

Re: commuting?/non-group cipher?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-10/1345.html>

From: Peter Fairbrother (zenadsl6186_at_zen.co.uk)

Date: 10/29/04

Date: Fri, 29 Oct 2004 08:22:50 +0100

bmm wrote:

- > *I don't see it. But first things first. You originally talked about:*
- >> $E(k3)[P] = E(k1)[E(k2)[P]]$
- > *Just to be explicit, you mean this for all P, right? If so, I would just*
- > *write it as something like $E(k3) = E(k1)[E(k2)]$ to make it clearer that we*
- > *are saying the permutations are equal.*
- >
- > *The set S are all of the permutations described by $E(k)$, where the operation*
- > *is composition. Let $a = E(k1)$ and $b = E(k2)$. Then $a*b = E(k1) * E(k2)$, ie*
- > *the permutation defined by $P \rightarrow E(k1)[E(k2)[P]]$. The question is about*
- > *whether this is $E(k3)$ for some $k3$. This is closure.*

Could you explain what you mean by "the operation is composition" please? I think I am beginning to understand, but that's confusing me.

Thanks,

--

Peter Fairbrother