

**NETWORK SECURITY**

**PROJECT PART 2 – HASHING AND BITCOIN MINING**

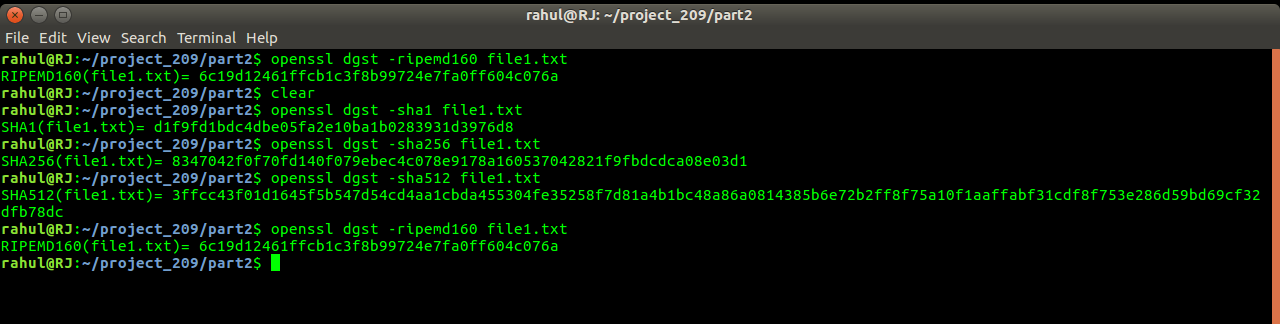
**RAHUL DILEEP JADHAV – 010687638**

**IFUNANYA NNOKA - 010754159**

**TASK 1: Generating Message Digest and MAC**

|  |  |  |
| --- | --- | --- |
| Hashing Algorithm | Hash Obtained | Length |
| SHA1 | d1f9fd1bdc4dbe05fa2e10ba1b0283931d3976d8 | 20 bytes |
| SHA256 | 8347042f0f70fd140f079ebec4c078e9178a160537042821f9fbdcdca08e03d1 | 64 bytes |
| SHA512 | 3ffcc43f01d1645f5b547d54cd4aa1cbda455304fe35258f7d81a4b1bc48a86a0814385b6e72b2ff8f75a10f1aaffabf31cdf8f753e286d59bd69cf32dfb78dc | 128 bytes |
| Ripemd160 | 6c19d12461ffcb1c3f8b99724e7fa0ff604c076a | 20 bytes |

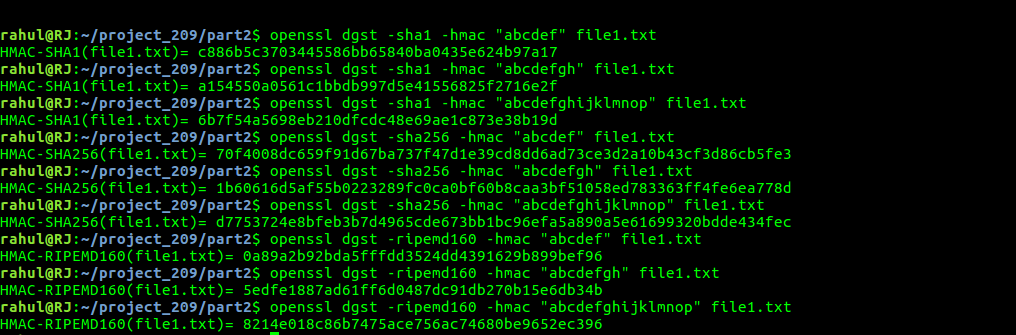
**Snapshot:**

****

**Task 2: Keyed Hash and HMAC**

|  |  |  |
| --- | --- | --- |
| Key Size | Hashing Algorithm | Output |
| 6 | SHA1 | c886b5c3703445586bb65840ba0435e624b97a17 |
| 8 | a154550a0561c1bbdb997d5e41556825f2716e2f |
| 16 | 6b7f54a5698eb210dfcdc48e69ae1c873e38b19d |
| 6 | SHA256 | 70f4008dc659f91d67ba737f47d1e39cd8dd6ad73ce3d2a10b43cf3d86cb5fe3 |
| 8 | 1b60616d5af55b0223289fc0ca0bf60b8caa3bf51058ed783363ff4fe6ea778d |
| 16 | d7753724e8bfeb3b7d4965cde673bb1bc96efa5a890a5e61699320bdde434fec |
| 6 | RIPEMD160 | 0a89a2b92bda5fffdd3524dd4391629b899bef96 |
| 8 | 5edfe1887ad61ff6d0487dc91db270b15e6db34b |
| 16 | 8214e018c86b7475ace756ac74680be9652ec396 |

