**DIGITAL FORENSICS LAB**

|  |  |
| --- | --- |
| Exercise 1 | |
| Name | S Shyam Sundaram |
| Registration Number | 19BCE1560 |
| Slot | L39+L40 |
| Faculty | Dr. Seshu Babu Pulgara |
| Date | 10th August, 2021 |

**AIM**

To verify the integrity of files or messages using Hash functions

**PART 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

MD5: 9e107d9d372bb6826bd81d3542a419d6

SHA-1: 2fd4e1c67a2d28fced849ee1bb76e7391b93eb12

SHA-256: d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592

1. The quick brown fox jumps over the lazy dogs

MD5: 3ee6f92b7cddc3f50b7d2ddd145b018b

SHA-1: f8c3c541257a6c31f6fbc697a50f46d9fc8bcc30

SHA-256: 1be9a63751d3af7ffa65b21ccc58d2b89eda7011d7fee2bb9229a74085f8eb2e

1. the quick brown fox jumps over the lazy dog

MD5: 5e48a737eaff799917707b2815af10fc

SHA-1: cbf88a749e1a87a236bee745f842f462b97e374f

SHA-256: b779f6eaff679cbf30b4b784c76eb04abda965800fe2e40f1f47b0a89177fe19

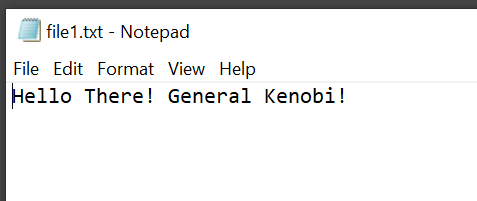
**OBSERVATIONS**

* For a unique string, the hash value will too, be unique.
* Even a difference of one character (the presence or absence too) can result in a completely different hash value (sentence 1 and 2).
* The case of the characters affects the hash value too. Even the change in case of one letter can result in a completely different hash value (sentence 3).
* Different hash functions and algorithms give a different hash value for the same input.
* The length of the hash value produced by MD5, SHA-1 and SHA-256 result in 32-, 160- and 256-bit long hash values, independent of the length of the input.

