

## Re: manual cryptography

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/3021.html>

---

**From:** Andrew Swallow ([am.swallow\\_at\\_eatspam.btinternet.com](mailto:am.swallow_at_eatspam.btinternet.com))

**Date:** 10/30/03

Date: Thu, 30 Oct 2003 00:35:58 +0000 (UTC)

"John Savard" <[jsavard@ecn.aSBLOKb.caNADA.invalid](mailto:jsavard@ecn.aSBLOKb.caNADA.invalid)> wrote in message  
news:3f9fa7fc.867997@news.ecn.ab.ca...

[snip]

- > *Given that a cipher system is not considered secure unless it can*
- > *withstand an attack on the key alone, with the adversary knowing the*
- > *basic method, that runs into a problem right there, because memorizing*
- > *a key that is effectively 128 bits long is tricky.*

>

128 bits may be hard to remember but 10 words are not.

Andrew Swallow