Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет Информационных технологий и управления

Кафедра Интеллектуальных информационных технологий

**ОТЧЁТ**

по дисциплине «Средства и методы защиты информации в интеллектуальных системах»

Лабораторная работа №1

Тема: Генерация паролей

Вариант: 11

Выполнил: Козырев Д. А.

гр. 221703

Проверил: Крищенович В. А.

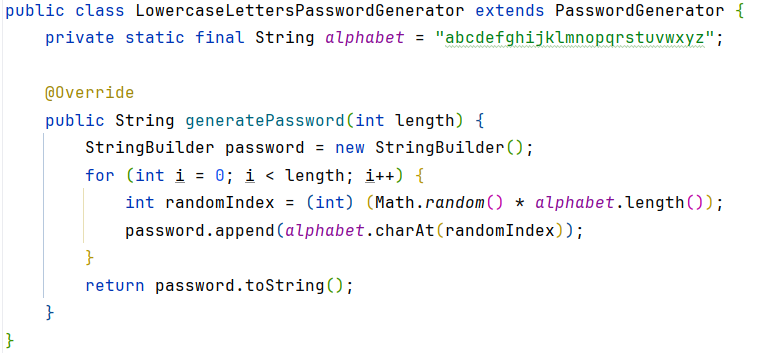
Минск 2024

**Задание 1:**

Генерация строки с заданной пользователем длиной, состоящей из

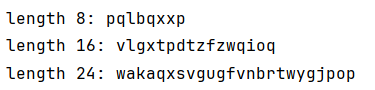
символов алфавита в соответствии с вариантом задания (использовать функции

rand( ), srand( ) и инициализацию от таймера).



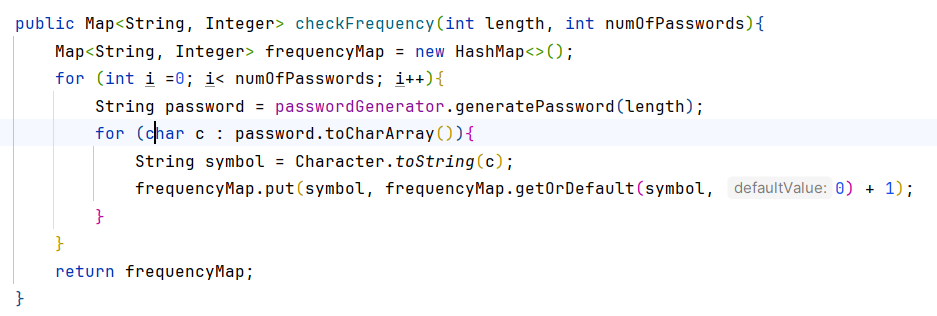
Для реализации метода была использована класс Math и ее метод random, который возвращает псевдослучайное число от 0 до 1, которое умножается на длину алфавита (по варианту лабораторной – это алфавит из строчных латинских букв). Результат умножения – индекс символа в алфавите.

Результат:



