

AES is not a group

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-04/2067.html>

From: azerty (azerty_qsd_at_yahoo.fr)

Date: 04/29/05

Date: 29 Apr 2005 01:33:02 -0700

I would like to know if we can apply the techniques describe in the article "DES is not a group" to demonstrate that AES is not a group (e.g we can't find k_3 such that $AES_{k_1} \circ AES_{k_2} = AES_{k_3}$)