Список топ 100 і топ 100.000 паролів був взятий з <https://github.com/danielmiessler/SecLists/tree/master/Passwords>

Використовувалось 3 методи хешування: MD5, SHA1 + Salt, Bcrypt. Програма створює 100.00 паролів для кожної схеми.

В середньому

1. 10% паролів – паролі зі списку топ 100
2. 70% паролів – паролі зі списку топ 100.000
3. 5% паролів – «безпечні» паролі (згенеровані як частина guid, не криптонрафічно випадковими)
4. 15% паролів – паролі, які є видозміненими паролями зі списку топ 100.000. Стратегії примінені до паролів:
   1. Считування пароля з кінця
   2. Дублювання
   3. Зміна деяких символів ( a -> @, e -> 3, i -> 1 і т.д.)
   4. Дублювання кожного символа
   5. Додавання 123 до пароля
   6. Написання кожного другого символа пароля у верхньому регістрі
   7. Додавання року (з 1960 до 2021) в кінець пароля
   8. Додавання xXx в кінець і початок пароля

Так хешування паролів за допомогою KDF функцій, у цьому випадку Bcrypt, займає багато часу та ресурсів, у репозиторій вкладені файли з вже хешами вже згенерованих паролів.

P.S: Функція, яка використовувалась для визначення відсотка не є криптографічно безпечною, тому розподіл може не повністю відповідати заданим значенням.