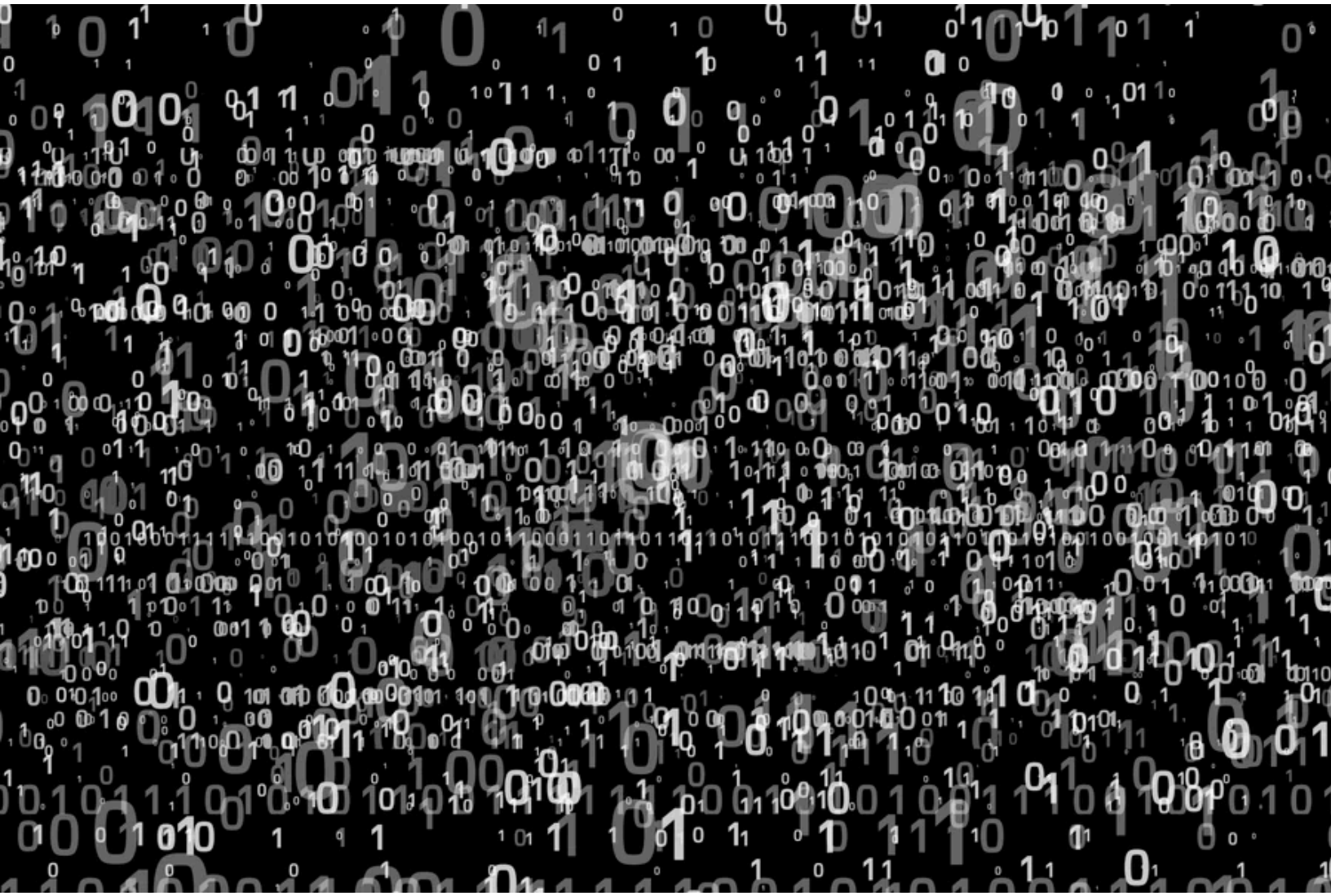
APRIL 9, 2025 | 5 MIN READ

This More Than 380-Year-Old Trick Can Crack Some Modern Encryption

A little math from the 1600s can make what people send to a printer more vulnerable

BY MANON BISCHOFF EDITED BY DAISY YUHAS



Arkadiusz Warguła/Getty Images

Mathematics

Hardly anyone is interested in my tax return—there's not much to it. And that's a good thing, given that an attacker might have fairly easily intercepted

the encrypted communication between my laptop and printer when I printed the return in recent years.

