**Gede Ria Ghosalya**

**50.020 Security**

Rainbow Tables for Unsalted Passwords

The normal parameters, which are 3800 chain length and 600000 chain number, were able to find all 15 unsalted passwords within 7.0 seconds.

For optimization, the chain length is halved and the number doubled – this is a change that we can easily afford as known password length means that the space is relatively small. After changing chain length to 1900 with 1200000 chain number, the time taken improved to 1.42 seconds, which is an 490% increase in speed.

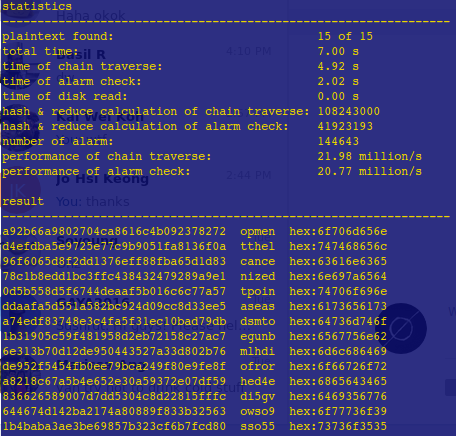
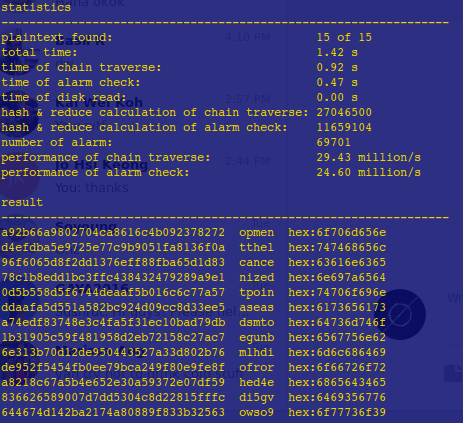
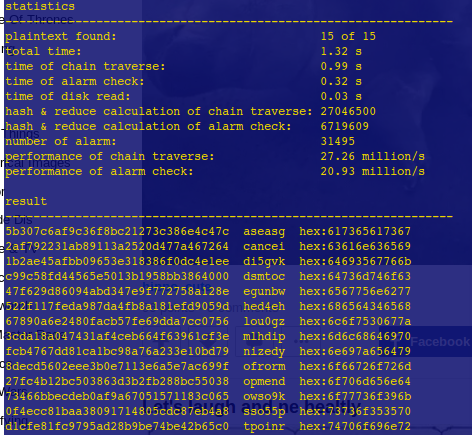


Fig 1. Performance with Normal Parameter

Fig 2. Performance with Optimized Parameter

Rainbow Tables for Salted Passwords

Following the optimized parameter (1900 chain length), the chain number is adjusted for the space of 6-length string, and slightly reduced to save space. Ending up with 10000000 chain number, the salted passwords are found within 1.32s – the shorter time is attributed to luck, as in general it would take more time to actually find salted hashes.



Competitive Hash Cracking

The code `md5hack.py` uses a list of english words (the list is commonly found in ubuntu machines, in ‘/usr/share/dict’), generate some possible modifications, and find the hashes of these. The code runs for 4.5 seconds and was able to find 15 hashes.