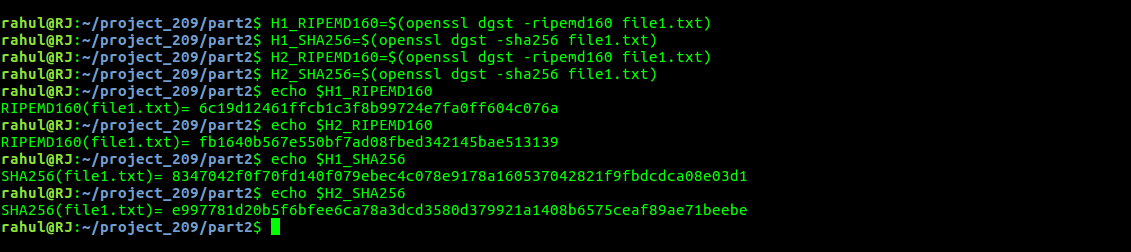
**Snapshot:**



**Task 3: The Randomness of Hash**

|  |  |
| --- | --- |
| H1 using RIPEMD160 | 6c19d12461ffcb1c3f8b99724e7fa0ff604c076a |
| H2 using RIPEMD160 | fb1640b567e550bf7ad08fbed342145bae513139 |
| H1 using SHA256 | 8347042f0f70fd140f079ebec4c078e9178a160537042821f9fbdcdca08e03d1 |
| H2 using SHA256 | e997781d20b5f6bfee6ca78a3dcd3580d379921a1408b6575ceaf89ae71beebe |

**Snapshot:**

****

**Observation:**

By changing a single bit of the file, hash value changes by a significant level.

Content of the file before bit manipulation : “This is a test file used for hashing!”

Content of the file after bit manipulation: “Qhis is a test file used for hashing!”

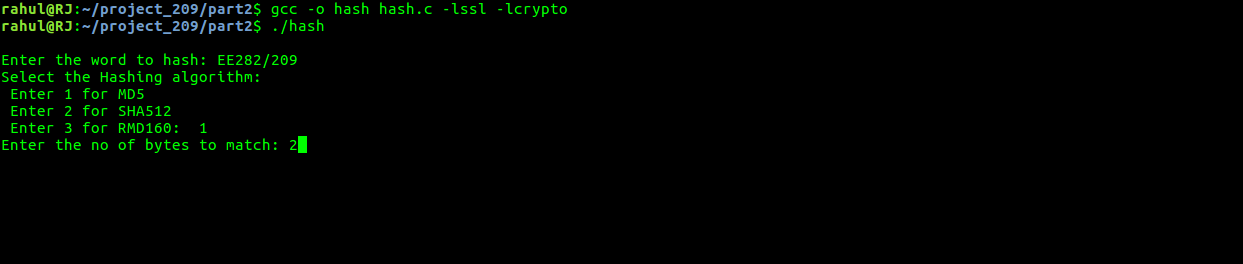
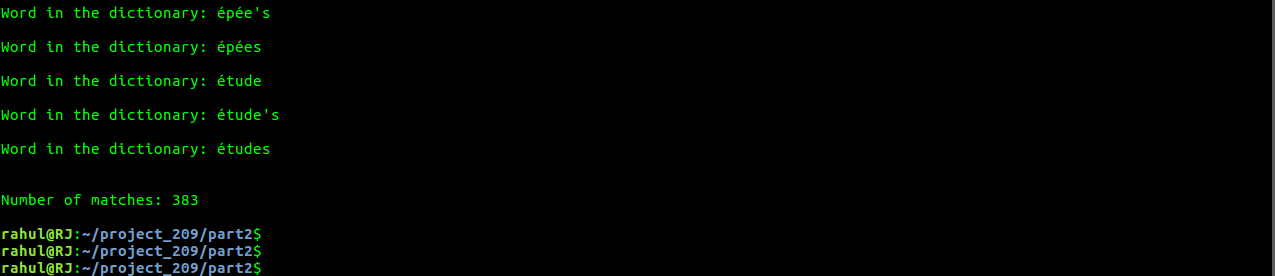
There is no significant change in the content after manipulation of single bit, but there is a great deal of variation in the hash value of the same file (please lookup the snapshot).

