CSE 4004

Digital Forensics

Lab
Session 1

TOPIC: Hash functions for verifying the integrity of files or messages

---

Name: Makesh Srinivasan
Registration number: 19BCE1717
Slot: L49 + L50
Date: 5-Aug-2021-Thursday
Faculty: Prof. Nagaraj

Q1) 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)

Question:
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

A	
1)	The quick brown fox jumps over the lazy dog

Hash Function:

Results	
Original text	The quick brown fox jumps over the lazy dog
Original bytes	54686520717569636b2062726f776e20666f78206a756d7073... (length=43)
Adler32	5bdc0fda
CRC32	414fa339
Haval	713502673d67e5fa557629a71d331945
MD2	03d85a0d629d2c442e987525319fc471
MD4	1bee69a46ba811185c194762abaeae90
MD5	9e107d9d372bb6826bd81d3542a419d6
RipeMD128	3fa9b57f053c053fbe2735b2380db596
RipeMD160	37f332f68db77bd9d7edd4969571ad671cf9dd3b
SHA-1	2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
SHA-256	d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592
SHA-384	ca737f1014a48f4c0b6dd43cb177b0afd9e5169367544c494011e3317dbf9a509cb1e5dc1e85a941bbee3d7f2afbc9b1
SHA-512	07e547d9586f6a73f73fbac0435ed76951218fb7d0c8d788a309d785436bbb642e93a252a954f23912547d1e8a3b5ed6e1bfd7097821233fa0538f3db854fee6
Tiger	6d12a41e72e644f017b6f0e2f7b44c6285f06dd5d2c5b075
Whirlpool-0	4f8f5cb531e3d49a61cf417cd133792ccfa501fd8da53ee368fed20e5fe0248c3a0b64f98a6533cee1da614c3a8ddec791ff05fee6d971d57c1348320f4eb42d null
Whirlpool-T	3ccf8252d8bbb258460d9aa999c06ee38e67cb546cffcf48e91f700f6fc7c183ac8cc3d3096dd30a35b01f4620a1e3a20d79cd5168544d9e1b7cdf49970e87f1
Whirlpool	b97de512e91e3828b40d2b0fdce9ceb3c4a71f9bea8d88e75c4fa854df36725fd2b52eb6544edcacd6f8beddfea403cb55ae31f03ad62a5ef54e42ee82c3fb35

A	
2)	The quick brown fox jumps over the lazy dogs

Hash Function

Results	
Original text	The quick brown fox jumps over the lazy dogs
Original bytes	54686520717569636b2062726f776e20666f78206a756d7073... (length=44)
Adler32	6c29104d
CRC32	444a08a0
Haval	90f0ea27177be192c52b5387f3523d54
MD2	ae742161d556aaa73ad11e4476c06cf2
MD4	6839dd600c6d4c84f8be3932723b97ad
MD5	3ee6f92b7cddc3f50b7d2ddd145b018b
RipeMD128	bea078ae5684e4b9e28514020ea9d699
RipeMD160	af7a2e207b3f7a664363aab46d724e354929d992
SHA-1	f8c3c541257a6c31f6fbc697a50f46d9fc8bcc30
SHA-256	1be9a63751d3af7ffa65b21ccc58d2b89eda7011d7fee2bb9229a74085f8eb2e
SHA-384	42f0aff2ecf3a112a05447ce4cd8b1b84f82b2217272a6746436d48759a1fc479d457ec297057c2dcbb60a0d8f40fbbf
SHA-512	0d52e77f1b76539a224c47af2326b32f5226add715dd7d08b31f1a9c37484f708c9a3ba26fdd2e6857ea43df641553b4fc941b2617b635ecea4003e290ee2236
Tiger	aecc43841d11ab953319aa618cad9e476569bac3b6fe53d8
Whirlpool-0	34071469b0319eb3e8341e7110f17bb5bfc12fcbe6f19ad1c0a358165e54ccd4c2df7bc36fb00e8f3452fc4a809b94db6580e2395d8838664f1bb430f83f2bb5 null
Whirlpool-T	54e414b570fc650266bfde731392225692452ef85ad37cb77bb9040a2b0dd5fa40bde48d4dcffa349424cbb1f346859fe91f7d353b3c21af5335f6cc97f99852
Whirlpool	fce26948c23fefe70c8a94327b081c1cd2c4a33485a8e9bbf0e420a4a2b92a89c80de89b3a53525990c0794e46d88fb78cb50d51f8144b60b5401142d3978eb0

The two strings above are slightly different, yet their hash values are quite different as shown above in the images.

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.

B	
1)	File 1: image1.png

Results	
Original text	*(binary only)*
Original bytes	89504e470d0a1a0a0000000d49484452000003f60000021808... (length=883758)
Adler32	861b460c
CRC32	b0bd3204
Haval	000e8f76195fdfb6319907f0da7fcd21
MD2	cd515e4148c31fe7dde154d88226a6e9
MD4	b2291e7554d252a7e3e47a333990ed02
MD5	51b728d737c3b3982d426eaeefaf4a55
RipeMD128	d42d50d93eb845a8e1cf4a1cb66e079c
RipeMD160	bcd602573a91961768a8fca3292046c4aefae6a9
SHA-1	4010a1d790c6b803dff4fbce1cae59bab2ef063a
SHA-256	243b30a2301bdb6f241bebc2b7f3860602fe97563d03d50de9cc08849971233a
SHA-384	53d899b4972106aaa9672301623fb70daadebed44d4a8567a3ea97b9c4c7cd5eceabee5f1f0d1eff054f86c393d7bbfd
SHA-512	a2e1f826b167b8a84aea4ca55a1c98ec31e7f0a2d2df94b0da13eeb179107ee6fecfe0879c6ea451dd22cef73ee08810126eef990e3a4e1d4fc32d9ad2de4863
Tiger	492d491656db1aa9737cea16a8a9cd69607c0e591e4bbacc
Whirlpool-0	6ad754ca79b5d9ea8e163370d8fedd8773bd162cfea6778184be253b6d30e3d74890edd9756c64beb4103d1907468e3a1b77a2000e308792057ccec70921e164null
Whirlpool-T	a79da94a4b20c229683ca05e3caca8918b152f7ab85085e0c2f476499d405e19e8b8f673603c48b21080631f4fe22016d0d8c4c6d61a61c5840033ee5ee1d93f
Whirlpool	5dc75f6ed393d42718d178da8e630e6e34c971b9ec27dda44ffe0d26ebefe7e5416054e7f9b6d330c1c95082fcd35a9433a376f9a33773c4146d9425f01c4d98

