

## Re: What math class to take to catch up on Modulus and DLP?

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-09/0519.html>

---

**From:** Tom St Denis ([tomstdenis\\_at\\_iahu.ca](mailto:tomstdenis_at_iahu.ca))

**Date:** 09/08/03

Date: Mon, 08 Sep 2003 03:17:46 GMT

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

Hash: SHA1

M.S. Bob wrote:

| On Mon, 08 Sep 2003 01:38:14 GMT, Tom St Denis <[tomstdenis@iahu.ca](mailto:tomstdenis@iahu.ca)>  
| wrote:

|

|

>M.S. Bob wrote:

>| On Sun, 07 Sep 2003 22:33:22 GMT, Tom St Denis <[tomstdenis@iahu.ca](mailto:tomstdenis@iahu.ca)>

>| wrote:

>|

>>Says who? I'm a high school grad with a lot of time on my hand. While

>>I'm certainly no pro I think I can safely say I at least am familiar

>>with the field.

>>

>>If you just pick up a few books, read them, toy with the math [e.g. do  
>>the exercises] you'll be able to talk shop too :-)

>

>

> Tom,

>

>| No offense, but you still do lack a fair bit of mathematical maturity.

>

>| Very true but I never assumed that position either. I think I've made

>| it rather clear that I'm a newbie in the field and if you understood

>| differently you should really spend more time reading what I write :-)

|

|

| I do love how you fall back to this defense when someone calls your

| bluff. "I'm a newbie" -- yet you claimed "safely say I at least am

| familiar with the field." -- make up your mind.

A newbie can be familiar with something. To me "newbie" is synonymous with an amateur. E.g. you don't have a complete mastery of the subject

sci.crypt: Re: What math class to take to catch up on Modulus and DLP?

matter.

I know a little bit of biology. That doesn't mean I'm a doctor but I do know enough to name say most of the parts of the human heart, etc...

In this case I know \*of\* many things in math and cryptography. Some of the things I can prove [e.g. I understand why they're true]. I don't think I've ever claimed I have a complete mastery of number theory, algebra, etc.

|>Also often in my own defense I'm only offering what I happen to know as  
|>I understand it. If more knowledgeable people would kick in some  
|>information things would improve.

|  
|

| Yes, those stupid professors, mathematics, and cryptographers like Bob  
| Silverman, Douglas Gwyn, David Wagner, Greg Rose, Brian Gladman, etc.  
| who all horde their information, and never try to inject knowledge or  
| understanding in sci.crypt. Hell, they never even try to correct your  
| factual mistakes or your misunderstandings. Thank you St Denis, you  
| are our saviour.

First off, David Wagner did most of his really cool work before he was a PhD. He was keen into cryptography when he was an undergrad. G