

# Re: How much must be revealed

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-02/msg00840.html>

---

- *From:* "Arthur J. O'Dwyer" <[ajonospam@xxxxxxxxxxxxxxxx](mailto:ajonospam@xxxxxxxxxxxxxxxx)>
  - *Date:* Tue, 27 Feb 2007 14:39:50 -0500 (EST)
- 

On Mon, 26 Feb 2007 HilltopLab@xxxxxxxxxxxxxxxx wrote:

On Feb 26, 9:35 am, Volker Hetzer <[firstname.lastn...@xxxxxxxx](mailto:firstname.lastn...@xxxxxxxx)> wrote:

Hilltop...@xxxxxxxxxxxxxxxx schrieb:> If I have an encryption program, is it possible to describe the

algorithm sufficiently to give people confidence in its security without revealing the source code? Or must it be given away before any worth is appreciated?

These are two different issues:

You can convince people to trust your /algorithm/ by publishing it. Or by choosing a well known one and saying "I use AES/CTR with that kind of Key/Counter management".

You can convince people that you are not a liar by providing source code. In cases without random numbers (i.e. if your program is fully deterministic) people can perhaps trust you if they can reproduce ciphertext by means of pencil and paper and it matches your output and you take reasonable pains to ensure integrity of the download (i.e. by providing pgp keys, checksums and the like).

I completely agree that you cannot trust a program that depends on the secrecy of the algorithm. Not only because the algorithm cannot be independently tested, but also because no one can ensure the secret will not get leaked. But that's why I asked the question. No matter how detailed an explanation is given of an algorithm, the devil is in the details. And, just because I claim the program does something doesn't mean it actually does. So, if the only recourse is to publish the source code, there is little incentive to develop a new algorithm, as no one can hope to market it. Except maybe as a hobby.

Re: How much must be revealed

Did you read my response to your original post? In part:

They just have to trust you --- maybe because you're a well-known good guy, or maybe because you offer a comprehensive warranty (hah!), or maybe because they're just stupid or lazy (likely).

There are plenty of stupid and/or lazy people out there to keep even Microsoft-built crypto software in the black. And there are a fair number of well-known good guys who provide crypto software, although admittedly they do go the open-source route.

However, nobody honest makes money on copies of a single program anyway. You make money on the support contracts, or on custom modifications, or things of that nature. And that business model applies just as well to crypto as to other fields --- possibly better, because crypto is so hard to get right. (Or possibly worse, because so many crypto customers are idiots \*cough\*MPAA\*cough\*, and those who aren't idiots would tend to have in-house crypto programmers and not contract out so much, I'd expect. Hmm.)

If your business proposition is essentially "Hey, look, I made an algorithm!", then yeah, you're not going to make any money.

HTH,  
-Arthur

.