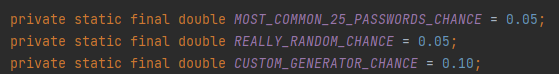
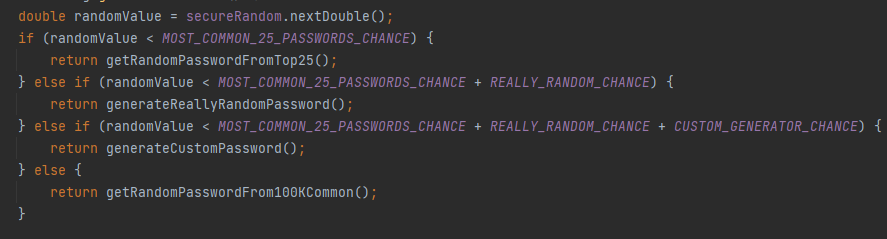
**Звіт 4 лаборатна 1 частина**

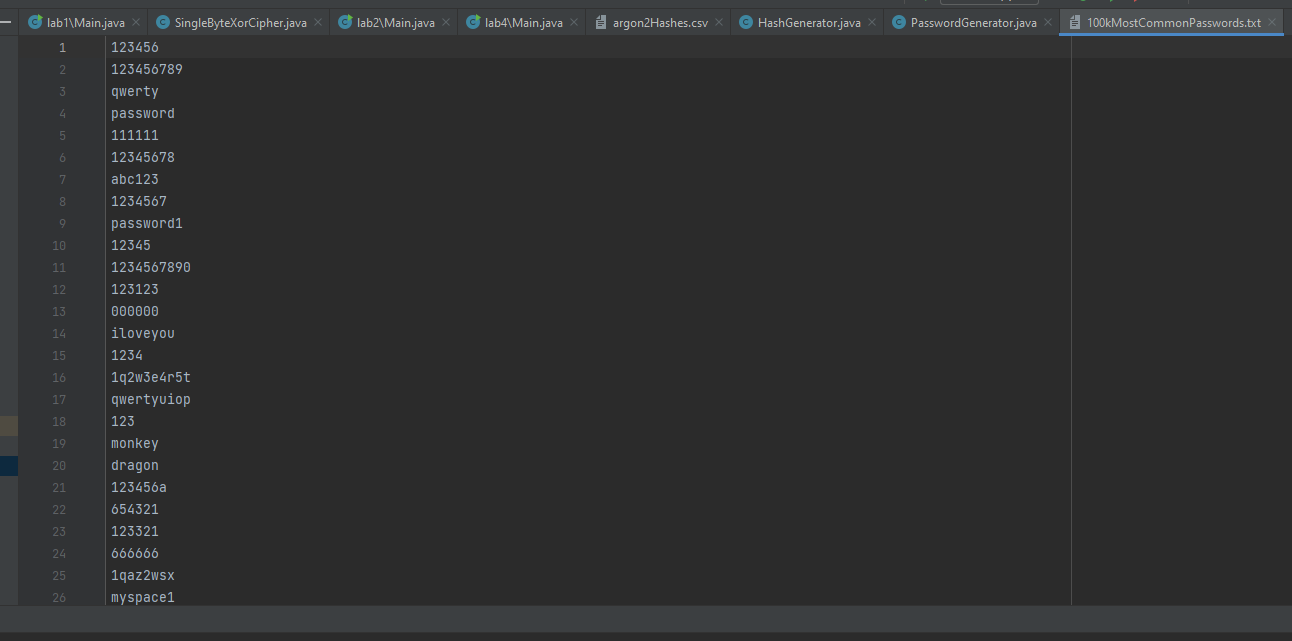
Для генерації паролів, було вибрано 4 способи, і підібрані наступні шанси:

