

Re: Unbreakable Encryption – Scenarios – What encryption method would be best?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-03/1276.html>

From: Tom St Denis (tomstdenis_at_yahoo.com)

Date: 03/16/04

Date: 15 Mar 2004 18:56:17 -0800

"Bartosz Zoltak" <QPbzoltak@vmpcffunction.com* (without "QP")> wrote in message news:<c34m7n\$9qc\$1@atlantis.news.tpi.pl>...

> *Tom St Denis wrote:*

> *[snip]*

>

> *The main point was my question :*

>

> *Is there really no known method of combining cryptographic algorithms*

> *in a way to build a provably unbreakable symmetric encryption? Certain*

> *modes of operation can be proved*

> *as-secure-as-the-underlying-block-cipher, but IS THERE no way to get*

> *"a level lower" with the proof – that the very cipher can be proved*

> *secure if some basic assumptions are satisfied?*

>

> *As far as I know there is no such scheme but I may be wrong. Is there?*

You can prove security against most attacks. The problem is not all attacks are known.

However, yes, you can get some "quantifiable" level of security. In fact there was a recent Crypto'03 paper on the subject. The problem is these schemes require a HUGE amount of ram [e.g. totally random round functions]. IIRC 7 rounds are enough for CPA and 10 rounds for CPCA.

So let's put numbers to that. For a 64-bit block cipher this amounts to 2^{34} bytes per round for a total of around 2^{38} [or 1/4 of a TB of ram] for 10 rounds.

Of course you may be able to extend that into heuristics... E.g. turtle style. Make a 16-bit Feistel [which would only require 2.5KB of ram] and use it over and over [e.g. 10 times for the 32-bit feistel giving 25KB of ram then 10 times for the 64-bit feistel giving 250KB of ram]. Such a design wouldn't have the provable chars but would most likely be secure [and definitely very slow].

sci.crypt: Re: Unbreakable Encryption – Scenarios – What encryption method would be best?

Tom