

## Re: Crypto Mini Faq

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-03/2441.html>

---

**From:** Joe Peschel ([jpeschel\\_at\\_no.spam.org](mailto:jpeschel_at_no.spam.org))

**Date:** 03/31/04

Date: Tue, 30 Mar 2004 22:06:10 -0000

Tom St Denis <[tom@seurescience.net](mailto:tom@seurescience.net)> wrote in  
news:NOlac.883\$js5.295@news04.bloor.is.net.cable.rogers.com:

> *Joe Peschel wrote:*  
>>>>> *p4 of that excerpt...*  
>>>>>  
>>>>> *"encrypt – Scrambling data to make it unrecognizable"*  
>>>>>  
>>>> *"Scrambling data" doesn't sound so so bad.*  
>>  
>> *Hmmm -- I seem to have stuttered.*  
>>  
>>>  
>>> *Scrambling is just such a lame word.*  
>>  
>> *One of the meanings of scramble is to disarrange the elements of*  
>> *telephone, teletype, and other electronic transmissions. To the*  
>> *average, ahem, Dummy, scramble means jumble. I think scramble is a*  
>> *good word to use because of the two meanings.*  
>  
> *I don't see how inventing yet another word is helping anything? I*  
> *mean seriously how many words in Math are equivalent?*

I'm not inventing another word.

>  
>>>>> *Um how about*  
>>>>>  
>>>>> *"encrypt [or encipher] – concealing the meaning of a message"*  
>>>>>  
>>>>> *Not only is the latter description accurate but it is more*  
>>>>> *meaningful.*  
>>>>>  
>>>> *How would this description be more meaningful to the intended*  
>>>> *audience?*  
>>>  
>>> *Well because... um ITS WHAT YOU ARE DOING!!!!!!!!!!*  
>>

sci.crypt: Re: Crypto Mini Faq

>> *Not in the eyes of the intended audience. Concealing the meaning of a message might be just re-writing it, or making a typo or grammatical error.*

>

> *Well that's because the audience are not well suited to be cryptographers just yet.*

People who read the "For Dummies" books don't intend to become experts on the subject.

>

>>>

>>> *Message has a meaning... you are concealing it.*

>>

>> *Concealing? That sounds more like steganography.*

>

> *Um no, Steg. hides the \*existence\* of a message in another.*

Uh, ok...

> *In crypto*

> *[er symmetric crypto] you are concealing the meaning not the existence.*

I still don't think your definition of encryption is as good a definition as "scrambling" I think yours is ambiguous and misleading.

>

> *Different goals and consequences entirely.*

>

>>>>> *The "books for [yuppy impatient] dummies" are just symptomatic of a greater problem.*

>>>>

>>>> *What problem is that?*

>>>

>>> *That people want a quick fix to all problems. Hey, you wanna learn a science? Great, pick up some books, learn, experience, rinse and repeat.*

>>

>> *You're too young to be so cynical.*

>

> *Says who? Maybe I'm just cursed with two helpings of critical thinking?*

Don't worry. Be happy.

>

>>> *No, instead people want a reward right now. Hence the low quality book. I bet if Knuth spent 3 months writing TAOCP it wouldn't be as popular as it is now.... Hard work is supposed to be rewarded not a hockey-season worth of tacking notes together.*

Re: Crypto Mini Faq

>>>  
>>> *Have you ever walked in a book store recently? I bought TAOCP from  
>>> a chapters for crying out loud [um about 5 years ago]. Now? You  
>>> can't even find a single math text in there. It's all "self-help"  
>>> and "ASP.NET for dummies" bulldung.*  
>>  
>> *Find a better bookstore, or buy books on-line.*  
>  
> *Um, better bookstore? You obviously don't know the reality of what a  
> Chapters or BN does to a locality. We used to have a decent shop at a  
> local mall [7 mins walk from my house] it ran out of business. The  
> chapters is a 45 mins walk and it's useless.*  
>  
> *As for books online that is reality but there is a certain quality to  
> picking up a book and looking at it before buying it. I've avoided  
> quite a few crappy textbooks that way in the past.*  
>  
>>> *Point is why can't people take things with a modicum of pride and  
>>> respect. Being a cryptographer is not "easy" by any stretch of the  
>>> imagination. You have to be good at math and computer science, you  
>>> have to be able to attack things from weird angles, think like the  
>>> "enemy" and use the rules of science. [This is not unlike other  
>>> fields I guess].*  
>>  
>> *Yup, being good at cryptography is like being good in another field,  
>> for instance, writing...*  
>  
> *I writes as a good as I requires.*

I didn't mean just you. I meant people who claim to care about how they write.

>  
>>> *Or put it another way. You spend [in my case] nearly 10 years  
>>> teaching yourself computer science via literally 1000s of different  
>>> "labs" [e.g. how todo BWT compression, how todo BN math, how  
>>> ...blah] only to find some jackass who read some fluffy book and can  
>>> spew out the latest verbiage gets a job instead of you....*  
>>>  
>>  
>> *Imagine my surprise when I discovered most of the readers can't or  
>> won't even punctuate a sentence correctly.*  
>  
> *yeah because my grammor is just that bad. Admittedly I could be a bit  
> better at the spellings but I don't think it's so bad that I can't  
> make a cogent point. Heck, I've found grammatical errors in Crypto'03  
> proceedings before yet the paper still made sense and was published.*  
>

Yeah, I know. Technical guys are horrible writers. That's why they become technical guys. :-)

J

--

---

When will Bush come to his senses?

Joe Peschel

D.O.E. SysWorks

<http://members.aol.com/jpeschel/index.htm>

---