TechXplore

How encryption holds our digital society together

January 12 2023, by Sole Bugge Møller

DTU has one of only around 300 remaining copies of the German encryption machine, Enigma. Credit: Thomas Steen Sørensen

Encryption is like the steel skeleton of a building: invisible, but holding everything together. In our digital age, encryption is an absolutely essential element and even if you think that you do not have any skeletons in the closet, there is good reason to keep your data secret.

"We all have something to hide and there is a good reason to. Because information is valuable, so it's important that we have the opportunity to decide for ourselves who can see the information we own. Encryption helps us with this," says Assistant Professor Tyge Tiessen from DTU Compute.

You usually say that if you do not encrypt your communication, it's equivalent to sending an open postcard, where everyone involved in handling the message can read it. In turn, if you encrypt your message, it's like a sealed envelope that only the recipient can read after opening it.

"Large parts of our communication system are based on the ability to encrypt, so, without it, we would be thrown back to the digital Middle Ages," says Tyge Tiessen.

You would have to pay with cash everywhere, physically visit Citizen Service to change your address, not be able to shop at Nemlig.com or other online stores, and unauthorized persons would easily be able to read your emails. In short, our entire digital everyday life would slowly crumble.

Electromechanical encryption

Today, most encryption is done digitally with lots of zeros and ones, but encryption was more difficult in the past. The most well-known encryption machine in history is probably the Enigma, which the Germans used to send secret messages during World War II, and it encrypted by electromechanically changing each letter typed on the machine into another letter. It is believed that there are only around 300 copies of the Enigma machine left in the world, and DTU has one of them.

The Enigma used rotors that rotated when one of the machine's keys was pressed and, through an electrical circuit, changed the letter to another, which then lit up on the Enigma machine. By knowing the start settings of the rotors, the recipient could easily decipher the message.

"The Enigma was not a unique way of encrypting, there were other similar encryption devices, but the way it was broken has been of great importance to us," says Tyge Tiessen.

The British team led by Alan Turing, who cracked the Enigma, developed a specific machine called The Bombe that automated the code-breaking, which enabled the Brits to decipher virtually all of Germany's encrypted messages towards the end of World War II. It is believed that it shortened World War II by up to two years and saved millions of lives, and Turing's work laid the foundation for the modern computer.

"It gave us a completely different understanding of how to attack encryption," says Christian Majenz, assistant professor of cryptology at DTU Compute.

"Modern cryptology is both easier and more complicated. It is much more difficult to crack than the Enigma but at the same time very easy to implement in computers."

Many non-military enemies today

Where encryption was previously primarily used by the military, it today reaches all corners of society, and this poses challenges.

"There are many more enemies today because we use cryptography in multiple contexts. The enemy may be your neighbor, who has found out that your network is not secure and then hacks it to discover what you're doing," says Tyge Tiessen.

Therefore, everyone from private companies to public authorities, banks, utility companies, and private individuals need encryption as a bulwark against hackers. And perhaps even against intelligence services—as whistleblower Edward Snowden's revelations have shown, even law-abiding citizens risk being monitored, and communications services have therefore started using encryption which is virtually impossible to monitor.

Quantum computers change everything

In the future, however, all our encryption may be broken once we have quantum computers that can solve complicated problems where even the fastest supercomputers fail. It is a ticking bomb under our digital society.

"This is the period of transition to quantum-proof encryption," says Assistant Professor Christian Majenz, who conducts research into precisely quantum encryption at DTU Compute.

"We're trying to develop cryptography before the arrival of quantum computers, because otherwise they can be used to access all our existing data. But once we have found quantum-proof algorithms, it's a bit like a Lego brick that you can build on."

Provided by Technical University of Denmark

Citation: How encryption holds our digital society together (2023, January 12) retrieved 4 May 2024 from https://techxplore.com/news/2023-01-encryption-digital-society.html