

Re: Hardware True Random Number Generator design / concept

Source: <http://sci.tech-archive.net/Archive/sci.electronics.design/2005-06/msg03120.html>

- *From:* Guy Macon <<http://www.guymacon.com/>>
 - *Date:* Thu, 23 Jun 2005 11:43:38 +0000
-

The Real Andy wrote:

>
>Yoy G0 <yoyg0@xxxxxxxxxxxx> wrote:
>
>>That is not one time pad. Not that it can't be done securely,
>>but you don't have the theoretical secrecy against an attacker
>>with unlimited computing power that OTP offers.
>>With unlimited power the attacker can try all possible seeds
>>(since there are only a finite number of them)
>>and find the one that decrypts to something sensible.
>>All the wrong decryptions will look like random data.
>>With OTP all plaintexts are equally likely,
>>including all the sensible ones, so there is no way to
>>tell which one is correct.
>>OTP will require a hardware random number
>>generator for every bit of the keystream.
>
>Given any number of unlimited resources, one can crack any
>cryptographic system.

BUZZ!!

WRONG ANSWER!!!

Nobody can crack a properly used one-time pad, even with infinite resources and infinite time. This is not an opinion or a guess; it is a mathematical certainty that they cannot be cracked.

That being said, there are any number of methods that are far more convenient and which require resources and time that, while not being infinite, are much larger than one could fit in the universe and which require more time than there is between the birth and death of the universe.

Guy Macon <<http://www.guymacon.com/>>

• **References:**

- ◆ **[Re: Hardware True Random Number Generator design / concept](#)**
 - ◇ *From:* The Real Andy
- ◆ **[Re: Hardware True Random Number Generator design / concept](#)**
 - ◇ *From:* The Real Andy

- Prev by Date: **[Re: VCO Design](#)**
- Next by Date: **[Re: VCO Design](#)**
- Previous by thread: **[Re: Hardware True Random Number Generator design / concept](#)**
- Next by thread: **[Re: Hardware True Random Number Generator design / concept](#)**
- Index(es):
 - ◆ **[Date](#)**
 - ◆ **[Thread](#)**