

sci.crypt: Re: Safe to transmit (symmetric) key encrypted with itself?

Re: Safe to transmit (symmetric) key encrypted with itself?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-06/2171.html>

tomstdenis_at_gmail.com

Date: 06/30/05

Date: 30 Jun 2005 05:59:34 -0700

[last reply on this subject...]

clem wrote:

- > > *Clem, the reason my response to Bob was "hostile" was to show him what*
- > > *his replies look like when coming the other direction. You seemed to*
- > > *be under the impression that someone who did some good can do no harm.*
- >
- > *No. I think that you are under that impression with LibTom, though.*

Yeah that's so easy to say isn't it. Given that the EXACT opposite is true...

- > *Someone who did much good over many years and gave their life to it is*
- > *deserving of more rhythm. If he wants to say "wrong", then he gets to*
- > *do that.*

Why?

- > *You started the ugliness (the real ugliness) with Bob, Tom. Not the*
- > *other way around. If you would just appoligize and really mean it, and*
- > *then back up your words with actions then you would be living in*
- > *another dimension.*

I have done nothing with regards to Bob for which I am ashamed.

- > *My thing about Bob Silverman is that he is a card carrying old school*
- > *crypto big dog, and because of his stature he deserves better.*

Why? "crypto big dog"?

HE WORKED FOR RSA FOR CRYING OUT LOUD.

It isn't like he wasn't already WELL COMPENSATED for his work there.

- > *Your postions are not equal. You are the underling and he is the*

Re: Safe to transmit (symmetric) key encrypted with itself?

sci.crypt: Re: Safe to transmit (symmetric) key encrypted with itself?

> *overling. You cannot accept that.*

Except that in "reality" where the rest of us live that's untrue. Despite what you think I'm moving up from a college grad to a developer in fairly short order. My salary has gone from 0 to around \$45,000/yr in only 3 months after graduating [one of those months I was on a freelance business trip to France]. I may be moving Stateside in the near future to being earning more money [and ideally travel more]. So despite what you think I am making progress.

> *That is the heart of the matter. You refuse to recognize, and refuse to pay your dues when it comes to protocol.*

Totally untrue. When I first met Greg and Serge [just two examples] I stood up, shook their hands, etc... out of respect. I offered them a seat and had civilized discussions with them.

Some "guy" who can't be bothered to correct mistakes in a polite fashion deserves no respect from me.

> *Your method flies in the face of established protocols of business and relationships and respect for your betters in that context.*

Yeah, except that I am working commercially...So maybe my approach while different and hard for the likes you to comprehend is effective and worthwhile in the long run.

Maybe I'm living MY life and not the standard issue life to which you seem to wholesale subscribe. Maybe I want to be a bit different not because I "just want to be different" but because I have based my life on a different set of principles. I give when I could take. I'm courteous without recognition, I'm hedonistic and can often be very pragmatic [when serious].

In short, I'm not you.

> *And Bob Silverman and Daniel Bernstein are in the most genuine sense of the word your betters in that context.*

How so? More people come to me [personally] for Crypto than I bet either of them... COMBINED.

Do you honestly want to know much software uses LibTom projects? I mean I don't even have a good track of it [since it's free] but when you start realizing that people like DemonWare and Sony use the code in video game engines that they license out to other companies, it's easy to say there are probably hundreds of thousands of users of my software. Then you take into account projects like MatrixSSL, Organic Networks, Dropbear, etc. it grows considerably.

Re: Safe to transmit (symmetric) key encrypted with itself?

sci.crypt: Re: Safe to transmit (symmetric) key encrypted with itself?

Sure bob and dan can run circles around my math knowledge. But have either of them stopped to donate something useful to the public? Hell no. Bob worked for RSA where they develop commercial software and Bernsteins code is so horribly unmanageable as to make it totally useless.

There are more than one way to contribute to society. And even so, neither of them do it as a personal sacrifice. Bob WORKED for RSA when doing the research and Dan WORKS for the university. Let's see them pursue open source projects [whether research with no goal of a patent or source code with no copyright] without getting paid. Then you can say they've sacrificed to make the world a better place.

> *You likely find it difficult to comprehend of anyone being better than
> you, but in the context of human endeavor and relationship and
> protocol in the study and the business of math/crypto that list is
> huge.*

The facts speak otherwise. I mean yeah there are people who know more about the innards of say SSL or IPSEC or about the fine details of the NFS than I but you vastly underestimate the influence my projects are having on the scene.

> *And this next thing is just my opinion, but if you could get the past
> the egocentric and disrespectful plateau you appear to be on, then
> that list would be small. That would be a miracle, though.*

I'll just keep relying on the occasional thank you emails I get to re-affirm that everything you're saying here is bogus.

> *He's not exactly beneficial to the
> >group as a whole since any one of us could fill in for "use the GNFS"
> >and "dumbass you're wrong!".
>
> I disagree. You devalue his abilities unfairly, but unfortunately
> that is typically what you do to Bob and Daniel and fill-in-the-blank.*

I have yet to see Bob really write a lengthy reply, even to a question that has "been asked before". He usually just writes "read this" and goes on his way...

Well yes, citations are helpful but sometimes people don't get the math [or the notation, for that matter I'd lump Alice Silverberg in with Bob in the "if you can't get my specific math notation then you suck"].

Tom