

## Re: commuting?/non-group cipher?

**Source:** <http://sci.tech-archive.net/Archive/sci.math/2004-10/8574.html>

---

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

**Date:** 10/30/04

Date: Sat, 30 Oct 2004 02:35:09 +0100

Peter Fairbrother wrote:

- > *I don't know the right word, "semigroup" and "groupoid" are wrong, so I'll*
- > *use "sabo" for a set-and-binary-operation, with no implications of closure*
- > *or associativity, where the binary operation can be, and can only be,*
- > *applied to any two members of the set, producing an output.*
- >
- > *We are investigating a generalised "cipher" sabo which also possesses a*
- > *particular property, and want to know whether it must be a group.*
- >
- > *The "cipher" part means that the sabo must function as a cipher. We will*
- > *also want to investigate ciphers which are not sabos, eg where the*
- > *encryption and decryption operations differ, to see if a cipher with the*
- > *particular property which is not a sabo can exist.*
- >
- > *The particular property is :*

Given a set  $S$  and a binary operation  $*$ ; the property that for all  $a, b$  in  $S$  there exists  $c$  in  $S$  such that, for all  $d$  in  $S$ ,  $c*d = a*(b*d)$ .

In crypto terms, the property that a double encryption under two keys is always equivalent to a single encryption under some different key.

I can only think of three ciphers which have the property – Caesar, Pohlig–Hellman and Vernam/otp. All are groups, where the group set is the set of texts and keys, and the group operation is the encryption/decryption operation.

All are also permutation groups, where the group set is the set of permutations (regarding an encryption under a specific key as a permutation) and the group operation is composing<sup>^</sup> the permutations. Kristian Gjøsteen has shown that any cipher with the property must be a permutation group.

(<sup>^</sup>doubly permuting)

- > *The elements of the set,  $S$  of the sabo consists of all the possible*
- > *messages, ciphertexts and keys. The binary operation  $*$  takes any two members*
- > *of the set and produces an output, and is the encryption/decryption*

sci.math: Re: commuting?/non-group cipher?

> operation.

>

> We want to know whether *\_that sabo\_* must be a group. We are not interested

> in whether there is an associated permutation group unless it tells us

> something about the sabo.

>

>

> On first glance I thought "obviously it doesn't have to be a group"; but now

> I'm not so sure.

So far I have: the sabo must have closure.

> Kristian Gjøsteen wrote:

>> Denoting the operation on  $K$  by  $\#$ , we get an induced operation  $\#$  on  $X$

>> given by  $f(k1, ) \# f(k2, ) = f(k1\#k2, )$ .

>

> Nope. lost me there.

Sussed it now, thanks.

--

Peter Fairbrother