

UCD Computer Science Seminar

November 20, 11:00 am

SO 126

Demise of MD5 and SHA-1 Designing the New Hash

Stanislaw P. Radziszowski
Department of Computer Science
Rochester Institute of Technology
spr@cs.rit.edu

ABSTRACT

A hash function $H: \{0,1\}^* \rightarrow \{0,1\}^m$ produces an m -bit digest of an arbitrary message, file, or even an entire file system. Typically, one wants hash functions to be easy to compute, but also infeasible to invert or to find collisions (pairs of inputs which hash to the same value). Hash functions are fundamental cryptographic primitives, and they are used extensively in authentication, preserving data integrity, digital signatures, and many other security applications. The two most widely used hash functions are MD5 (Message Digest, $m=128$) and SHA-1 (Secure Hash Algorithm, $m=160$), the latter supported by the US government as a standard [FIPS-180-2](#). The collisions for MD5 were found three years ago, and by now they can be produced quickly by software available on the Net. The SHA-1 algorithm seems also to be in trouble (and other algorithms in the SHA family, with $m=256, 384, 512$, might follow). No collisions for SHA-1 have been found so far, but attacks much better than the simple birthday attack approach have been designed. Breaking SHA-1 soon is a likely possibility.

On January 23, 2007, NIST (National Institute of Standards and Technology) [announced an initiative](#) to design a new hash for this century, to be called AHS (Advanced Hash Standard). The competition will be open and it is planned to conclude in 2012. These developments are quite similar to the recent history of symmetric block ciphers - breaking of the DES (Data Encryption Standard) and an emergence of the AES (Advanced Encryption Standard) in 2001 as the winner of a multiyear NIST competition.

This talk will outline the attacks on MD5 and SHA-1 and overview a likely scenario of what the teams submitting new designs for the AHS will consider.