

Re: exploring the use of manual encryption of passwords (newbie)

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-09/1033.html>

From: Paul Rubin (//phr.cx_at_NOSPAM.invalid)

Date: 09/29/04

Date: 28 Sep 2004 15:15:13 -0700

"Alex D" <anon@anon.anon> writes:

- > 1. (Being a newbie in crypto) I am investigating some time in trying
- > to find an easy manual encryption scheme (i.e. no software involved
- > other than my own brain) to "encrypt" my passwords used on various
- > places (websites, e-mail, ISP, ...). I would like to encrypt the
- > password list because the idea is to carry them on a piece of paper
- > that cannot be used by crackers. The idea is to have a list of
- > (system, password) pairs (maybe also the user id as a third column).

Why do you care about this? Suppose you just write down the plaintext. How are the crackers going to get hold of the piece of paper, if you carry it in your pocket? You can even put it in a secure container, i.e., your wallet. There is then some chance that a mugger or pickpocket might get it someday, but is such a person likely to also be a cracker?