

Re: determining algorithm used

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-10/1389.html>

From: Mok-Kong Shen (mok-kong.shen_at_t-online.de)

Date: 10/30/04

Date: Sat, 30 Oct 2004 19:56:28 +0200

WTShaw_1@hotmail.com wrote:

- > *One could misdirect an attack to another cipher by saying falsely is*
- > *what it isn't or bury the quest for cipher identity by looking very*
- > *ordinary like using only 26 different characters in five character*
- > *groups. As might be recalled, I have worked out fairly good ways to*
- > *do the later from any existing ciphertext of any N set.*

Misleading the opponent is certainly a 'legitimate' means in the realm of security. In the same vein, entirely nonsensical stuff could be rendered 'cryptic'. There is a rather recent paper in Cryptologia arguing for the hypothesis that the Voynich manuscript is a pure hoax.

M. K. Shen