

## Re: Why unhashing is not possible?

---

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.misc/2007-12/msg00065.html>

---

- *From:* "Sebastian G." <[seppi@xxxxxxxxxx](mailto:seppi@xxxxxxxxxx)>
  - *Date:* Wed, 26 Dec 2007 02:41:39 +0100
- 

Unruh wrote:

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.

A hash is a function of  $A^* \rightarrow B^m$  for a fixed value of  $m$ . Nothing else.

A very interesting example would be: Take the first 12 bytes of the input (pad with zero if necessary), concatenate it with the SHA1 checksum of the input. This hash has a length of 256 bit, is cryptographically collision-resistant, yet leaks information and for any message up to 12 byte is trivially invertible.

This is only true for cryptographic hashes.

That was what he said, in the parts you erased.

You were the first to talk about cryptographic hashes. The OP just talked about hashes, and hashes serve a wide variety of purposes other than cryptography.

.