

## commuting?/non-group cipher?

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-10/1257.html>

---

**From:** Peter Fairbrother ([zenadsl6186\\_at\\_zen.co.uk](mailto:zenadsl6186_at_zen.co.uk))

**Date:** 10/28/04

Date: Thu, 28 Oct 2004 06:56:03 +0100

Some ciphers have the property that a double encryption can always be replaced by a single encryption, ie  $E(k_3)[P] = E(k_1)[E(k_2)[P]]$

Does anyone know the correct name for this property? If there isn't one, does anyone know a reason why "commuting (adj.)" cipher would not be okay?

Can anyone think of an example of a cipher with this property that is not a group?

--

Peter Fairbrother