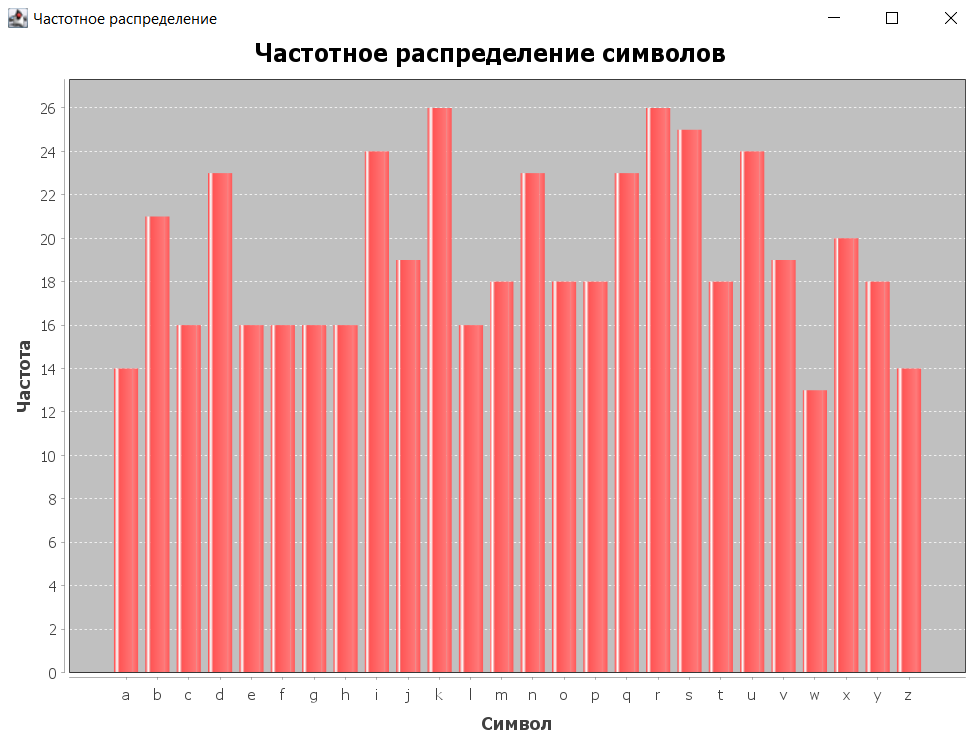
**Задание 2:**

Проверка равномерности распределения символов путем визуализации частотного распределения.

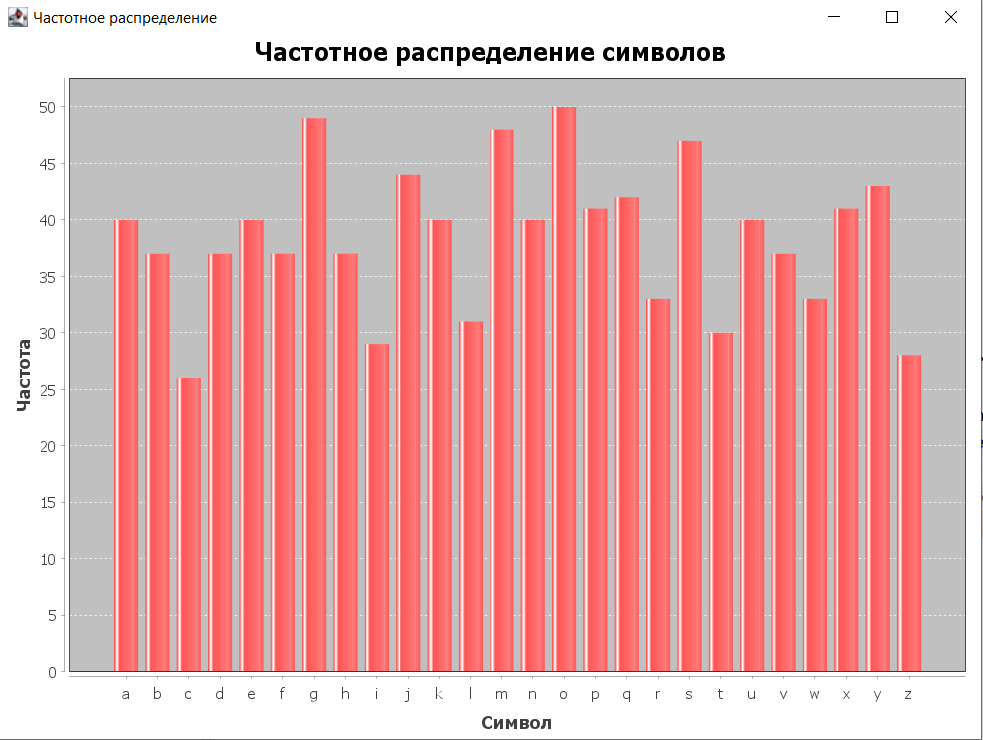


Метод принимает размер генерируемых паролей, а также их кол-во. Возвращает ассоциативный массив, в котором ключ – символ алфавита, а значение – количество раз, которое встречается символ во всех паролях.

