Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра информационных технологий автоматизированных систем

Отчет по лабораторной работе №1

по курсу «ИТОКБ»

на тему: «Генерация паролей»

Вариант 4

|  |  |
| --- | --- |
| Выполнил магистрант группы 025941: | Колесников В.Г. |
| Проверил: | Боброва Т.С. |

МИНСК

2021

**Задание 1:** Разработать программу на языке C++, реализующую следующие функции:

- генерация строки заданной пользователем длины, состоящей из символов русского алфавита (строчные и прописные);

- проверка равномерности распределения символов путем визуализации частотного распределения;

- вычисление среднего времени подбора пароля, выбираемого из сгенерированной строки.

Код программы приведен в конце лабораторной работы.

Результаты работы программы генерации пароля приведены на рисунках 1.1, 1.2 и 1.3.



Рисунок 1.1 — Результат генерации пароля на 10 символов



Рисунок 1.2 — Результат генерации пароля на 20 символов



Рисунок 1.3 — Результат генерации пароля на 30 символов

Была произведена проверка равномерности распределения на 660000 символов. Результат проверки приведен на рисунке 1.4.

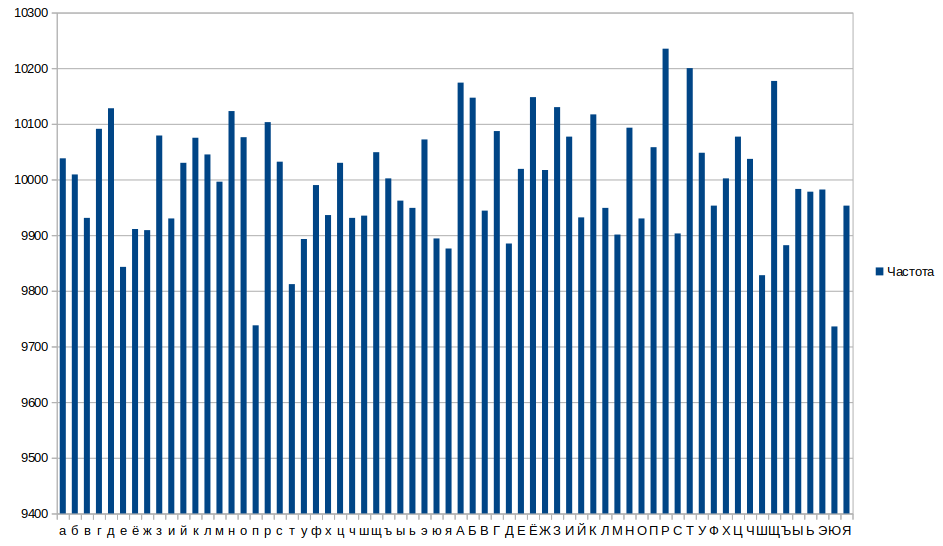


Рисунок 1.4 — Частотное распределение символов

Результаты подбора паролей на определенное количество символов приведены на рисунке 1.5.

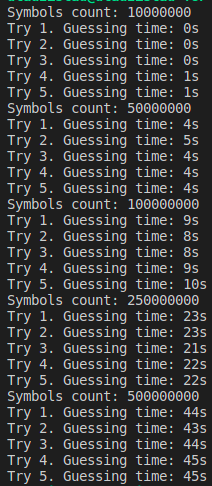


Рисунок 1.5 — Результаты подбора паролей

Среднее время подборов паролей по количеству символов приведено в таблице 1.1.

Таблица 1.1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Количество символов | 10000000 | 50000000 | 100000000 | 250000000 | 500000000 |
| Среднее время подбора (секунд) | 0.4 | 4.2 | 8.8 | 22.2 | 44.2 |

**Задание 2:** Построить график зависимости среднего времени подбора пароля от его длины.

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

Время на подбор остальных паролей рассчитывается вручную, т.к. оно слишком велико.

|  |  |
| --- | --- |
| 6 элементов | 1.7 часа |
| 7 элементов | 3.79 дня |
| 8 элементов | 197 дней |
| 9 элементов | 28 лет |
| 10 элементов | 1458.8 лет |

**Оценка подбора:** Время подбораэкспоненциально зависит от мощности алфавита и длины подбираемого пароля. Дольше всего будет подбираться пароль, состоящий полностью из последней буквы в алфавите (Z), быстрее всего – из первой (a).

Даже в условиях сильно ограниченного времени, 121 секунды должно хватить на подбор пароля по модели «скринсейвера», когда оператор машины временно за ней отсутствует. Так что пароль рекомендуется делать не меньше 6ти символов.

Если в систему имеется доступ извне и нет ограничений по вводу паролей, нежелательно делать пароль короче, чем 8 символов.

Если система обладает высокой ценностью и пароль на ней меняется редко, желательно использовать пароли от 9 и более символов.