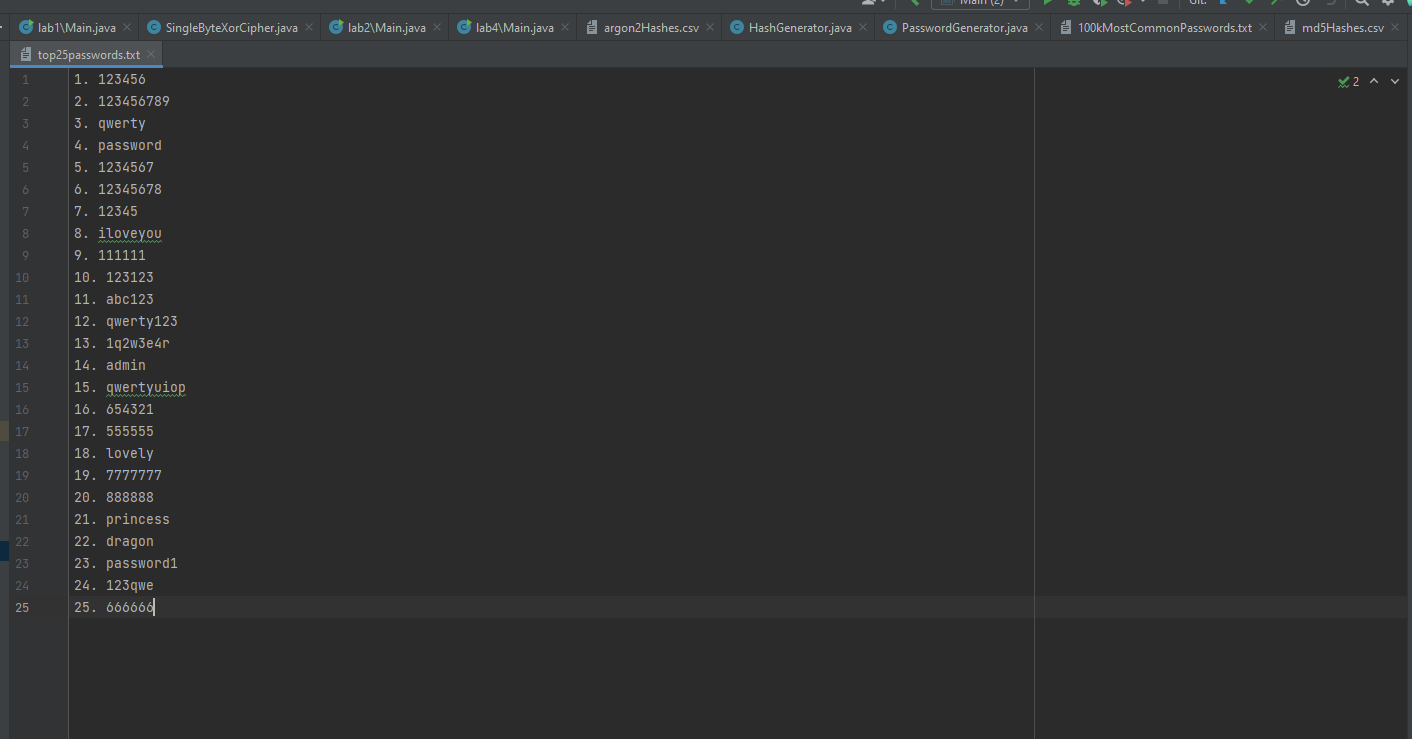
1. 25 найпоширеніших паролів з ймовірністю 5%
2. 100к найпоширеніших паролів з ймовірністю 80%
3. Рандомні паролі з ймовірністю 5%
4. Кастомні паролі (додавання в кінець ключового набору символів та заміни символів) з ймовірністю 10%





Генерується рандомне число від 0 до 1 (double) і відповідно якщо воно менше 0.05 то попадає в топ 25, якщо менше 0.1 то в рандомні, якщо менше 0.2 то в кастомні, інші в 100к найпоширеніших паролів.

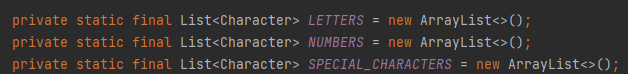




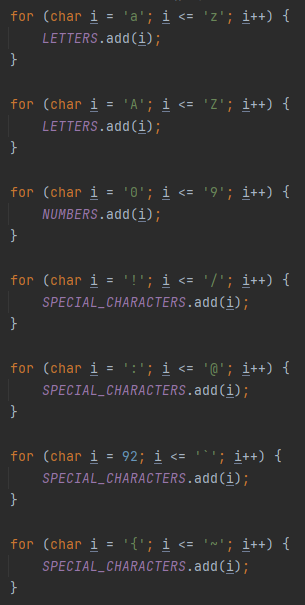
З цих файлів вибирається рандомний рядок:



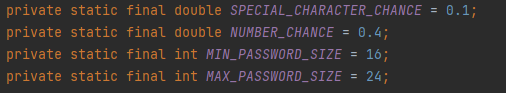
Для рандомного пароля я зробив наступне: створив списки з спец символів, букв та цифер



