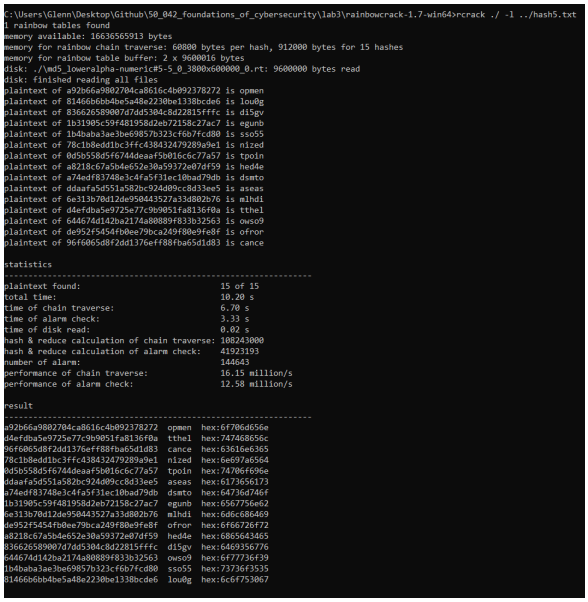
Glenn Chia 1003118 (Lab 3 Section 5)

1. Generating the salt

For this lab, to ensure consistency of the results, imported the `random` library and initialised it with a seed `random.seed(1)`. Generate the random lowercase letters with `random.choice(ascii_lowercase)`

