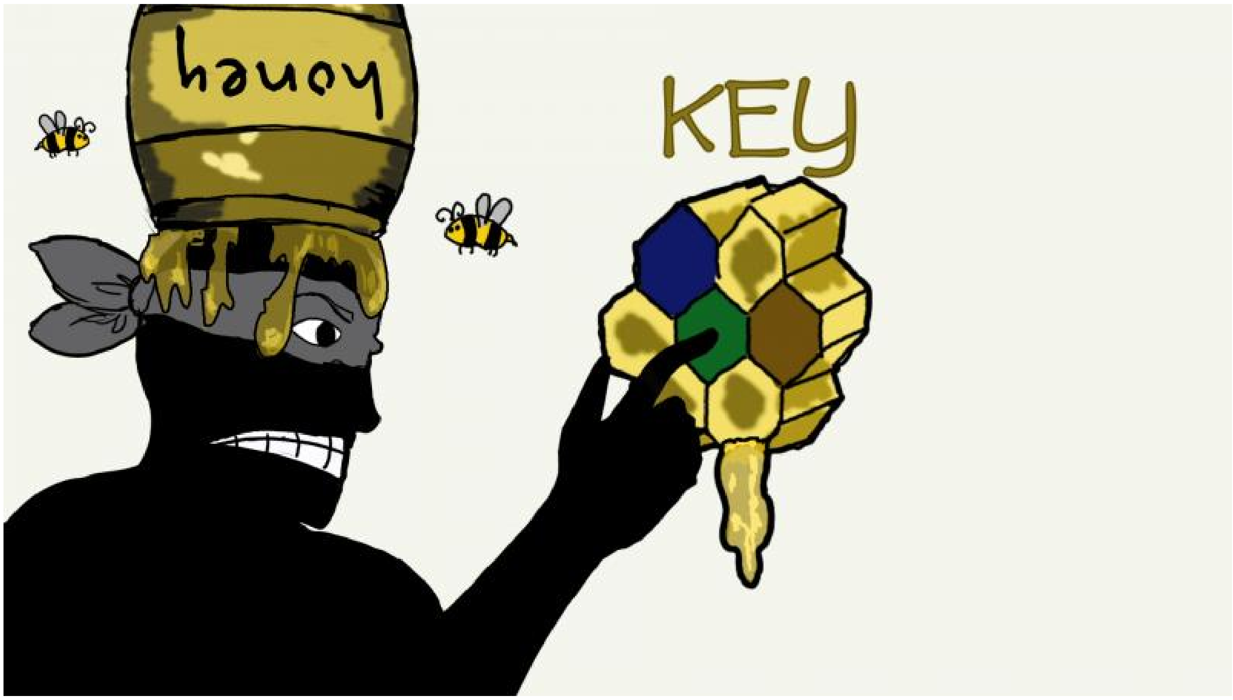
The future of encryption

October 23 2015, by Amina Khan



"Honey encryption" describes a method where wrong guesses of a key produce information that looks accurate but isn't. Credit: Amina Khan, NSF

If you want to protect valuable information, wouldn't you keep it under lock and key?

Today, modern encryption uses "keys" to keep data on our computers, mobile devices, and communication networks safe. Encryption converts data into digital gibberish, which prevents it from being used maliciously. The data then needs to be decrypted to be processed by a computer or mobile device. To do so, the recipient of the message needs the right keys.

But even encrypted data can sometimes be intercepted and accessed. So how can we keep our data safe?

Fully homomorphic encryption

In 2010, Craig Gentry, a graduate student supported by the National Science Foundation, thought of a new way to protect data. He called it fully homomorphic encryption: a way to process data without ever decrypting it.

To explain this concept, he invented an imaginary character named Alice who owns a jewelry store. Alice doesn't trust her workers with her expensive gems, so she gets an impenetrable box for which only she has the key.

When Alice wants her employees to make a new piece of jewelry, she locks the materials inside the box and hands it off to her workers. Using special gloves, employees can work on the gems inside the box, but can't get them out. Once the work is done, Alice opens the box with her key and takes out the finished jewelry. In this way, her workers process raw materials into jewelry without ever truly having access to the materials themselves.

In 2010, Craig Gentry, a graduate student supported by the National Science Foundation, thought of a new way to protect data. He called it fully homomorphic encryption: a way to process data without ever decrypting it. Credit: Amina Khan, NSF

Fully homomorphic encryption basically does the same thing. As data and computation move to the cloud, fully homomorphic encryption would allow your data to be processed without ever having to give away access to it. For instance, a web application could process your tax return using encrypted financial information without actually seeing any of it.

Cryptographers, including Gentry, are still figuring out how to turn the idea of homomorphic encryption into a practical reality.

Other new approaches to cryptography

Fully homomorphic encryption isn't the only forward-looking cryptographic protocol that researchers are exploring. Another promising approach is "honey encryption"—where wrong guesses of the key produce information that looks accurate but isn't. A second approach is "functional encryption"—where restricted secret keys enable a key holder to learn about only a specific function of encrypted data and nothing else. In a third approach, called "quantum key encryption," the quantum nature of atoms protects the data. All are active areas of study the National Science Foundation supports.

The goal of all of this research is that one day, it will be possible to ensure security of important information wherever it might be—on our computers, mobile devices and even in the cloud.

More information: Functional Encryption: Definitions and Challenges. *Theory of Cryptography*, DOI: 10.1007/978-3-642-19571-6_16

A Fully Homomorphic Encryption Scheme. crypto.stanford.edu/craig/craig-thesis.pdf

Provided by National Science Foundation

Citation: The future of encryption (2015, October 23) retrieved 10 April 2024 from https://phys.org/news/2015-10-future-encryption.html