Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет інформатики та обчислювальної техніки

Кафедра інформатики програмної інженерії

Основи захисту інформації

Лабораторна робота № 4

Тема: Human-like password generator

**Виконав:**

Студент гр. ІТ-82

Фолькін Д. О.

**Перевірив:**

ст. вик. Ісаченко Г. В.

Оцінка:\_\_\_\_\_\_\_\_\_\_\_

(\_\_)\_\_\_\_\_\_\_\_\_\_2021

Київ – 2021

**Хід роботи**

1. Генерація «людських» паролів.

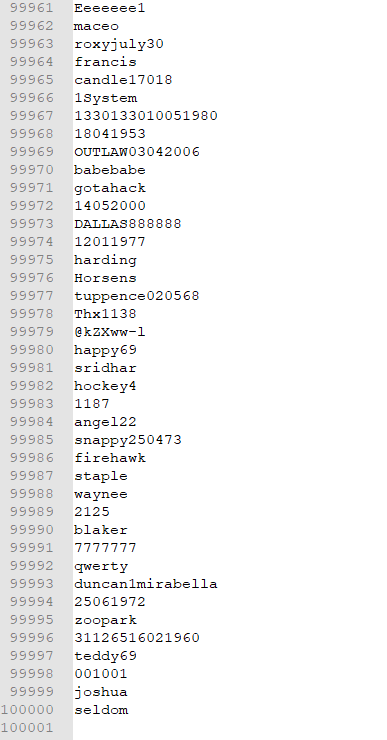
За умовою завдання необхідно запрограмувати генератор паролів, які схожі на ті, що люди часто використовують. При цьому 5-10% має бути просто готовими паролями з інтернету, що їх найчастіше використовують.

Далі 1-5% - істинно випадково згенеровані паролі. І решта – комбінації популярних символьних конструкцій.

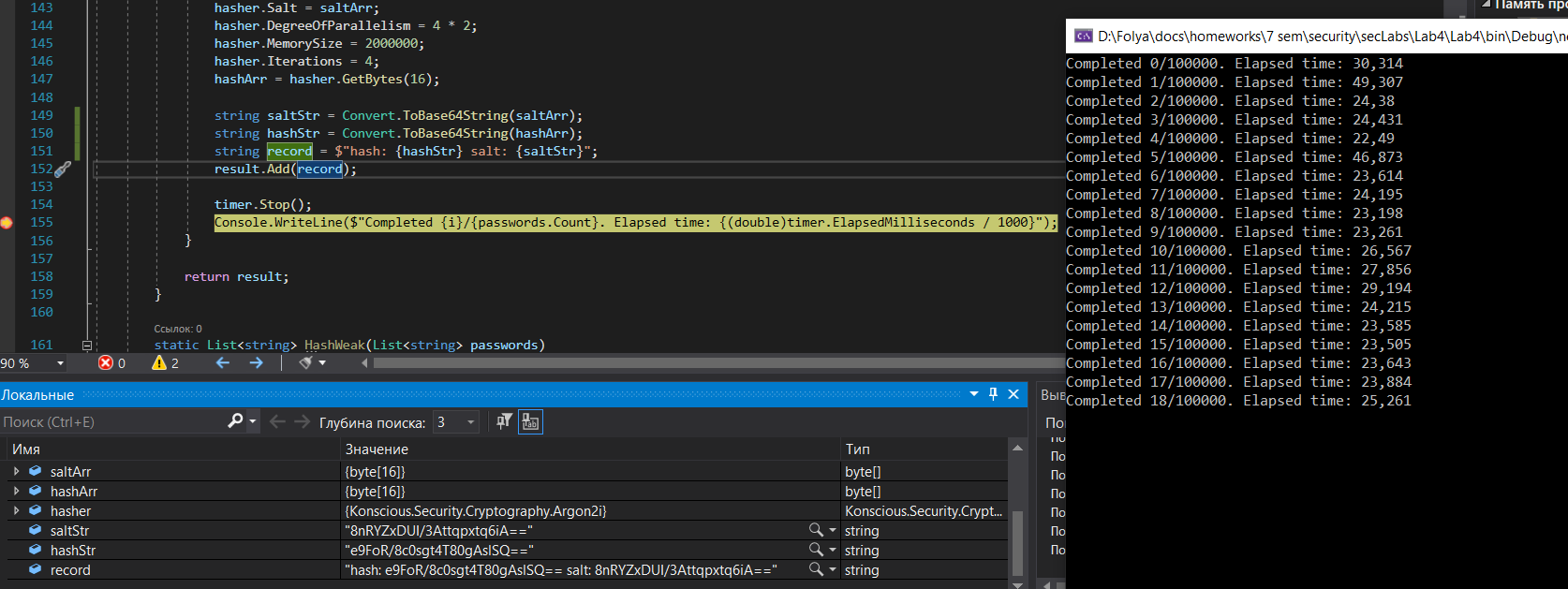
Далі треба захешувати отримані паролі популярними способами. Оберемо SHA1 та Argon2, варіант і. Захешуємо по 100000 паролів.

