

## Re: MD5 Implemented in JavaScript 1.3

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2002-11/0688.html>

---

**From:** Jim Ley ([jim@jibbering.com](mailto:jim@jibbering.com))

**Date:** 11/28/02

From: [jim@jibbering.com](mailto:jim@jibbering.com) (Jim Ley)

Date: Thu, 28 Nov 2002 10:28:25 GMT

On Wed, 27 Nov 2002 22:17:54 GMT, Grant Wagner

<[gwagner@agricoreunited.com](mailto:gwagner@agricoreunited.com)> wrote:

>*There may be uses for an MD5 implementation in client-side JavaScript, but  
>securing login passwords isn't one of them.*

And of course <http://pajhome.org.uk/crypt/md5/> has had them for ages, and Paul Johnston has established a reputation, I'd certainly not choose someone who doesn't even understand the need to post to on-topic groups, and not to quite so wildly crosspost (left in in case anyone wants an MD5 implementation, use the above one, the author understands the limitations. SHA1 is also available.

Jim.

--

comp.lang.javascript FAQ - <http://jibbering.com/faq/>