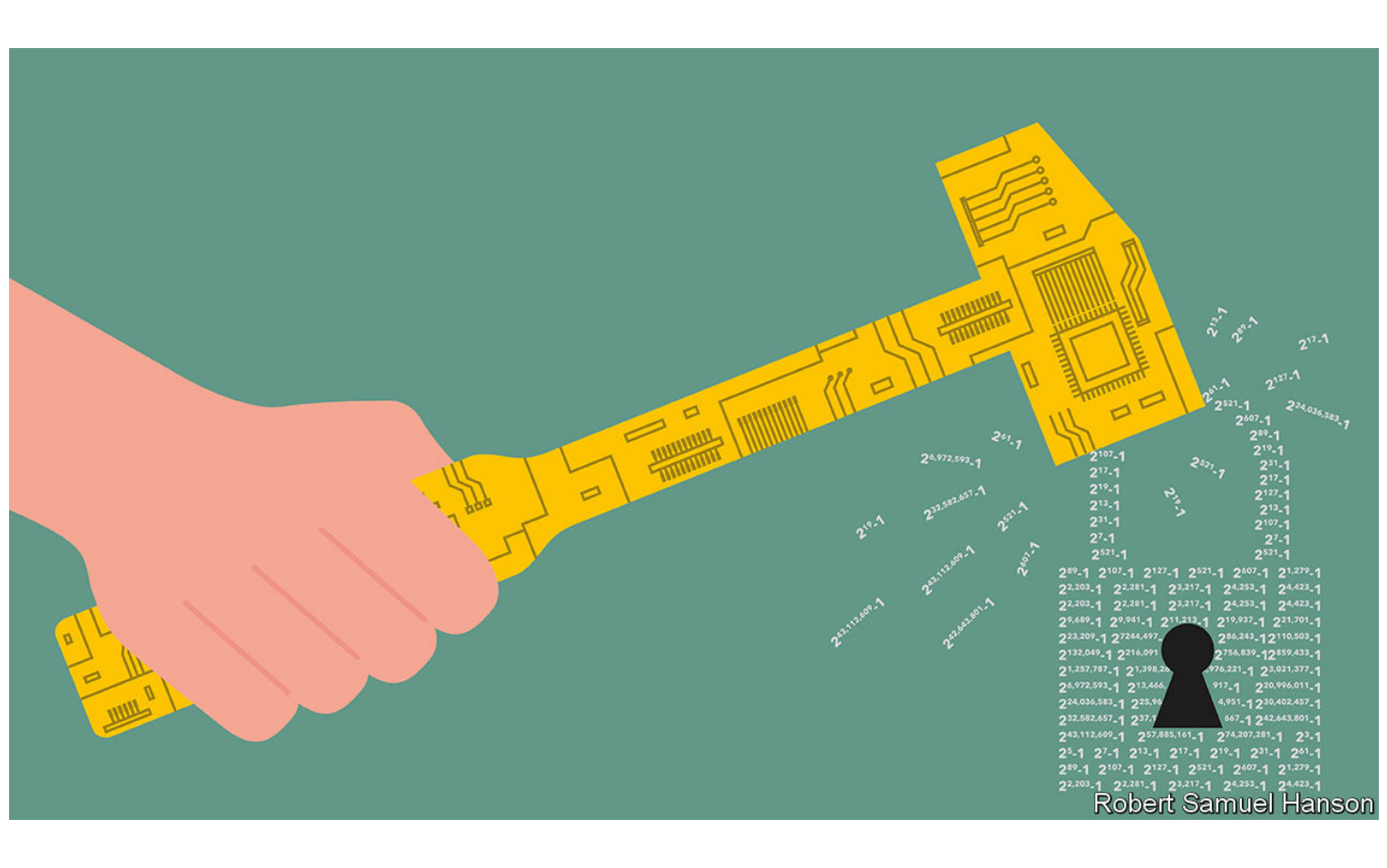
Future-proofing the internet

Quantum computers will break the encryption that protects the internet

Fixing things will be tricky



Robert Samuel Hanson

Print edition | Science and technology ›

Oct 20th 2018

As every schoolchild knows, some sorts of mathematics are harder than others. In the classroom, that is annoying. Outside, it can be useful. For instance, given two prime numbers, however large, multiplying them together to find their product is easy. But the reverse—factorising that product back into its constituent primes without knowing in advance what those primes are—is hard, and becomes rapidly harder as the number to be factorised gets bigger.