Використаємо для нашої роботи засоби мови С# та NuGet – бібліотеку Konscious.Security.Cryptography, що дозволяє використовувати алгоритм Argon2i.

Генерація паролів:



Хешування:



Результати збережені у csv-файлах. Weak – sha1 (без солі), strong – argon2i.

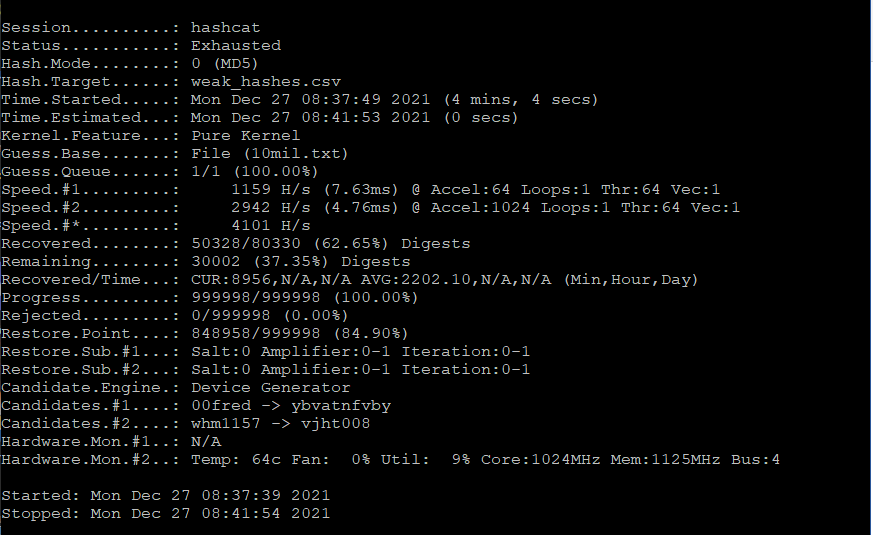
На моїй машині в середньому йшло 25 секунд на хешування одного пароля за алгоритмом argon2i та менше 1 мілісекунди для sha1.

1. Розхешування чужих паролів

Маємо 100 тисяч слабких паролів md5 без солі і 100 тисяч sha1 із сіллю.

У завданні запропоновано використати інструмент hashcat.

Задамо як параметр словник з інтернету на 1 мільйон паролів.



Отримали 62,65% паролів успішно розхешованих md5.

Час виконання – приблизно 4 хв.

Спробуємо SHA1 + сіль:



Процес продовжувався близько 15 хв і за цей час було розхешовано близько 17000 паролів. Можемо припустити, що для 100 тисяч процес зайняв би приблизно 88 хв.

Перевага SHA1 очевидна, хоча і не вирішальна, адже ми все ще можемо отримувати прості паролі, захешовані ним.

Найпотужніший засіб розхешування hashcat не впорався із істинно випадковими паролями, захешовані усіма розглянутими алгоритмами, що наштовхує на певні висновки щодо способів універсального захисту від розшифрування пароля незалежно від способу його хешування. Але не виключено, що наявність потужнішого обладнання дозволила б успішно провести bruteforce атаку на надійні паролі, хоч це і зайняло б масу часу.