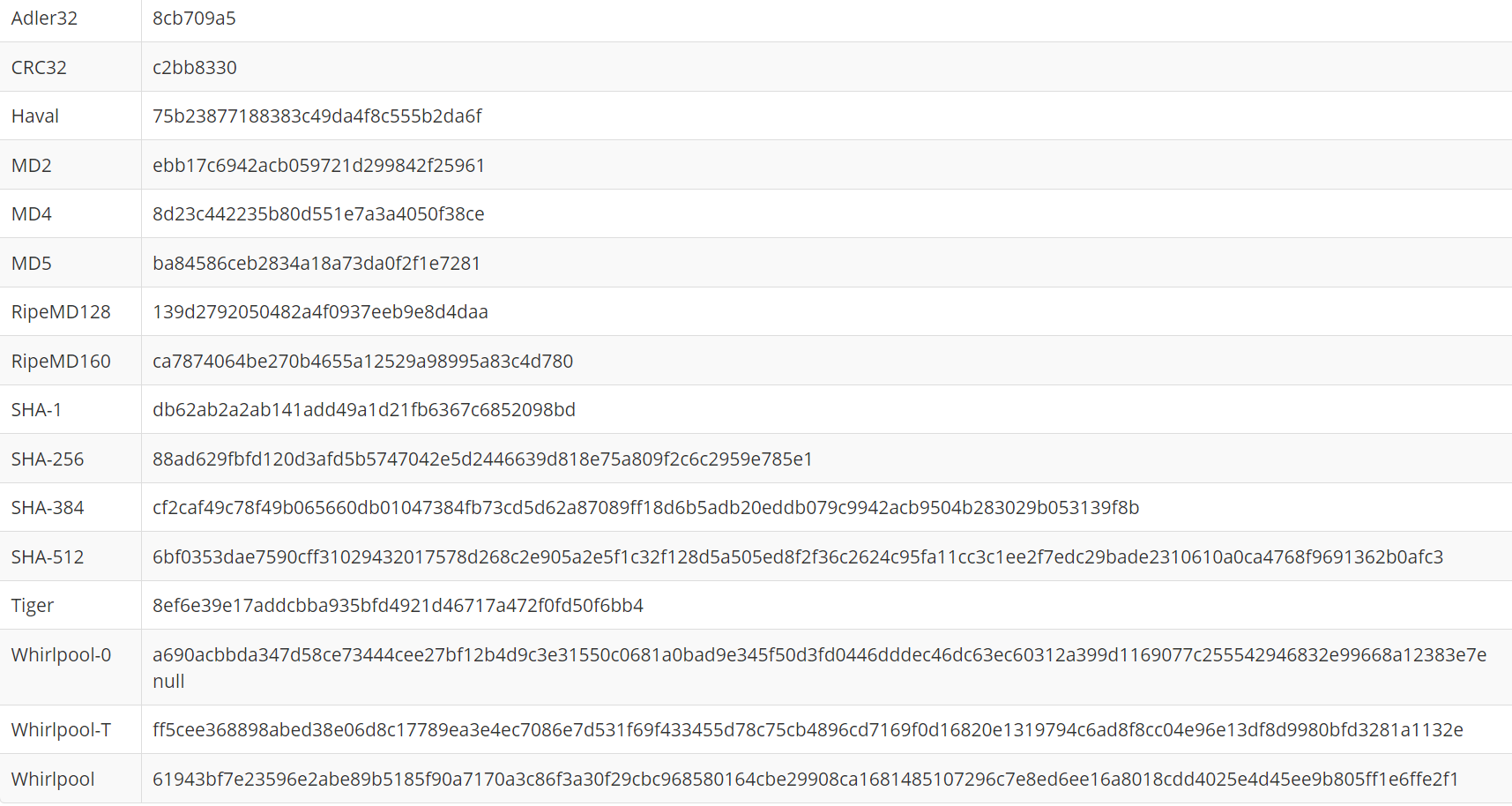
**PART B**

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.

