

Re: Anyone wanna help with a compression routine (new type)

## Re: Anyone wanna help with a compression routine (new type)

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math.research/2007-12/msg00062.html>

---

- *From:* WM <mueckenh@xxxxxxxxxxxxxxxxxxxx>
  - *Date:* Tue, 25 Dec 2007 23:31:40 +0000 (UTC)
- 

On 19 Dez., 13:51, Ian Parker <ianpark...@xxxxxxxx> wrote:

In fact this would be required if we wanted to use these numbers as individuals for some applications, because we cannot address any number which has an infinite complexity. I think this is undisputed. I am not so sure however, that this requirement is satisfied "for most numbers" as you seem to believe. If you are right, then Kolmogorov was wrong.

Regards, WM– Hide quoted text –

Of course there are. To take a trivial example we can repeatedly multiply in a pseudoprime modulus. With anything like large numbers (1024 bits or so) it is extremely difficult (by extremely difficult I mean impossible with present knowledge) to reconstruct them. Apply an exclusive OR and you have an unbreakable code (essentially a one time pad). There are also modular functions that have the same property.

Of course. But please don't misunderstand me. I believe that there are very many very large natural numbers, or infinite sequences, which can be constructed (and therefore also be addressed or identified) by means of short rules.

One aside – why aren't these used for standard encryption? The beauty of RSA is that it is set up with a public key and can be set up without having to travel or give the code in plain text. Enigma worked fine until you had to say "Die Radstellung ist ....." in plain text. These generating functions therefore have to be set up using RSA.

In theoretical Kolmogorov terms the fact that you can't easily find the simplest form does not invalidate the fact that the Kolmogorov complexity is low. Your estimate of the complexity of a set of numbers

Re: Anyone wanna help with a compression routine (new type)

depends on where it came from.

I am interested in the set of \*all\* natural numbers. (In order to minimize the problem use the set of numbers between  $10^{10^{100}}$  and  $10^{10^{101}}$ .) Why do I ask? We know any conceivable program consists of far less than  $10^{78}$  bits (the number of hydrogen atoms in the universe). Therefore we can say: Unless it is possible to construct a number by such a program, we will never have a chance to use it in any mathematical sense. Hence it would be a fairly "useless" claim if we claimed that such a number existed.

Could it be shown however that we can construct every natural number (by a program of less than  $10^{78}$  bits) then we could uphold this claim.

Regards, WM

.