The Cryptography Wars and the real need for backdoors

Keith Martin, Professor of Information Security at Royal Holloway, University of London's world-leading Cyber and Information Security Group, provides a detailed look at the history of cryptography and the ongoing Crypto Wars, which have been brought to a head by the Snowden revelations. Keith ponders on the possible outcomes of the Crypto Wars and explains that the tensions that arise over the use of cryptography are just one manifestation of the wider tensions between liberty and control in a civilised society.

In January 2015 UK Prime Minister David Cameron wanted to outlaw it. FBI Director James Comey was "concerned" about it but by May 2015 "depressed" about it. In October 2015 BBC Security Correspondent Gordon Corera reported that, according to "the authorities," it was the post-Snowden fallout event having the most significant impact on national security. We're clearly talking about something really bad. The trade in nuclear weapon components?

They were all referring to the increasing use of cryptography, the toolkit of mathematical techniques used to provide security for digital data. In particular, their comments concerned encryption, which can be used to scramble data and render it unreadable to anyone other than the desired recipients. Cryptography lies at the heart of almost all digital security systems and is widely regarded as the only means of providing the core security services (confidentiality, integrity and authentication) that we need to secure cyberspace. Yet it is clearly causing many influential figures of authority sleepless nights (something openly confessed to by Brian Snow, a former NSA Technical Director). Rarely has an application of mathematics charged such political controversy!

Cryptography has been at the centre of slanging matches between different sections of society for several decades, an ongoing debate which has somewhat provocatively run under the moniker 'the Crypto Wars.' However, as time goes by, the stakes seem to increase for all sides. The real question is whether anyone can win.

The world that once was

Before there were wars about cryptography, wars were really the only motivation for the use of cryptography. Cryptography was used by military powers during times of conflict to communicate strategic information. In the Napoleonic Wars encrypted instructions were written down and carried by messengers. By the Second World War information was encoded by mechanical devices and transmitted in encrypted form by radio. Why were the military the only historical users of cryptography? Were the rest of us just ignorant of its benefits?

Put simply, in daily life we had no need for cryptography. We lived and communicated in a physical world. When we had secrets to exchange we whispered them in person, or transferred them in sealed envelopes that were safely locked away. We recognised people by faces, voices and handwriting. These physical security mechanisms were not foolproof, but they were good enough in most situations (and they still are). The military, however, had mission critical information to protect. So they did use cryptography and came to regard it as a vital technology.

A short history of computing

After the Second World War came the advent of modern computing and the beginning of what we now refer to as cyberspace. Early computers were substantial standalone devices usually located in a physically secure room. However, from the 1960s computers started to communicate with one another. The data transferred between devices was potentially vulnerable to interception and cryptography was exactly what was needed to protect it.

Until the 1970s computers largely remained expensive luxuries of government and the military. In the 1970s business adoption of computing commenced, hence the need for non-government organisations to have access to cryptographic technology. This decade saw the development of the first open cryptographic standards. By the 1980s computers became consumer devices.

The 1990s saw development of the internet, which for cryptography was a 'game changer.' The internet enabled entire businesses to be built around the provision of digital services. Data exchanged across the internet can be from anyone, read by anyone, changed by anyone. It is the use of cryptographic tools that provide assurances that data can be sourced, cannot be viewed, and has not been altered along its journey. The spectacular success of the internet had one very significant cryptographic outcome. During the 21st century, computers, and thus cryptography, slipped into almost every pocket.

A brief explanation of cryptography

The goal of encryption is to convert a plaintext (the data to be protected) into a ciphertext (random-looking data that should

make no sense to any unauthorised party who intercepts it). This is done by passing the plaintext through an encryption algorithm, which is simply a set of mathematical rules that jumble the data up. The intended recipient of the plaintext then uses a decryption algorithm to convert the ciphertext back into plaintext. We generally assume that the encryption (decryption) algorithm is known to everyone (in many applications these are open standards). The intended recipient thus needs something that the rest of the world does not know in order to make sense of the ciphertext. This 'something' is known as the decryption key, a number that is also fed into the decryption algorithm. The decryption key must be kept secret by the recipient.

The cryptography dilemma

From a strategic government perspective, the dilemma presented by technologies such as cryptography is that they are extremely useful so long as they are in the hands of the 'right' people. This is a challenging, but (thus far) reasonably solvable, problem for technology that is very difficult to build, such as nuclear warheads. But cryptography is just a set of mathematical rules. In the hands of the 'wrong' people cryptography can lock out intelligence agencies and law enforcement from access to information about what these people are doing. From a government perspective this, in a nutshell, is the cryptography dilemma.

Backdoors

The earliest users of cryptography were governments and the military. One of the first manifestations of the cryptography dilemma came when some governments wanted to sell cryptographic technology to other governments who were not 'fully trusted.' High-grade cryptography prior to the 1980s was implemented in hardware devices. Hence the mathematical details of how the cryptography actually worked could be embedded into hardware in ways which were hard to extract. This provided an opportunity for backdoors to be secretly inserted into the devices, making the strength of the cryptography less than it appeared to be. Naughty perhaps, but effective.

The arrival of commercial cryptographic standards in the 1980s made backdoors much less feasible, since users of cryptographic technology wanted open assurance of the strength of the cryptography being deployed. Backdoors are also deeply unattractive features since, if they are discovered and publicised, the security provided by the cryptography is lost for everyone. Alas, as we later mention, this aspect of backdoors appears to have been lost on some in the NSA.