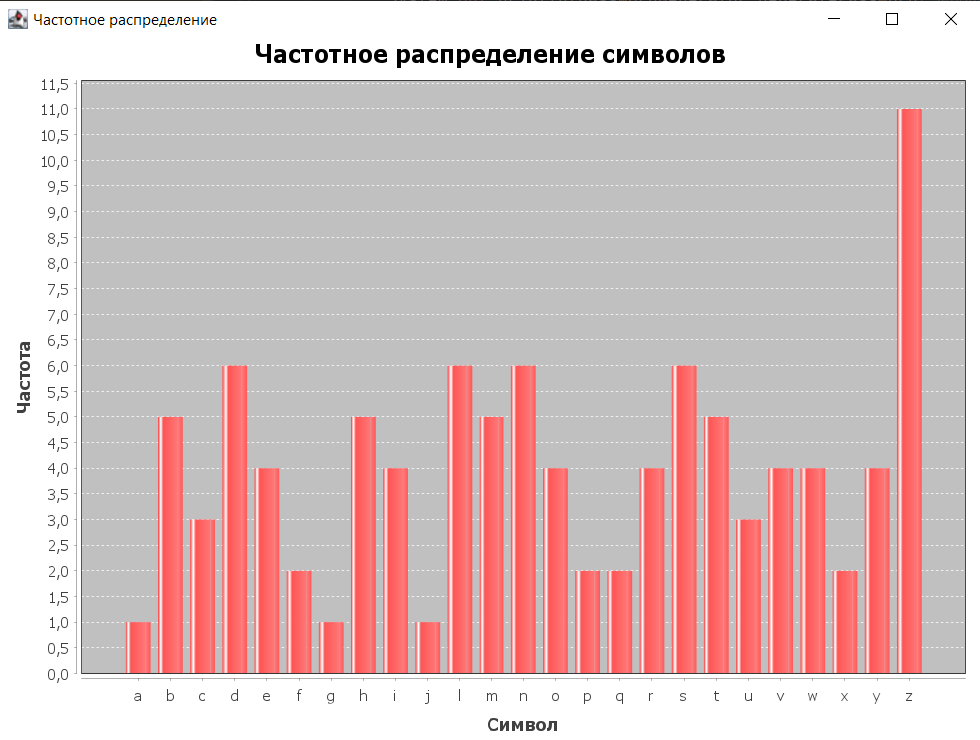
Частотное распределение для 100 паролей, состоящих из 5 символов.



Частотное распределение для 100 паролей, состоящих из 10 символов.



Частотное распределение для 1000 паролей, состоящих из 16 символов.

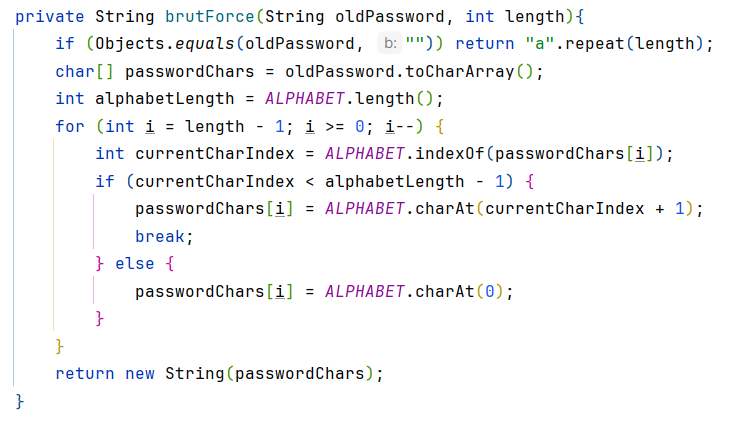


Исходя из результатов, можно сделать вывод, что чем длиннее пароль и чем паролей больше, тем рамномернее будет частотное распределение.

**Задание 3:**

Вычисление среднего времени подбора пароля, выбираемого из сгенерированной строки.

Для подбора пароля был использован метод грубой силы. В моей реализации – это последовательный перебор всех возможных паролей из данного алфавита и данной длины.



Метод для получения данных для графика, возвращает ассоциативный массив, в котором ключ – длина пароля, а значение – время его подбора.