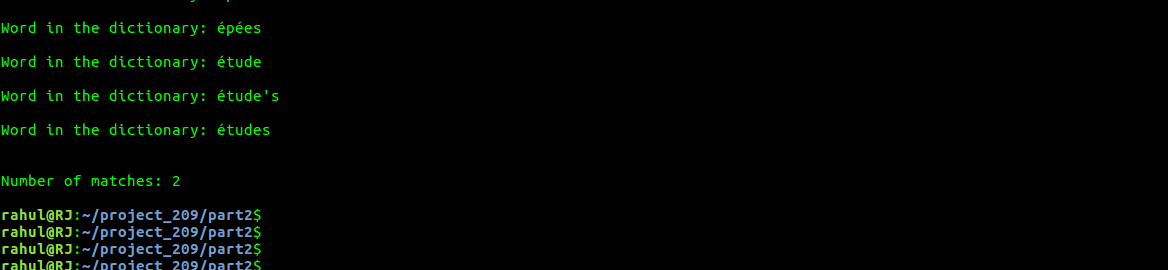
This show the property of high reliability on hashing algorithms.

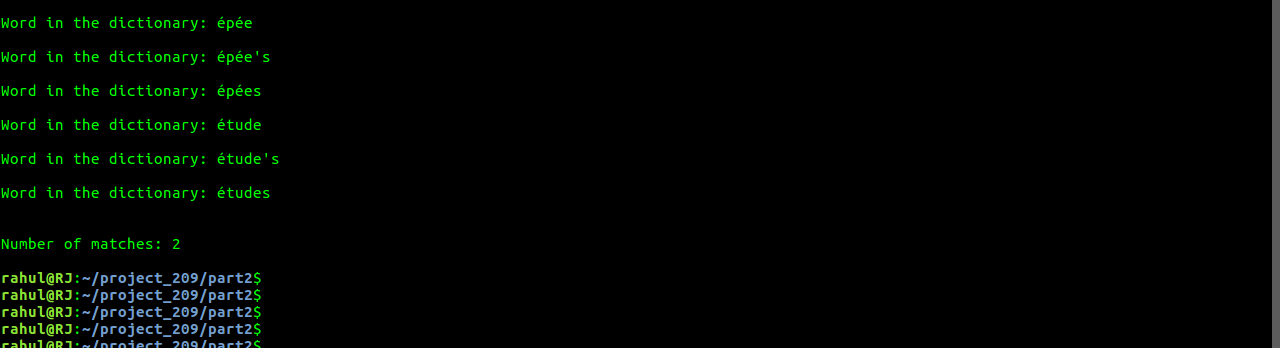
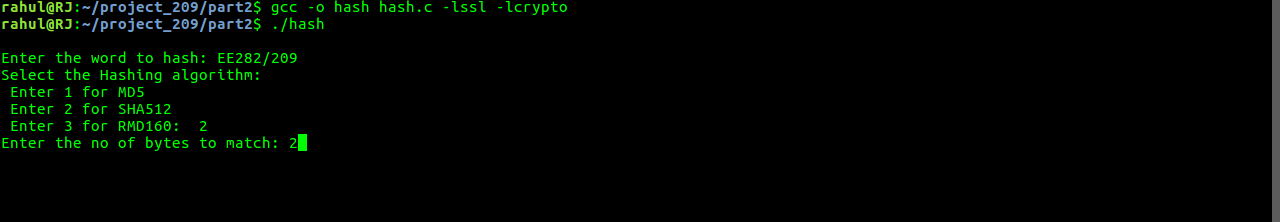
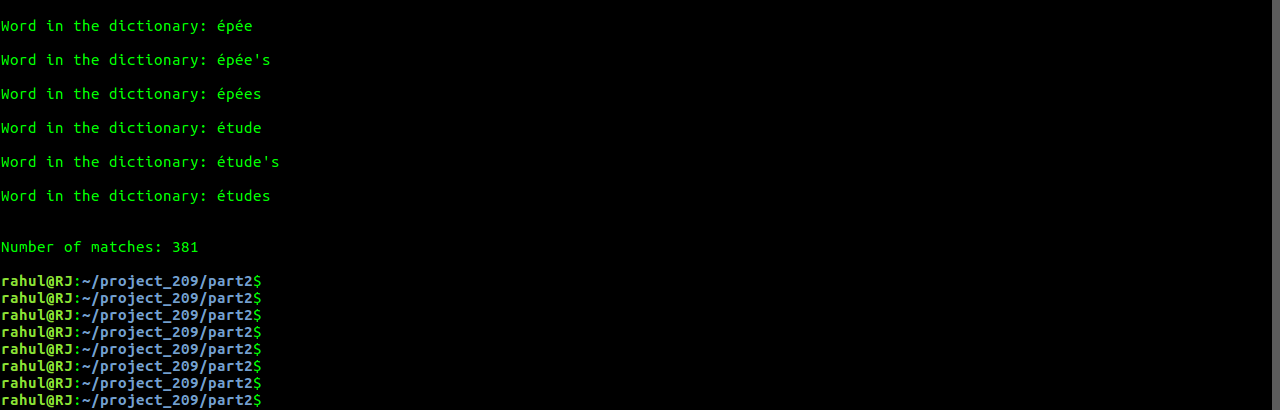
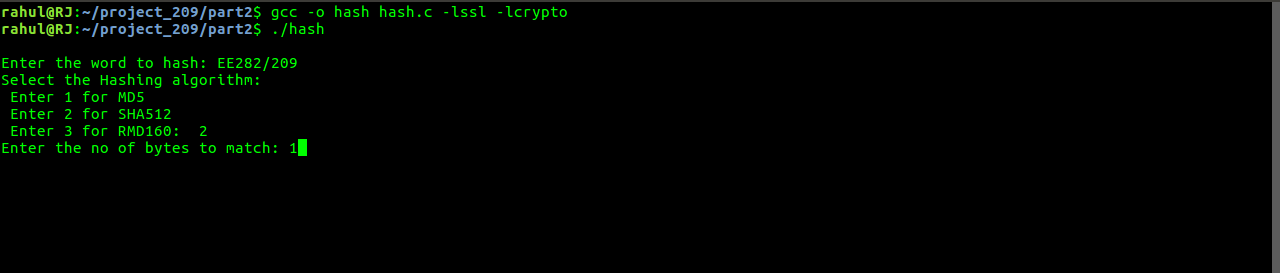
**Task 4: Testing One-Way and Collision Properties**

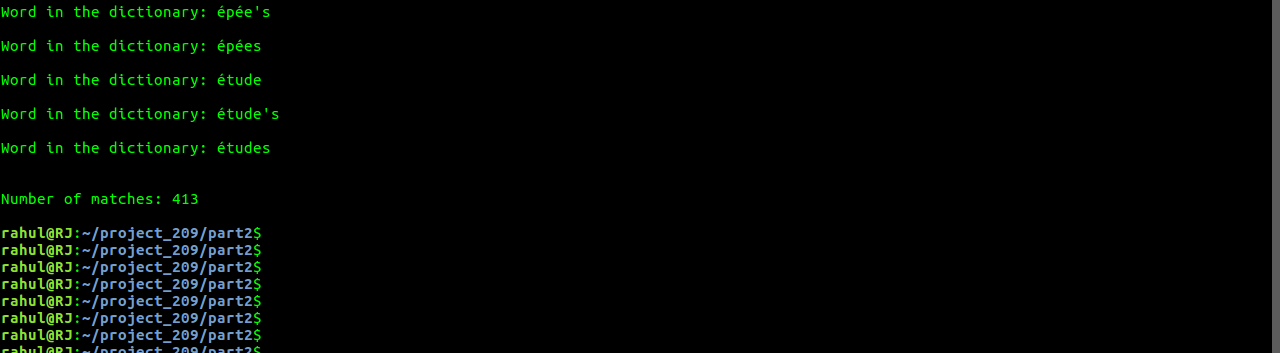
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Test | Hashing Algorithm | Plain Text | Bytes to match | Number of matches |
| 1 | MD5 | EE282/209 | 1 | 383 |
| 2 | MD5 | 2 | 2 |
| 3 | SHA512 | 1 | 381 |
| 4 | SHA512 | 2 | 2 |
| 5 | RMD160 | 1 | 413 |
| 6 | RMD160 | 2 | 1 |

