Lab 4.1 Report

Для генерації паролів використовуються чотири схеми:

1. Паролі з списку топ-100000 часто вживаних паролів
2. Паролі з списку топ-100 часто вживаних паролів
3. Паролі згенеровані випадковим чином
4. Паролі згенеровані випадковим чином, але так, щоб вони були схожими на паролі реальних людей

Загальна кількість згенерованих паролів - 100000. Спочатку ми вибираємо від 5-ти до 10-ти відсотків від необхідної кількості паролів з списку топ-100 найбільш вживаних паролів. Після чого вибираємо від 50 до 90 відсотків від необхідної кількості паролів з списку топ-100000 найбільш часто вживаних паролів. Потім від 1-го до 5-ти відсотків від необхідної кількості паролів генеруються випадковим чином. Для цього вибирається випадкова довжина паролю від 5 до 16 символів. Після чого пароль заповнюється випадковими символами з таблиці ASCII в межах від 32 до 126 символа (великі та малі літери, цифри, спецсимволи). Далі генеруються human-like паролі. Для того щоб згенерувати такі паролі використовується список найбільш часто вживаних слів англійської мови та наступний алгоритм:

1. Вибираємо випадкове слово з списку
2. Якщо воно коротше ніж 5 символів - вибираємо ще одне і додаємо до цього
3. З ймовірністю 0.25 добавляємо на початок або в кінець паролю рік, вибраний випадково від 1980 до 2020, так як користувачі часто вживають роки в паролях.
4. З ймовірністю 0.7 та якщо довжина поточного паролю менша, ніж 8 символів добавляємо на початок або в кінець чотири випадкові цифри.
5. З ймовірністю 0.6 замінюємо деякі літери на цифри за наступним правилом:

```
const LETTERS_TO_NUMBERS_MAP = {
    'l': 1,
    'i': 1,
    'o': 0,
    's': 5,
}
```

6. З ймовірністю 0.4 добавляємо до паролю спецсимвол
7. З ймовірністю 0.5 замінюємо від 1 до 4 букв на відповідні букви верхнього регістру.

В результаті отримуємо набір з 100000 паролів.