

Re: How about MD5(NewHash(DATA))?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-10/1400.html>

From: Tom St Denis (*tomstdenis_at_iahu.ca*)

Date: 10/31/04

Date: Sun, 31 Oct 2004 06:26:19 -0500

JiXian Yang wrote:

- > *IF MD5(MD5(DATA)) is not stronger than MD5(DATA)*↯
- > *suppose there is a new hash algorithm NewHash(DATA) stronger than MD5(DATA).*
- > *How about MD5(NewHash(DATA))?*

Why does this question come up every 6 months.

Why would you think MD5 o MD5 would be stronger than MD5 [supposedly against finding collisions, though you could have meant against inversion]

Tom