

Re: The crazy encryption madmans codebook

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-03/msg00146.html>

- *From:* "Joseph Ashwood" <ashwood@xxxxxxx>
 - *Date:* Sun, 04 Mar 2007 23:16:49 GMT
-

<jt64@xxxxxxx> wrote in message
news:1173012045.031483.180180@xx
On 4 Mar, 01:55, "Joseph Ashwood" <ashw...@xxxxxxx> wrote:

<j...@xxxxxxx> wrote in message

news:1172925208.343013.187300@xx

[snip point for point demonstration of cryptographic lack, just the bullet points:

- * In order to be even remotely possibly minimally secure would require an absolute minimum of 5 000 000 000 000 000 000 000 000 petabytes of storage, even that assumes perfect compression of the database
- * The system as designed leaks information at an incredible rate as per the proof supplied earlier
- * By the proofs supplied earlier the entire security rests on the minimum security of either the permutation (which is fixed and so insecure) and the chaining mode (which was proven to be heavily biased and therefore highly insecure)

Well Joe i never said that the database only had 5 000 000 entries it was an example,

Unless you can approach 2^{128} entries, the system will be insecure.

And that is why you really fear this approach to cryptography, it is your buisness and these type of algorithms rends your knowledge of attacks useless.

Quite the opposite really, once again I refer you back to the proofs supplied earlier. Your design is a simple subset of all possible permutations, so proofs that show it is weak if all possible permutations are achievable show that the design given, and every possible variation of it, are insecure.

Re: The crazy encryption madmans codebook

And that is why you try to very fast discard the whole approach as useless Joe.

I will certainly argue that my reasoning, and the proofs behind it, provide a very plain reason why I did this. My goal as always is to eliminate all pointlessly insecure cryptography, of which your design is one of the gravest offenders I have seen in a long time.

Clark – I agree, it was quite predictable, in particular form the inability to recognise logic.

As for what (sic) means, it is actually an abbreviation of the "psych-out" that to the best of my knowledge first appeared in the early to mid 1980s as slang in Southern California, due to it's closeness with hollywood and the music industry usage of the word spread. As for meaning it implies a reversal in meaning of the previous text.

Joe

.