

## Re: Newbie question(s)...

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-09/1242.html>

---

**From:** M.S. Bob ([msbob\\_at\\_hotmail.com](mailto:msbob_at_hotmail.com)-edy)

**Date:** 09/17/03

Date: Tue, 16 Sep 2003 19:09:44 -0300

On 16 Sep 2003 07:13:58 -0700, jonathanrbaker@yahoo.com (Jonathan Baker) wrote:

>Hey all,  
>Been enjoying this group for a couple days... Although, I must admit,  
>the Linear Algebra and Statistics are a bit over my head most of the  
>time... (I'm hitting the books again, please recommend any online  
>materials, books, magazines, etc.)  
>  
>Anyway, if you all would tell me what you think of this, I'd  
>appreciate it...

Honestly in my opinion, to learn mathematical skills you should look for textbooks you can understand, and the majority of students find it easier to have an instructor or tutor available to ask questions.

I would recommend you look at starting with something along the level of Discrete Mathematics, focusing on topics like understanding the basic language of mathematics (e.g. conjecture, theorem, proof, lemma), and the basic types of proofs (induction, proof by contradiction -- reductio ad absurdum), and learn some classic proofs in topics like geometry (just because it's fun), number theory, and abstract (aka modern) algebra.

Modern cryptography (and cryptanalysis) is based upon mathematics, so if you seriously want to learn all the details and really understand cryptography you need strong math skills. The most important resource (in my opinion) is access to study material, that is books. The cheapest way to get access to a good collection of books is with a library card, or several. If you are a student, learn how to find stuff in your library. Consider getting a library card from your local public library, if it is small you should be still able to do interlibrary loans, possibly for free or a very modest fee (e.g. \$1). Look into library access at nearby colleges or universities, many state or government sponsored places offer library access to the public for \$20/annum or less. If you want your own copies, Dover Books makes numerous cheap (often <\$20 US) paperback books about various mathematical topics. The one down side is in their efforts to keep the

books cheap, the book layout is simple, and very if any diagrams in the text.

- >So you generate irrational numbers... Like the square root of 2.
- >
- >They are good little numbers because there is no way to predict the
- >next digit from previous digits... Unlike psuedo-random numbers...
- >Which could be predictable if the period is too small, right?

I know this sounds mean and nasty....

If you new to this topic, why do you expect to come up with a novel method of encryption? It is better than most first posts, but really why do people new to cryptography think they can whip off some neat novel new method that is secure, given that there are professionals that spend years evaluating new algorithms....

Learn first, then try to create later. Trust me, it is the path of less flames, and in my own experience thee more enjoyable path.

- >And there are an infinite number of them. A loose proof:
- >- Given, there are an infinite number of prime numbers ... (any good
- >references to this?)

- >From the ancient Greeks,
- <<http://www-users.cs.york.ac.uk/~susan/cyc/p/primeprf.htm>>
- <[http://mathforum.org/library/drmath/sets/select/dm\\_infinite\\_primes.html](http://mathforum.org/library/drmath/sets/select/dm_infinite_primes.html)>
- <<http://mathworld.wolfram.com/EuclidsTheorems.html>>
- <<http://www.utm.edu/research/primes/notes/proofs/infinite/euclids.html>>

- >- I *\*think\** that the square root of any prime number is irrational
- >(need to write some code...)

No, you want a proof. I doubt you could write any computer program that can prove there the square root of every prime number is irrational.

If I remember correctly, there is a proof that is proof by contradiction; assume that for a prime number, the square root is rational, find a contradiction.

- >This is symmetric encryption, right? You can use this number as a key
- >to say, XOR bits, shuffle them around, pad the data, etc...
- >
- >Downside, you have to find a secure way to share the key (doesn't
- >matter if you encrypt for your own use)... which kinda sucks...

Key distribution is a standard problem with symmetric secret key algorithms.

- >Also, it could take a damn long time to generate enough bits of an
- >irrational number... especially the square root method because you end

sci.crypt: Re: Newbie question(s)...

>*up keeping track of (and subtracting) larger and larger strings...*

How slow? You should try to find that out...It could be educational.

>*Hopefully, it would take less time to make a decent sized key then to  
>figure out the plaintext, right?*

You need to figure that part out, if you are going to "promote" such a method. You shouldn't expect the critics to do all the work. :-)

>*What do pro's use to make text look "random"?*

Stream ciphers

<<http://www.rsasecurity.com/rsalabs/faq/2-1-5.html>>

I hope you get some useful facts and direction out of this. You may find <<http://www.geocities.com/plcurechax/learn.txt>> useful for recommendations of books and material about cryptography.

-msbob