пМинистерство 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

Вариант 8

Выполнил: Робилко Т. М.

гр. 221701

Проверил: В. В. Захаров

Минск 2024

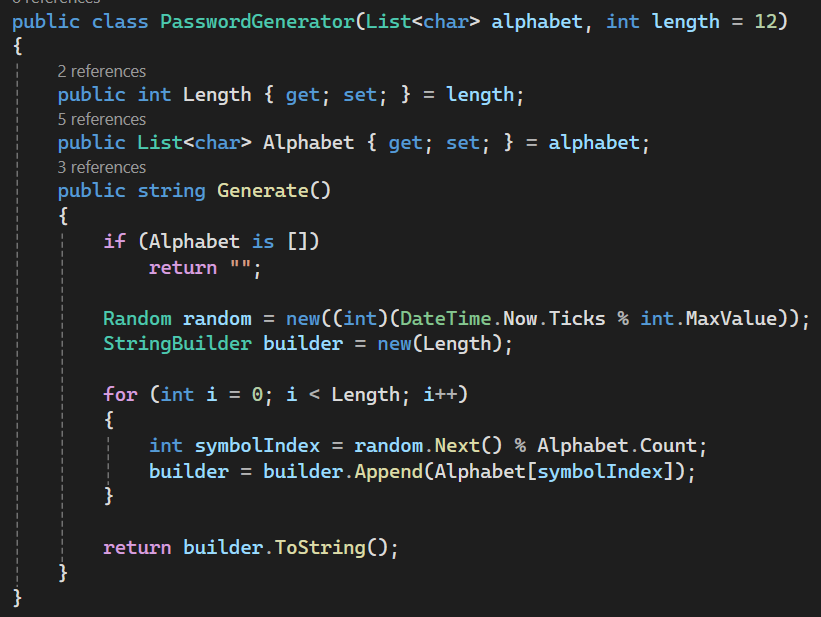
**Задание:**

1. Разработать программу, реализующую 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 сгенерированного пароля;

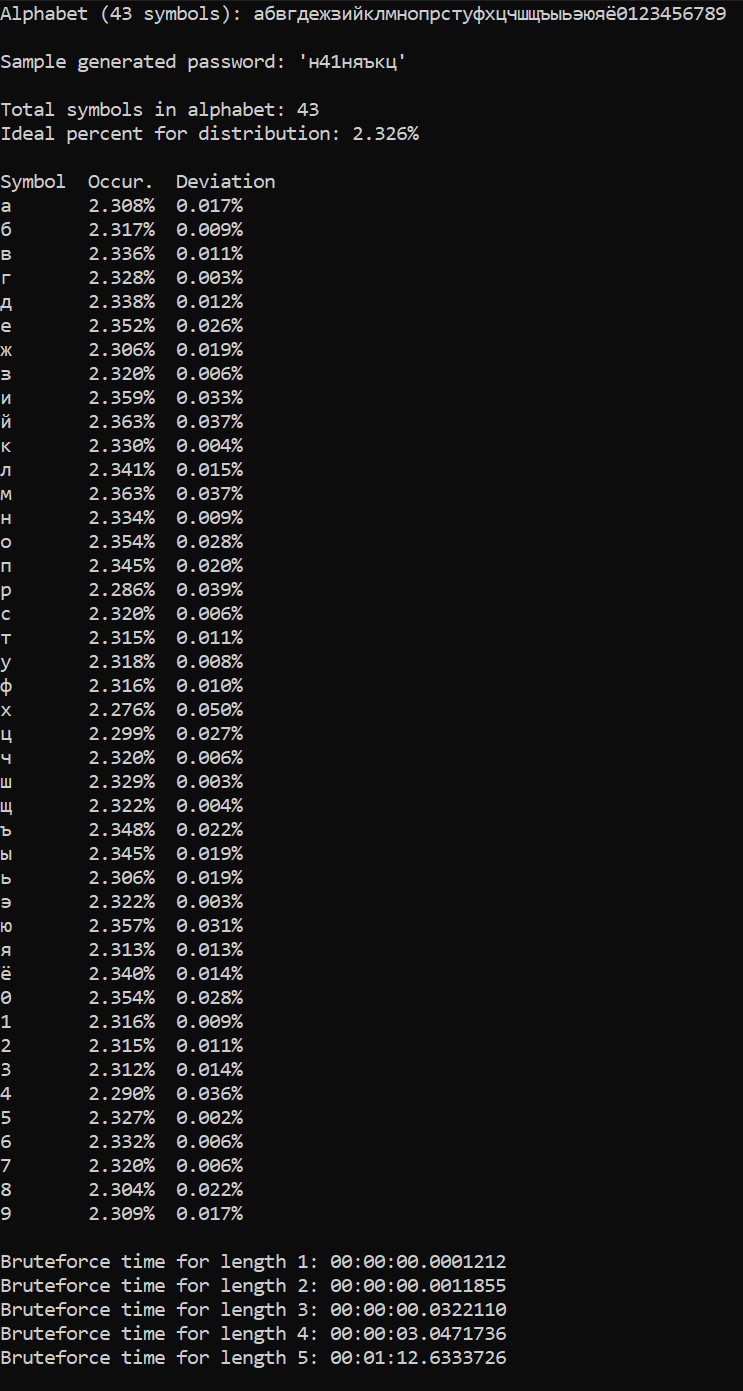
2) Построить график зависимости времени подбора пароля от его длины.