In early 2022 information technology security researcher Hanno Böck discovered that some of these encryptions could be cracked in a process that he went on to describe in a 2023 preprint paperposted to the International Association for Cryptologic Research's Cryptology ePrint Archive. His method can be traced back to one developed by the French scholar Pierre de Fermat in the 17th century.

Fermat—most famous for his mysterious "last theorem," which vexed experts for decades—contributed all kinds of useful things to the world of science in his lifetime. For example, he laid the foundations for the theory of probability and also worked a lot on prime numbers—those values that are only divisible by 1 and themselves.

Mathematicians suspected they could use Fermat's work to break encryption—and Böck demonstrated that case.

COMPLEX PROBLEMS FOR SECURITY

Modern encryption systems are based on difficult math problems. They work like a padlock: the problem (the lock) cannot be solved without additional information (the key). A common procedure is so-called RSA cryptography, which is related to prime numbers. Decomposing large numbers into a product of prime numbers is difficult, making them useful keys.

Prime numbers are often referred to as the atoms of number theory—indivisible building blocks from which the natural numbers are constructed. Any other number can be written as a unique product of primes, for example $15 = 3 \times 5$ or $20 = 2 \times 2 \times 5$. For small values, it is easy to determine the prime divisors. But what about, say, 7,327,328,314? So far, no computer program can quickly calculate the prime divisors of arbitrarily large numbers.

This limitation is precisely what RSA cryptography exploits. To understand how that kind of protocol works, consider a simplified example, where RSA is used to encrypts data with the help of large numbers. Suppose a person wants to send the word SCIENCE, which consists of seven letters, to a recipient in encrypted form. To do this, they use a large seven-digit number such as 6,743,214 and shift each letter of SCIENCE by the respective digit—so S shifts six letters over to become Y, C shifts seven letters to become J, and so on. The end result is the encrypted word CJMHPDI. A sender can now dispatch this to another person without a listener being able to decode the message.

The recipient, however, should be able to determine the original word SCIENCE, either with the key itself (6,743,214) or a clue for calculating the key. As the former always carries a risk—an attacker could eavesdrop on the communication between the two parties and thus intercept the key—RSA cryptography offers a way of reconstructing the key securely. The basic idea is that before sending the secret message, the sender and receiver jointly generate a key from publicly available information. Security is guaranteed by the fact that the sender and recipient each secretly use large prime numbers, which they multiply together, and only send each other the results of this calculation. An eavesdropper needs the prime numbers to generate the key. But because that person can only intercept the products and cannot factorize them, the eavesdropper is helpless. (The actual RSA protocol for the key generation is a bit more complicated, but that is the general idea behind it).

FERMAT FACTORIZATION

Nearly four centuries ago, Fermat was working on related problems. He wanted to know how to factorize numbers into their prime number components. He did this purely out of mathematical curiosity—at the time, no cryptographic methods for secure key exchange were known.

And indeed, Fermat found a way to factorize even large numbers that are the product of two prime numbers. His method is not complicated; you can do it with a calculator (though Fermat, incidentally, did not have one). To impress his contemporaries, Fermat demonstrated the method using the example number $n = 2{,}027{,}651{,}281$.

Fermat factorization works as follows: You take the number n, in this case 2,027,651,281, and take the root of it. As a rule, this will result in an odd value, as is the case here: $\sqrt{2{,}027{,}651{,}281} \approx 45{,}029.45$. You round up to get 45,030. This number is squared, and the original value n is subtracted from the result: $45{,}030^2 - 2{,}027{,}651{,}281 = 49{,}619$. Now you have to check whether the result is a square number. As it happens, 49,619 is not square.

So you continue. Start again with the rounded root 45,030, add 1 and then square the result in order to subtract the original value n from it—that is, $45{,}031^2 - 2{,}027{,}651{,}281 = 139{,}680$—and check again whether the result is a square number. Once more, this is not the case.

So you repeat the whole thing. This time you add 2 to 45,030 and square the result, from which you subtract the original value n: $45{,}032^2 - 2{,}027{,}651{,}281 = 229{,}743$. Again, this is not a square number.

