

Re: Data encryption 360 degrees the nsa cannot break -- 01

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-12/0545.html>

From: Benoit (benoit.sansspam_at_leraillez.sansspam.com)

Date: 12/27/03

Date: Sat, 27 Dec 2003 04:25:50 +0100

Walter Roberson <roberson@ibd.nrc-cnrc.gc.ca> wrote:

- > *I don't understand what the original poster is talking about,*
- > *about folding and cancelling: I'm having trouble getting through*
- > *the English to understand the proposed algorithm.*

His idea is this : you put your binary code in a square form when you "fold" your square in the middle you add the bits and get the result, then you fold it the other way in the middle and you do the math again, and you go on until you're left with one or two bits. Now the way you folded it is the key. Here's a small example :

01

10 first I fold it vertically so I get this addition :

$0 + 1 = 1$

$1 + 0 = 1$

Now I fold what is left vertically and $1 + 1 = 0$

What's funny about his idea is that the same procedure on this data:

10

01 gets the same result. So If I have the key of the folding procedure and I have the 0 we got above:

- How do I know this 0 is the result of a 1+1 and not from a 0+0?
- If I ever know it came from a 1+1 how do I detect the first 1 is the result of a 0+1 and the second the opposite, a 1+0?

Sure the NSA wont figure out the message but the one it is destined to wont read it either.

My 2 cents

--

Benoît Leraillez

La douleur des autres est tout à fait supportable, hors les cris.