More from The Economist | Subscription | Log in or register

The Economist | World politics | Business & finance | Economics | Science & technology | Culture | Blogs | Debate | Multimedia | Print ec

Babbage

Science and technology

Comment (4) Print

E-mail Perm

Reprints & permissions

Previous | Next | Latest Babbage | Latest from all our blogs

About Babbage

Reports on the intersections betwee technology, culture and policy, in a b after Charles Babbage, a Victorian r and engineer

Follow @EconSciTech 41.3K followers

RSS feed

Breaking cryptography

The NSA's crypto "breakthrough"

Sep 2nd 2013, 15:00 by T.C.

Like 17 Tweet 27

Reuters

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 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 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.

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 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 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 everyone thinks that it is difficult to find the prime factors of big numbers, no one has actually formally proved this. In other words, just because no mathematician has ever found an efficient non-quantum algorithm for finding prime factors does not mean that one does not exist.

Indeed, earlier in the year, there was some excitement in cryptographic circles when a pair of new papers 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

Economist video

Explore trending topics

Comments and tweets on popular to

Readers' comments

other. The advance in question was limited to a specialised subcategory of the problem, and the consensus seems to be 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 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 mathematicans in Maryland improved their algorithm 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.

Previous

Remembering John Mainstone: Guardian of the Pitch Drop

Next

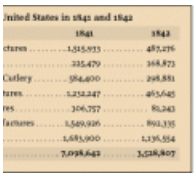
Recommend 10 Like 17 Tweet 27 Share 3 3

View all comments (4) Add your comment

More from The Economist

Cartography: The true true size of Africa

New York City: You probably can't make it here



Jnited States in 1841 and 1842

	1841	1842
ctures	1,515,933	487,276
	335,479	368,873
Cutlery	584,400	298,881
tures	1,232,247	463,645
res	306,757	81,243
factures	1,549,926	892,335
	1,683,900	1,136,554
	7,098,642	3,528,807

Our expiring commercial treaty with the Brazils

Full version

Recent Activity

Sign Up Create an account or **Log I** your friends are doing.

Lucky no more
8,266 people recommend this.

Get a life!
21,529 people recommend this.

One person recommends this.

Hit him hard
2,190 people recommend this.

Facebook social plugin

Follow *The Economist*

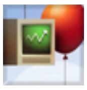
Latest blog posts - All times are GI

Azerbaijan: How not to pre election
Eastern approaches - 1 hour 40 n

Breaking cryptography: T "breakthrough"
Babbage - 2 hours 19 mins ago

Hawaiian Airlines: Mini re
Gulliver - 3 hours 7 mins ago

What to read: On Syria
Pomegranate - 3 hours 37 mins a



Money talks: September peculiar row
Schumpeter - Sep 2nd, 12:36