

## Re: Book on Pre-MATH for cryptography and cryptanalysis. Reply

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-04/msg00828.html>

---

- *From:* "Douglas A. Gwyn" <DAGwyn@xxxxxxx>
  - *Date:* Fri, 27 Apr 2007 16:37:22 GMT
- 

rolof789@xxxxxxx wrote:

What abstract algebra subject's should I home in on?

Group theory (not group representations, however);  
elementary number theory (esp. modular arithmetic);  
finite fields;  
maybe rings and lattices.

There are of course other useful math topics, but the  
above are essential if you want to do any real research  
in modern encryption schemes.

Some people think computational complexity theory is  
important, and you need to understand the rudiments to  
read some of the literature.

A certain amount (not a lot) of set theory etc. is needed  
to cope with math papers in general.

.