



© 1997–2004, Millennium Mathematics Project, University of Cambridge.

Permission is granted to print and copy this page on paper for non-commercial use. For other uses, including electronic redistribution, please contact us.

Mar 2002

News

Terrorists' code of honour



Until recently, it was over 300,000,000,000,000,000,000,000 times easier to steal private information (such as credit card details) transmitted over the web by someone living outside of North America than someone living within. This was due to regulations banning the export of strong encryption technology from the United States, where most of the web browsers are produced. At the end of last year, changes to these regulations were finalised to allow products incorporating strong encryption to be exported to most countries in the world.

The major reason for the ban was the US Government's fear that high-quality, effectively unbreakable, encryption posed a security risk. However, most encryption experts were pretty sure that once strong encryption was available in the US, criminals and terrorists elsewhere would be able to get hold of it, legally or otherwise, and so the export ban would be pointless.

Ironically, it appears that these experts may have been overestimating the intelligence – or underestimating the lawabidingness! – of terrorists. *Wall Street Journal* reporters bought computers from looters in Kabul – and found files believed to have been created by al-Qaeda members. The files were only encoded using 40-bit encryption, which was broken by brute force – trying all possible keys.

Cryptography, the mathematics behind encryption, has been an important military tool for centuries and played a significant part in the outcome of the second world war. In fact, many governments classify encryption technology as a munition along with tanks, missiles and machine guns. In recent years it has become part of our everyday lives as we make purchases and conduct banking over the internet, requiring protection of our private information from prying eyes. At the same time cryptography has provided criminals and terrorists with access to secure communication, hampering the efforts of government surveillance of those

Terrorists' code of honour

activities. This was one of the reasons that the US government had been imposing restrictions on the export of cryptography, and the changes to the regulations do not alter the ban on exporting to the those countries regarded as supporting international terrorism, such as Cuba, Iran, Iraq – and Afghanistan.

These regulatory changes have major repercussions for your average web user. When you wish to keep the information you transmit over the web, such as credit card details, private, your web browser uses encryption to scramble information as it is sent across the internet. If the site you are connecting to offers secure connection, any information that passes between your browser and the website will be encrypted using a symmetric key algorithm (most retail sites do offer secure connections; your browser should alert you to the fact by showing a closed padlock in the corner of the screen or by means of a message). A symmetric key algorithm is a method in which the same key is used to both encrypt and decrypt the data and is secure if the key is known only to the the sender (you) and the receiver (the retail website). But how can your browser and the website agree on this secret key without anyone else finding out? The key can be transmitted securely thanks to the RSA public key algorithm. This method is used to communicate the key, but is not used to encrypt all of the data sent, as it is slower to apply than a symmetric key algorithm. The symmetric key algorithms used today are, for all practical purposes, unbreakable. That is, for large enough key sizes, available computing resources are insufficient to break the keys in anything like a short enough time to be useful.

After the changes to US laws, international browsers now use 128 bit keys, replacing the 40 bit keys in use previously. (A bit, short for binary digit, is the way computers store data as a series of zeroes or ones). Breaking the symmetric key algorithms used today usually involves exhaustively searching through all the possible keys. Using keys that are 128 bits long means that there are 2^{128} possible keys to search through, whereas with a 40 bit key there are only 2^{40} keys, making the 40 bit key encryption 2^{88} (approximately 3×10^{26}) times easier to crack. According to Paul Kocher, who was involved in breaking a 56 bit symmetric encryption challenge set by RSA corporation in 1998, a dedicated code breaking machine could break 40 bit encoded data in an average 5.9 secs (see <http://www.rsa.com/rsalabs/pubs/cryptobytes.html> winter 1999 edition), whereas current estimates for breaking 128 bit key encryption with available computing resources approach the age of the universe.

All new browsers now come with 128 bit encryption. If you use Internet Explorer, you can check the level of encryption your browser supports by looking for the cipher strength information under 'About Internet Explorer' choice on the 'Help' menu. If you do not already have it, you can download 128 bit encryption for Internet Explorer from <http://www.microsoft.com/windows/ie/download/128bit/default.asp>. For further information on how to check what level of encryption your Netscape browser uses, and to download 128 bit encryption, see <http://help.netscape.com/kb/consumer/19970621-7.html>.

For more information you can browse the [frequently asked questions](#) on the RSA site. And while you browse, you can ponder the fact that the world's most active terrorist organisations is considerate enough to observe the fine print of US export regulations!

Rachel Thomas



Plus is part of the family of activities in the Millennium Mathematics Project, which also includes the [NRICH](#) and [MOTIVATE](#) sites.