

Re: Real-time sound cyphering algorithm

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-05/1193.html>

From: Mike Amling (*nospam_at_nospam.com*)

Date: 05/29/05

Date: Sun, 29 May 2005 21:42:49 GMT

David Eather wrote:

>

> *I think this is the hard way to do this – a good way that will get a
> perfect result, but still a hard way. The OP wanted to decrypt and
> identify the sound by ear, so it doesn't have to be bit perfect.*

>

> *Encode the sound stream by adding (not xoring) the stream cipher
> output.*

This is dubious. If you add white noise to a recorded conversation, it sounds like a conversation with tape hiss. Noise, which is what I presume a stream cipher would sound like, has to be overwhelming before a conversation becomes totally unintelligible.

> *Decode is just receive the sound (normalise it first) and
> subtract the same stream cipher output. The result will probably
> have bit errors in most bytes but still have the identifiable sound.*

—Mike Amling