NIST Brief Comments
on
Recent Cryptanalytic Attacks on Secure Hashing Functions
and
the Continued Security Provided by SHA-1

Cryptographic hash functions that compute a fixed size message digest from arbitrary size messages are widely used for many purposes in cryptography, including digital signatures. At the recent Crypto2004 conference, researchers announced that they had discovered a way to "break" a number of hash algorithms, including MD4, MD5, HAVAL-128, RIPEMD and the long superseded Federal Standard SHA-0 algorithm. The current Federal Information Processing Standard SHA-1 algorithm, which has been in effect since it replaced SHA-0 in 1994, was also analyzed, and a weakened variant was broken, but the full SHA-1 function was not broken and no collisions were found in SHA-1. The results presented so far on SHA-1 do not call its security into question. However, due to advances in technology, NIST plans to phase out of SHA-1 in favor of the larger and stronger hash functions (SHA-224, SHA-256, SHA-384 and SHA-512) by 2010. SHA-1 and the larger hash functions are specified in FIPS 180-2. For planning purposes by Federal agencies and others, note also that the use of other cryptographic algorithms of similar strength to SHA-1 will also be phased out in 2010.

SHA-1 and the stronger hash functions in FIPS 180-2 are all NIST approved. NIST encourages the implementers of the FIPS 180-2 hash algorithms to have the correctness of their implementations validated though the Cryptographic Module Validation Program; such validation is required for Federal use.

NIST applauds the recent analysis and encourages more published research into hash functions and their resistance to attack, particularly for newer algorithms such as SHA-256 and SHA-512. Such analysis helps us continue to gain assurance in the security of the algorithms we use.

8-25-2004