

Re: Why unhashing is not possible?

Re: Why unhashing is not possible?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2007-12/msg00072.html>

- *From:* "Sebastian G." <seppi@xxxxxxxx>
 - *Date:* Thu, 27 Dec 2007 12:08:08 +0100
-

Barry Margolin wrote:

In article <[k1hcj.12858\\$vd4.5964@pd7urf1no](mailto:k1hcj.12858$vd4.5964@pd7urf1no)>, roberson@xxxxxxxxxxxxx (Walter Roberson) wrote:

In article <[uvgcj.20007\\$wy2.19474@edtnps90](mailto:uvgcj.20007$wy2.19474@edtnps90)>, Unruh <unruh-spam@xxxxxxxxxxxxxxxx> wrote:

"Sebastian G." <seppi@xxxxxxxx> writes:

Barry Margolin wrote:

How could the hash possibly be guaranteed to be unique?

For a limited set of inputs, this is very easy.

Yes, then it is not a hash. It may be an encryption, or a translation.

http://en.wikipedia.org/wiki/Perfect_hash_function

<http://burtleburtle.net/bob/hash/perfect.html>
"Minimal perfect hashing"

I've never seen Perfect Hashing referred to as an encryption or translation, only ever as a "hash function".

These are not the kind of hashing that the OP is talking about. He's asking about cryptographic hashes, which are claimed to be non-reversible.

The OP asked about non-reversible hashes, which are not just the cryptographic hashes.

Re: Why unhashing is not possible?

Re: Why unhashing is not possible?

In this case, an important reason for the non-reversibility is that they're many-to-one.

Which is true for only the set of inputs, not arbitrary subsets of inputs.

The word "hash" is used in a number of different contexts in computer science, you have to be careful not to confuse them.

Nonsense, it's always the same: A hash is a function $A^* \rightarrow B^m$ for fixed alphabets A and B and a fixed integer m.