

## **Ron Rivest (MIT)**

Professor Rivest is the Viterbi Professor of Computer Science in MIT's Department of Electrical Engineering and Computer Science. He is a member of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL), a member of the lab's Theory of Computation Group and is a leader of its Cryptography and Information Security Group.

He received a B.A. in Mathematics from Yale University in 1969, and a Ph.D. in Computer Science from Stanford University in 1974.

Professor Rivest has research interests in cryptography, computer and network security, voting systems, and algorithms.

Professor Rivest is a co-inventor of the RSA public-key cryptosystem. He has extensive experience in cryptographic design and cryptanalysis, and has published numerous papers in these areas. He has served as a Director of the International Association for Cryptologic Research, the organizing body for the Eurocrypt and Crypto conferences, and as a Director of the Financial Cryptography Association. He is also a founder of RSA Data Security and of Verisign.

Professor Rivest is a member of the National Academy of Engineering and of the National Academy of Sciences, and is a Fellow of the Association for Computing Machinery, the International Association for Cryptographic Research, and the American Academy of Arts and Sciences.

He is also on the Advisory Board for the Electronic Privacy Information Center.

Professor Rivest has won numerous awards. Together with Adi Shamir and Len Adleman, he has been awarded the 2000 IEEE Koji Kobayashi Computers and Communications Award and the Secure Computing Lifetime Achievement Award. He is a recipient of the Marconi Award, and has also received, together with Shamir and Adleman, the 2002 ACM Turing Award and the 2009 NEC C&C Award.

Most recently, Professor Rivest has served on the U.S. Technical Guidelines Development Committee, which has drafted proposed standards for certifying voting system in the U.S.