

## Re: Newbie question(s)...

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-09/1615.html>

---

**From:** Jonathan Baker ([jonathanrbaker\\_at\\_yahoo.com](mailto:jonathanrbaker_at_yahoo.com))

**Date:** 09/19/03

Date: 19 Sep 2003 06:35:49 -0700

"Ernst Lippe" <[ernstl-at-planet-dot-nl@ignore.this](mailto:ernstl-at-planet-dot-nl@ignore.this)> wrote in message news:<3f685555\$0\$10196\$48b97d01@reader20.wxs.nl>...

> *On Tue, 16 Sep 2003 07:13:58 +0000, Jonathan Baker wrote:*

>

> > *They are good little numbers because there is no way to predict the*

> > *next digit from previous digits...*

>

> *It is not true that the digits in an irrational numbers are*

> *always hard to predict.*

> *The following number is irrational:*

> *0.101001000100001000001.....*

> *but it is very easy to predict the next digit.*

>

> *greetings,*

>

> *Ernst Lippe*

Another thought Ernst...

(I'm pretty sure something like this was proposed for quantum crypto key exchange)...

Suppose my key "source" (if that term is appropriate) is the square root of 2 in base 2...

Suppose my key "bit-selector" (loose terminology here, please correct/criticize me!) is the square root of 3 in base 2...

So I generate roughly twice as many bits of the key "source" as I would want for my actual key... Same goes for the key "bit-selector"...

If the "bit-selector" is a 1, then add the current bit of the "source" to our key. If the "bit-selector" is a 0, then skip the current bit of the "source"...

This is a REALLY simple idea (could go anywhere with this idea... But how would an attacker go about analyzing this?)

sci.crypt: Re: Newbie question(s)...

Say Alice and Bob secretly exchange their key "source" and "bit-selector" as square roots of 2 and 3 respectively... (obviously, we would really use a hard to guess irrational number)... Charlie, that scheming bastard... does he stand a chance of figuring this out?

Suppose there are two more key sources... another irrational number, say the square root of 5... if a bit is a zero, skip the current key bit... if it is a one, then exchange the current bit with the bit in front of it... (unencode in reverse)...

And the fourth irrational number, say Pi, or something... You could have zero mean XOR the plaintext and key, and one mean IFF the plaintext and key...

But I guess the sci.crypt crew is going to tell me you can't add a bunch of simple things up to make anything really, provably secure... right?

THANKS AGAIN FOR YOUR INPUT GUYS/GALS!!!

Have a good one!

Jon