages typically credit card transactions across the internet. This can be switched on from a server without a digital certificate.
- S/MIME (Secure/Multimedia Internet Message Exchange) takes the data and scrambles it before wrapping it. It is integrated into email packages such as Microsoft Outlook 98 and Netscape Messenger almost as well as PGP is integrated into Eudora.
- SET (Secure Electronic Transaction) is a standard for electronic transactions developed by VISA. It's to be used in the next-generation of credit cards, that will use smart cards.
- DES is the US Government's Data Encryption Standard, a product cipher which operates on 64-bit blocks of data, using a 56-bit key. A product cipher applies several weak operations such as substitution, transposition and multiplication in order to scramble a message.

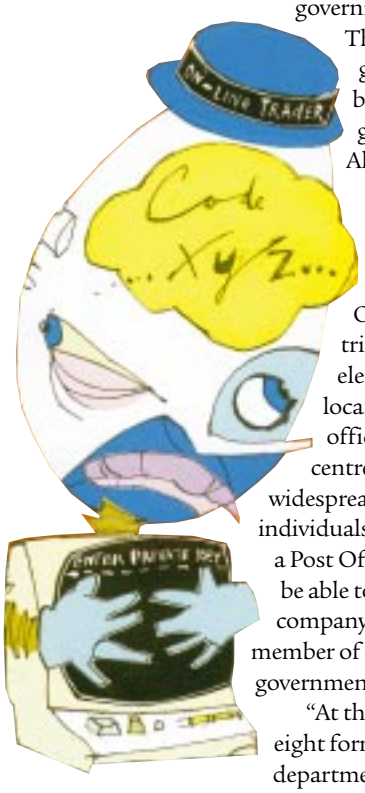
Cracking the code

Security experts divide hackers into three categories.
Rogues — often children in their bedroom.
Exploiters — a.k.a. "Black Hat Hackers" who act through personal profit, political motive or revenge.
White Hat Hackers — who hack for research purposes.

Many hackers love nothing better than to crack "unbreakable" codes. Generally, the longer the key length the more possible keys there are and the harder it is to crack a code. That's why it's important to use strong encryption with long key lengths.
The starkest example of hacking came when the original, exportable, 40-bit SSL encryption on the Netscape Navigator browser was broken. DES, since it is touted by the US Government, is also a particular favourite. Privacy advocates group the Electronic Frontiers Foundation (EFF) cracked the 56-bit DES in 56 hours with a $220,000 computer — down from the previous mark of 39 days. The EFF used a standard PC outfitted with custom chips. It's estimated this task would take an intelligence agency 12 seconds. Some experts, however, feel that the widespread use of encryption is the most important factor. Their argument is: why would a criminal break an encryption code to find a credit card number when inadequate security might allow them to lift thousands of numbers from a credit card database? John Botting, UK general manager of Security Dynamics which owns RSA, said: "All this talk of long bit lengths is just mathematical masturbation."

needs to be able to access information if there is evidence of law-breaking.

The Government have signaled that digital certificates will become the standard access to benefits and be required for online tax preparation, payments and access to governmental proceedings and documents. The Government has set an ambitious goal of transacting a quarter of business between citizens and government electronically by 2002. Already this process is beginning.



The Post Office has launched a £3m trial scheme to offer branded services in non-post office locations to help new business start-ups. The Open for Business scheme will be trialed for a year in Norwich, with electronic kiosks and computers in eight locations within post offices, council offices, libraries and business advice centres. Open for Business heralds the first widespread use of a database holding individuals' confidential encryption keys. Using a Post Office smartcard, small businesses will be able to register the start-up of a new company, or the employment of a new member of staff without needing to visit government offices.

"At the moment you have to fill in up to eight forms from three government departments to register. The failure rate is 40 percent," said David Clark, the then public services minister when he launched the scheme. Similarly, Barclays Bank is running a smart-card-based digital signature service that will allow an individual to register via the internet as self-employed.

People who are starting their own businesses are required to register with three government departments: the Contributions Agency, Inland Revenue and HM Customs and Excise. Using smart cards and readers in their home PCs or in select Barclays branches, the trial will enable users to submit streamlined electronic intelligence forms, digitally sign the forms, and submit them to the Government. However, unlike the Post Office scheme, the bank's cards will not store personal encryption keys used for sending and receiving encrypted messages. Sources say the bank is unhappy with government proposals to attach special requirements to licences granted to issuers of encryption keys. However, Nigel Hickson said that minimum standards for licensed CAs would be necessary to win public confidence in electronic commerce.

SOME MAY SAY THAT THE ENCRYPTION debate is central to the relationship between government and the individual. That's overhype, but only just. The widespread availability of strong ciphers means that shady characters have no need to use licensed encryption service providers. It's also possible to bury encrypted data text within, say, an image file via a process called steganography. The encryption genie is out of the bottle. Those who will use licensing regimes — and that means the man or woman in the street and the small business person — have the right to privacy as well as trust. The Labour Government could do a lot worse than reflect on its statements in opposition: "Attempts to control encryption are wrong in principle and un-workable in practice."

PCW CONTACTS

DTI www.dti.gov.uk
Electronics Frontiers Foundation www.eff.org
PGP www.pgp.com
Verisign (online CA) www.verisign.com