Cryptographic Hash Workshop
October 31 – November 1, 2005

Arjen K. Lenstra, *Lucent Technologies Bell Laboratories and Technische Universiteit Eindhoven*
akl@lucent.com

BIOGRAPHY:

Arjen K. Lenstra is Distinguished Member of Technical Staff at Bell Laboratories, Lucent Technologies. Before joining Bell Labs in 2004 he was Vice President at Citibank's Information Security Office, Citibank, New York, Senior Scientist at Bellcore, Visiting Professor at The University of Chicago and he held visiting positions at IBM Thomas J. Watson Research Center, AT&T Bell Labs, and DEC Systems Research Center. Furthermore, since May 2000, he is professor of cryptology at the Technical University Eindhoven, The Netherlands. His main research interest is cryptanalysis of public key cryptosystems, in particular the RSA cryptosystem. Lenstra wrote the software that was used to break the famous 1977 Scientific American RSA challenge, and he was involved in the first successful attack on a 512-bit RSA modulus in 1999. He is co-inventor of the public key cryptosystem XTR. He received his PhD from the University of Amsterdam, The Netherlands.