

Re: crypto for Tom St Denis ?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-07/0111.html>

From: \ (jonez_at_norcom.ca)

Date: 07/03/05

Date: Sun, 3 Jul 2005 12:22:52 -0600

Tom St Denis wrote:

> *Dane Metcalfe wrote:*

> <snip>

>

> *In the real world it's upto the designer to prove their worth.*

>

> *This guy is layering on various diffrent algorithms all of which have*

> *differing levels of security [some are broken even]*

Which one's are "broken" ?

Prove it.

>*in a vain attempt*

> *to say "you have to break all these first".*

Nothing vain about lamination, it's an accepted practice
and endorsed by all the True Experts® in the field of crypto.

While you self-appointed cryptocritic dipshits vainly search for the Holy Grail
Perfect Algorithm that "can't be broken" (eventually they all fail),
the real world is left to use the material that is available. Lamination,
even using imperfect layers, does add to the level of difficulty
(resources, time, \$\$) to break any given message.

I suppose you don't bother to lock your car when you park it,
because you know after all the car can still be broken into,
and when you park your car in the garage, you don't lock the
garage, because after all that lock is also known to be breakable,
and, you don't take the keys out of your locks that you do
ironically use, because given the rather short differentiation of
possible keys, some criminal is bound to have a ring/set with your
key on it anyway, and the people that have car alarms might as well
not bother setting them, because there are people/devices out there
that can crack them, so why don't you just undo ALL the layered/laminated
levels of security that you vainly practice in nearly every aspect of your
everyday life, withdraw all your life savings \$\$ from the bank, place it in the
trunk of your car, and leave the keys in it, motor running and doors
open, parked on the street tonight when you go to sleep, because

in your world, layered security/lamination is vain, insecure, and a complete waste of time, eh?

>
> *First off, that's bad engineering.*

Tell it to the structural plywood manufacturers, and structural glue–lam beam manufacturers, engineers, architects and builders, after all everyone knows those individual thin layers of wood aren't perfect, and break quite readily, so laminating them together couldn't possibly obtain any given target of strength or structural soundness, could it moron?

Better to wait around, searching for that perfect single material/layer beam, stronger than steel, that can/will "never" fail, eh?

>*Perhaps it could be secure [I'm not saying one way or the other without seeing code] but it's also inefficient. It's the job of a competent cryptographer to not only address the security needs but also to do so with a minimal use of resources. In this, he fails miserably.*

Sez the jackass who can't comprehend lamination.

>
> *Second, nowhere on his site does he talk about authentication. So people can alter files and nobody is the wiser...*
>
> *At anyrate it's not upto Joe to analyze it.*

It is when he laughably makes the unsubstantiated claim that he, or anyone smarter than some bubble–headed housewife, can readily break a given piece of encryption in less than "an hour".

>*Just to point out the clear "bad engineering"*

Except everyone knows that Joseph the blowhard Asswood, and you too, simply make unsupported, and laughably false, assertions, and expect idiots to believe you on the sheer volume of your bluster.

> *and infer that it's an amateur job.*

Then pro's like you and Asswood could surely break the code in less than "an hour" and prove your heretofore unsupported assertions — it's been over 250 hours and neither Asswood nor anyone else has cracked such a simplistic, inherently defective, and amateurish code.

sci.crypt: Re: crypto for Tom St Denis ?

So, put up or shut up.

>

> *Tom*