Michael Lawrence

CSC 447.001

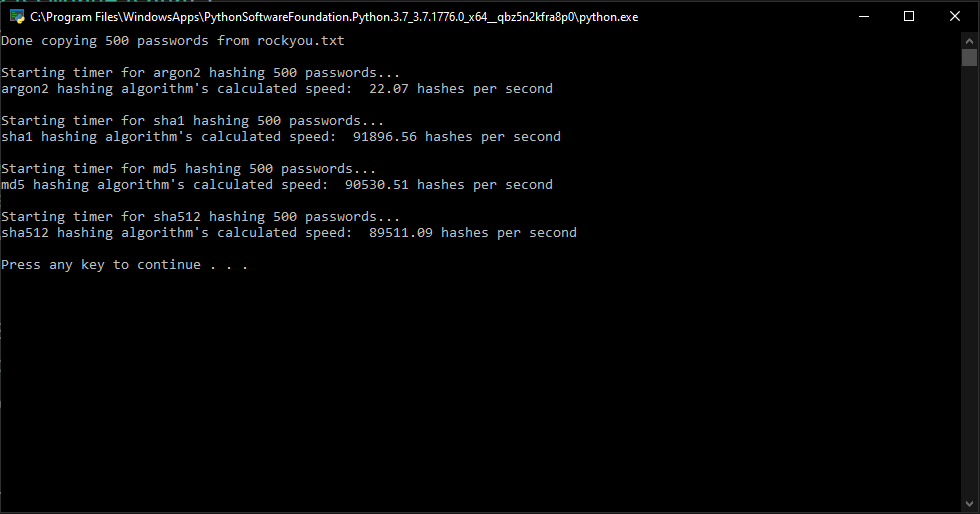
2/5/2020

Lab 1: Password Hashing

System Specs used in Test:

CPU: AMD Ryzen 7 3800x 8-Core Processor 4.20 GHz

RAM: 32.0 GB



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Argon2 | Sha1 | Md5 | Sha512 |
| Hashes/s | 22.07 | 91,189.56 | 90,530.51 | 89,511.09 |

Hashing Algorithm breakdown:

1. list = 500 passwords from rockyou.txt
2. Hashing function:
   1. Determine which hash function was called (md5, sha1, ext…)
   2. For each string stored in a specified password list:
      1. Create hash object
      2. Update hash object with byte string in list
      3. Store the hex digest in a temporary string.
3. For each hashing algorithm:
   1. Call Timer function of the timeit module to calculate time to hash list
   2. Calculate hashes per second: length of list / time