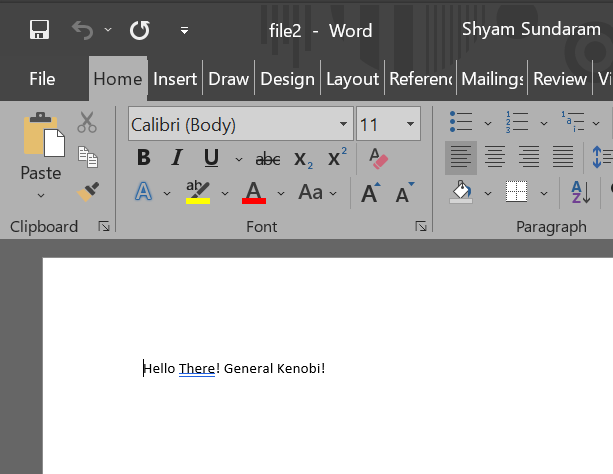
File 1: file1.txt



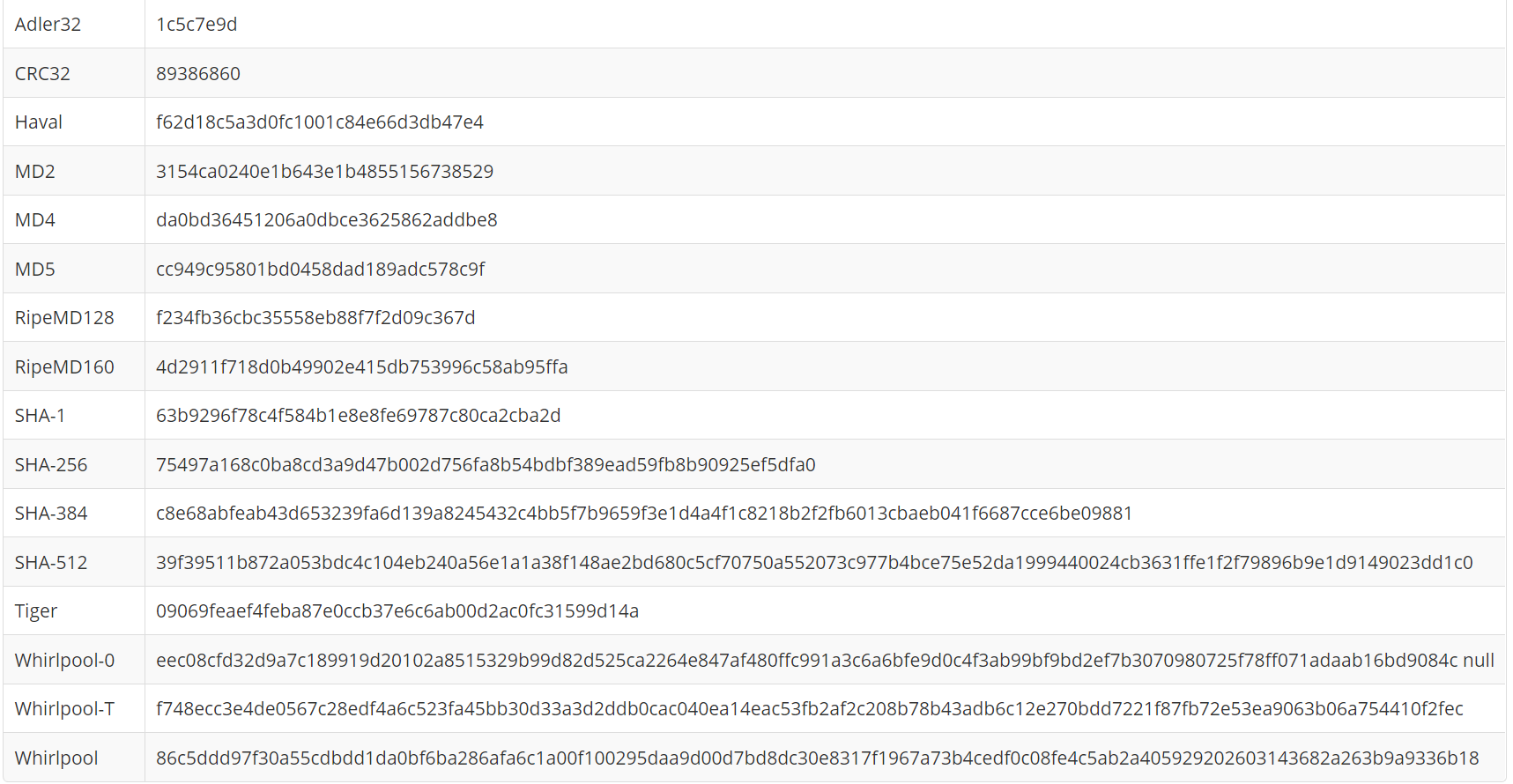
Hash Values:



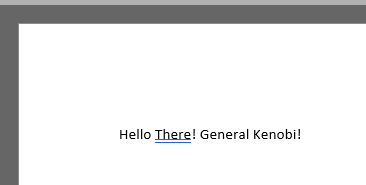
File 2: file2.docx



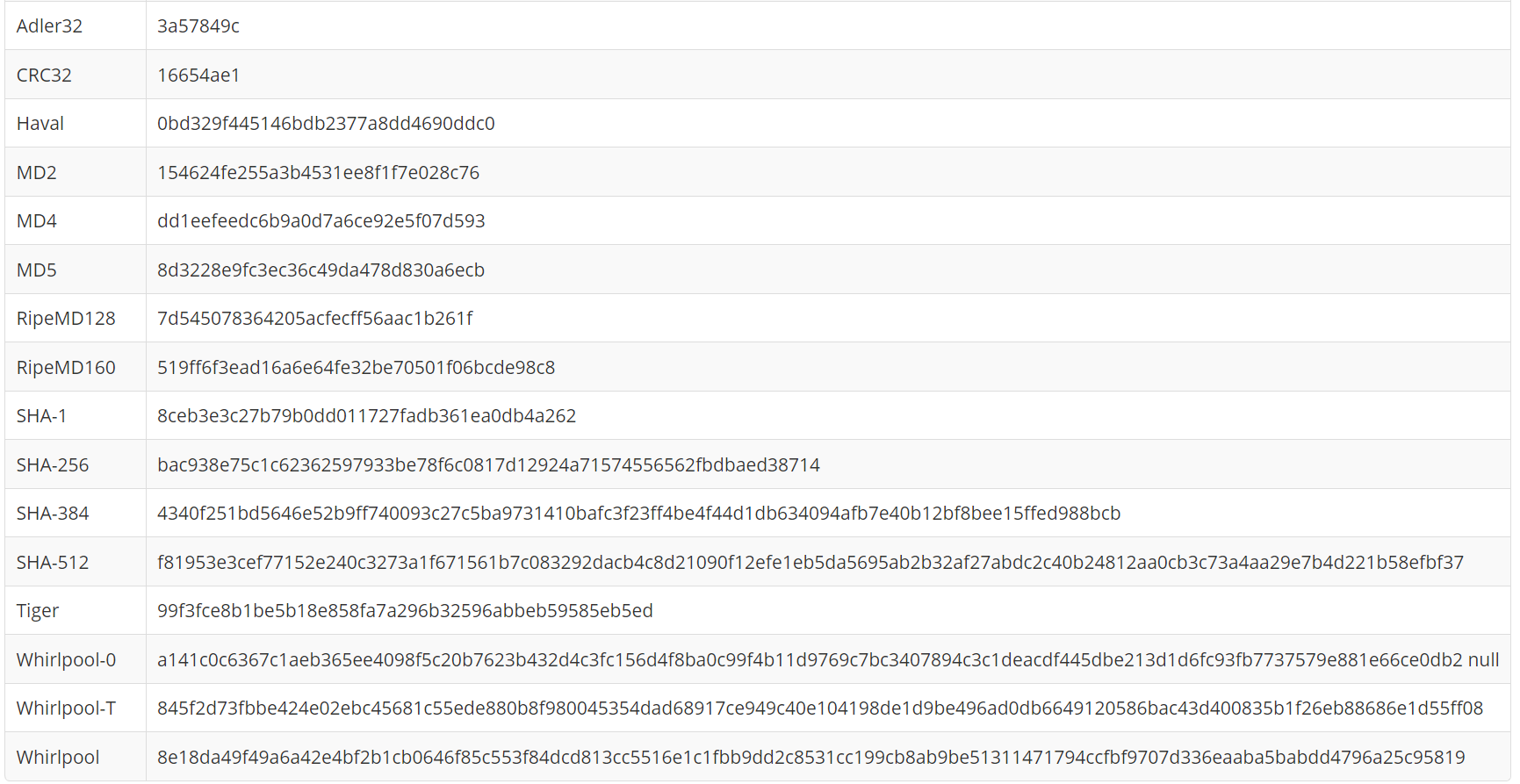
Hash Values:



