Now using the Online Hash Calculator, calculate the hash values of *message.txt* file and write the result in the following table.

|  |  |
| --- | --- |
| **Hash Algorithm** | **Hash Value** |
| MD5 | 0cc175b9c0f1b6a831c399e269772661 |
| MD4 | bde52cb31de33e46245e05fbdbd6fb24 |
| SHA1 | 86f7e437faa5a7fce15d1ddcb9eaeaea377667b8 |
| SHA256 | ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb |
| SHA384 | 54a59b9f22b0b80880d8427e548b7c23abd873486e1f035dce9cd697e85175033caa88e6d57bc35efae0b5afd3145f31 |
| SHA512 | 1f40fc92da241694750979ee6cf582f2d5d7d28e18335de05abc54d0560e0f5302860c652bf08d560252aa5e74210546f369fbbbce8c12cfc7957b2652fe9a75 |

Now change the contents of *message.txt* and replace “a” with “A” which means that you are changing only 1 bit inside the contents of the *message.txt* file because “a” is represented by ASCII code 01100001 whereas “A” by 01000001. Calculate the hash value of this file again with new contents and fill the following table.

|  |  |
| --- | --- |
| **Hash Algorithm** | **Hash Value** |
| MD5 | 7fc56270e7a70fa81a5935b72eacbe29 |
| MD4 | d5ef20eeb3f75679f86cf57f93ed0ffe |
| SHA1 | 6dcd4ce23d88e2ee9568ba546c007c63d9131c1b |
| SHA256 | 559aead08264d5795d3909718cdd05abd49572e84fe55590eef31a88a08fdffd |
| SHA384 | ad14aaf25020bef2fd4e3eb5ec0c50272cdfd66074b0ed037c9a11254321aac0729985374beeaa5b80a504d048be1864 |
| SHA512 | 21b4f4bd9e64ed355c3eb676a28ebedaf6d8f17bdc365995b319097153044080516bd083bfcce66121a3072646994c8430cc382b8dc543e84880183bf856cff5 |

Change the text of file with “Lahore Leads University”, calculate its hash values again and fill the following table. Now change the text to “Lahore Leads university”, calculate its hash value and fill in the second column. Please note that you have changed only 1 bit in the text, i.e. changed “U” of University to “u” of university. You can verify this by representing these strings in binary format using any hex editor.

|  |  |  |
| --- | --- | --- |
| **Hash Algorithm** | **Hash Value of “Lahore Leads University”** | **Hash Value of “Lahore Leads university”** |
| MD5 | bb55dc8df657cb105fa8be903ccfa1ee | d15d982129e1ea78a974561450ab910c |
| MD4 | a08034546b113193f1af57d227fd1017 | 62bdbec1d4abd06669da3c8f2e1304cd |
| SHA1 | 83452d3318fd6486f2de111a48cbda3fa9da4584 | 3818a842e9e6e953b487471562a31513f322644e |
| SHA256 | 547103776a84133fd665daca737b5559a54c535b12dc770674497e494c3cf965 | d05a9441221616c36c550d256cc7bcc33cce0acebe11d6dcbe064cd110fd295e |
| SHA384 | 973f389652e60c71c14eac3ce54d4d0996ec36641c1f2d18f29ccc2b5e4bb7e2afb9b2eb34cb4b6669fd689c340dda77 | ba9fb795338a3173c002ff5bb52475025ba6622c71e0d4a01402109c0aa47c70bf309c8bac99a813fcd7fbc55b6a2a1b |
| SHA512 | 19af5f416e78ac57757db4422727eaf663f216b7daf9b347ab34a95ebebcca929624dc705f4872bcbff13411e113d083c0f849a5588756775be0415e4561c1e0 | 021fbfcba176d2646699d9acb291cc44ad19fe2c9b7f053985963ccd803669240a690343faff714385da3d876387c5fb8d9d21b8cec72ce5a933ad06ce1c63c7 |

1. There is only 1-bit of difference between the ASCII codes of “U” and “u” in “Lahore Leads University” and “Lahore Leads university”. “U” is represented by ASCII code 01010101 and “u” by 01110101. It means that there is only 1-bit of difference between the two messages. Looking at the difference between input messages and their corresponding hash values, write what you conclude about the Hash functions according to the properties given above in description. Write your analysis in not less than 200 words. **(5)**

**Ans 6** : The thing we observed for two values is the length of both the ouputs are same and the ouputs are different we can say they are unique for given word or character.

'U'= 01010101

'u'= 01110101

There is no collision as the output value of each input is different and unique . So, these hash function can be safely used for encryption and we can have key value pair for the given characters. It will be difficult for the hacker to get the pattern easily to decode the hash. With the help of hash functions it will be very easy to search in the given group of number because every number have a unique hash code of their own by which you can search .

We can surely say hash functions are computationally hard to reverse. If a hash function h produced a hash value z, then it is very difficult process to find any input value x that hashes to z as there are many functions that exist so you cannot actually decode it without hard computation.

Now calculate the hash values of both pdf files provided with this midterm exam i.e. *shattered-1.pdf* and *shattered-2.pdf*, and fill in the following table.

|  |  |  |
| --- | --- | --- |
| **Hash Algorithm** | **Hash Value of *shattered-1.pdf*** | **Hash Value of *shattered-2.pdf*** |
| MD5 | ee4aa52b139d925f8d8884402b0a750c | 5bd9d8cabc46041579a311230539b8d1 |
| MD4 | 38373b377cf16c032d08cef0855cb820 | 4881d13b4265c952a9ed032ea4a1a043 |
| SHA1 | 38762cf7f55934b34d179ae6a4c80cadccbb7f0a | 38762cf7f55934b34d179ae6a4c80cadccbb7f0a |
| SHA256 | 2bb787a73e37352f92383abe7e2902936d1059ad9f1ba6daaa9c1e58ee6970d0 | d4488775d29bdef7993367d541064dbdda50d383f89f0aa13a6ff2e0894ba5ff |
| SHA384 | 27f937a0849be559affa109f97744024bc494b2b81dcd9684845cd14574953cc6310398b89e150ad3819188309e59996 | e04944841a251d5bbed5dbb0d07486d254bcddd2c11341ee9bb045bfd678aa7b784e1b7a7d56ece5d5ede17e143ffe2b |
| SHA512 | 3c19b2cbcf72f7f5b252ea31677b8f2323d6119e49bcc0fb55931d00132385f1e749bb24cbd68c04ac826ae8421802825d3587fe185abf709669bb9693f6b416 | f39a04842e4b28e04558496beb7cb84654ded9c00b2f873c3ef64f9dfdbc760cd0273b816858ba5b203c0dd71af8b65d6a0c1032e00e48ace0b4705eedcc1bab |

1. Now these two files are entirely different. Do you notice any strange behavior of any of the Hash functions? If yes, what is the malfunctioning behavior and what are your suggestions about that algorithm? Write your analysis in not less than 200 words. **(5)**

**Ans 7 :**