

Re: commuting?/non-group cipher?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-10/1356.html>

From: Kristian Gjøsteen (*kristiag+news_at_math.ntnu.no*)

Date: 10/29/04

Date: Fri, 29 Oct 2004 14:21:17 +0000 (UTC)

Peter Fairbrother <zenadsl6186@zen.co.uk> wrote:

>I am slightly less confused now; but I still have to prove that a cipher
>with the property is a group (not a permutation group), in terms of the set
>S of texts and keys and the encryption operation * (or not, if it isn't).
>Anyone got a clue for me?

I don't exactly understand what you are asking for, so I'll talk about something that may or may not be related. I hope it helps.

Let's ignore randomized encryption, and only consider insecure things, so the cipher is a function f taking a key k (from a set K) and a message m to a ciphertext c .

Second, let's assume that the set of messages (say $S1$) and the set of ciphertexts (say $S2$) are independent of the key k . So we really have a function $f:K \times S1 \rightarrow S2$.

For a fixed key k , we get a function $f(k,):S1 \rightarrow S2$. It is a function taking messages to ciphertexts. So we can consider our cipher as a set of functions $X = \{ f(k,):S1 \rightarrow S2 \}$.

In your notation that $E(k)[P] = f(k, P)$, where P is in $S1$.

It is now clear that a decryption function exists only if the cardinality of $S2$ is larger than or equal to the cardinality of $S1$.

We may also, without loss of generality assume that $f(,)$ is onto $S2$ (if it is not, replace $S2$ by the image of $f(,)$ in $S2$).

Now, unless $S2$ is a subset of $S1$, we cannot compose encryption functions: $f(k1, f(k2,))$ doesn't make sense.

If $S1$ and K are finite, every $f(k,)$ must be a set isomorphism of $S1$ and $S2$, and we may as well assume $S1=S2$ and consider X to be a subset of the permutation group, and my previous post applies, and X is a group and is a subgroup of the group of permutations on $S1$.

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

If S_1 isn't finite, and S_2 is a subset of S_1 , then we may have a composition operation on X , and the property that $f(k_1, f(k_2,)) = f(k_3,)$ for some k_3 in K could be described as "X is closed under composition". In this case, the cipher set X need not be a group.

Now, let's switch to alternative interpretations, where S_2 need not be a subset of S_1 :

Note that there is a map from the set of keys K to the cipher set X given by $k \mapsto f(k,)$. We may assume that this map is a bijection (the map is onto by definition; it induces an equivalence relation on K , so by replacing K with the set of equivalence classes, we have a bijection). This means that if we have some kind of binary operation on K that is closed, that operation will induce an operation on the cipher set X that is also closed.

Denoting the operation on K by $\#$, we get an induced operation $\#$ on X given by $f(k_1,) \# f(k_2,) = f(k_1 \# k_2,)$.

If we decide to get confusing, we could render this as $f(k_1, f(k_2, P))$, or in your notation, $E(k_1)[E(k_2)[P]] = E(k_3)[P]$, where $k_3 = k_1 \# k_2$. This is of course an abuse of notation.

This works both ways, so if we have some structure on X , that induces a structure on K . This may or may not be a group structure.

--
Kristian Gjøsteen