File 3: file2.docx (The same file content. But the file was deleted and the content was copy pasted to a new document with the same name and extension. Thus, essentially, the same file)



Hash Values:



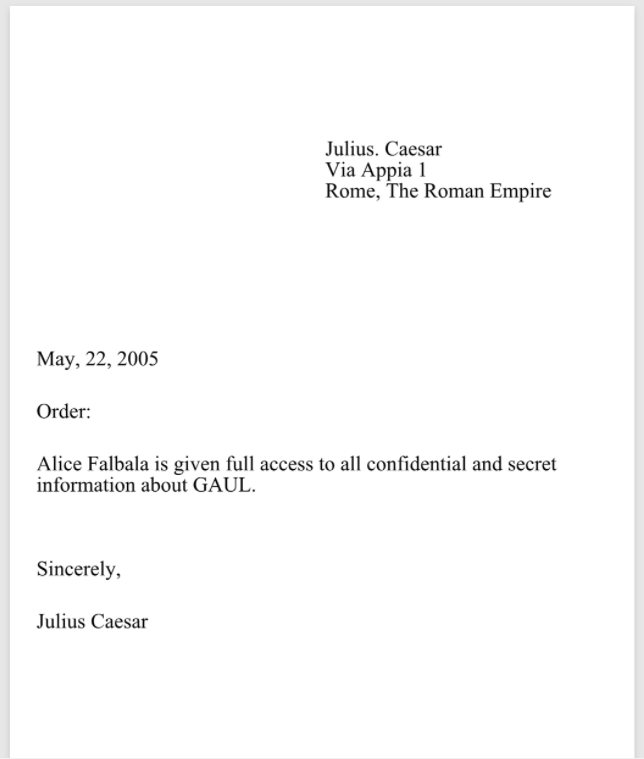
**OBSERVATIONS**

* The same observations from part A are seen here. Length of the hash values (of MD5, SHA-1 and SHA-256) are independent of the input length (or type). Also, a minute difference in data can give very different hash values.
* Though file1 and file2 have the same content, they are of different file types. One is a text file while the second is an MS Word docx file. Yet, they yield distinct hash values. Thus, files of different type yield different hash values.
* Another very interesting observation is made. File 2 was deleted and another with the same name and type was created. The content was also the same (as seen in input 2 and 3 above). But they still return two different hash values. This indicates that the algorithms implemented use the metadata of the files too (here, it may be the time of creation). Thus, two files created separately no matter how similar, yield two different hash values.

