Exercise 1

10/08/2021

Hash functions for verifying the integrity of files or messages

One of the well-known applications of hash functions is for verifying the integrity of files or messages. (See https://en.wikipedia.org/wiki/Cryptographic_hash_function under applications)

a) Make use of any online tool such as http://www.fileformat.info/tool/hash.htm to compute the MD5, SHA-1, SHA-256 hash values of the two strings given below

1) The quick brown fox jumps over the lazy dog

2) The quick brown fox jumps over the lazy dogs

Note that the two strings above are slightly different yet their hash values are quite different.

b) Perform hash calculations for any TWO files of your choice using the following hash functions: Adler32, CRC32, Haval, MD2, MD4, MD5, RipeMD-128, RipeMD-160, SHA-1, SHA-256, SHA-384, SHA-512, Tiger, and Whirlpool.

c) Collision

Consider the two postscript files at

http://web.archive.org/web/20071226014140/http://www.cits.rub.de/MD5Collisions/

Are the two files identical?

Now compute the MD5 hash values for each of them. Are they equal? If so why does this happen?

See more examples at https://www.mscs.dal.ca/~selinger/md5collision/

Screenshots must be included in your submission.

Note: Questions a) and b) carry equal marks