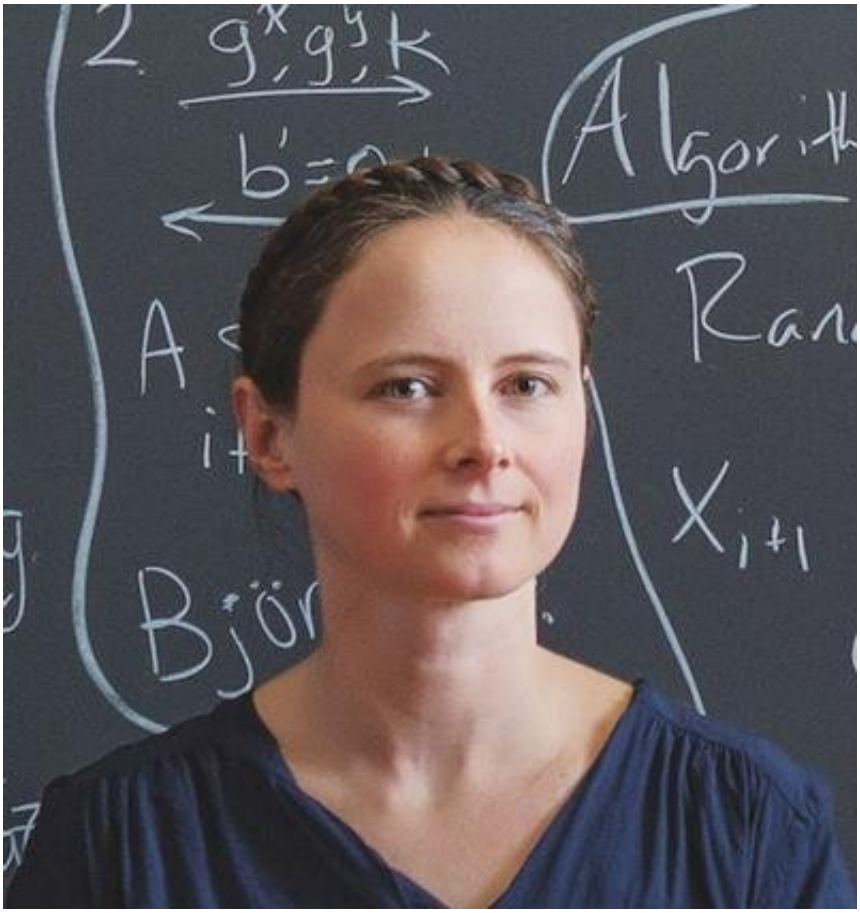
New record set for cryptographic challenge

March 12 2020, by Ioana Patringenaru



Nadia Heninger is a professor of computer science and engineering at the Jacobs School at UC San Diego. Credit: University of California - San Diego

An international team of computer scientists has set a new record for integer factorization, one of the most important computational problems underlying the security of nearly all public-key cryptography currently

used today.

Public-key cryptography is used for a number of applications including encrypting sensitive and confidential data and digital signatures. In public-key cryptography, keys that protect data come in pairs, one public, and one private. The security of the encryption or digital signature relies on the assumption that it's impossible to compute the private key from the public key.

One of the most commonly used public-key cryptographic algorithms for both encryption and digital signatures is the RSA cryptosystem, invented in 1977. It's named for its inventors Rivest, Shamir, and Adleman. Its security is based on the fact that it is believed to be difficult to factor large integers of a specific form.

To encourage research into integer factorization, the "RSA Factoring Challenges" were created in 1991. These challenges consisted of challenge integers of varying sizes, named for the number of integer digits.

The team of computer scientists from France and the United States set a new record by factoring the largest integer of this form to date, the RSA-250 cryptographic challenge. This integer is the product of two prime numbers, each with 125 decimal digits. In total, it took 2700 years of running powerful computer cores to carry out the computation, which was done on tens of thousands of machines around the world over the course of a few months.

The key broken with this record computation is smaller than keys that would typically be used in practice by modern cryptographic applications: it has 829 binary bits, where current practice dictates that RSA keys should be at least 2048 binary bits long. Researchers use these types of computations to choose key strength recommendations that will

remain secure for the foreseeable future.

"Achieving computational records regularly is necessary to update cryptographic security parameters and key size recommendations," said Nadia Heninger, a professor of computer science at the University of California San Diego, and a member of the research team.

The same team set the previous integer factoring record back in December 2019, when they factored the RSA-240 challenge, a 795-bit integer.

The researchers carried out this computation using CADO-NFS, which is free software developed by the team at INRIA Nancy. They used a number of computer clusters, including research group, university, and national research clusters in France, Germany, and UC San Diego.

Provided by University of California - San Diego

Citation: New record set for cryptographic challenge (2020, March 12) retrieved 27 April 2024 from https://phys.org/news/2020-03-cryptographic.html