

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

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-08/msg01687.html>

---

- *From:* Kristian Gjøsteen <kristiag+news@xxxxxxxxxxxx>
  - *Date:* Thu, 31 Aug 2006 07:34:47 +0000 (UTC)
- 

Shamus Husheer <s.husheer@xxxxxxxx> wrote:

For example, if the function  $\text{SHA1}(\text{data} + \text{MD5}(\text{data}))$  were used (i.e. append the MD5 of the data to the data, and take the SHA1 of the combination), would it be a lot harder to find collisions?

No. You find a collision in SHA-1, say  $x_0$  and  $x_1$ , then you simply choose random messages  $y$  until  $\text{MD5}(x_0 || y) = \text{MD5}(x_1 || y)$ , which by the birthday paradox is feasible. Then

$$\text{SHA-1}(x_0 || y || \text{MD5}(x_0 || y)) = \text{SHA-1}(x_1 || y || \text{MD5}(x_1 || y))$$

Multiple hash functions isn't a good idea.

PS. You need to deal with some padding stuff as well, but that's easy.

—  
Kristian Gjøsteen

.