

Re: Algorithm suggestions

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-09/msg00983.html>

- *From:* "Geoffrey Summerhayes" <sumrnot@xxxxxxxxxxxx>
 - *Date:* 27 Sep 2006 11:56:53 -0700
-

Unruh wrote:

"Geoffrey Summerhayes" <sumrnot@xxxxxxxxxxxx> writes:

I expect that every time someone invents a better lock, people start working on better lockpicks. I fully expect any system to be broken, I'd just prefer that the cost of their time and effort is more than their expected return.

Yes, but that depends on your knowing very very well what lockpicks are out there right now. For example the famous bic pen hack of the Kryptonite locks made them (the pin type circular key locks) useless, but I am sure lots of people still believe that if it is Kryptonite it must be secure.

Ie, rolling your own shortcut could well be way on the wrong side of that cost benefit analysis simply because of your ignorance of what "lockpicks" are out there.

Sure, rather than rolling my own, I could ask for algorithm suggestions on a relevant NG. Any suggestions on the newsgroup to post to?

Geoff

.