

Re: Real-time sound cyphering algorithm

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-05/1069.html>

From: Andrew Swallow (am.swallow_at_btopenworld.com)

Date: 05/25/05

Date: Wed, 25 May 2005 16:59:32 +0000 (UTC)

John Hadstate wrote:

>
> *Astier Anisse wrote:*
>
>> *Hello,*
>> *My problem is quite simple:*
>> *I'am willing to find a simple algorithm to cypher a sound:*
>> *I need the cyphered sound to be audible, but not understandable,*
>> *and that we can decypher it from a recorded sound (verbatim copy not needed).*
>>
>> *This seems simple, but in fact, i tried a few algorithms and i had no results.*
>
>
>> *The objective is to have an output sound that seems to be a random sound.*
>> *And that we can decypher after recording. "real-time" is achieved by a small*
>> *buffer (0.5 sec for example).*
>>
>
>
> *Let me suggest the use of a device known as a "modem" to transmit your*
> *encrypted data.*
>

Try –

Record sound in MP3 digital format
Encrypt the MP3, either as a file or a bit stream
Use a modem to transmit the encrypted data
Receive the data using a second modem
Decrypt the incoming data giving the MP3
Play the MP3 producing the original sound.

AES in CTR mode is a good method of encryption.

Andrew Swallow