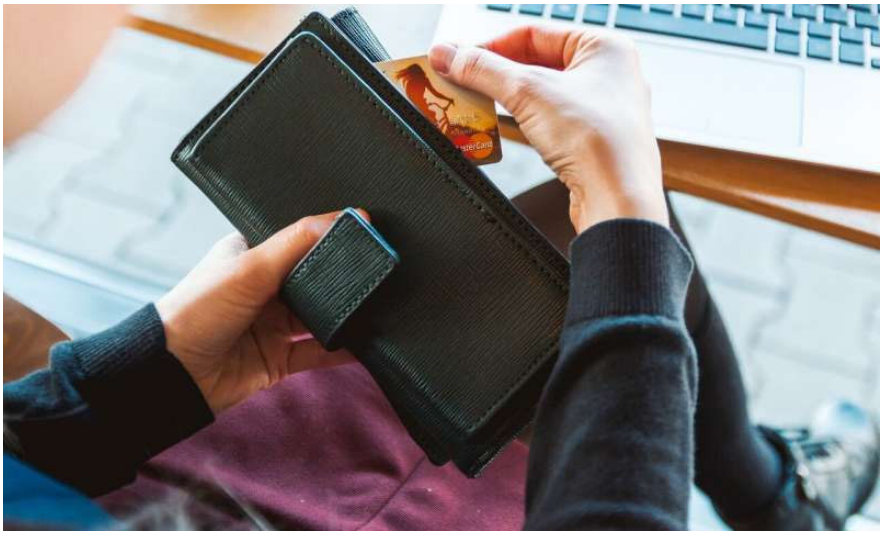
JULY 17, 2019

Researchers hail the demise of an online security algorithm

by University of Surrey



Credit: CC0 Public Domain

An international team of mathematicians has hailed the end of a variant of a code that is widely used to protect online transactions.

These algorithms, which stretch to hundreds of digits, are created to help protect banking details, but these can be broken if discrete logarithm problems can be solved. These are infamously difficult mathematical problems that should take trillions of years to solve, even with a state-of-the-art supercomputer. The numbers used need to be large enough to stop criminals, while being small enough for practical online usage.

Five researchers from the University of Surrey, Ecole Polytechnique Federale de Lausanne (EPFL), Switzerland, the University of Passau, Germany, and Centrum Wiskunde & Informatica (CWI), The Netherlands, have built on their previous record-breaking techniques to solve the problem in an object called a finite field, which has 2^{30750} elements. The 30750-bit number beats the previous record of 9234 bits set in 2014 by Robert Granger, Thorsten Kleinjung and Jens Zumbrägel.

After a flurry of theoretical breakthroughs, in 2014 the trio of Granger, Kleinjung and Zumbrägel broke an industry standard 128-bit secure system based on this problem and designed an even faster algorithm, which had not been tested until now. However, some cryptographers have proposed to continue using these "small characteristic" problem variants for large enough numbers, such as those of 16000 bits. The 30750-bit break, which took three years to run on various computer clusters—the equivalent of 2900 years on a desktop computer with a single core—demonstrates that such proposals are very unwise.

Dr. Robert Granger, Lecturer in Secure Systems at the University of Surrey, said: "This is a fantastic achievement for our team, proving that this once integral part of the cryptographic world should be consigned to history. However, there are also constructive applications of such fast algorithms, even in cryptography, so this is a win-win situation.

"Also, it happens that 30750 is the seating capacity of the AMEX, home of the mighty Seagulls —Brighton and Hove Albion Football Club. So if there were a full house and every fan tossed a coin, guessing the discrete logarithm would be as hard as correctly guessing every single coin toss."

Jens Zumbrägel, Professor in Mathematics and Cryptography at the University of Passau, added: "Large-scale computations like this help us to understand where the dangers lie and can lead to insights that can be applied in other scenarios, so they are fundamental for assessing the security of cryptography in use today."