Fermat must have had a lot of patience. In his example, you have to carry out the procedure a total of 12 times until you find a square number: $45{,}041^2 - 2{,}027{,}651{,}281 = 1{,}040{,}400 = 1{,}020^2$.

And how does this help? In the above equation, a squared number y^2 (in this case $45{,}041^2$) minus n equals another squared number x^2 (in this case, 10,202). The equation $y^2 - n = x^2$ can be rearranged as $y^2 - x^2 = n$. The left-hand side corresponds to an equation known as the third binomial formula, $(y - x)\cdot(y + x) = n$. This automatically factorizes the number n into two numbers $y - x$ and $y + x$. For the example with $n = 2{,}027{,}651{,}281$, the two factors are therefore $45{,}041 - 1{,}020 = 44{,}021$ and $45{,}041 + 1{,}020 = 46{,}061$. Both are prime numbers.

ATTACKING THE PRINTER

In fact, this factorization method always works for odd *n*. But computers can only perform it fast enough if the two prime factors of *n* are not too far apart. And this was precisely the problem that Böck discovered in a program library used by various companies at the time. The prime numbers generated for encryption were not random enough, and the program often selected two prime numbers that were close to each other. This means that Fermat's factorization method can be used to circumvent the encryption.

Böck realized that the printers of certain companies used such inadequate encryption. They used RSA cryptography, for example, to protect confidential documents that were sent to the printer via a network. After his finding in 2022, these companies issued alerts and fixes to address the problem. We can only hope that other companies have closed such security gaps.

In any case, many companies will have to rethink their encryption standards in the coming years. Even if ordinary computers fail to factorize large numbers, it will be different with powerful quantum computers. Fermat would never have dreamed that more than 380 years after his discovery, computers that rely on complicated principles of quantum mechanics for their calculations might make use of it.

This article originally appeared in Spektrum der Wissenschaft *and was reproduced with permission.*

MANON BISCHOFF is a theoretical physicist and an editor at *Spektrum der Wissenschaft*, the German-language sister publication of *Scientific American*.

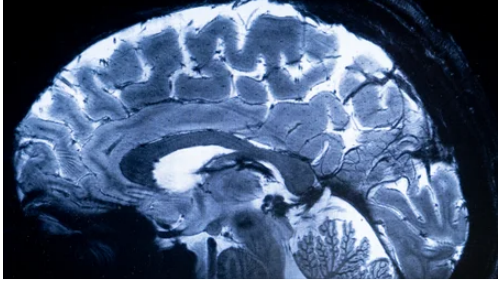
More by Manon Bischoff

QUANTUM PHYSICS | APRIL 8, 2025

Quantum Physics Is on the Wrong Track, Says Breakthrough Prize Winner Gerard 't Hooft

After netting the world's highest-paying science award, preeminent theoretical physicist Gerard 't Hooft reflects on his legacy and the future of physics

LEE BILLINGS



CONSCIOUSNESS | APRIL 4, 2025

Scientists Identify a Brain Structure That Filters Consciousness

Our conscious awareness may be governed by a structure deep in the brain

SMRITI MALLAPATY, NATURE MAGAZINE

EVOLUTION | JANUARY 13, 2021

Dire Wolves Were Not Really Wolves, New Genetic Clues Reveal

The extinct giant canids were a remarkable example of convergent evolution

RILEY BLACK

MATHEMATICS | APRIL 6, 2025

Dennis Gaitsgory, Who Proved Part of Math's Grand Unified Theory, Wins Breakthrough Prize

By solving part of the Langlands program, a mathematical proof that was long thought to be unachievable, Dennis Gaitsgory snags a prestigious Breakthrough Prize

MANON BISCHOFF

THE UNIVERSE | APRIL 4, 2025

How Many Rogue Planets Roam the Milky Way?

According to new simulations, many, even most, planets get ejected from their star early in their history

PHIL PLAIT

BIOTECH | APRIL 8, 2025

Did Scientists Actually De-Extinct the Dire Wolf?

Colossal Bioscience says it has "de-extincted" the dire wolf, but other scientists disagree and say more important conservation science is being lost in all the hype

ANDREA THOMPSON