Cryptographic Hash Workshop
October 31 – November 1, 2005

Ronald L. Rivest, *MIT EECS Dept*
rivest@mit.edu

BIOGRAPHY:

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, and Head of its Center for Information Security and Privacy.

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, and algorithms. Professor Rivest is an inventor, with Adi Shamir and Len Adleman of the RSA public-key cryptosystem, and a co-founder of RSA Data Security. Together with Shamir and Adleman, he received the 2002 ACM Turing Award, perhaps the most prestigious award in Computer Science. He has extensive experience in cryptographic design and cryptanalysis, and is the designer of the hash functions MD4 and MD5. He has served as a Director of the International Association for Cryptologic Research.

Professor Rivest is a member of the National Academy of Engineering, 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.