Factorising numbers into their constituent primes may sound esoteric, but the one-way nature of the problem—and of some other, closely related mathematical tasks—is the foundation on which much modern encryption rests. Such encryption has plenty of uses. It defends state secrets, and the corporate sort. It protects financial flows and medical records. And it makes the $2trn e-commerce industry possible. Without it, credit-card details, bank transfers, emails and the like would zip around the internet unprotected, for anyone so minded to see or steal.

Nobody, however, is certain that the foundation of all this is sound. Though mathematicians have found no quick way to solve the prime-factors problem, neither have they proved that there isn't one. In theory, any of the world's millions of professional or amateur mathematicians could have a stroke of inspiration tomorrow and publish a formula that unravels internet cryptography—and most internet commerce with it.

Send in the qubits

In fact, something like this has already happened. In 1994 Peter Shor, a mathematician then working at Bell Laboratories, in America, came up with a quick and efficient way to find a number's prime factors. The only catch was that for large numbers his method—dubbed Shor's algorithm—needs a quantum computer to work.

Quantum computers rely on the famous weirdness of quantum mechanics to perform certain sorts of calculation far faster than any conceivable classical machine. Their fundamental unit is the "qubit", a quantum analogue of the ones and zeros that classical machines manipulate. By exploiting the quantum-mechanical phenomena of superposition and entanglement, quantum computers can perform some forms of mathematics—though only some—far faster than any conceivable classical machine, no matter how beefy.

When Dr Shor made his discovery such computers were the stuff of science fiction. But in 2001 researchers at IBM announced that they had built one, programmed it with Shor's algorithm, and used it to work out that the prime factors of 15 are three and five. This machine was about the most primitive quantum computer imaginable. But there has been steady progress since. Alibaba, Alphabet (Google's parent), IBM, Microsoft and the like are vying to build commercial versions, and the governments of America and China, in particular, are sponsoring research into the matter.

Big quantum computers will have applications in fields such as artificial intelligence and chemistry. But it is the threat posed by Shor's algorithm that draws most public attention. Large organisations may be able to get around the problem using so-called quantum cryptography. This detects eavesdroppers in a way that cannot be countered. But it is expensive, experimental and unsuitable for the internet because it must run on a special, dedicated network. For most people, therefore, the best hope of circumventing Shor's algorithm is to find a bit of one-way maths that does not give quantum computers an advantage.

There are candidates for this. Cryptographers are debating the relative merits of such mathematical curiosities as supersingular isogenies, structured and unstructured lattices, and multivariate polynomials as foundations for quantum-proof cryptography. But translating a piece of maths into usable computer code and then delivering it to the zillions of machines that will need updating will not be easy.

One question is, when is the deadline? When will an internet-breaking computer actually be available? Today's best machines can manipulate a few dozen qubits. Brian LaMacchia, who runs the security and cryptography team at Microsoft Research, thinks a "cryptographically interesting" quantum computer might be able to handle somewhere between about 1,000 and 10,000 of them. Predicting progress is hard. But Dr LaMacchia reckons such a machine might be ready some time between 2030 and 2040.

That sounds reassuringly far away. But several researchers argue that things have already been left too late. Though many communications are ephemeral, some people encrypt messages that they hope will remain secret for a long time. Spies and policemen around the world already store reams of online data in the hope that, even if they cannot decrypt them now, they may be able to do so in future. As Peter Schwabe, a cryptographer at Radboud University in the Netherlands, observes: "If someone ten or 20 years from now can decrypt my present-day communications with my bank, well, I probably don't care too much about that. But if I'm a dissident in some repressive country, talking to other dissidents? That might be a different story."

