

Re: Thank you all for the constructive comments

# Re: Thank you all for the constructive comments

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-01/msg00164.html>

---

- *From:* [tomstdenis@xxxxxxxx](mailto:tomstdenis@xxxxxxxx)
  - *Date:* 4 Jan 2007 05:08:42 -0800
- 

Peter van Liesdonk wrote:

This is not meant directly to you, but in a more general way: I think it is fair to expect people know steps B–Y when they want to reach Z. Otherwise you should not aim at Z, but at C.

Personally I wouldn't aspire to obtain some pre-defined goal known as Z. Maybe Z' or something other. Who wants to aspire to achieve what others have already achieved as their final goal?

It sounds silly to say it about your own science, but cryptography is definitely not an easy science.

Like any field of study there are a multitude levels of understanding. I think most adults have a basic understanding of chemistry and medicine (e.g. drink water when you have a headache, too much diuretics and you get dried out, etc) but that's leagues away from saying you're a doctor.

Cryptography is no different. You can understand that AES "encrypts" a block of text, without really knowing how it does it, or why it was designed the way it was.

For the OP to understand chaining modes all you need to do is look at cryptography as a blackbox. At that level, understanding isn't like going from A to Z but from A to B.

Most people accept they cannot do rocket science or quantum mechanics when they have only read a few books. But it surprises me every time that in this newsgroup people do expect that they can immediately do difficult crypto when they read a few articles or books. It takes years of research and work to become anywhere near decent. I have been working in this area for 5 years full-time now and still learn new things from the posts in this group.

Re: Thank you all for the constructive comments

Re: Thank you all for the constructive comments

Crypto, physics and math fall under the hollywood notion of "spook" which is why they attract the most amount of trolls. Everyone who's seen an episode of star trek or the movie Swordfish (or Mercury Rising or about a dozen others) thinks they can quantum encrypt the storage matrix, or whatever.

Dispelling that notion is often hard, especially when the poster is not seriously interested in learning the subject.