

Babbage

Breaking cryptography

The NSA's crypto "breakthrough"

Has the NSA found a way to crack existing internet-security systems?



Babbage

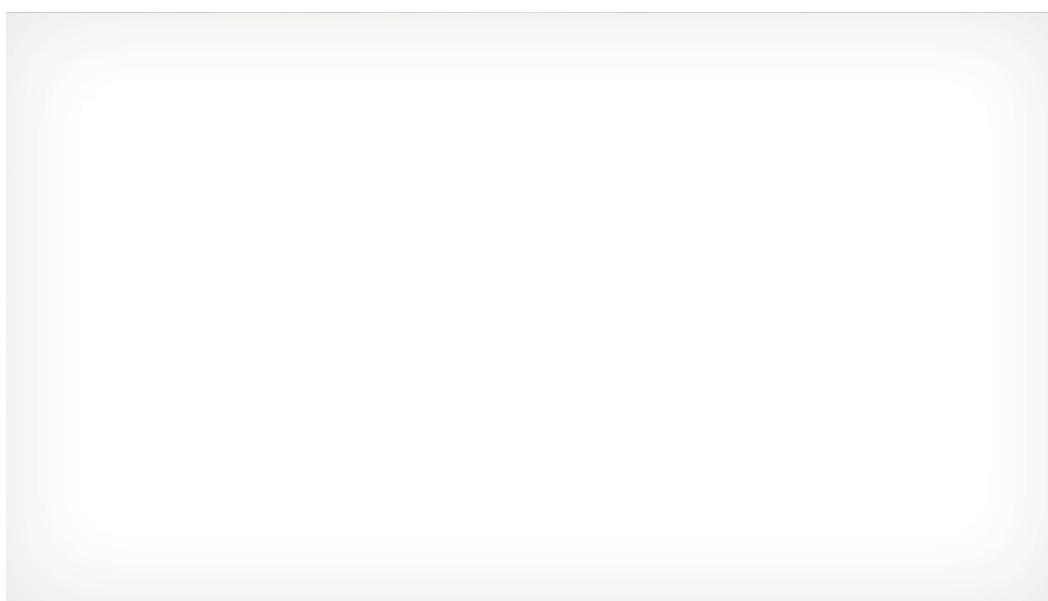
Sep 2nd 2013 | by T.C.

ONE difficulty of reporting on spy outfits like America's National Security Agency is the veil of secrecy they operate behind. This makes it hard to know exactly what they are and aren't capable of. It is also one reason why Edward Snowden's revelations have been so fascinating. They offer a glimpse—limited and incomplete, to be sure—behind the curtain, and help to constrain the bounds of just what such agencies can do.

Take a recent [post](http://www.wired.com/threatlevel/2013/08/black-budget/) (<http://www.wired.com/threatlevel/2013/08/black-budget/>) on *Wired*'s security blog. It discusses the latest Snowden leak, which details the size of America's secret-intelligence budget. In particular, *Wired* picks up on James

Clapper, the Director of National Intelligence, talking about investing in "groundbreaking cryptanalytic capabilities to defeat adversarial cryptography and exploit internet traffic". And it links to another [post](http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/) (http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/) in which James Bamford, a veteran chronicler of the NSA, describes the agency as having made "an enormous breakthrough several years ago in its ability to cryptanalyze, or break, unfathomably complex encryption systems employed by not only governments around the world but also many average computer users". That sounds a lot like saying that the the spooks have managed to break at least some of the cryptographic codes that protect everything from secure e-mail to e-commerce.

ADVERTISING



inRead invented by Teads

Latest updates

The shifting toll of America's drug epidemic

GRAPHIC DETAIL

Independents stampede into Mexico's presidential election

AMERICAS

The European Central Bank starts its exit from quantitative easing

BUSINESS AND FINANCE

[See all updates](#)

If true, it would be a very big story indeed. Such codes are ubiquitous because they are widely thought to be secure. If such a breakthrough has indeed happened (and Mr Snowden, for one, [has said](http://www.businessinsider.com/edward-snowden-email-encryption-works-against-the-nsa-2013-6) (<http://www.businessinsider.com/edward-snowden-email-encryption-works-against-the-nsa-2013-6>) that it hasn't) what would it look like? Not being privy to the NSA's deepest secrets, Babbage has no idea. But

he can speculate.

The most likely (and least interesting) answer is that the NSA has found a bug in the way that specific programs implement cryptographic protocols. Such flaws are fairly common, and can usually be fixed simply by patching the software. (Though that relies on people finding the flaws and then sharing that information widely, which NSA would be unlikely to do.) However, Mr Clapper's and Mr Bamford's use of "groundbreaking" and "breakthrough" to describe the NSA's advances could be read as suggesting that something more fundamental could be at hand—perhaps even a flaw in the mathematics that underpin cryptography.

