Cryptographic Hash Workshop
October 31 – November 1, 2005

John Kelsey, *NIST*
john.kelsey@nist.gov

BIOGRAPHY: John Kelsey is a cryptographer at NIST with research interests in cryptanalysis and design of symmetric crypto primitives (block and stream ciphers, hash functions), random number generation, electronic voting, chaining modes, key derivation functions, side-channel attacks, and cryptographic protocols. Before working at NIST, Mr. Kelsey worked at Certicom and Counterpane Internet Security. He is one of the designers of the Twofish encryption algorithm, the Helix authenticating stream cipher, and the Yarrow and Yarrow-160 cryptographic random number generators.