Why RSA might fail

Hanging by a mathematical thread

The encryption system that powers our entire e-economy could collapse with the release of a single defective line of microprocessors. Keith Devlin explains why

Keith Devlin, National Post Published: Tuesday, February 12, 2008

How safe is your credit card number when you order something online? The answer is: It is very safe. But as encryption pioneer Adi Shamir [**Shamir is one of the founders of RSA – he's the S**] pointed out in a message posted on the internet in November, that safety hangs by a fragile thread. All it would take is one particular advance in mathematics, or one tiny error in a computer chip, and the entire edifice of Internet commerce (including online banking) would come crashing down.

The reason is that the method used to keep Internet messages secret depends upon the inability of mathematicians to solve a very simple kind of problem. The idea goes back to 1977, when Ronald Rivest, Adi Shamir and Leonard Adleman, all then at MIT, invented an ingenious and seemingly impregnable way to encode messages sent over open networks like the internet, then still in its infancy. The encryption system they invented is called RSA, after their initials.

RSA is a "public key" system. That means that to encode a message, all you need is a publicly available key code, whereas decoding requires a secret key. (All the encoding and decoding here is done by mathematics inside computers, and the "keys" actually are large numbers having a hundred or more digits.)

Here is how it works. Suppose you wanted to buy something from an online vendor, using your credit card. Your computer would ask the vendor's computer for its public encoding key for sending messages to them, and would use that key to encode your credit card details before sending them. The vendor's computer would use its secret key to decode the message and complete the purchase.

Anyone can buy from the vendor, since the encoding key is publicly available, but only the vendor has the key to decode the incoming messages, so even if a criminal intercepted your order en route, she or he would be unable to decode it.

This is analogous to building a safe whereby unlocking it requires a different key from the one you use to lock it. On the surface, that sounds impossible. After all, unlocking is just the opposite of locking, right? Indeed so, and for physical locks, you probably could not do this. But for mathematical locks, you can.

Obviously, since the secret decoding key will unscramble a message encoded using the public key, it must in principle be possible to figure out the secret key from the public one. But the system is set up so that it would take the most powerful computers hundreds of years to do this. This is why the keys are such large numbers.

In the RSA system, the secret key consists of two large prime numbers, each a hundred or more digits long, and the public encoding key depends on their product. The system's security depends on the fact that there is no method known to find the prime factors of a 200-digit product of two large primes within a human lifetime.

A potential danger with this system is that one day some clever mathematician will find a new way to factor large numbers. If that ever happens, internet security will collapse immediately. But mathematicians think this is unlikely to happen.

A greater threat, encryption experts suggest, is that someone will exploit some feature of the way the RSA algorithm is implemented in order to break the code. In his November posting, RSA co-inventor Shamir suggested one way this could happen.

The danger Shamir posited was that a computer chip manufacturer brings out a new model of arithmetic chip that has a hidden flaw, one that causes it to give the wrong answer when it performs certain calculations. This is not as unlikely as you might think.

Because of their incredible complexity, it is likely that any chip on the market has some flaw. In 1994, for instance, Dr. Thomas Nicely, a college math professor, discovered that the newly released Pentium chip gave the wrong answer when it divided certain numbers. Intel quickly brought out a new version of the chip with the error corrected. But by then, millions of computers had been sold with the faulty chip inside them. This is precisely the kind of error that could lead to a collapse of the RSA system.

As Shamir explained, if a computer chip is released that gives the wrong answer for just one multiplication problem, then a clever hacker could break any key (i.e., find the secret decoding key from the public encoding key) in any implementation of the RSA encryption system running on any computer containing that chip, anywhere in the world. In one fell swoop, there would be no internet security. (See sidebar for more detail.)

As it happens, there is a way to modify the RSA system to prevent the kind of attack Shamir described, and certain implementations in use have incorporated that modification for some time. But Shamir's purpose was not to highlight a specific weakness, rather to highlight the fact that the system should not be assumed to be foolproof. A tiny flaw anywhere in the system may potentially be exploited to bring it down.

In the world of encryption, it's a constant battle of mathematical and engineering wits between the good guys and the bad guys.

kdevlin@stanford.edu - Dr. Keith Devlin is a mathematician at Stanford University, and "the Math Guy" on National Public Radio.

HOW RSA ENCRYPTION WORKS --AND WHY IT MIGHT FAIL:

The mathematics used by the RSA system goes back to the 17th century, and can be understood by anyone who has taken a college-level course in algebra. But the details are a little too intricate for a general-interest newspaper. A good description is given at http://mathaware. org/mam/06/Kaliski.pdf. The general idea is as follows:

The private decryption keys consists of two large prime numbers, p and q, generated in a random fashion by the receiver's computer. That same computer then computes their product n = pq (called the modulus for the system) and finds an odd number e (called the public exponent of the system) between 3 and n-1 that has no factors in common with either of p-1 and q-1. The two numbers p and q comprise the private decryption key; n and e constitute the public encryption key. There are simple, fast algorithms for doing all of this, but (to all intents and purposes) there is no known method for recovering p and q from n and e other than an exhaustive search, which will take hundreds of years for numbers having a hundred or more digits.

