

**CSE3501- Information security
analysis and audit**

Lab Assignment 3

Reg.No:19BCE2555

ALOKAM NIKHITHA

Rainbow Cracking:

RainbowCrack is a computer program which generates rainbow tables to be used in password cracking. RainbowCrack differs from "conventional" brute force crackers in that it uses large pre-computed tables called rainbow tables to reduce the length of time needed to crack a password drastically. Rainbow tables are tables of reversed hashes used to crack password hashes. Computer systems requiring passwords typically store the passwords as a hash value of the user's password. When a computer user enters a password, the system hashes the password and compares it to the stored hash

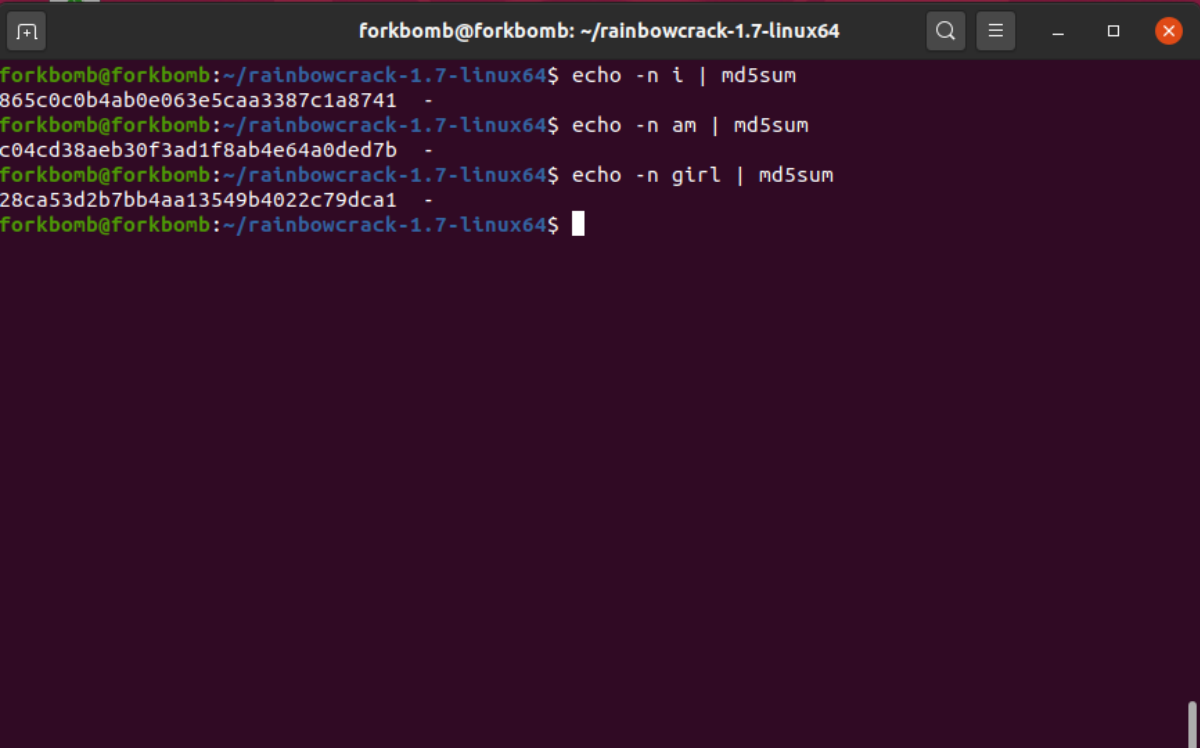
Password Cracking:

Here I have demonstrated on how to decrypt the hash codes of different words.