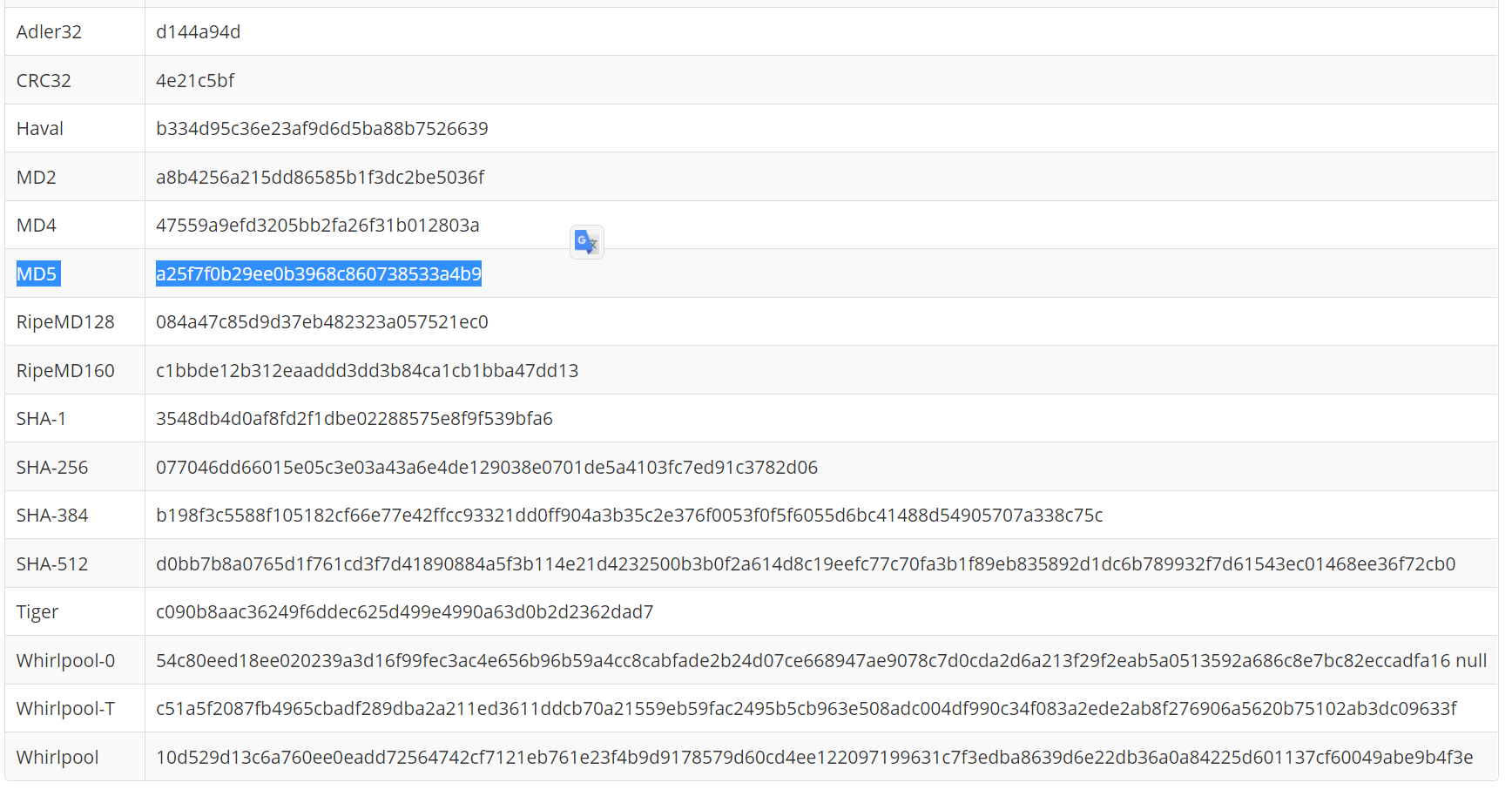
**PART C**

Two files shown below are different. These are passed as input to the MD5 hash function.