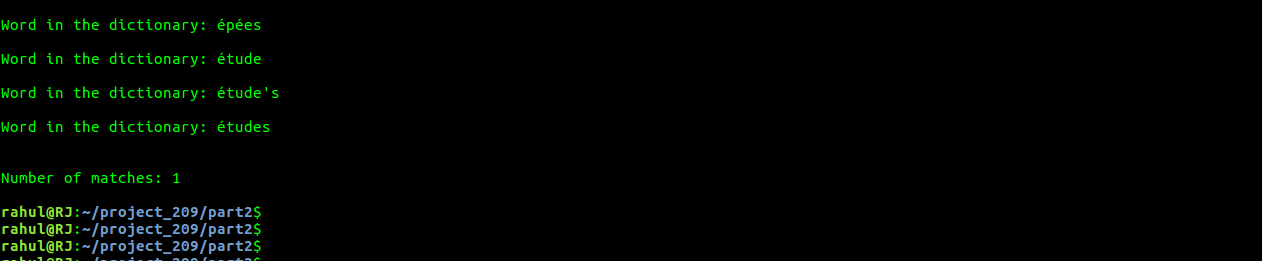
**Snapshots:**



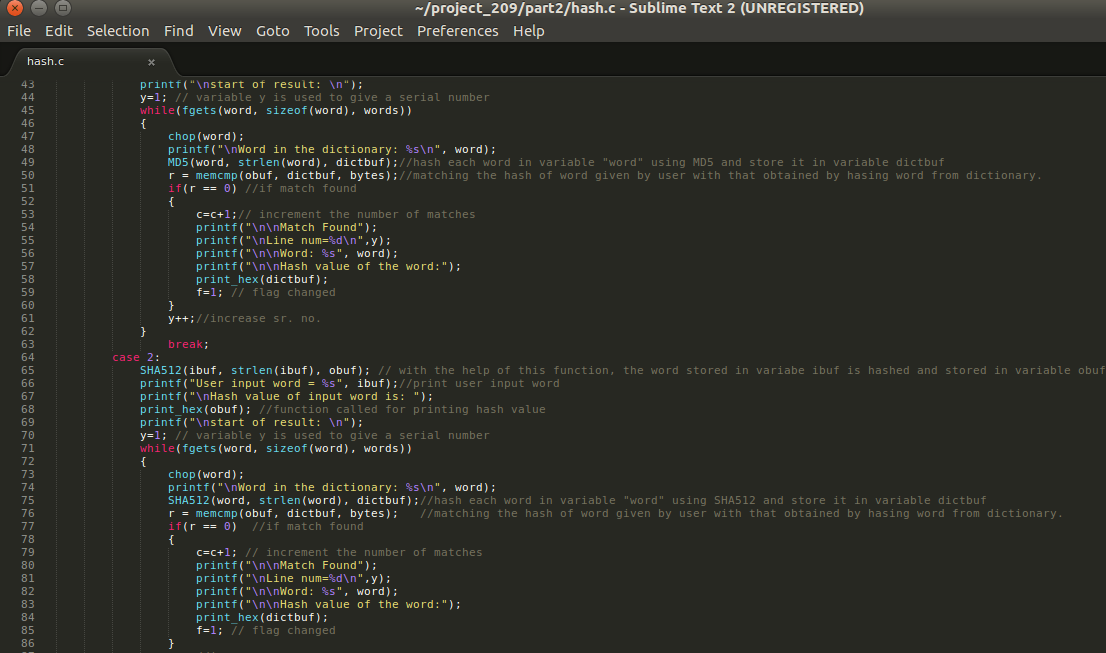
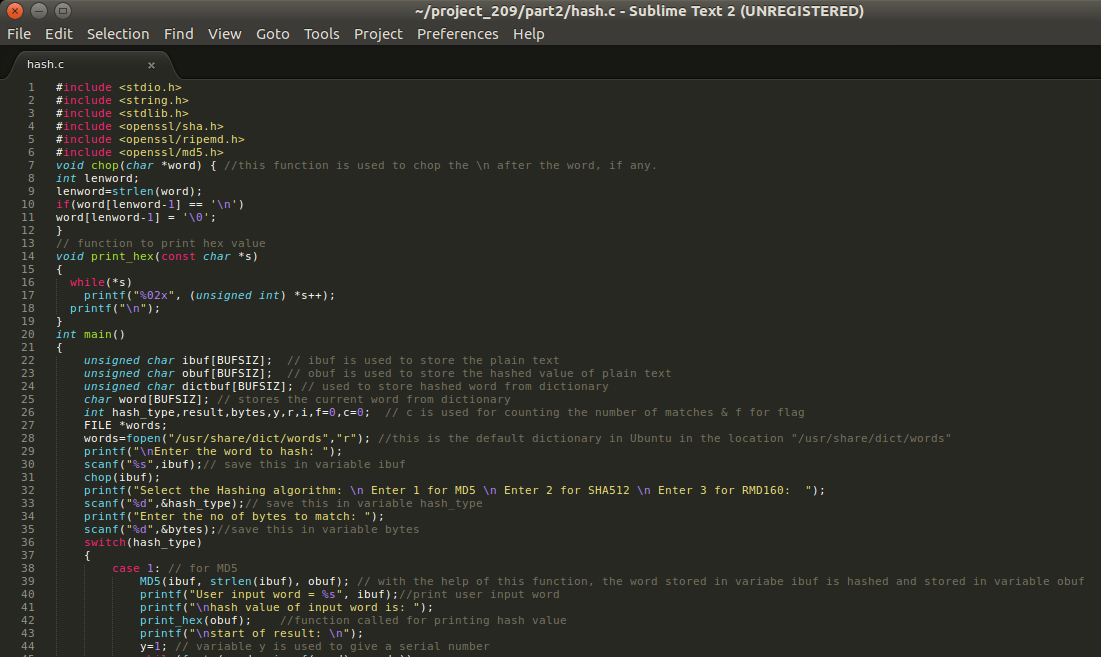


