

Re: comments on cipher please

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-10/msg00920.html>

- *From:* "Antony Clements" <antony.clements@xxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 30 Oct 2006 10:35:20 +1100
-

<snip>

No would you PLEASE read Bruce Schneier's comment about amateur cryptographers? He explicitly tells why your break-fix-break-fix-cycle is utterly nonsense.

<end snip>

why does everyone assume i have not read the available material? I have read that comment and i am even a member of his mailing list. in his comment he says that the likelihood of an amateur design being secure is highly unlikely verging on the impossible. that is not to say that it doesnt happen, it is saying that the likelihood of an amateur designing a secure cipher is 1 in several billion.