Re: A secure, trustworthy Win XP compitable encryption program with GUI interface?

Source: http://www.derkeiler.com/Newsgroups/sci.crypt/2004−03/0243.html

---

From: Benjamin Choi (*nospam_at_technosoft21.com*)
Date: 03/02/04

```
Date: 2 Mar 2004 04:57:39 −0800
```

"MacGregor K. Phillips" <mkp@topsecretcrypto.com> wrote in message news:<c20q1d$1m0v90$1@ID−201989.news.uni−berlin.de>...
> *Read the documentation. I recommend face to face exchange.*

It doesn't say anything about difficulty of factoring 16kbit RSA. The only reference which suggests that 128−bit symmetric encryption is broken is

"Rainbow Six by Tom Clancy − © 1998 − paperback edition pages 436 and 437. Here Tom Clancy writes that the NSA, with the application of quantum theory to communications security can decipher codes with 128 bit keys, and it appears from his writing that it hardly takes any time at all. The conventional key used by PGP™ is only 128 bits. Does Tom Clancy know something we do not, and has he incorporated this knowledge into his novel?"

Which is clearly fiction... besides, doesn't recent versions of PGP allow for 256−bit keys (AES and Twofish algorithms in addition to the 100+ bit key algorithms CAST (128−bit), IDEA (128−bit), 3DES (112−bit)).

"The Optiset E privacy module offered by Siemens AG for voice encryption over the telephone "uses one of 10 to the 38th power keys for each call" which works out to only a 128 bit key. 2 to the 128th power equals 3.4028 times 10 to the 38th power. Do you think the NSA can break this one too?"

Why do you think the NSA can break this one too besides the references I quoted above?

```
−−
Benjamin Choi
```