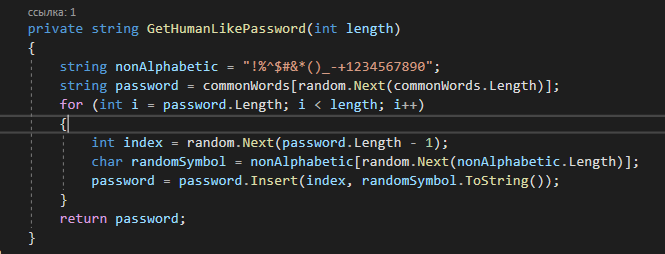
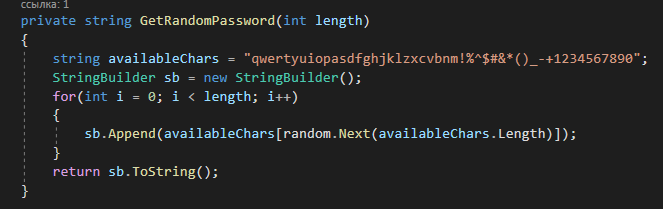
В лабораторній я згенерувала 500 000 паролів, з яких 7% належать до топ 100 найслабших паролів, 75% до мільйона найслабших, 4% згенеровані рандомно, 14% згенеровані подібними до реальних людських паролів.

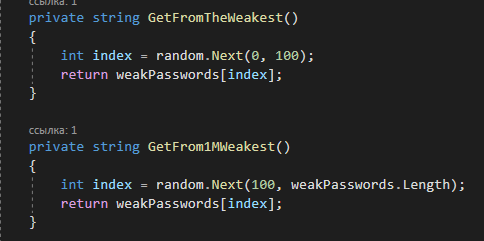
«Подібний до реального людського паролю» пароль генерується із використанням списку найпоширеніших англійських слів. Береться випадкове слово та доповнюється цифрами та спецсимволами до потрібної довжити, якщо її не вистачає. При генерації була вибрана довжина паролю 10. На рисунку зображена відповідна функція



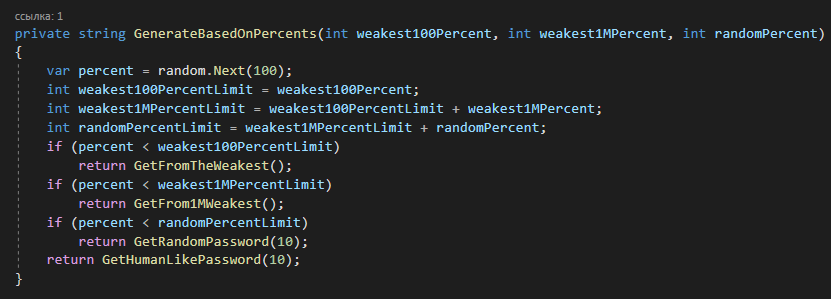
Рандомний пароль генерується доволі простою функцією, що є на наступному рисунку



Найслабші паролі беруться просто із файлу найпростіших паролів випадковим чином



Для того щоб дотриматися відсоткового співвідношення і одночасно з цим паролі були перемішені (щоб не було ситуації, що спочатку найслабші, потім сильніші і в кінці рандомні) була написана наступна функція



Вона генерує рандомне число в відрізку від 0 до 100. Якщо воно входить в відрізок [0-7], то генерується пароль, що входить до 100 найслабших паролів, якщо в відрізок [8-82] – то пароль, що входить до мільйона найслабших, якщо в відрізок [83-86] – то пароль, що є випадковим, а якщо в відразок [87-100] – то пароль, що схожий на людський.

Хешуються паролі за допомогою MD5, SHA1 та BCrypt. Оскільки BCrypt вимагає дуже багато часу я використала зменшений workFactor для обрахунків в алгоритмі (використовується число 5 при максимальному рівні 31).