Any message sent with RSA encryption is first converted into numeric form; it can be thought of as a single big number, C. Encryption amounts to computing the remainder after computing the power Ce and dividing it by n, a number generally denoted by Ce mod n. This can be done efficiently on a modern computer.

The number D = Ce mod n is the encrypted message (in numeric form). There is a simple formula to produce C from D, but it involves p and q. This means that only the intended receiving computer, the only one that knows p and q, can recover C from D.

Since C will be much bigger than the length of the words the computer uses (typically 64 or 128 bits), the computer must break C into word-length pieces, and carry out all arithmetic by manipulating those pieces, in much the same way that a human calculator does multi-digit arithmetic in terms of its individual digits. (The familiar high school arithmetic procedures.) This is the potential loophole that could enable a bug attack.

Suppose that a computer chip gives an incorrect result when it multiplies the two inputs a and b. A hacker who knows a and b can then break the code as follows. Hacker computes the square root of n and takes c to be the nearest whole number. Then c will be between p and q. Hacker then creates a "Trojan horse" message m that is numerically equal to c except that two low order words in it are replaced by a and b. Hacker then encrypts the message and sends it to the receiving computer, which promptly decrypts it.

The decryption process begins with the computation of m2 mod p and m2 mod q. Since p < m < q, the first of these will essentially randomize m2, and hence will almost certainly not contain a or b, but m mod q = m, so the second will definitely involve multiplication of a and b. The remainder of the decryption process involves several multiplications, and hence will almost certainly be correct mod p but (because it involves multiplying a by b) incorrect mod q. This difference in behaviour will propagate through to the output sent back to the hacker by the receiver, and (because of the way RSA encryption/ decryption works) is sufficient for the hacker to carry out a simple computation to determine p, and hence break the code.

Source: Keith Devlin

One of the most enduring problems in mathematics might be solved in the next few months, but not everyone will be dropping their calculators to read the proof.

A 75-year-old maverick named Louis de Branges has claimed he has the answer. Again.

The blunt-spoken, beret-wearing Frenchman has spent more than two decades at Indiana's Purdue University trying to crack the elusive Riemann Hypothesis, a solution that would bring a much greater understanding of the nature of prime numbers and about nature itself. So far, his peers have rejected his various calculations. A seismic accomplishment, it could reap him a $1-million award. But perhaps more important for Mr. de Branges, it might bring vindication. "There has been a lot of unprofessional action on part of people who should know better," the MIT-and Cornell-trained professor said in a rare interview. "They're beginning to see that they're wrong."

Despite its pursuit of rational explanations, high-stakes mathematics can be as whimsical and unforgiving as any academic field, fraught with cranks, snobs and busybodies who instinctively knock peers for their checkered track records, schools of thoughts or personalities. While Mr. de Branges earned a measure of scientific immortality when he cracked the daunting Bieberbach Conjecture more than 20 years ago, some peers feel he has shouted "Eureka!" too many times already.

"He has produced several incorrect proofs, and people are having difficulties with reading another one," said Andrew Odlyzko, director of the Digital Technology Centre at the University of Minnesota. "They're rolling their eyes, saying, Why should I inflict this on myself ?' "

Dozens of mathematicians submit proposals each month to various publications, subjecting their calculations --and their reputations -- to an inscrutable winnowing process. Not every proposal in the slush pile can or should be read. In the world of deep math, claiming that one has cracked the Riemann Hypothesis is almost tantamount to saying that you have penned the Great American novel. Only a few are capable of this such an august accomplishment.

Introduced by Bernard Riemann in 1859, the theory concerns prime numbers, whole numbers such as three or seven or 11 that are divisible only by themselves or by one. While they are building blocks of mathematics, their pattern remains elusive. "If you understand the patterns of primes, you are three-quarters of the way to understanding all numbers," said Keith Devlin, a Stanford University math professor perhaps best known as "The Math Guy" on National Public Radio in the United States.

While the Riemann Hypothesis has been verified on computers for millions of cases, Mr. Devlin said, no one has been able to prove that it is true for every single case. It remains a generalization of sorts: To oversimplify, perhaps, it's like saying that everyone is born with ten toes.

