A forgotten coding puzzle has a decoded 20-year life span

According to estimates by Ron Rivest, who created the puzzle, to calculate the answer people will need to take about 35 years.

In early April 1999, the famous architect Frank Gehry was designing a building that would later become the "capital" of MIT's Artificial Intelligence and Computer Science Laboratory (abbreviated). is CSAIL), received a "time capsule" with instructions to integrate it into his designs.

Basically, this "Time Capsule" is a museum of the early history of computers, containing 50 memorabilia contributed by people who have contributed greatly to the development of computer technology such as Bill Gates and Tim Berners-Lee.

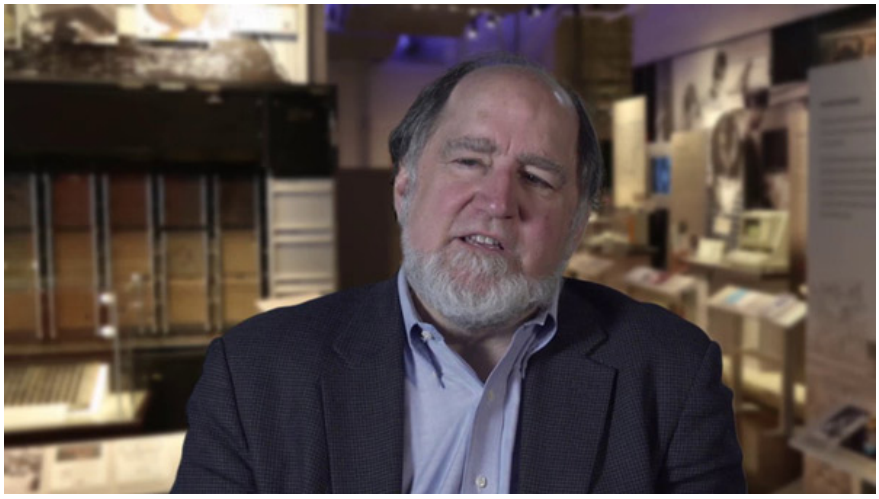
This "time capsule" is locked with an encrypted puzzle in the Java language designed by Ron Rivest. If you don't know, Ron Rivest is the one who gets the name for the "R" in RSA - one of the most important encryption protocols ever created. According to Ron Rivest's estimate, to calculate the answer to this coding puzzle, people will need about 35 years.

On April 15 last, after nearly 20 years of Rivest published the puzzle, Bernard Fabrot a self-taught Belgian programmer found the answer. The initial instruction of the puzzle states that the solution must be sent to the director of the Computer Science Laboratory. But in 2003, that lab was imported into MIT's AI lab to create CSAIL. Therefore, Fabrot contacted Daniela Rus, CSAIL's director, but she did not even know the existence of the puzzle.

Basically, the Rivest puzzle revolves around finding the number obtained from performing squared calculations nearly 80 trillion times, then using it to run a mathematical equation. The results of the equation are translated into a congratulatory phrase. The exact phrase will be announced by Rivest and Fabrot on May 15, when the "time capsule" is opened.

To solve this puzzle, you need to perform a series of sequential calculations sequentially. That means having the results of the previous calculation, then using it to perform the next calculation, cannot use parallel computing to find a faster answer. Even supercomputers can't solve the problem.

Based on the amount of time it takes to run squared calculations in 1999 and Moore's Law, Rivest estimates that it takes about 35 years to calculate the answer to your riddle.