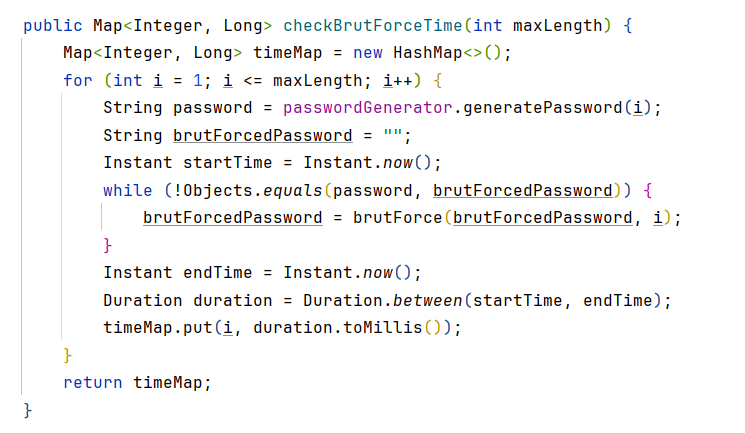
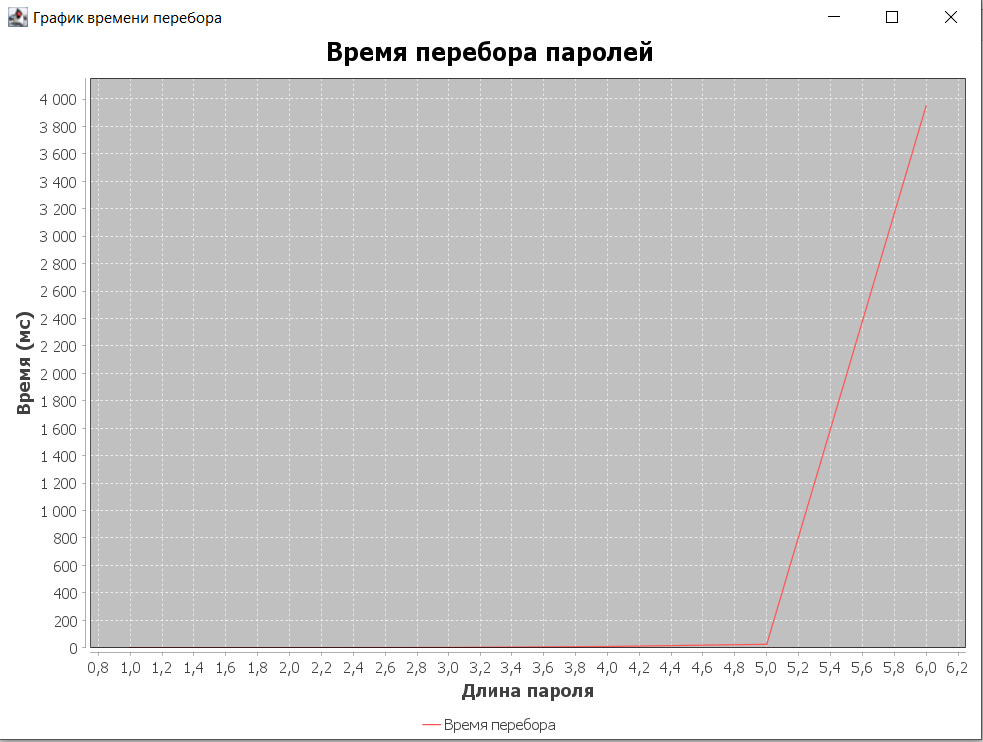
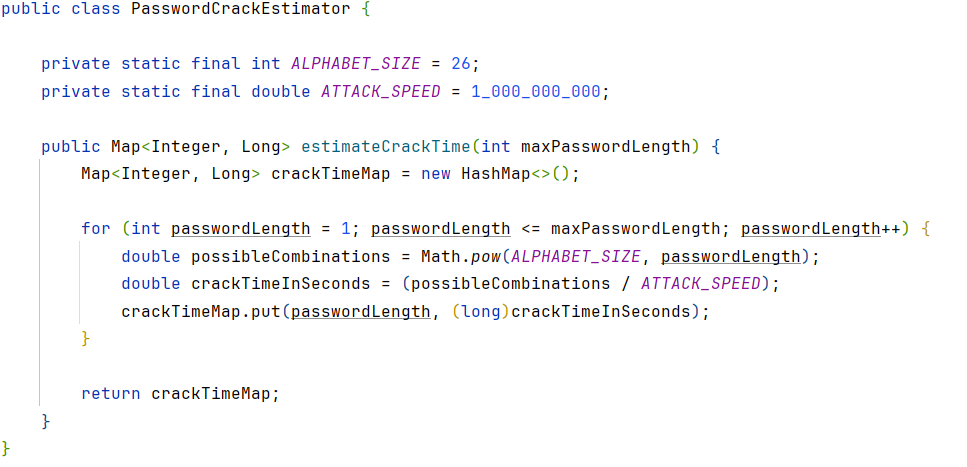