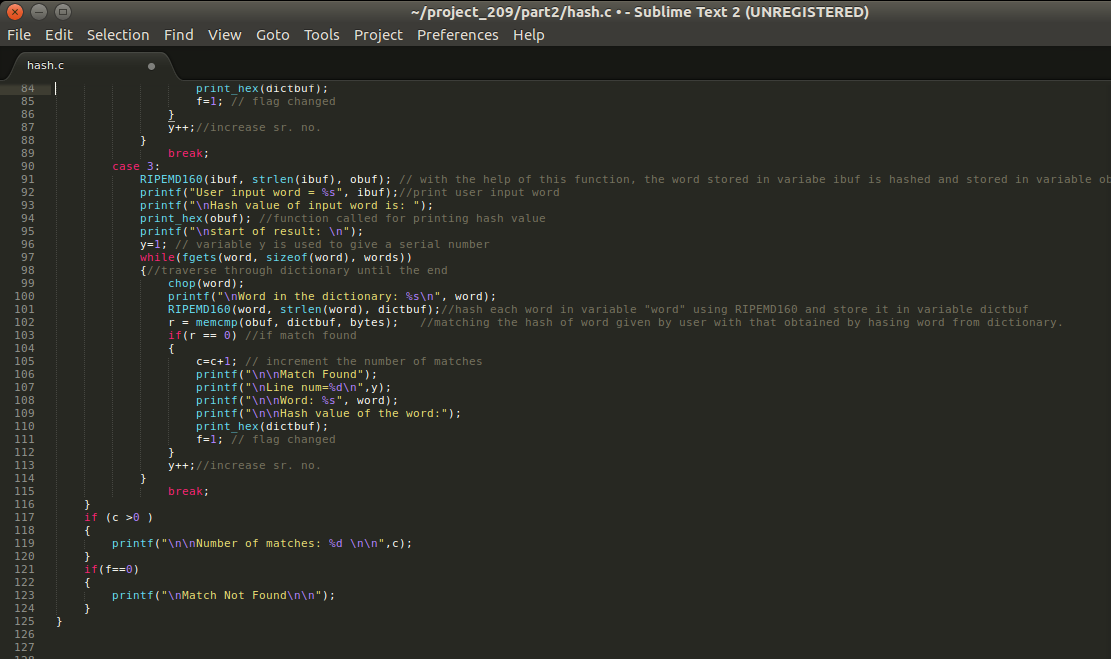






**Snapshot of the C program:**

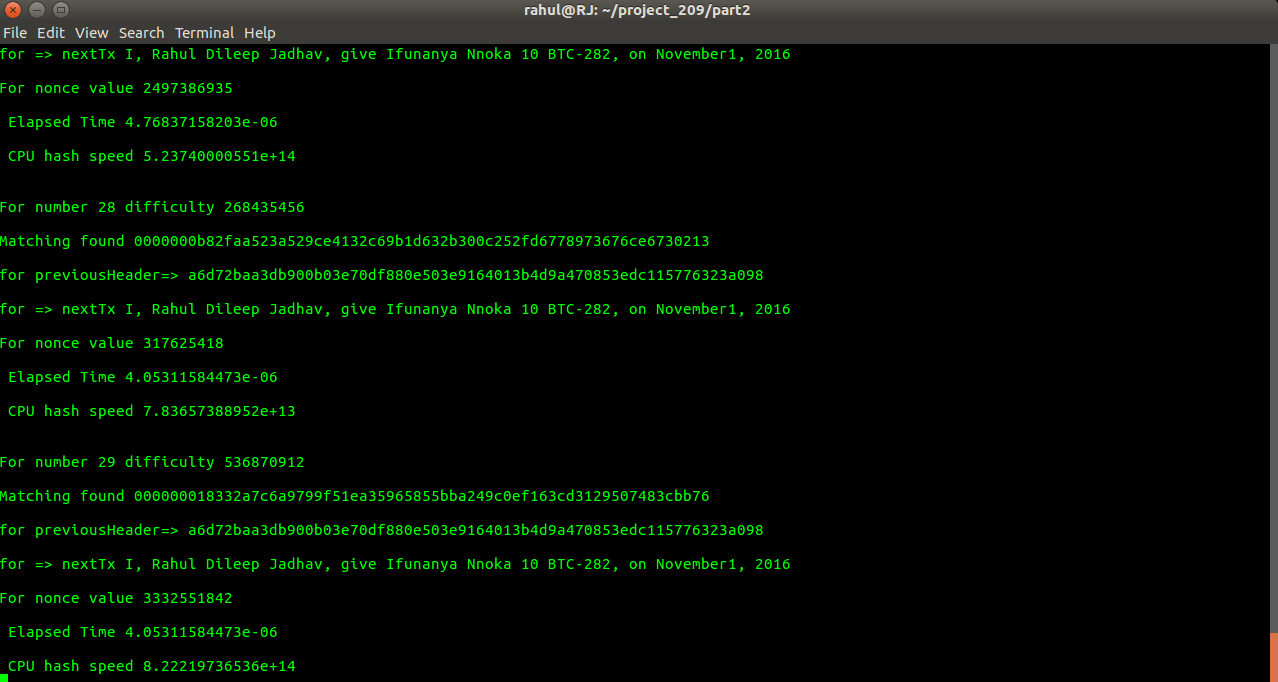




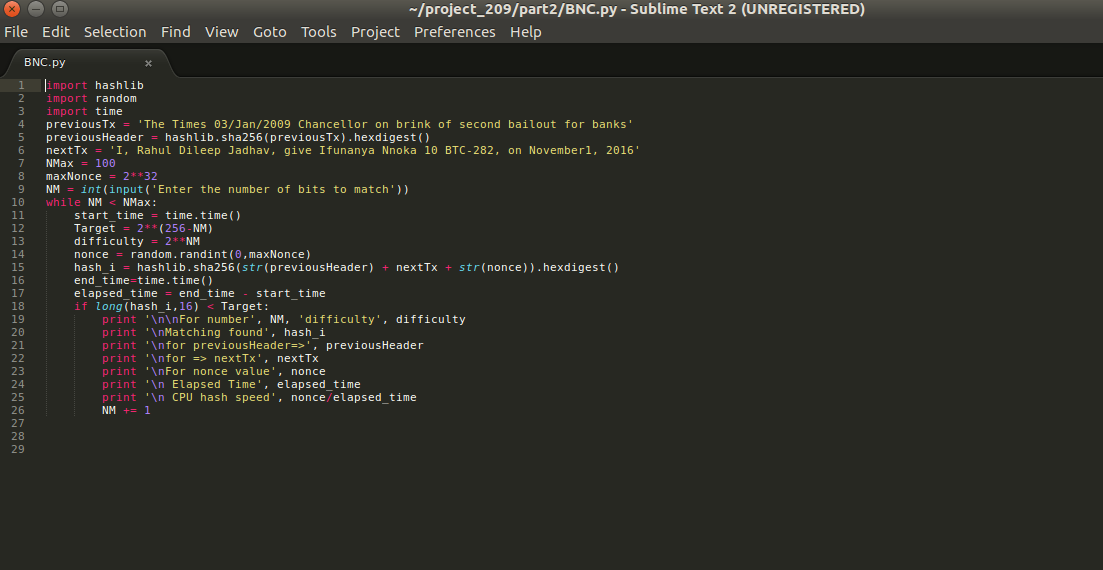
**Task 5: Hashing in BTC: Mining and Proof of Work**

|  |  |  |  |
| --- | --- | --- | --- |
| Difficulty (bits) | Nonce | Elapsed Time | Hashing Power |
| 5 | 1723032166 | 1.50203704834e-05 | 1.14713027079e+14 |
| 6 | 1853853988 | 1.59740447998e-05 | 1.16054137273e+14 |
| 7 | 2885163516 | 1.69277191162e-05 | 1.70440181349e+14 |
| 8 | 3753710614 | 1.50203704834e-05 | 2.49907991161e+14 |
| 9 | 863625665 | 6.91413879395e-06 | 1.24907192456e+14 |
| 10 | 1053279933 | 5.00679016113e-06 | 2.10370296957e+14 |
| 11 | 2989863909 | 5.00679016113e-06 | 5.97161816808e+14 |
| 12 | 3570061074 | 5.00679016113e-06 | 7.13043878234e+14 |
| 13 | 1611936480 | 5.00679016113e-06 | 3.2195007742e+14 |
| 14 | 983437071 | 5.00679016113e-06 | 1.96420668602e+14 |
| 15 | 213476051 | 4.05311584473e-06 | 5.26696149773e+13 |
| 16 | 653407631 | 4.05311584473e-06 | 1.61211190608e+14 |
| 17 | 852796033 | 5.00679016113e-06 | 1.70327895828e+14 |
| 18 | 209800217 | 4.05311584473e-06 | 5.17626993744e+13 |
| 19 | 2045340596 | 5.00679016113e-06 | 4.08513344913e+14 |
| 20 | 3407968779 | 4.05311584473e-06 | 8.40826887155e+14 |
| 21 | 1022716769 | 4.05311584473e-06 | 2.52328531476e+14 |
| 22 | 1008571563 | 5.00679016113e-06 | 2.0144074957e+14 |
| 23 | 3480565235 | 5.00679016113e-06 | 6.95168985115e+14 |
| 24 | 2370328139 | 5.00679016113e-06 | 4.7342270451e+14 |

**Snapshot:**



**Python Code:**



**\*\*Note: PreviousHeader value of this file is attached in a separate file for verifying the optional part submission**