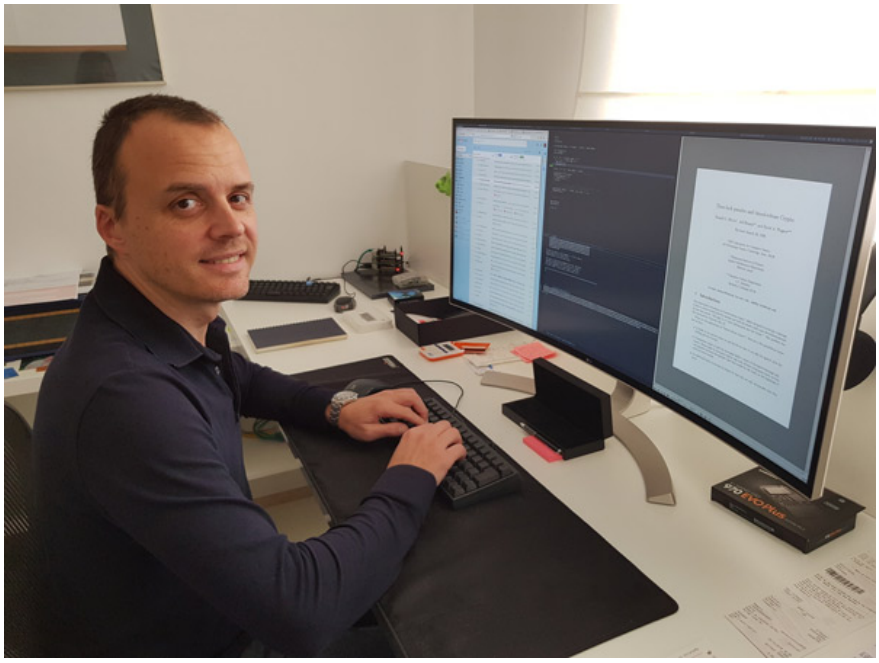
Ron Rivest, creator of coding puzzles.

In 2015, Fabrot, now an independent developer, accidentally met this puzzle. Although the puzzle is encoded in the Java language, Fabrot realized that using GNU Multiple Precision Arithmetic Library, a free software dedicated to performing precise arithmetic operations written in C language, would can solve faster.

To solve the puzzle, Fabrot dedicated a CPU core on his desktop to run squared calculations. Fabrot's computer runs calculations 24/7, and only breaks when he travels or loses power.

Fabrot said, in addition to his very close friends, he never told anyone about trying to solve the puzzle because he was afraid that others might use a more powerful CPU to overcome him.

Eventually Fabrot also completed more than 80 trillion squared calculations and found the answer to Rivest's puzzle after 3.5 years.



Bernard Fabrot.
However, there is a group of computer scientists and encryption experts, led by former Intel engineer Simon Peffers, who is also working on a project called Cryptophage. They also use specialized hardware designed specifically for decoding that MIT puzzle.

Fabrot is completely unaware of this.

The Cryptophage team is studying verifiable delay functions, a more modern form of Rivest's stalled time-delay encryption method, to provide security mechanisms for blockchain such as Ethereum. During the study, they met the puzzle of Rivest and used it to test their research.

In mid-March, the group started running an algorithm designed to reduce the delay between squared calculations, on an FPGA multi-function chip. The chip is programmed to run a single specific algorithm, which is 10 times more efficient than a high-end commercial CPU running unoptimized software.

As a result, the Cryptophage team calculated that it would take only 2 months for them to have an accurate answer to the puzzle of MIT, on the evening of May 10 But when they contacted MIT to announce that the results were coming, knowing that Fabrot was one step ahead!

Rivest said, he was surprised when both of them appeared on the same day to announce that they had solved their riddle. Rivest also admitted that he overestimated the difficulty of the puzzle, he did not expect the emergence of technological breakthroughs such as FPGA chips.

The "time capsule" opening ceremony will be held on May 15, the Cryptophage group will also be present even though they are not the first to solve the puzzle.

In 'capsules' contains contributions from Tim Berners-Lee, inventor of the World Wide Web; Bill Gates, who contributed the original version of Altair BASIC, Microsoft's first product, Bob Metcalfe, who invented ethernet. But only those who designed it know what the content is all about.

Fabrot said he was excited to wait until the 'capsule' was opened to see an original copy of Zork, one of the first PC games, which was stored in it.