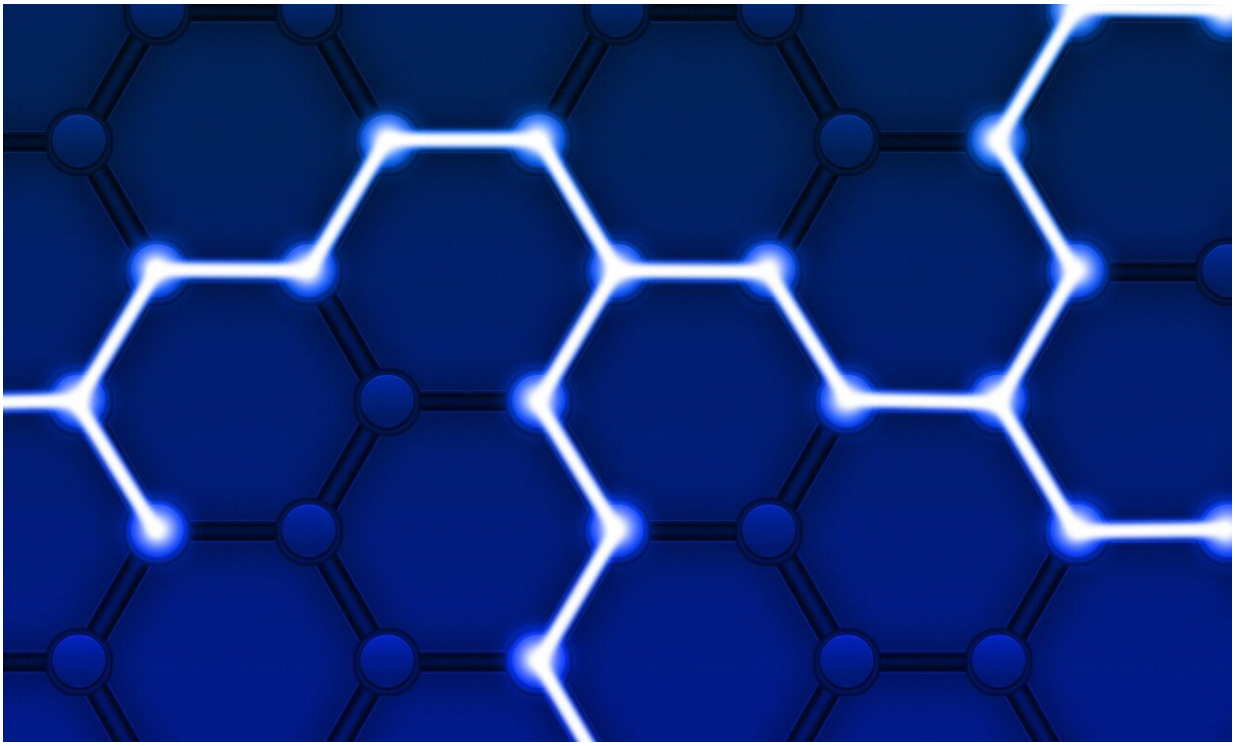
Randomness theory could hold key to internet security

July 28 2020, by Melanie Lefkowitz



Credit: Pixabay/CC0 Public Domain

Is there an unbreakable code?

The question has been central to cryptography for thousands of years, and lies at the heart of efforts to secure private information on the internet. In a new paper, Cornell Tech researchers identified a problem

that holds the key to whether all encryption can be broken—as well as a surprising connection to a mathematical concept that aims to define and measure randomness.

"Our result not only shows that cryptography has a natural 'mother' problem, it also shows a deep connection between two quite separate areas of mathematics and computer science—cryptography and algorithmic information theory," said Rafael Pass, professor of computer science at Cornell Tech.

Pass is co-author of "On One-Way Functions and Kolmogorov Complexity," which will be presented at the IEEE Symposium on Foundations of Computer Science, to be held Nov. 16-19 in Durham, North Carolina.

"The result," he said, "is that a natural computational problem introduced in the 1960s in the Soviet Union characterizes the feasibility of basic cryptography—private-key encryption, digital signatures and authentication, for example."

For millennia, cryptography was considered a cycle: Someone invented a code, the code was effective until someone eventually broke it, and the code became ineffective. In the 1970s, researchers seeking a better theory of cryptography introduced the concept of the one-way function—an easy task or problem in one direction that is impossible in the other.

For example, it's easy to light a match, but impossible to return a burning match to its unlit state without rearranging its atoms—an immensely difficult task.

"The idea was, if we have such a one-way function, maybe that's a very good starting point for understanding cryptography," Pass said.

"Encrypting the message is very easy. And if you have the key, you can also decrypt it. But someone who doesn't know the key should have to do the same thing as restoring a lit match."

But researchers have not been able to prove the existence of a one-way function. The most well-known candidate—which is also the basis of the most commonly used encryption schemes on the internet—relies on integer factorization. It's easy to multiply two random prime numbers—for instance, 23 and 47—but significantly harder to find those two factors if only given their product, 1,081.

It is believed that no efficient factoring algorithm exists for large numbers, Pass said, though researchers may not have found the right algorithms yet.

"The central question we're addressing is: Does it exist? Is there some natural problem that characterizes the existence of one-way functions?" he said. "If it does, that's the mother of all problems, and if you have a way to solve that problem, you can break all purported one-way functions. And if you don't know how to solve that problem, you can actually get secure cryptography."

Meanwhile, mathematicians in the 1960s identified what's known as Kolmogorov Complexity, which refers to quantifying the amount of randomness or pattern of a string of numbers. The Kolmogorov Complexity of a string of numbers is defined as the length of the shortest computer program that can generate the string; for some strings, such as 12121212121212121212121212121212, there is a short program that generates it—alternate 1s and 2s. But for more complicated and apparently random strings of numbers, such as 37539017332840393452954329, there may not exist a program that is shorter than the length of the string itself.

The problem has long interested mathematicians and computer scientists, including Juris Hartmanis, professor emeritus of computer science and engineering. Because the computer program attempting to generate the number could take millions or even billions of years, researchers in the Soviet Union in the 1960s, as well as Hartmanis and others in the 1980s, developed the time-bounded Kolmogorov Complexity—the length of the shortest program that can output a string of numbers in a certain amount of time.

In the paper, Pass and doctoral student Yanyi Liu showed that if computing time-bounded Kolmogorov Complexity is hard, then one-way functions exist.

Although their finding is theoretical, it has potential implications across cryptography, including internet security.

"If you can come up with an algorithm to solve the time-bounded Kolmogorov complexity problem, then you can break all crypto, all encryption schemes, all digital signatures," Pass said. "However, if no efficient algorithm exists to solve this problem, you can get a one-way function, and therefore you can get secure encryption and digital signatures and so forth."

More information: eprint.iacr.org/2020/423.pdf

Provided by Cornell University