Restrictions on key length

During the 1980s cryptography became commercialised and also took off as an academic pursuit. Governments thus had to face the cryptography dilemma head on. Could a balance be struck between allowing everyone access to cryptography, while still facilitating the circumvention of cryptography by authorities in extreme circumstances?

Recall that to obtain the plaintext from a ciphertext it is necessary to have knowledge of a secret decryption key. In the absence of knowledge of this key, one costly solution is to try out every possible key until the correct one is found. This is no idle Sunday afternoon task, but if an organisation has powerful computers (or at least more powerful computers than the typical users of cryptography) then perhaps the key can be found. The length of a cryptographic key essentially determines how difficult this task is.

The solution of choice to the cryptography dilemma in the 1980s was to impose restrictions on the length of cryptographic keys, particularly if they were being used in any technology that was being exported across national borders. The chosen length restrictions were designed to offer 'enough' security for the day-to-day users while (presumably) offering 'not enough' security to keep out the government agencies setting the controls.

This idea almost made sense at the start of the 1980s when cryptographic technology was restricted to hardware. However, as the decade proceeded, it became much more feasible to implement cryptography in software, particularly as strong cryptography was now being designed by the open community. Cryptography was code, which could be written down in a book or even printed on a t-shirt.

This was the birth of the true 'Crypto Wars' as voices spoke out against cryptography controls. There were claims that cryptography enabled fundamental human rights such as privacy from oppression. There were arguments that cryptography was freedom of speech. Control of cryptography, on the other hand, was the action of 'Big Brother.' Control of cryptography constrained the security of businesses. It was the latter argument that won the day.

Key escrow

As the 1990s unfolded and the internet emerged, it was broadly recognised that strong cryptography was necessary for secure business. Key length

restrictions faded away but the cryptography dilemma remained. How could governments allow strong encryption to be used while still retaining some means of access to protected information?

The idea that emerged from the US, and was swiftly echoed in the UK, was the concept of key escrow. The basic idea was to allow strong cryptography to be used, but not 'any old' cryptography. Instead certain bespoke licensed technologies could be used and, critically, the decryption keys required to reveal the data would be held in escrow. This meant that trusted agencies would be given a copy of the decryption key which would be kept sealed and protected 'for a rainy day.' Should that rainy day arrive in the form of a legal warrant, the trusted agency would hand over the decryption key within the full terms of the law. The ciphertext could then be decrypted to reveal the plaintext.

It is hard to know where to begin to critique this idea, other than to observe that it was deeply unpopular with business (the overheads, the restrictions, etc.) and somewhat obviously any real miscreants would presumably just bypass the official mechanisms in the first place and use their own cryptography. Key escrow died a death before it ever really breathed.

Mr Snowden

As the 21st century dawned, there were many who believed that the Crypto Wars had been won by those hostile to control of cryptography. The UK Government passed a law that made it illegal not to provide decrypted data if required to do so under warrant. This left everyone free to use their own strong cryptography and still provided a legal channel to access plaintext.

Meanwhile we all did more and more in cyber space, and protected much of what we did do with cryptography. How frustrating this must have been for those who wished to control cryptography!

The FBI Director is depressed about cryptography because one response to the Snowden revelations has been a further increase in the use of cryptography

Clearly it was frustrating. What we learned in 2013 when Edward Snowden started leaking information about national security practices was that government agencies in some countries have essentially been 'throwing the book' at cryptography. They have, it seems, been using almost every conceivable means of trying to get around the use of strong cryptography. They have been chasing plaintext wherever they can find it on a system, they have been colluding with commercial organisations to get copies of critical decryption keys and, somewhat disappointingly, they have been corrupting standardisation processes in attempts to put backdoors into some cryptographic tools. In order to address the cryptography dilemma they have been, to an extent, compromising the security of the systems that we have all been using in cyberspace. The Crypto Wars have, it seems, been raging on, with fury.

Who will win the Crypto Wars?

The FBI Director is depressed about cryptography because one response to the Snowden revelations has been a further increase in the use of cryptography, particularly end-to-end encryption, which protects data pretty much from creation to destruction. David Cameron has clearly considered that this is something that needs attention. New legislation on cryptography and powers of interception are brewing in several parts of the world. So, who is winning the Crypto Wars now?

Watch this space, but I am willing to make several predictions. We don't look like we'll be abandoning cyberspace anytime soon. We're going to have smart homes, cyber cars, intelligent implants and wearable internet-connected accessories. We are clearly going to continue to need security in cyberspace. We are thus going to be using more and more cryptography in the future. This means that the cryptography dilemma will perpetuate, probably accentuate, and certainly not resolve itself.

But here's the bottom line. The tensions that arise over cryptography are just one specific manifestation of the wider tensions between liberty and control in civilised society. Indeed one could argue that governance itself is all about finding compromises between these two ideas. These compromises are dynamic and need to be adjusted as society evolves. And in any democratic society these compromises can, and should, be the subject of public negotiation. Indeed Edward Snowden has claimed that it was an absence of public negotiation about recent surveillance practices that motivated his action.

Given the ubiquitous future use of cryptography there can only be one conclusion. Long live the Crypto Wars.

Keith Martin Professor of Information Security
Royal Holloway, University of London
keith.martin@royalholloway.ac.uk

Keith Martin is a Professor of Information Security at Royal Holloway, University of London. His research interests include the design and management of cryptographic applications. He is the author of Everyday Cryptography (Oxford University Press).