Activity 1 : Hacking Password

1. The original value of `d54cc1fe76f5186380a0939d2fc1723c44e8a5f7` is `ThaiLanD`.

2. The time used to create tha rainbow table is average 107.48 s (Measured 5 times: 106.83 / 106.92 / 108.27 / 106.73 / 108.66 s). The size is 2,684,354,656 Bytes (2.68GB), with a total of 46,290,307 items.

3. It takes 107.48 s / 46,290,307 items = 2.32 ms per item to hash a password, and the written code can try 430,688 items per second.

4. Assume the valid characters are:

- all lowercase letters of the Latin alphabet
- all uppercase letters of the Latin alphabet
- numbers 0 - 9
- @ I $ (These characters were used during substitution)

   Thus the total number of variations for a character is 26 + 26 + 10 + 3 = 65.

   When the password is of length n, the hacker would have to try at most $\sum_{i=1}^{n} 65^i$ combinations to crack the password with brute force, assuming the password is required to have a length of at least 1.

   Since it takes 2.32 ms to try 1 combination, the time needed would be maximum 2.32e-6 * $\sum_{i=1}^{n} 65^i$ seconds.

   In this link is a table showing the calculated time for each password length.

5. Based on 4., a password that takes longer than a year to break has to be at least 8 characters long. From our data an 8-char password takes 8557 days (23 years) to brute force.

6. Salt is certain string, kept private, that is added/concatenated to a password before hashing to make it more difficult to find the original value of the hash. If the hacker does not know the salt, a brute force approach to cracking the hash would be highly unlikely to be successful.