

Point taken (Was Re: ADVERT: Secure communications)

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-10/msg00862.html>

- *From:* "Peter S. May" <psmay@xxxxxxxxxxxxx>
 - *Date:* Fri, 27 Oct 2006 16:40:54 -0400
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

David Wagner wrote:

Peter S. May wrote:

sci.crypt readers: I would like to request, on Robin Carey's behalf, comment by experienced cryptanalysts on the L15 algorithm.

Not a chance! Why would I spend my time analyzing an algorithm designed by someone who doesn't seem to understand the most basic tenets of cryptosystem design and evaluation? What would be the point? How much are you paying? What do I get out of it?

It's a total waste of time. Based on what I've seen, I would never entrust important data to Caesarion/Leopard/L15/whatever the thing-a-ma-jig is called these days.

Schneier's essay on amateur cipher designers makes the point pretty well.

....yeah, I really should have known not to respond to that post. I don't like discouraging people with a genuine interest just because the way it's already done is way better, since if anyone had done that with me I might have run away from the subject. It takes more pragmatism than some can muster to admit that most of the good work in cryptography has already been done, most of the rest is the subject of high-budget research, and what's left to be done has very little to do with the technology itself but instead with packaging the extant primitives in a way that isn't flawed and is easy enough for the end user to swallow. For me, that level of pragmatism came around high school graduation, but for some it comes later. :-)

Anyway, I wouldn't have bothered if I'd known this were a repeat offense. Sorry.

Point taken (Was Re: ADVERT: Secure communications)

PSM

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.2.2 (GNU/Linux)

Comment: Using GnuPG with Mozilla – <http://enigmail.mozdev.org>

iD8DBQFFQm7Qei6R+3iF2vwRAsEEAJ9n+TwcViEPpFPFkqgW1sEAgkTF/gCeJfaV

coEJLU1PsrWs74a2AoT0X08=

=t2y1

-----END PGP SIGNATURE-----

.