本次作業使用了 python 來完成。

How to run the code

先將要執行的 password file 與 main.py(主程式)放在同一個資料夾，接著執行 main.py 按照程式的提示依序輸入對應的東西即可並會產生 Dictionary.txt 在同個資料夾。
若是要產生 results_pa2.txt，則需先將 list_pa2.txt 放在跟 main.py 同個資料夾，接著註解掉程式的最後幾行，直接執行即可。

How to implement

一開始先將 input 的 password file 用雙層的 dictionary 儲存，儲存的格式為 {password:{salt: hash-value, salt: hash-value, …}, password:{salt: hash-value, salt: hash-value, …}, …} (例如: {XEGUOQ:{0: 23411352, 1: 47711352, …}, WBBIPR:{0: 28040920, 1: 52340920, …}, …})，其中計算 hash-value 是去 call hash(salt, password)這個 function 就會回傳 hash-value，接著將 dictionary 依序 print 出來就是 Dictionary.txt。

在 recover password 的時候，是運用 findPassword(hashValue, dictionary)這個 function，將要 recover 的 hash value 及儲存好的 dictionary 傳入就會回傳 password，在 function 中是去 traverse 整個 dictionary 的 hash value 去一一比對輸入值，若找到相同的值會回傳 password, salt, entry。