The repercussions of this discovery would seep beyond the rarified world of deep math into the real world: ravaging internet security, just for starters. "Internet encryptions depend on prime numbers," Mr. Devlin said. "With the knowledge they've gained from a solution, the bad guys could get into medical records, financial records, everything."

http://www.math.purdue.edu/~branges/apology.pdf

A leap in technology

Quantum breakthrough comes with security risks

Nicole Visschedyk, National Post Published: Friday, January 04, 2008

The National Post presents a week-long series about some of the most interesting ideas to emerge in the past year -- innovative notions that helped define 2007 and will shape the way we live in 2008. Today: quantum computing.

In a major technological step, a team of Canadian and Australian researchers has completed the first quantum calculation--an experiment that brings the theoretical idea of a quantum computer closer to reality.

"Functional large-scale quantum computers may be many years away, and it is hard to know exactly how they will change the world--but change the world they will," said Daniel James, a researcher at the University of Toronto and lead Canadian researcher on the team.

However, some of the applications are likely to include voice-recognition software, auto-navigating cars and extremely accurate weather forecasting.

"It's mind-boggling what we'll be able to do. We haven't seen anything yet," said Raymond Laflamme, the director of the Institute for Quantum Computing at the University of Waterloo, who predicts the quantum computer will make today's computers look like dinosaurs.

Modern computers work on a binary system of ones and zeros and are limited in their ability to compute large, complex problems.

"When you go to a bank, why don't you just talk to the machine rather than using a PIN?" Dr. Laflamme asked. The answer, he said, is because the voice-recognition technology does not exist yet. "The computational processes are just not powerful enough to it."

Quantum refers to the idea that very small, subatomic particles can have two locations or energies at once. Thus, quantum computers are based on a system of ones, zeros and simultaneously one and zero at the same time. They will use light particles, or photons, to perform complex computations virtually instantly.

The phenomenon is counterintuitive because everyday physics works under Newtonian laws. (If you drop a piano out a window, it falls to the ground.) At the level of the atom, things are governed by a different set of rules: the laws of quantum mechanics. (The piano would be simultaneously a piano and a wave of energy.)

These special and confusing laws are what make the proposed computers so incredibly powerful, Dr. James said.

"The quantum computer allows you to process all available outcomes of a problem at once," he said.

If the problem was cleaning a house, a traditional computer would clean one room at a time until the house sparkled. A quantum computer cleans the whole house all at once.

While the Canadian-Australian team performed a simple calculation -- three multipled by five -- the major step was that it was done using a quantum process.

"This is really the beginning of the era," said Dr. Laflamme, who said he expects usable quantum computers to exist 15 to 20 years from now.

However, Dr. Laflamme said society needs to start paying attention to the technology today because it could soon pose major security problems.

Bank PINs, credit cards, Interac, e-mail and government systems all rely on cryptography to keep private information safe. Data is encrypted or coded to allow only an authorized source to see it. In the case of banks, only someone with a password has access to the uncoded information.

Quantum computing would allow most current computer security codes to be broken in a fraction of a second.

"Most systems would need to be updated, everything relying on current encryption would be obsolete," Dr. Laflamme said. Updating all information to quantum would not be enough once the computers are available.

Since most information on the Internet is archived, once quantum cryptography is developed almost everything ever transmitted online would be completely accessible.

The U.S. National Security Agency has supposedly invested heavily in the technology. Since quantum computing would allow virtually anyone to access President George W. Bush's or any other government official's e-mail, the organization is not keen on being the last to learn the science.

"With everything we send today, you have to think its encryption could be broken when we build a quantum computer," Dr. Laflamme said. "For a company that

sends an encrypted e-mail outlining their strategy for the next 10 years, that's a problem."

If the technology becomes available in 2020 and the e-mail was sent in 2017, a hacker could conceivably access seven years' worth of secret corporate strategy.

The positive side of the technology is, once in place, quantum cryptography would offer unprecedented online security.

Several centres of quantum research exist in Canada. Dr. James estimates the total cost of worldwide research to be $250-million annually.

WHAT THEY DID

Quantum information versus binary information

Computers store information in a binary or basic code of ones and zeros called bytes. An analogy can be made to a light bulb, in a binary system the light is either on or off. In a quantum system of computer information the basic quantities of information are stored in qubits. Unlike the on or off model, qubits can be on, off or a combination of both at the same time.

The complex theory behind the computer works on the concept that at the atomic level something can have a blend of energies or locations.

What Daniel James and his research team did

By manipulating photons with a crystal the team managed a simple calculation. The computer calculated the two prime numbers that multiply to make 15.

Why this calculation?

A popular form of computer cryptography works on a simple concept of sums of prime numbers, numbers divisible by themselves and one.When prime numbers get very large computers have a difficult time finding the two prime numbers that are the multiples of the sum. This process is the basis of modern cryptography.