Electronic cryptography relies on the curious fact that some mathematical operations are easy to do in one direction but virtually impossible to perform in reverse. For example, multiplying two enormous prime numbers together to get a third colossal number is easy. But, analysing a colossal number produced in this way and trying to determine its prime factors is colossally difficult. So difficult, in fact, that it stumps even the world's snappiest supercomputers. This bit of mathematics—integer factorisation in the argot—forms the foundation of most of the internet's cryptographic systems (codes based on other kinds of mathematical operation exist, but they aren't as commonly used).

Researchers already know that it is possible, in theory, to break such encryption by building a quantum computer, an unusual machine that relies on various kinds of quantum weirdness to perform its calculations. A mathematician called Peter Shor proved (http://en.wikipedia.org/wiki/Shor%27s_algorithm) in 1993 that such a computer could be used to speed up integer factorisation drastically, to the point where much of the internet's existing security infrastructure would be useless.

Does the NSA have a quantum computer in the basement of its headquarters in Maryland (pictured above)? It is theoretically possible, but pretty unlikely. For building a working quantum computer is itself terribly tricky. University laboratories have been trying for years, but the technology is finicky and progress has been slow. The record for prime factorisation using Shor's algorithm currently stands at the number "21", which was split into its prime factors (7 and 3) in 2012. A Canadian firm called D-Wave is presently selling a specialised kind of quantum computer—Lockheed Martin, an American defence giant, and Google have each bought one—but it is not suitable for this kind of work. And contrary to spy thrillers and conspiracy theories, it is far from obvious that a government agency could be so much more advanced than the academic cutting-edge, especially in a hardware and technology-heavy field like quantum computing.

There is another option, though. Mathematicians are much easier to get hold of than quantum computers, and do not require any fancy technology to work (a computer, a stack of paper and a bin will suffice). Signals-intelligence agencies employ them by the hundreds. And although it is difficult at present to find the prime factors of big numbers, no one has actually formally proved that it has to be so. In other words, no one knows whether the present state of the art is the fastest way to do things. Quicker ways may well exist.

Indeed, earlier in the year, there was some excitement in cryptographic circles when a pair of new (<http://eprint.iacr.org/2013/095.pdf>) papers (<http://eprint.iacr.org/2013/400.pdf>) reported the first significant progress in years in something called the "discrete logarithm problem". The discrete logarithm problem is intimately related to the problem of prime factorisation; progress in one usually leads to similar progress in the other. The advance in question was limited to a specialised subcategory of the problem, and the consensus seems to be (http://www.schneier.com/blog/archives/2013/08/the_cryptopocal.html) that it does not, by itself, pose a threat to existing encryption protocols. But in mathematics success often builds on itself. A development can suggest new tactics for attacking a puzzle. And the scent of a hot topic can lure clever mathematicians with fresh ideas.

Babbage will now put on his tinfoil hat. Crypto-cognoscenti will tell you that spy agencies can sometimes be ahead of the game. The mathematics that enable modern cryptography (specifically, those which allow secure communication over a public network like the internet) were for a long time thought to have been invented by two groups of Americans—Whitfield Diffie, Martin Hellman and Ralph Merkle on the one hand, and Ron Rivest, Adi Shamir and Leonard Adleman on the other. But in 1997 GCHQ, Britain's signals-intelligence agency, admitted that a group of its own in-house mathematicians, Clifford Cocks, James Ellis and Malcolm Williamson, had actually come up with something very similar (http://www.ieee.org/about/news/2010/6october_2010.html) a few years earlier.

Science often works like that: once the tools become available to tackle some problem, several researchers come up with similar ideas independently in a short space of time. Famous examples include Isaac Newton and Gottfried Leibniz inventing the calculus, Charles Darwin's nearly being scooped to the theory of evolution by natural selection by Alfred Russell Wallace, or the discovery of the mechanism which gives elementary particles mass, associated with the British

physicist Peter Higgs but which two other groups of theorists also cracked, all within months of each other.

Could something similar have happened with the problem of finding prime factors of large numbers? Has some group of anonymous mathematicians in Maryland improved their algorithms to the point where attacks on encrypted communications might become feasible? Again, probably not. But it is impossible to know—unless, of course, another set of more candid researchers come up with something similar in short order.

Update: this post was updated at 18:13 GMT to clarify some sentences in the 8th paragraph.

[Next](#)

And it's goodnight from us