The second problem is how long a fix will take. The National Institute of Standards and Technology (NIST), an American standards organisation whose decisions are often followed around the world, is running a competition to kick the tyres on various quantum-resistant proposals. But its conclusions are not due until 2024. And as Nick Sullivan, who is in charge of cryptography at Cloudflare, an internet-infrastructure firm, observes, history suggests that, even once a new standard is agreed, the upgrade will be slow and messy. Despite—or perhaps because of—the information-technology industry's obsession with novelty, the internet resembles ancient cities like Rome and Istanbul, with modern structures built atop forgotten layers of old, unmaintained code.

For example, in 1996 researchers reported the first weaknesses in MD5, a type of widely used cryptographic algorithm called a hash function. A drop-in replacement that was readily available in the form of another algorithm called SHA-1. After more than two decades of exhortations to upgrade, though—not to mention high-profile cyber-attacks exploiting MD5's weaknesses—the older algorithm is often still used. Similarly, a vulnerability called FREAK, discovered in 2015, relied on the fact that many modern applications, including the default browser in Google's Android operating system and the White House's website, could be persuaded to revert to old, easily breakable cryptography installed in order to comply with long-abandoned American export regulations.

Testing, testing

Those with the most power to chivvy things along are the big companies that control much of the internet's pipework. Even while NIST deliberates, they are beginning to run tests of their own. At Microsoft, Dr LaMacchia plans to test quantum-resistant encryption on the links that connect the firm's data centres. Google has already tried integrating different kinds of quantum-resistant cryptography into experimental versions of Chrome, its web browser, and has worked with Cloudflare to test the impacts in the real world.

The results have been mostly encouraging, but not wholly so. Changing the encryption changes the way browsers negotiate connections with websites. In Google's tests of the 2,500 most popular websites, some 21 of them—including LinkedIn, a social network, and Godaddy.com, a domain registrar—could not cope with the extra data involved, and refused to connect. And all of the proposed quantum-resistant schemes imposed noticeable delays compared with conventional cryptography.

Big firms will have power in other ways, too. Vadim Lyubashevsky, a quantum-computing researcher at IBM, points out that quantum computers need lots of coddling. Most must be cooled to a temperature close to absolute zero. This means that, for the

is full, says Dr Lyubashevsky, which could help limit nefarious uses. (Governments, though, will be able to shell out for their own machines.)

There are other wrinkles. The new cryptographic schemes generally require more computational grunt than the old sort, says Mr Sullivan. For desktop machines and smartphones, that is unlikely to be a problem. But smaller chips, embedded in gizmos from industrial-control systems to sensors, may struggle. Another worry is that the new algorithms may come with unforeseen weaknesses of their own. Mathematicians have had decades to attack the prime-factor problem, says Graham Steel, the boss of Cryptosense, a cryptography-focused security firm. The maths that underlie post-quantum schemes have not been similarly battle-tested. For that reason, the first implementations may hedge their bets by using both old and new sorts of cryptography at once.

The big companies are unlikely to commit themselves fully to an upgrade until the NIST has decided on the new standards. And even when that happens, the sheer size of the task is daunting. Mr Steel says one of his clients has thousands of apps that need updating. As chips migrate into everything from cars and children's toys to lighting systems and smart electricity meters, the amount of work will only grow.

All this means that quantum-proofing the internet is shaping up to be an expensive, protracted and probably incomplete job. Dr Steel compares it to dealing with the millennium bug, when a quirk in how a lot of programs handled dates meant they had to be retrofitted, at great expense, to cope with the transition from the year 1999 to the year 2000. In the event, thanks to the efforts of thousands of programmers, the millennium bug was mostly dodged. These days, the stakes are higher. The world is now considerably more computerised than it was then. Either way, it means plenty of steady work for cryptographers.

This article appeared in the Science and technology section of the print edition under the headline "Prime factors"

Print edition | Science and technology ›

Oct 20th 2018