Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет информационный технологий и управления

Кафедра интеллектуальных информационных технологий

Дисциплина: «Средства и методы защиты информации в  
интеллектуальных системах»

Лабораторная работа №1 по теме:  
«Генерация паролей»

Студент гр. 121702

Заломов Р.А.

Проверил:

Сальников Д.А.

Минск 2023

**Тема**

Генерация паролей

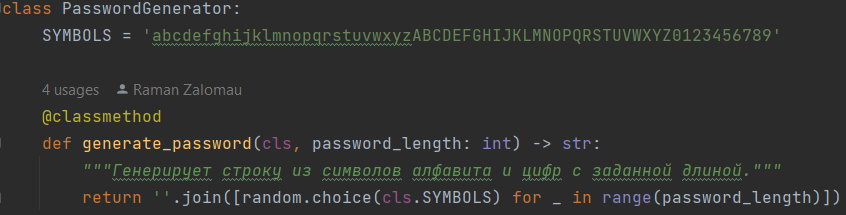
**Задание**

Разработать программу, реализующую следующие функции:

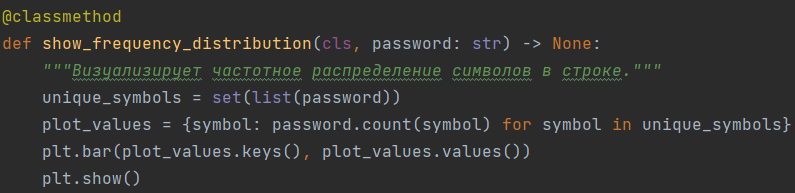
1. Генерация строки с заданной пользователем длиной, состоящей из символов алфавита в соответствии с вариантом задания.
2. Проверка равномерности распределения символов путем визуализации частотного распределения.
3. Вычисление среднего времени подбора пароля, выбираемого из сгенерированной строки.
4. Построение графика зависимости среднего времени подбора пароля от его длины.

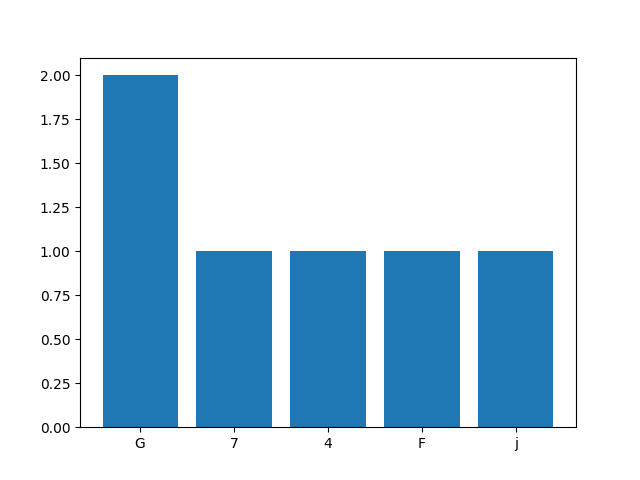
**Выполнение задания**Вариант 7 – алфавит генерируемого пароля состоит из   
**Задание 1**

Листинг

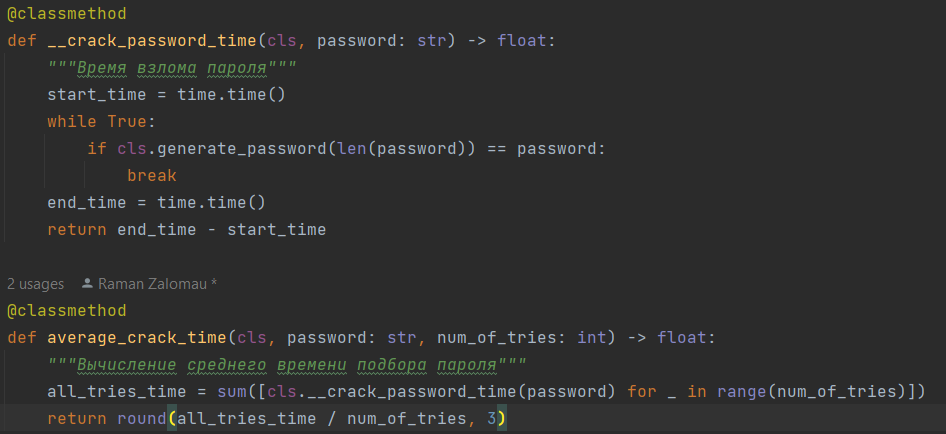
  
  
Результат работы  


**Задание 2**

Листинг  


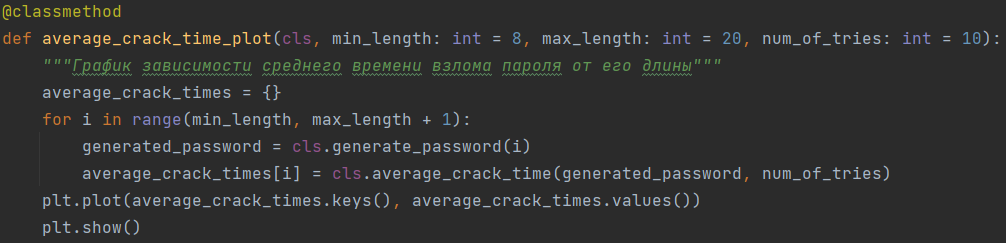
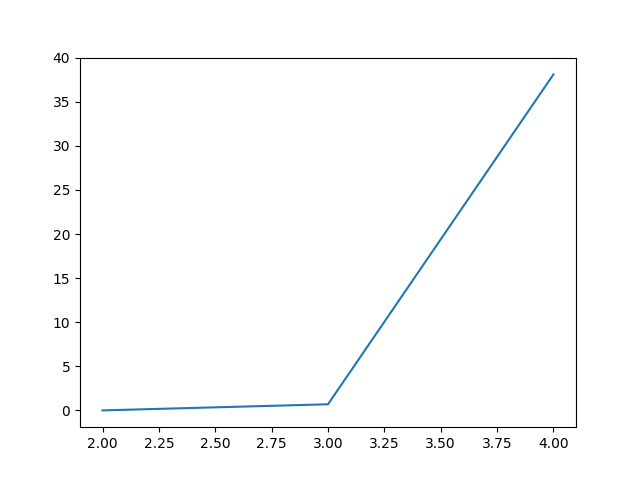
Результат работы (для пароля из задания 1)  


**Задание 3**

Листинг  


Результат работы (для пароля из 3-х символов)  


**Задание 4**

Листинг  
  
  
Результат работы:  


Как видно для данного алфавита среднее время скорости взлома пароля резко возрастает при увеличении длины пароля с 3-х символов (среднее время взлома ~0.5с) до 4-х символов (среднее время взлома ~39с).

**Вывод**

В ходе лабораторной работы были реализованы программные средства генерации паролей. Помимо этого, были наглядно продемонстрированы показатели зависимости стойкости паролей в зависимости от их длины. Графики, представленные в Задании 4, показывают, что стойкость пароля может резко возрасти при увеличении его длины. Также стоит отметить, что стойкость пароля может возрасти при расширении алфавита (т.е. добавлении туда различных символов), ведь увеличение алфавита снижает вероятность правильного подбора очередного символа при брутфорсе. Стойким паролем может быть пароль длинный и состоящий из различных символов. В идеале использовать пароли, представляющие собой долгие и осмысленные фразы (для облегчения процесса запоминания пароля).