

sci.crypt: Re: LibTomCrypt [v0.83] and LibTomMath [v0.16] release

Re: LibTomCrypt [v0.83] and LibTomMath [v0.16] release

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-03/2321.html>

From: mklooptbd (mklooptbd@yahoo.com)

Date: 03/31/03

From: mklooptbd@yahoo.com (mklooptbd)

Date: 31 Mar 2003 05:39:52 -0800

Hey Tom, it's a bit OT for this thread but since you were bug fixing... I found a bug in your sha256 implementation. It's something to do with overflows, for example try hashing 2^{29} 'a's and comparing the result to the test vector.

Cheers.