

Re: student wanting to learn about cryptography...

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-07/2088.html>

From: Paul Rubin (//phr.cx_at_NOSPAM.invalid)

Date: 07/30/03

Date: 29 Jul 2003 19:57:11 -0700

ncs8@email.byu.edu (Alex Truman) writes:

- > *Hi, I'm a college student interested in learning cryptography. How*
- > *would you recommend I begin? Is there a book out there you'd*
- > *recommend or something? I know what a prime number is and I know a*
- > *few substitution & transposition coding schemes, but that's as far as*
- > *my knowledge goes. I pretty much need to start at the very beginning.*
- > *Any help would be greatly appreciated!*

Um, say a little more. Why do you want to learn cryptography?

Knowing what interests you about the subject will help in suggesting books for you. Some possibilities:

If you want to learn to program computers to use modern encryption methods, try "Applied Cryptography" by Bruce Schneier.

If you want to learn about classical ciphers and the history of cryptography, try "The Codebreakers" by David Kahn.

"The Code Book" by Simon Singh is a good general intro, giving both classical and modern stuff, but in nowhere near the depth and detail of the other two books mentioned.

If you're interested in the theoretical side, I could recommend a couple other books, but it's probably best for you to develop a deeper math background (take some math classes at your school) first.