

Re: This Week's Finds in Mathematical Physics (Week 226)

Source: <http://sci.tech-archive.net/Archive/sci.physics.research/2006-02/msg00197.html>

- *From:* baez@xxxxxxxxxxxxxxxx (John Baez)
 - *Date:* Mon, 13 Feb 2006 22:36:01 +0000 (UTC)
-

In article <Pine.LNX.4.61.0602102025360.19201@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>, <tessel@xxxxxx> wrote:

On Sat, 11 Feb 2006, John Baez mentioned that md5sum was "broken" about a year ago. I just wanted to add:

1. If I am not mistaken, sha-1 and md5sum are different algorithms (IIRC, both are known to be insecure).

Yeah, I said SHA-1 and MD5 are different, and I said they were both vulnerable to collision attacks. MD5 is very vulnerable in practice, while the vulnerability of SHA-1 is still theoretical: you'd have to have big computers or lots of time or another clever idea to exploit it. (Guess who's likely to have all three!)

I gave this reference for MD5:

Magnus Daum and Stefan Lucks, Attacking hash functions by poisoned messages: "The Story of Alice and Her Boss", <http://www.cits.rub.de/MD5Collisions/>

and this one for SHA-1:

SHA hash functions, Wikipedia, http://en.wikipedia.org/wiki/SHA_hash_functions

The latter has some good links, including this nice review:

Arjen K. Lenstra, Further progress in hashing cryptanalysis, February 26, 2005, <http://cm.bell-labs.com/who/akl/hash.pdf>

For more on cryptographic hash functions and their woes, try these:

Re: This Week's Finds in Mathematical Physics (Week 226)

9) Cryptographic hash function, Wikipedia,
http://en.wikipedia.org/wiki/Cryptographic_hash

Of course, bear in mind that anyone can edit, blah, blah (including unregistered users, contrary to widely publicized news reports based upon a fundamental misunderstanding).

Yes, I could have tried to give references to dated versions of Wikipedia articles, so I could be sure they're good... but I'm an optimist.