The MD4 Message Digest Algorithm

Burton S. Kaliski Jr.
RSA Data Security Inc.
Redwood City, CA

Abstract. *MD4 is a new, fast message digest algorithm. It inputs a message of any length and outputs a digest of 128 bits. It is conjectured that it is computationally infeasible to find two messages with the same digest or a message with a prespecified digest. MD4 processes 1.45M bytes/s on a SUN Sparc station, 70K bytes/s on a DEC MicroVax II, and 32K bytes/s on a 20MHz 80286. MD4 is also quite compact. MD4 is being placed in the public domain for review and possible adoption as a standard.*

Details of the MD4 message digest algorithm will be presented by Ronald L. Rivest at CRYPTO '90 and will appear in the proceedings of that conference.

I.B. Damgard (Ed.): Advances in Cryptology - EUROCRYPT '90, LNCS 473, p. 492, 1991.