# Rivest unlocks cryptography's past, looks toward future

February 15 2011, by David L. Chandler


The most widely used cryptographic system today may eventually be vulnerable, said computer science professor Ronald Rivest -- one of the system's primary creators -- but even if it fails, new systems are already waiting to be deployed.

Rivest, the Andrew and Erna Viterbi Professor of Computer Science, reviewed the history of code-making and code-breaking through the ages — the field known as cryptography — and made some predictions about the field's future during MIT's prestigious Killian Faculty Achievement Award Lecture, held on Tuesday, Feb. 8.

The cryptographic system currently used for the vast majority of all

financial transactions and secure communications over the Internet was developed in 1977 by Rivest and two of his colleagues — professors Adi Shamir and Len Adleman of MIT's mathematics department — and is known by their initials: RSA. The system depends on the fact that it is extremely difficult and time consuming to determine the prime factors of a large number (the prime numbers that can be multiplied together to produce the given number).

But Rivest said that it has not been shown mathematically that such factorization into primes is necessarily difficult. "Factoring could turn out to be easy," Rivest said. So it remains possible, he told the audience, that "maybe someone here will find the method" that renders the RSA encryption system vulnerable, in which case companies would be forced to switch quickly to some other encryption system. Fortunately, he said, a variety of alternative schemes have been developed in the decades since RSA was published, and a new system could probably be adopted quickly.

RSA is an example of a "public key" code system, in which one key is used to encrypt a message, and another key is used to decrypt an encrypted text. One of those keys is publicly known, but it nevertheless is extremely difficult to discover the other key. The concept of public-key codes was developed and published by researchers at Stanford in 1976, who declared that "we are at the brink of a revolution in cryptography." However, Rivest said, "they didn't know how to implement them at all." Rivest and his colleagues were the first to translate the concept into a practical, workable system, and they founded a company in 1982, RSA Data Security, to commercialize it. The company was ultimately sold to EMC Corp.

At the time, there was little interest or active research on factoring, Rivest said. But when they came up with their encryption system, Martin Gardner wrote a column about it in Scientific American and offered a

challenge: a $100 reward for the first person to find the prime factors of a 129-digit number he published. Rivest at the time estimated that the puzzle would take 40 quadrillion years to solve. That proved to be a bit of an overestimate, he acknowledged: It was solved 17 years later, in a group effort involving 8 months of work by 600 volunteers — and Rivest cheerfully paid up the $100.

While early codes go back at least as far as the ancient civilizations of Egypt and Greece — one early version used a strip of paper that had to be wound around a stick of a specific diameter in order for the letters to line up so a message could be read — it is advances in technology that have provided the impetus for more advanced code systems, Rivest said. For example, it was the spread of radio in the 20th century that made new codes imperative, and mechanical coding and decoding devices became a key factor on both sides during World War II. Then, with the creation of the World Wide Web in the 1990s, the need for stronger and easier-to-implement codes became significant.

For example, one spinoff of technology related to the RSA system is the digital certificate company VeriSign, which uses digital signatures, a concept also developed by some of the same researchers, to authenticate the identity of websites. The company now provides 1.3 billion certificate authentications every day, he said.

In theory, a newer technology could render RSA useless, Rivest said. A large quantum computer — if one is ever built — could theoretically factor numbers quickly enough to defeat the code. On the other hand, he said, there's not likely to be any motivation for building such a complex device, since it might have no other real purpose than defeating RSA — and once it was in existence, everyone would stop using RSA, so "there would be no use for it anymore."

In the meantime, the whole field of cryptography has really taken off,

with real or potential applications in such areas as the creation of a secure micropayment system, although such a system developed by Rivest in 2001, called Peppercoin, never got off the ground. Another possible application is secure voting, such as a system that allows a voter to confirm online that his or her vote was correctly tallied, without allowing anyone else to determine which candidate was voted for.

Ironically, Rivest said, the development of such a secure, verifiable cryptographic system for voting verification "actually increases transparency and verifiability," by allowing individual voters to check their own votes, while also providing a paper trail for possible recounts. Developing a secure voting system that meets all the different requirements for such a system — including allowing voters to verify their votes, but without making it possible for them to sell their votes, and while achieving a high degree of usability — remains a tough technical challenge. "We'll get there," he said, "but there's work to be done."

As an area of research, Rivest said, cryptography remains an active and fascinating area, one that brings together disciplines as varied as mathematics, statistics, theoretical computer science, electronic engineering and even psychology. "It's like the Middle East of research," he said, "because everything goes through it."

---



Provided by Massachusetts Institute of Technology