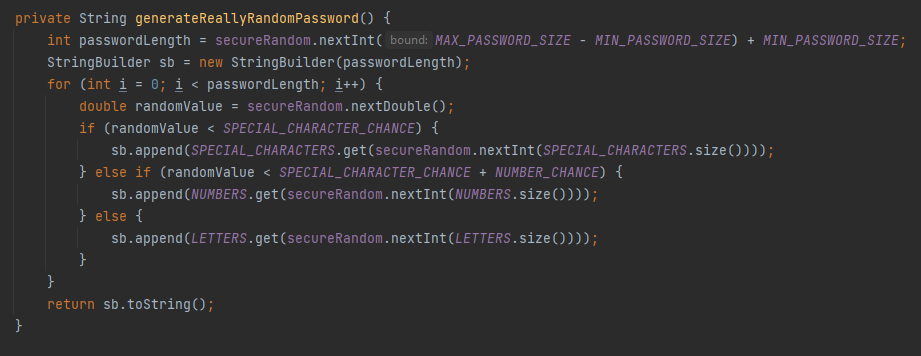
Заповнив їх



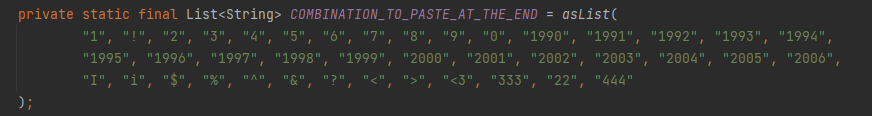
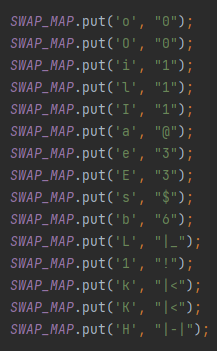
Добавив шанси для їх випадання та мінімальну й максимальну довжину



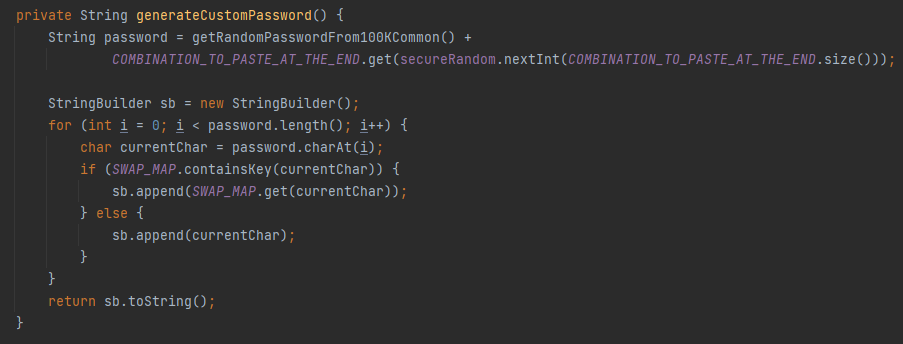
І сама реалізація



Для кастомного пароля, я вибрав два правила

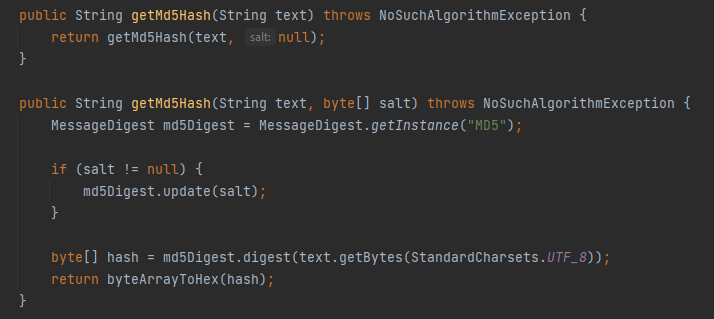
1. Вставляти в кінець ключові символи (звісно рандомно):   
   
2. Заміняти певні символи на певну комбінацію:  
   

І відповідно я брав паролі зі 100к найпопулярніших та додавав вкінець комбінації + міняв символи:

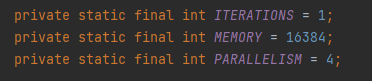


Для створення хешу я вибрав два алгоритми: MD5 та Argon2i (найслабший та найсильніший)

Реалізація MD5 елементарна, без лишніх параметрів (для легкості я не генерував md5 з солями):



Аргон впринципі теж легкий, але є цікаві параметри:



Щоб зробити алгоритм максимально важким та повільним потрібно збільшити кількість ітерацій, збільшити кількість пам’яті та зменшити паралелізм. Для себе я взяв ці настройки (100 хешів за 1,5 секунди на моєму досить швидкому ноуті)

А далі я просто їх закинув у файл:

