

## Re: Self Decrypting Archive Freeware?

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/2045.html>

---

**From:** Paul Rubin (*//phr.cx\_at\_NOSPAM.invalid*)

**Date:** 04/29/05

Date: 28 Apr 2005 18:40:51 -0700

Jean-Luc Cooke <jlcooke@engsoc.org> writes:

- > *Windows .EXEs prompt for password. Password is salted, and passed*
- > *through 2<sup>16</sup> iterations of the hash function. Encryption uses CTR mode.*
- > *Try it out, see if you like it. I'd welcome comments.*

What about authentication? Is there none? You know what a silly idea THAT is. Is there some? In that case, you expect the file may have been tampered with by an attacker. Are you REALLY telling your customers to run .exe's that they think might have been concocted by attackers?

Self decrypting archive = bad, bad, bad.