2. Results

Time taken for **Unsalted** (Left): 10.20s. Time taken for **salted**(Right): 16.30s



```
C:\Users\Glenn\Desktop\Github\50_042_foundations_of_cybersecurity\lab3\rainbowcrack-1.7-win64>rcrack ./ -l ../hash5.txt
1 rainbow tables found
memory available: 16636565913 bytes
memory for rainbow chain traverse: 60800 bytes per hash, 912000 bytes for 15 hashes
memory for rainbow table buffer: 2 x 9600016 bytes
disk: ./md5_loweralpha-numeric#5-5_0_3800x600000_0.rt: 9600000 bytes read
disk: finished reading all files
plaintext of a92b66a9802704ca8616c4b092378272 is opmen
plaintext of 81466b6bb4be5a48e2230be1338bcde6 is lou0g
plaintext of 836626589007d7dd5304c8d22815fffc is di5gv
plaintext of 1b31905c59f481958d2eb72158c27ac7 is egunb
plaintext of 1b4baba3ae3be69857b323cf6b7fcd80 is sso55
plaintext of 78c1b8edd1bc3ffc43843247928 9a9e1 is nized
plaintext of 0d5b558d5f6744deeaf5b016c6c77a57 is tpoin
plaintext of a8218c67a5b4e652e30a59372e07df59 is hed4e
plaintext of a74edf83748e3c4fa5f31ec10bad79db is dsmto
plaintext of ddaafa5d551a582bc924d09cc8d33ee5 is aseas
plaintext of 6e313b70d12de950443527a33d802b76 is mlhdi
plaintext of d4efdba5e9725e77c9b9051fa8136f0a is tthel
plaintext of 644674d142ba2174a80889f833b32563 is owso9
plaintext of de952f5454fb0ee79bca249f80e9fe8f is ofror
plaintext of 96f6065d8f2dd1376eff88fba65d1d83 is cance

statistics
--------------------------------------------------------------
plaintext found:                    15 of 15
total time:                         10.20 s
time of chain traverse:             6.70 s
time of alarm check:                3.33 s
time of disk read:                  0.02 s
hash & reduce calculation of chain traverse: 108243000
hash & reduce calculation of alarm check:    41923193
number of alarm:                    144643
performance of chain traverse:      16.15 million/s
performance of alarm check:         12.58 million/s

result
--------------------------------------------------------------
a92b66a9802704ca8616c4b092378272  opmen  hex:6f706d656e
d4efdba5e9725e77c9b9051fa8136f0a  tthel  hex:747468656c
96f6065d8f2dd1376eff88fba65d1d83  cance  hex:63616e6365
78c1b8edd1bc3ffc43843247928a9e1  nized  hex:6e697a6564
0d5b558d5f6744deeaf5b016c6c77a57  tpoin  hex:74706f696e
ddaafa5d551a582bc924d09cc8d33ee5  aseas  hex:6173656173
a74edf83748e3c4fa5f31ec10bad79db  dsmto  hex:64736d746f
1b31905c59f481958d2eb72158c27ac7  egunb  hex:6567756e62
6e313b70d12de950443527a33d802b76  mlhdi  hex:6d6c686469
de952f5454fb0ee79bca249f80e9fe8f  ofror  hex:6f66726f72
a8218c67a5b4e652e30a59372e07df59  hed4e  hex:6865643465
8366265890070d7dd5304c8d22815fffc  di5gv  hex:6469356776
644674d142ba2174a80889f833b32563  owso9  hex:6f7736f739
1b4baba3ae3be69857b323cf6b7fcd80  sso55  hex:73736f3535
81466b6bb4be5a48e2230be1338bcde6  lou0g  hex:6c6f753067
```

```
C:\Users\Glenn\Desktop\Github\50_042_foundations_of_cybersecurity\lab3\rainbowcrack-1.7-win64>rcrack ./ -l ../salted6.txt
3 rainbow tables found
memory available: 15646212096 bytes
memory for rainbow chain traverse: 60800 bytes per hash, 912000 bytes for 15 hashes
memory for rainbow table buffer: 3 x 9600016 bytes
disk: ./md5_loweralpha-numeric#6-6_4_3800x600000_0.rt: 9600000 bytes read
disk: ./md5_loweralpha-numeric#6-6_5_3800x600000_0.rt: 9600000 bytes read
disk: ./md5_loweralpha-numeric#6-6_6_3800x600000_0.rt: 9600000 bytes read
disk: finished reading all files
plaintext of 071d5cf0bd929bba7897e974e3d2735a is owso9m
plaintext of 6b903d7eba1d35e742e59313286dcbcf is mlhdiy
plaintext of f89b9d7b998e0daf57424f6babc2525e is sso55z
plaintext of fcb4767dd81ca1bc98a76a233e10bd79 is nizedy
plaintext of fb294a4a4e39716ffe48e41060cd2c93 is tpoinc
plaintext of 2146a6b407a7fc1dd025aa5fa8c16022 is tthels
plaintext of 85a5542c63fa3452fec3ed5497ac7e5c is cancez
plaintext of bf98d92258e10da31650d25c7f5d9b75 is di5gvu
plaintext of 9d5c531edc2d81be9d20c702546a7dc9 is ofroro
plaintext of 239992d745c05aee50d6c2e2c96d7592 is opmene
plaintext of 2fc4bcccc0d388d37b00aad8c4b0d839 is egunbp
plaintext of 19792f999053db806426ecf1262cf0a3 is lou0gg
plaintext of 9652d704ee7ae48dabbf37c8dbeeb30 is aseasi
plaintext of 148240ec6d94f6cc08e9149435364d1d is hed4ep
plaintext of 255c302f5a0aa68b4f9a151bd0e420d6 is dsmtod

statistics
--------------------------------------------------------------
plaintext found:                    15 of 15
total time:                         16.30 s
time of chain traverse:             13.38 s
time of alarm check:                2.83 s
time of disk read:                  0.03 s
hash & reduce calculation of chain traverse: 194837400
hash & reduce calculation of alarm check:    40422510
number of alarm:                    36440
performance of chain traverse:      14.57 million/s
performance of alarm check:         14.30 million/s

result
--------------------------------------------------------------
239992d745c05aee50d6c2e2c96d7592  opmene  hex:6f706d656e65
2146a6b407a7fc1dd025aa5fa8c16022  tthels  hex:747468656c73
85a5542c63fa3452fec3ed5497ac7e5c  cancez  hex:63616e63657a
fcb4767dd81ca1bc98a76a233e10bd79  nizedy  hex:6e697a656479
fb294a4a4e39716ffe48e41060cd2c93  tpoinc  hex:74706f696e63
96652d704ee7ae48dabbf37c8dbeeb30  aseasi  hex:6173656173697369
255c302f5a0aa68b4f9a151bd0e420d6  dsmtod  hex:64736d746f64
2fc4bcccc0d388d37b00aad8c4b0d839  egunbp  hex:6567756e6270
6b903d7eba1d35e742e59313286dcbcf  mlhdiy  hex:6d6c6864697979
9d5c531edc2d81be9d20c702546a7dc9  ofroro  hex:6f66726f726f
148240ec6d94f6cc08e9149435364d1d  hed4ep  hex:6865643465703
bf98d92258e10da31650d25c7f5d9b75  di5gvu  hex:6469356776756
071d5cf0bd929bba7897e974e3d2735a  owso9m  hex:6f77736f396d
f89b9d7b998e0daf57424f6babc2525e  sso55z  hex:73736f35357a
19792f999053db806426ecf1262cf0a3  lou0gg  hex:6c6f75306767
```

3. Analysis and difference between salted and non salted rcrack

Adding a salt increases the cracking time by 6.10s. which is a 159.8% increase in the time.

Adding a different (Or in this case random) salt for each entry ensures that the attacker cannot use the same Rainbow table. For this lab, I had to generate 3 rainbow tables to break all 15 hashes. These rainbow tables had to work on strings of 6 characters. Each of these rainbow tables utilize their own reduction functions. When I combined them, there were more inputs and outputs that could match with the rainbow table after relevant iterations of hashing and reduction. Since more rainbow tables are used, more space is occupied and also more time is needed to vary the parameters to crack this particular combination of hashes.

With reference to the notes, adding an n bit salt essentially increases the effort by 2^n times. In our case, adding 26 lower case characters to the mix increases the effort by 26 times for an attacker who is pre-computing the rainbow table