

Re: Real-time sound cyphering algorithm

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-05/1166.html>

From: Unruh (unruh-spam_at_physics.ubc.ca)

Date: 05/28/05

Date: 28 May 2005 14:24:47 GMT

"David Eather" <eather@tpg.com.au> writes:

>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. 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.

>(I skipped over the necessity of keeping both stream ciphers in sync
>– –If you can make sure there is no similar frequency in the ciphered
>sound stream I suggest periodically adding a few bytes of high
>frequency as sync bytes . Or if there is enough computational power
>superimpose the whole waveform on a low frequency carrier and use the
>zero crossings for sync – because of the errors in transmission this
>will take a bit of trial and error but you will know when you have
>the correct result – a FFT will show the result is no longer white
>noise).

This problem of sync is one problem. A worse problem is that of differential phase shifts. Remember that a phase shift is the same as a time delay. speakers are notorious for introducing differential phase shifts into the sound. Thus, let us say you use the low freq carrier idea and the system introduces a phase shift (time delay) into that low freq sound. The ear is almost completely insensitive to such phase shifts— but they can almost completely alter the shape of the wave form. Your encryption system would be highly sensitive to such phase shifts.

The problem with his scheme in general is precisely this problem which arises from the demand that the sound be played over a speaker system (which I assume he has no control over, and has not been optimised for minimal phase shifts). If it were audio transmitted over a wire, my worry would disappear.

>-----BEGIN PGP SIGNATURE-----

sci.crypt: Re: Real-time sound cyphering algorithm

>Version: PGP 8.1

>iQA+AwUBQpfzUJS9Fk5okqe7EQLqUACgmd+313eDHaU+gjuIWC5W8scXopsAmMor

>t6ZgpyP8vWIwLlIfcn0uomo=

>=es3n

>-----END PGP SIGNATURE-----