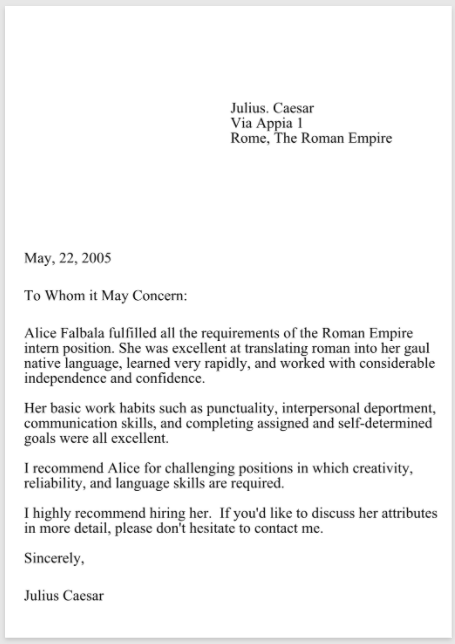
File 1: order.ps



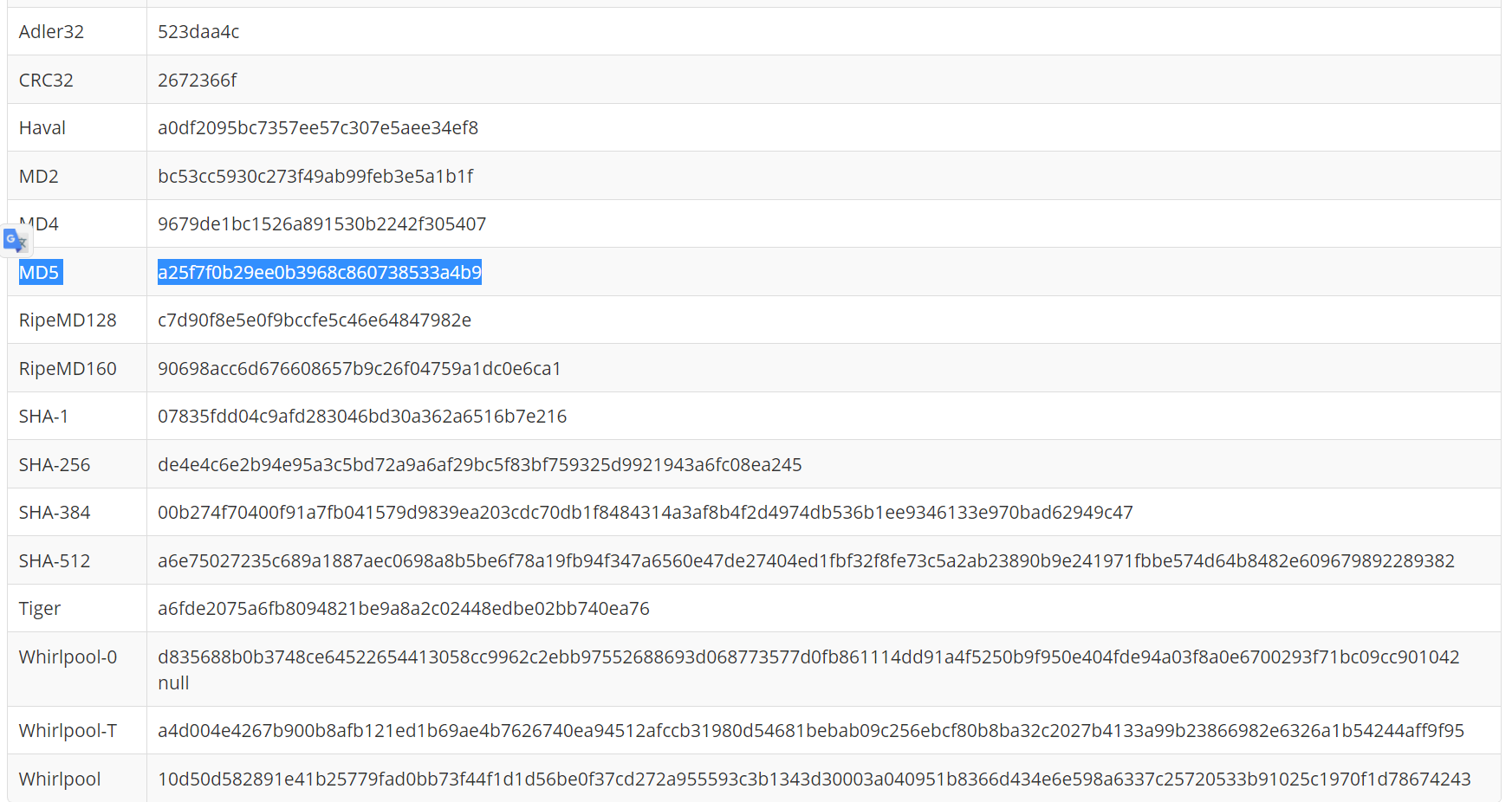
Hash Values:



File 2: letter\_of\_rec.ps



Hash Values:



**OBSERVATIONS**

* Both these files are different in every way: from their names to the contents. Yet, they still yield the same hash value for MD5. Other algorithms result in different hash values. This is what is called as a ‘collision’.