B	
2)	File 2: image2.png

Results	
Original text	*(binary only)*
Original bytes	89504e470d0a1a0a0000000d49484452000002ec0000036408... (length=1752633)
Adler32	54e6906d
CRC32	1f10c203
Haval	e80a8474d6942f227f2d3b77dc047986
MD2	db013a228ce48aac1896246fb57ea4f3
MD4	0919a0ac817fa4b661205b9cee55b99e
MD5	6ba0da7b834ff7ef6e35f8efc3de98a0
RipeMD128	f0660bf8178cab67c920a5c0161416f8
RipeMD160	fddcee0f80f97c963ff798a36594d98c805fdb62
SHA-1	30412e83ec5bbda276ebf8e5d8ae7933bcf4c27b
SHA-256	343f66b8c62ba3ee183c66e55d0e24a7b894b2dc9fdb9101e19de2e04006a4ef
SHA-384	646a8984f8ccd345b1158af9ab1f71e3e608d6be67410058c9bbc8e3457310f7902385753edd38cf4b1033d754809967
SHA-512	edf05902fa7c04da80bfb540a99200392755ce6fee71805862a1e7f3709b5bcfe38d43ec312724bfb3ca71f2b188b39071a12313ba442b1a5a5204b6a424d7e3
Tiger	2dae118fa477b917057451bff20b59ba1b6d171940134783
Whirlpool-0	5026abb0499ff9ac1bbb2bcb31e96c02a88fcbd3d58d2a0c666b8c8aa39f10b832957b551b82eb35ffa82367d54cf78b9620ba0b030cc71f5e5517c249375c7e null
Whirlpool-T	418bfc38473c81c3a4778ad8728f4b3739487fcd08a2557686d7c1038d792e7a6d57379a49c723f4680bd9dff5f2a1d984f1feeb71f7c65ee660d4526c65ac95
Whirlpool	9ee1a7e48221177c36ee85839e8c37433f9864385a4254444d327adc79d4098d75653781110c5a1b0b9face48199160bcaa96198c804df5df3af4662f735d7a8

C) Collision

Consider the two postscript files at http://web.archive.org/web/20071226014140/http://www.cits.rub.de/MD5Collisions/

1) Are the two files identical?
2) 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.

C)1)	Are the two files identical?
	File 1: order.ps Julius. Caesar Via Appia 1 Rome, The Roman Empire May, 22, 2005 Order: Alice Falbala is given full access to all confidential and secret information about GAUL. Sincerely, Julius Caesar

C)1)	Are the two files identical?
	File 2: letter_of_rec.ps
	Julius. Caesar Via Appia 1 Rome, The Roman Empire May, 22, 2005 To Whom it May Concern: Alice Falbala fulfilled all the requirements of the Roman Empire intern position. She was excellent at translating roman into her gaul native language, learned very rapidly, and worked with considerable independence and confidence. Her basic work habits such as punctuality, interpersonal deportment, communication skills, and completing assigned and self-determined goals were all excellent. I recommend Alice for challenging positions in which creativity, reliability, and language skills are required. I highly recommend hiring her. If you'd like to discuss her attributes in more detail, please don't hesitate to contact me. Sincerely, Julius Caesar
	As shown above, the two files are clearly different in print. Hence, they are **not** identical.

C)2)	Now compute the MD5 hash values for each of them. Are they equal? If so why does this happen?
	File 1: order.ps
	MD5 value of file 1: MD4 47559a9efd3205bb2fa26f31b012803a MD5 a25f7f0b29ee0b3968c860738533a4b9 a25f7f0b29ee0b3968c860738533a4b9
	File 2: letter_of_rec.ps
	MD5 value of file 2: MD4 9679de1bc1526a891530b2242f305407 MD5 a25f7f0b29ee0b3968c860738533a4b9 a25f7f0b29ee0b3968c860738533a4b9
	As shown above, the MD5 values of both the files (order.ps and letter_of_rec.ps) are exactly the same. NOTE: To show that the files uploaded to check this are different, I have pasted the screenshot of MD4 as well, and they are distinct whereas, MD5 are not

Question: Why does this happen?

Answer:

Collision occurs when two distinct files produce the same hash value for a given hash-function. MD5 is a 128 bits encryptor, and even though the probability of collision is extremely less (2^{128} different combinations), it is not impossible. Even though the file may be seeming distinct, the meta data of the two files when hashed may produce an identical message digest. This can affect the evaluation of integrity of files; however, it can be easily avoided by using 2 or more hashing functions or hash-functions with longer bit length. In the above scenario, since I took MD4 and MD5 hash values it was possible to infer that they were indeed distinct files, which would not have been possible with only one hashing function - MD5.
