Lab on Attack on Digital Signature/Hash Collision

Find two messages with the same hash value.

1. Select “Analysis” \“Hash” \“Attack on the Hash Value of the Digital Signature” from the menu.

2. Click “Options”.

Options for the Attack on the Hash Value of the Digital Signature

- Hash function: Choose a hash function and the minimum required number of matching bits for the attack to be considered successful.
  - MD2
  - MD4
  - MD5
  - SHA
  - SHA-1
  - RIPEMD-160
  - Significant bit length: 40 (0: default, 1 - 128)

- Options for the modification of messages: Determine the way messages are modified throughout the attack.
  - In block and out of line
  - Double blocks
  - Insert characters
  - Delete characters (demonstration)
  - Unprintable characters

Start search / Set options: Click “Start search” to initiate the attack. The program will search for modifications of the two messages that hash to the same value. The message will not appear to change, since only unprintable characters will be used to modify them. In the “Options” you can select the hash function, the required minimum number of matching bits, and the message modification method.
3. Choose **MD5** under **Hash function** and **40** for **Significant bit length**, and click **Apply**.

4. click “**Start Search**” in dialog of **Attack on the Hash Value of the Digital Signature**.

5. click “**OK**” and “**Print Statistics**”.

6. After modifying the two messages, the hash value of them are the same. The message will not appear to change, since only unprintable characters will be used to modify them.
A 72-bit partial collision (i.e., the first 72 hash value bits are identical) was found in a couple of days using a single PC. Today signatures with hash values of 128 bits or less are vulnerable to a massive parallel search. It is therefore recommended to use hash values with a length of at least 160 bits.