

Re: Enigma machine strenght using a computer

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-12/msg00718.html>

- *From:* Unruh <unruh-spam@xxxxxxxxxxxxxxxx>
 - *Date:* 30 Dec 2006 23:52:40 GMT
-

"=?iso-8859-1?q?Jean-Fran=E7ois_Michaud?=" <cometaj@xxxxxxxxxxxx> writes:

Ignacio aecbi wrote:

The analog these days is point of sales authentication. You can limit the amount of time an intruder has to steal or break the authenticating key that secures the transaction.

Maybe, but I'm talking about the algorithm in itself. If fine tuned,

I'm certain it could be fairly efficient and secure.

Enigma is not efficient. To have to do 50 table lookups as suggested in the original post is not efficient. And the fact that each table is fixed and assumed known to the enemy makes the procedure much dicier. You have 50 transopision cyphers going with the transpositions stepping by a single wheel at each step (also known to the attacker). The only thing unkown is the order of the wheels (lookup trasposition tables) and the initial settings of them. It sound both very slow and insecure to me.

For higher security needs solutions like IPV6 and modern methods like closed loop quantum cryptography give better security.

closed loop quantum cryptography is what exactly?

But aren't we talking about an idea for an algorithm versus a whole security scheme here? I'm talking about the specifics of an algorithm

Re: Enigma machine strenght using a computer

and you broadened the scope by bringing up a communication protocol and
(as far as I know), a cutting edge cloud shoveling method?

Regards

Jean-Francois Michaud