

Re: manual cryptography

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/3032.html>

From: Bill Unruh (unruh_at_string.physics.ubc.ca)

Date: 10/30/03

Date: Thu, 30 Oct 2003 12:03:04 +0000 (UTC)

Mxsmanic <mxsmanic@hotmail.com> writes:

]Bill Unruh writes:

]> Why? As a couple of us have suggested, RC4 could be done by hand, and if
]> you have a way of breaking RC4 with computer, people would love hearing
]> about it. It's only problem would be key scheduling/control

]I suppose you have a point. RC4 could probably be done pretty quickly.
]But what about the precalculation time to set it up?

Depends on how worried you are about the initial weak stream. Ie, the
usual advice is to run 256 times to clear that initial state.

The precomputations would take a bit of time, but far less than an
average of 1 min a letter if the message is a reasonably long one.