Part 5

The time taken to generate the rainbow table for length = 6 takes longer compared to length = 5

The total time taken to crack the password is almost twice longer for length = 6

A single rainbow table can be used to crack passwords without salt. However for salted a rainbow table have to be generated for each specific salt, making it extremely inefficient.

Furthermore, salts can unique to each specific user and of any length. Salts extending the password to extremely long lengths can make rainbow tables and brute force attack obsolete.

For example :

Initial password : password (easily to crack)

Password with salt: passwordfjaoij120381902831ijdfojadfaj (impossible to brute force)

However hardcoded salt can be extracted from source code and used by hackers to generate rainbow tables or brute force passwords.

Part 6

I have used several approached to crack the md5 password

Dictionary attack using the wordlist from /usr/share/dict/word

Dictionary attack with common substitution (maximum of 3 substitutions) such as using

(e->3,o->0,a->@)

And lastly brute force of permutations of characters from string.printable for up to length=6

See md5_part6.py for script