Here We are actually decoding the hash which actually has

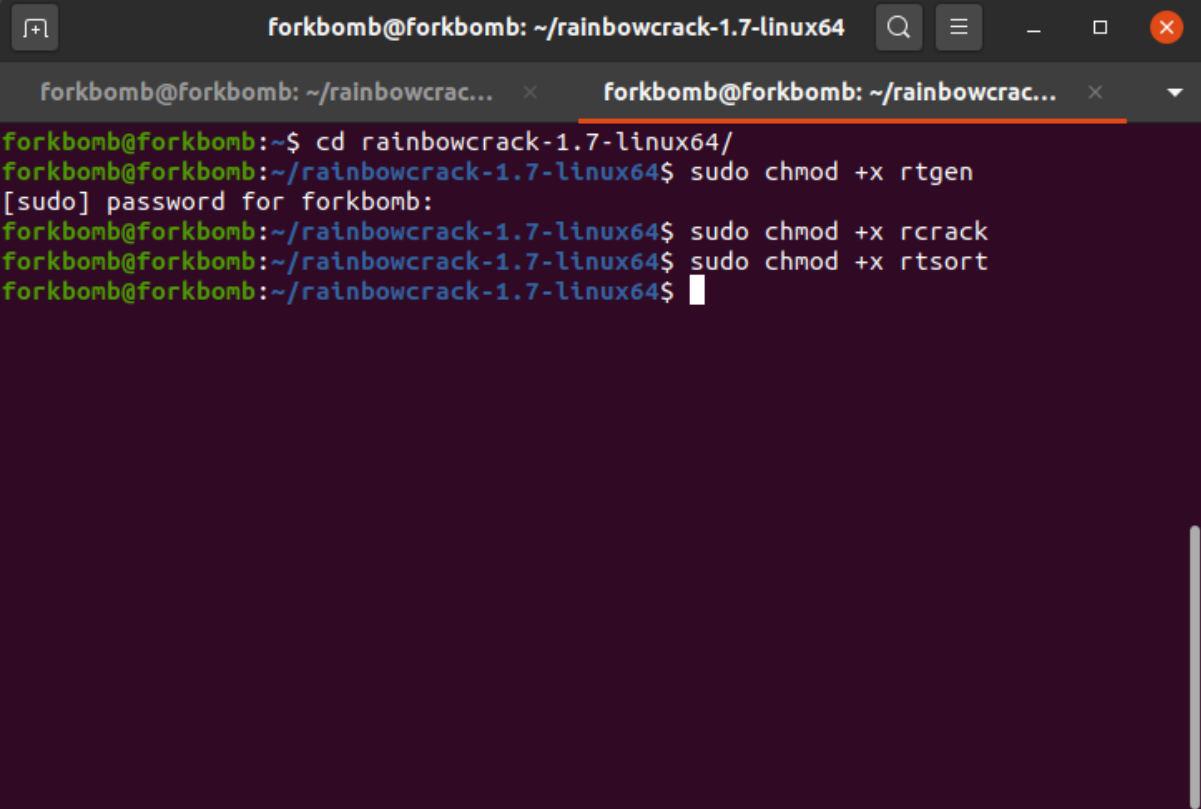
("i am girl")

Generate the hashes of the words to be decrypted.

A terminal window titled 'forkbomb@forkbomb: ~/rainbowcrack-1.7-linux64' with standard window controls. The terminal shows three commands being executed to generate MD5 hashes: 'echo -n i | md5sum' resulting in '865c0c0b4ab0e063e5caa3387c1a8741 -', 'echo -n am | md5sum' resulting in 'c04cd38aeb30f3ad1f8ab4e64a0ded7b -', and 'echo -n girl | md5sum' resulting in '28ca53d2b7bb4aa13549b4022c79dca1 -'. The prompt is currently at the fourth line.

```
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$ echo -n i | md5sum
865c0c0b4ab0e063e5caa3387c1a8741 -
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$ echo -n am | md5sum
c04cd38aeb30f3ad1f8ab4e64a0ded7b -
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$ echo -n girl | md5sum
28ca53d2b7bb4aa13549b4022c79dca1 -
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$
```

Navigating to root directory.



```
forkbomb@forkbomb: ~/rainbowcrack-1.7-linux64
forkbomb@forkbomb: ~/rainbowcrack-1.7-linux64$ cd rainbowcrack-1.7-linux64/
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$ sudo chmod +x rtgen
[sudo] password for forkbomb:
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$ sudo chmod +x rcrack
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$ sudo chmod +x rtsort
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$
```

Creating rainbow table

```
forkbomb@forkbomb: ~/rainbowcrack-1.7-linux64
forkbomb@forkbomb: ~/rainbowcrac... x forkbomb@forkbomb: ~/rainbowcrac... x
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$ ./rtgen md5 loweralpha 1 4 0 2000
0 20000 0
rainbow table md5_loweralpha#1-4_0_20000x20000_0.rt parameters
hash algorithm:      md5
hash length:         16
charset name:         loweralpha
charset data:         abcdefghijklmnopqrstuvwxyz
charset data in hex:  61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 7
3 74 75 76 77 78 79 7a
charset length:       26
plaintext length range: 1 - 4
reduce offset:        0x00000000
plaintext total:      475254

precomputation of this rainbow table is finished
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$ ./rtsort .
./md5_loweralpha#1-4_0_20000x20000_0.rt:
679538688 bytes memory available
loading data...
sorting data...
writing sorted data...

forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$
```