3) Дать практические рекомендации по выбору пароля исходя из предположений об алфавите пароля; ценности информации, доступ к которой защищается с помощью этого пароля; производительности вычислительного средства, атакующего и времени атаки.

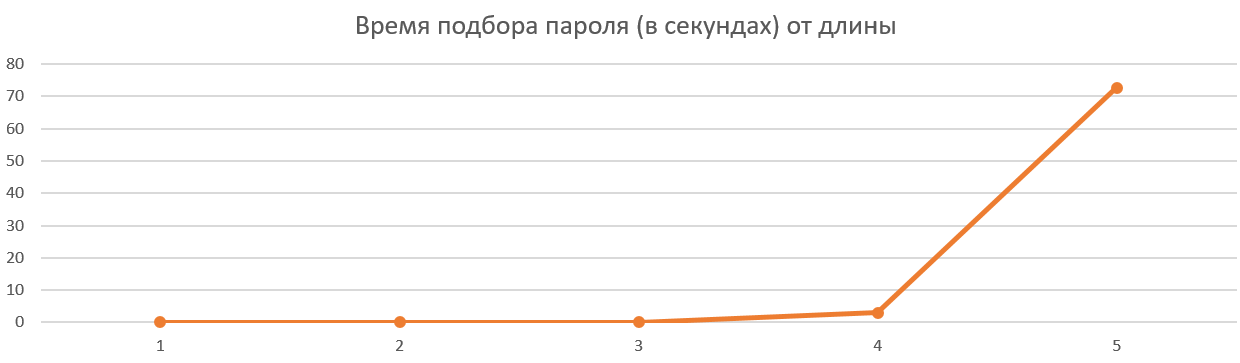
**Ход работы:**

1. Описание алгоритма генерации пароля:
   * Инициализировать алфавит для генерации посредством передачи списка символов в конструктор генератора; аналогично указать длину пароля
   * Инициализировать генератор случайных значений с помощью текущего времени в тактах процессора (ticks)
   * Добавить к строке генерируемого пароля новых символ из алфавита, взятый по индексу, полученному с помощью генератора случайных значений (по модулю количества символов в алфавите, чтобы избежать выхода за пределы массива)
   * Повторять предыдущий пункт до достижения указанной длины пароля
2. ****Класс PasswordGenerator, реализующий алгоритм генерации пароля
3. Методика анализа стойкости полученных паролей:

* Частотное распределение символов алфавита получается путём генерации указанного числа паролей (для описанных ниже результатов взято значение 50000) и расчёта отношения вхождений каждого символа к общему числу символов всех паролей. Программа выводит также эталонный процент вхождения каждого символа (рассчитан делением 100% на количество символов в алфавите) и девиацию фактических значений от эталонного.
* Вычисление среднего времени подбора пароля эмпирическим путём производится перебором всевозможных комбинаций символов заданного алфавита с остановкой таймера при совпадении с вновь сгенерированным случайным паролем данной длины. Для уменьшения ошибок, связанных со случайностью генерации, производится несколько повторов подбора (в случае данной работы – 10 раз для каждой заданной длины пароля)

1. Вывод программы, включающий процент вхождения каждого символа и время подбора пароля методом полного перебора, а также заданный вариантом алфавит и пример сгенерированного пароля

**График зависимости среднего времени подбора пароля от его длины**



**Выводы и практические рекомендации по выбору пароля**

* *Используйте сложные алфавиты*. Для увеличения стойкости пароля необходимо увеличивать размер алфавита. Увеличение размера алфавита нелинейно влияет на время подбора пароля, поэтому рационально использовать как можно больше различных символов.
* *Длина пароля значительно влияет на его стойкость.* 12 символов и более – оптимальная длина для защиты критически важной информации. Как показали теоретические и эмпирические результаты оценок стойкости паролей, длительность подбора зависит от длины нелинейно.
* *Избегайте использования легко угадываемых или часто используемых паролей.* Атакующие могут использовать базы известных паролей и словарные слова, почему использование распространённых паролей и простых слов на любом языке крайне нежелательно. Также стоит избегать использования слов, связанных с портретом пользователя. В частности, стоит избегать использования имён, дат, объектов интереса.
* *Пользуйтесь средствами генерации случайных паролей.* Примером такой системы является встроенный в iOS генератор паролей. Указанный генератор позволяет создавать случайные пароли с использованием латинского алфавита, арабских цифр 0-9, а также специальных символов. Случайность, длина и использование немаленького алфавита обеспечивает выполнение указанных выше рекомендаций, сводя к минимуму возможность взлома.
* *Регулярно сменяйте используемые пароли; используйте разные пароли для разных сервисов.* Нередкой причиной взлома пароля является утечка данных на стороне компании, хранящей пароли. Использование одних и тех же паролей к нескольким аккаунтам приводит к потере доступа ко всем аккаунтам сразу в случае такой утечки. Для защиты рекомендуется регулярно сменять пароль и не устанавливать одинаковый пароль на аккаунты разных сервисов.
* *Используйте дополнительные средства аутентификации.* Для дальнейшего ограничения доступа к чувствительной информации стоит применять двухфакторную аутентификацию. К средствам таковой относятся средства биометрии, подтверждение доступа с помощью второго устройства, подтверждение по мобильному телефону.