Subject: Reversing Hashing Algorithums
Posted by gibberish on Sat, 24 Apr 2004 17:20:07 GMT
View Forum Message <> Reply to Message

It has been stated several times that is is not possible to reverse a CRC hash to get back to the original file.

While in principal this is true, one theme that occurs repeatedly in encryption based technologies is that great care has to be taken in order to ensure some of the golden rules are not broken.

Generally hashes cannot be reversed simply because for any hash value there is a large (possibly infinite) number of possible source values.

This does not hold true when the length of the source text is known or known to be less than a given number. At this point there is a finite number of possible source keys, additionally given the length of the Renegade key it is likely that less than 10 possible source keys would be present for a given hash.

At a minimum a CRC based hash could be broken with a brute force attack, in order to retrieve the set of possible source keys.

Additionally the CRC hash has published flaws which means that a skilled cryptographer could probably do better than an brute force attack.