Decrypting words.

```
forkbomb@forkbomb: ~/rainbowcrack-1.7-linux64
writing sorted data...

forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$ ./rcrack . -h 865c0c0b4ab0e063e5caa3387c1a8741
1 rainbow tables found
memory available: 542641356 bytes
memory for rainbow chain traverse: 320000 bytes per hash, 320000 bytes for 1 hashes
memory for rainbow table buffer: 2 x 320016 bytes
disk: ./md5_loweralpha#1-4_0_20000x20000_0.rt: 320000 bytes read
disk: finished reading all files
plaintext of 865c0c0b4ab0e063e5caa3387c1a8741 is i

statistics
-----
plaintext found:                1 of 1
total time:                    36.76 s
time of chain traverse:         36.76 s
time of alarm check:            0.00 s
time of disk read:              0.00 s
hash & reduce calculation of chain traverse: 199980000
hash & reduce calculation of alarm check:    733
number of alarm:                 733
performance of chain traverse:    5.44 million/s
performance of alarm check:       0.73 million/s

result
-----
865c0c0b4ab0e063e5caa3387c1a8741 i hex:69
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$
```

The Decrypted word is “i”

```
forkbomb@forkbomb: ~/rainbowcrack-1.7-linux64
forkbomb@forkbomb: ~/rainbowcrack-1.7-linux64 x forkbomb@forkbomb: ~/rainbowcrack-1.7-linux64 x
-----
865c0c0b4ab0e063e5caa3387c1a8741 i hex:69
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$ ./rcrack . -h c04cd38aeb30f3ad1f8ab4e64a0ded7b
1 rainbow tables found
memory available: 524307660 bytes
memory for rainbow chain traverse: 320000 bytes per hash, 320000 bytes for 1 hashes
memory for rainbow table buffer: 2 x 320016 bytes
disk: ./md5_loweralpha#1-4_0_20000x20000_0.rt: 320000 bytes read
disk: finished reading all files
plaintext of c04cd38aeb30f3ad1f8ab4e64a0ded7b is am

statistics
-----
plaintext found: 1 of 1
total time: 37.55 s
time of chain traverse: 37.54 s
time of alarm check: 0.00 s
time of disk read: 0.00 s
hash & reduce calculation of chain traverse: 199980000
hash & reduce calculation of alarm check: 112
number of alarm: 112
performance of chain traverse: 5.33 million/s
performance of alarm check: 0.11 million/s

result
-----
c04cd38aeb30f3ad1f8ab4e64a0ded7b am hex:616d
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$
```

The Decrypted word is “am”

```
forkbomb@forkbomb: ~/rainbowcrack-1.7-linux64
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$ echo -n girl | md5sum
28ca53d2b7bb4aa13549b4022c79dca1 -
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$ ./rcrack . -h 28ca53d2b7bb4aa13549b4022c79dca1
1 rainbow tables found
memory available: 806813696 bytes
memory for rainbow chain traverse: 320000 bytes per hash, 320000 bytes for 1 hashes
memory for rainbow table buffer: 2 x 320016 bytes
disk: ./md5_loweralpha#1-4_0_20000x20000_0.rt: 320000 bytes read
disk: finished reading all files
plaintext of 28ca53d2b7bb4aa13549b4022c79dca1 is girl

statistics
-----
plaintext found: 1 of 1
total time: 27.31 s
time of chain traverse: 27.31 s
time of alarm check: 0.00 s
time of disk read: 0.00 s
hash & reduce calculation of chain traverse: 199980000
hash & reduce calculation of alarm check: 6911
number of alarm: 2721
performance of chain traverse: 7.32 million/s
performance of alarm check: 3.46 million/s

result
-----
28ca53d2b7bb4aa13549b4022c79dca1 girl hex:6769726c
forkbomb@forkbomb:~/rainbowcrack-1.7-linux64$
```

The Decrypted word is “girl”

