

## Re: Probably naive question – SHA1 + MD5 combination

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-08/msg01688.html>

---

- *From:* "Christian Siebert" <[iBBiS@xxxxxx](mailto:iBBiS@xxxxxx)>
  - *Date:* 31 Aug 2006 01:51:08 -0700
- 

Multiple hash functions isn't a good idea.

What if we can find a set of hash functions that can be proven to be independent? Can't we combine them to create a stronger hash function?

Simple example: Let's take the four hash functions {HAVAL-160, RIPEMD-160, SHA-1 and Tiger(2)-160}, and let's assume that they are independent (it's very likely that they are not!).

All of them take a message as input and produce a 160 bit message digest as output. The output of the combined hash could be calculated using XOR: 'C(M) = (H(M) + R(M) + S(M) + T(M)) mod 2<sup>160</sup>'.

If the assumption would be true, then isn't breaking this combined hash as difficult as breaking all of the used hashes separately? Provided that at least 1 out of those 4 hashes remains invulnerable, the combined hash should be invulnerable too. Or in other words: an attacker needs to break all 4 hashes to break the combined hash.

Is this approach correct? If yes, how difficult would it be to prove independence of hash functions?

Christian

.