

# CAST self-decrypting archive; RC6

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-02/2176.html>

---

**From:** RPK ([webmaster\\_at\\_hypercypher.zzn.com](mailto:webmaster_at_hypercypher.zzn.com))

**Date:** 02/29/04

Date: 28 Feb 2004 21:13:33 -0800

Why CAST-128 is mostly used for creating self-decrypting archives?

I heard of CAST5 previously, what is the difference?

Many cryptographers had good faith in this algorithm, but I did not see its name in the AES race. Any report of serious weakness found in it.

Some of the algorithms like RC6 which support 2040-bit keys are often not seen, whereas RC4 is still popular.