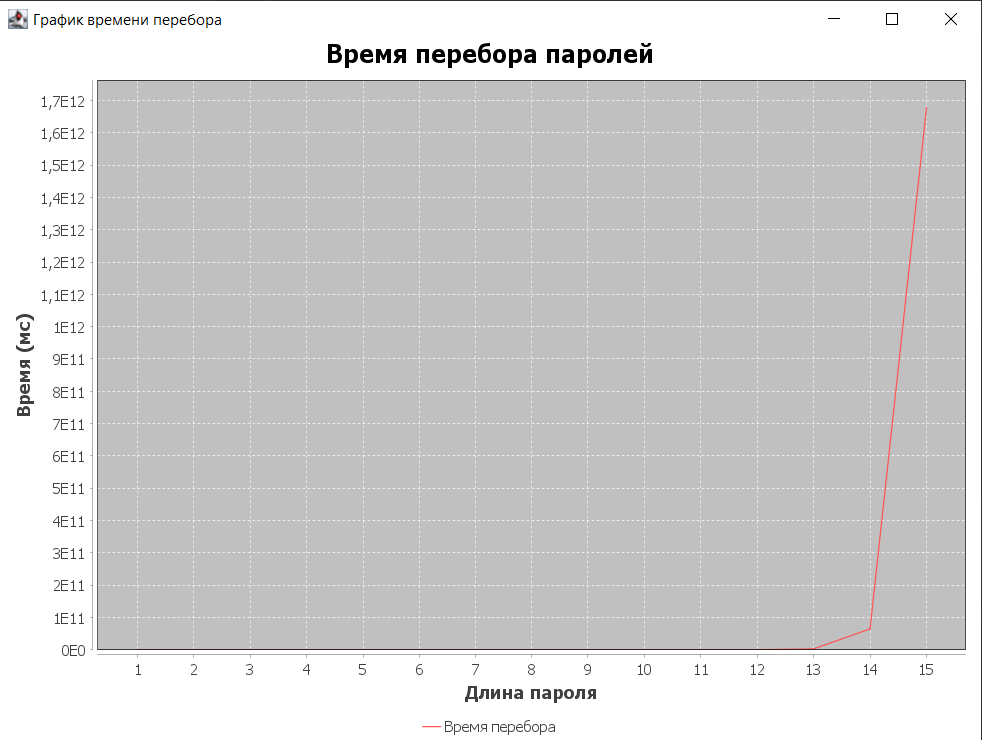
График зависимости среднего времени подбора пароля от его длины:



Также для вычисления времени подбора пароля была использована формула , где m – длина алфавита, n – длина пароля, avg – среднее кол-во генерируемых паролей в секунду(было использовано 1 млрд).

**

**Результат:**

****

Вывод: на основании проделанной работы можно сделать вывод, что время подбора пароля зависит от его длины, а также от количества символов в алфавите. Пусть длина алфавита – n, а длина пароля – m, тогда паролей длины n из символов данного алфавита можно сгенерировать . Поэтому при создании пароля важно следовать рекомендациям, которые дают многие сайты: использовать строчные и прописные буквы, цифры, а также специальные символы, а также делать пароли длинными (чем важнее защищаемый ресурс, тем длиннее следует делать пароль), ведь увеличение пароля на один символ увеличит и кол-во возможных паролей в n раз. Современные компьютеры, особенно при использовании специализированного оборудования, могут подбирать миллиарды паролей в секунду. Для защиты от таких атак важно выбирать пароли, которые невозможно подобрать в разумные сроки даже с использованием мощного оборудования. Например, если атакующий может проверять 1 миллиард паролей в секунду, а количество возможных комбинаций составляет (что больше 43 квинтиллионов), то подбор такого пароля займёт долгое время.