

Re: FileCopy overwrites the existing file

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2006-12/msg00298.htm>

- *From:* Grzegorz Wróbel </dev/[null@xxxxxxxxxxxxxxxxxxxxxx](mailto:xxxxxx@xxxxxxxxxxxxxxxxxxxxxx)>
 - *Date:* Sun, 10 Dec 2006 23:03:09 +0100
-

anton bassov wrote:

> Here we speak about the data samples of the size of *hunderds of GB*

with some "plain-text" (i.e. OS-related stuff) known in advance, so that symmetric algorithms that are perfectly safe for encrypting some files or messages may be not-so-reliable here – probably, you would have to go for asymmetric ones, and, hence, pay performance penalties

The problem of "plain-text" messages and risk of "finding patterns" is usually solved (at least I'll do it this way) by mixing the plain text with values returned by good pseudo-random number generator (say 256bit seed + at least 2^{1000} period). Distinguish an output of pseudo-random generator from random output is not doable in polynomial time so you are safe with this technique, and mixed plain-text with such pseudo-random sequence is as chaotic as such sequence itself.

I consider symmetric algorithms much safer than asymmetric ones (there is no proof there aren't breakable in polynomial time, no one just did it) and there are quite advanced factoring algorithms (like GNFS) that pushes the limit of breakable keys further and further (1024bit RSA encryption in few years won't be considered that much secure).

The asymmetric algorithms have wider range of usage, but for disk compression nothing more than symmetric encryption is needed.

--

Grzegorz Wróbel

<http://www.4neurons.com/>

677265676F727940346E6575726F6E732E636F6D

.