Assignment 1

1. For the given hash code (md5) “e91e6348157868de9dd8b25c81aebfb9”, find the original value of this hash.
*Hint: Brute force, rainbow table, or google?

Answer : security

2. md5 is a commonly used hash algorithm in password application. If you were a hacker obtaining a password file from a system. Estimate how long will it take to break the password with brute force.
*Hint: GPU can also be applied.

Answer : By using a common GPU-based cracking systems like AMD R9 290X GPU that can compute about 93.8 billions combinations per seconds.

If user use a complex password that can be an english alphabet with both uppercase and lowercase and a number it will come out with 62^n , n is length of a password so it would take 62^n/ (93.8 x 10^9) seconds to crack a password.

3. Given your analysis in q.1 and q.2, do you think that md5 is secure for the password application? Please justify your answer.

Answer : it can come out with secure or insecure

because it depend on both user password and encryption method , time that need to crack a password depend on how long a password is and it complexity , which md5 can provide a standard security with a acceptable long length password.

If a password is set correctly it would be secure but if it set with short or easy words to guess it wouldn’t secure.

4. Based on your analysis of md5, how long should a password be to be considered secure enough?

Answer : 12+ characters

because it gives over three sextillion (3,279,156,381,453,603,096,810). which brute-force guessing time more than a *centuries*.

5730196321 DANUPAT KHAMNUANSIN