

Re: Key entropy, stream entropy, block entropy, block population entropy AKA uniique stream length

Re: Key entropy, stream entropy, block entropy, block population entropy AKA uniique stream length

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-02/msg00313.html>

- *From:* jt64@xxxxxxx
 - *Date:* 10 Feb 2007 09:07:20 -0800
-

On 10 Feb, 14:50, clark <c...@xxxxxxxxxxxx> wrote:

On 10 Feb 2007 04:11:42 -0800, j...@xxxxxxx wrote:

On 10 Feb, 12:33, clark <c...@xxxxxxxxxxxx> wrote:

<snip>

You don't understand entropy, do you?

And this argument help you in what way, it looks like handwaving but it could also a desperat call for help.

Yes i do in a binary with the given length x the entropy is 2^x , in plaintext english the number of possible unique states a binarystring of that *SPECIFIC LENGTH*

You should though try to decode the meaning of *SPECIFIC LENGTH* and try to logically deduce the connection to *KEYEXPANSION* and *SHUFFLES*

If the key expansion or shuffles are generated from an algorithm only and do not include input from a hardware RNG or cryptographically sound CSPRNG like /dev/random or from another entropic source like random mouse movements or the outcome of rolling dice... things like that, then what is there to decode?

Re: Key entropy, stream entropy, block entropy, block population entropy AKA uniique stream length

Re: Key entropy, stream entropy, block entropy, block population entropy AKA uniique stream length

I will give you an *EXAMPE* now suppose there is a generator(PRNG) for one *STRING "STREAM"* of the length $256! \cdot 2^{2048}$.

Suppose there is a very clever *DUDE* that realise he just can reach different offsets within that string even with passwords of different length, that would make some people very *NERVOUS*.

Because they do not now what the *STREAM* contains and they never will. Because the offsets is very far between eachother. In fact so far they realise they have no option then to bruteforce to find the offsets in the *STREAM*

Now this *DUDE* not only make the key totally scaleable, also the actual algorithm is totally scaleable *AND NOW REAL CRYPTOGRAPHERS* get *REALLY NERVOUS*
Because they realise they can not distinguish the different sizes of the *ALGORITHM* from eachother.

At this point they pretty much give up every hope, and *REALLY* *REALLY* hope that this just all will blow away without anyone taking notice of the *DUDE*.

They even send some of their *PETS* who do not understand the subject to try riddicule hime and scare him away.

And that is just all fine.

Jonas Thörnvall

there would be no way to actually generate the complete string

You cannot derive entropy where none exists.

I do not hold high hopes that it will enlighten you, the least.

But, then again, you appear to be the one who needs to be enlightened.

How are your high hopes doing with that issue?

I mean... you use the word constantly... but you appear to not understand what it means, particularly as regards crypto.

Re: Key entropy, stream entropy, block entropy, block population entropy AKA uniique stream lengt

Re: Key entropy, stream entropy, block entropy, block population entropy AKA uniique stream length

Blah blah blah

Well... yes... that is all you are doing. Why don't you say something knowledgable about entropy?

Really. Instead of speaking about it using terms you made up and have no basis in reality, why not try to actually apply the real meaning to what you are saying.

Then you would quickly see that maybe your high hopes and dreams and shmeems and fleems about entropy may indeed be true in some other parallel universe, but not here on planet earth.

Re: Key entropy, stream entropy, block entropy, block population entropy AKA uniique stream length