

## Re: ADVERT: Secure communications

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-10/msg00865.html>

---

- *From:* [daw@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:daw@xxxxxxxxxxxxxxxxxxxxxxxxxxxx) (David Wagner)
  - *Date:* Fri, 27 Oct 2006 20:21:19 +0000 (UTC)
- 

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.

.