

Re: SHA1 Question

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-03/2422.html>

From: Michael Amling (*nospam_at_nospam.com*)

Date: 03/31/05

Date: Thu, 31 Mar 2005 04:16:10 GMT

Igor Tebelev wrote:

- > *Suppose I have some unknown sequence of 7 bytes.*
- > *Those bytes are encrypted using SHA1 which produces 20 bytes hash value*
- > *Of those 20 bytes first 12 are known.*
- >
- > *So, the question is: having first 12 bytes of SHA1 result is there anyway to*
- > *find original 7 bytes sequence used to produce that SHA? Brute force*
- > *solution is not acceptable: I'm looking for something fast. Any references*
- > *would be appreciated.*

Someone will correct me if I'm wrong, but AFAIK, brute force is the fastest way to find SHA-1 pre-images. If some sequences of 7 bytes are more likely than others (which you could not find out just from looking at the hash), try them first.

--Mike Amling