Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет информатики и радиоэлектроники

Факультет информационных технологий и управления
Кафедра интеллектуальных информационных технологий

Отчет по лабораторной работе №1
по курсу “Средства и методы защиты информации в интеллектуальных системах”
Вариант 4

Выполнил:
Студент гр. 321703 Титов А.В.

Проверил: Сальников Д.А.

Минск 2025

ЛАБОРАТОРНАЯ РАБОТА № 1 “ГЕНЕРАЦИЯ ПАРОЛЕЙ”

Цель:

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

— генерация строки с заданной пользователем длиной, состоящей из символов алфавита в соответствии с вариантом задания (использовать функции rand( ), srand( ) и инициализацию от таймера);

– поверка равномерности распределения символов путем визуализации частотного распределения;

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

2) Построить график зависимости среднего 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.

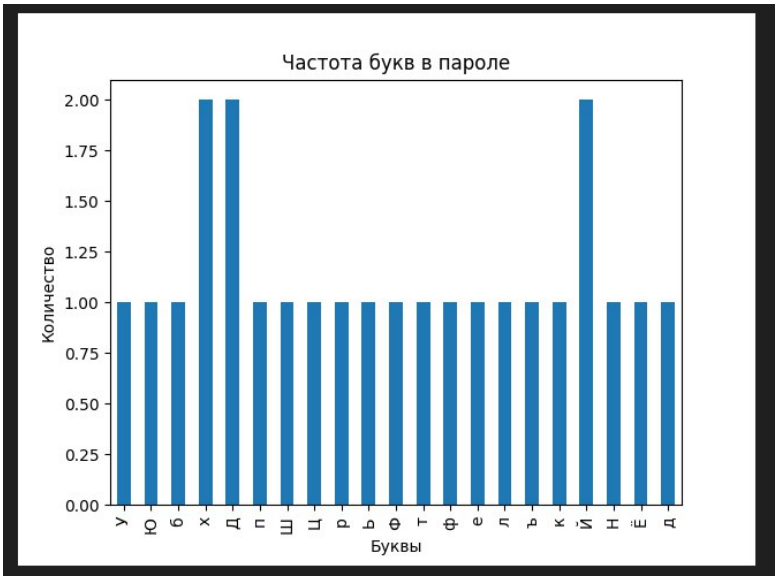
Варианты алфавита для генерации пароля:

4) Буквы русского языка строчные и прописные.

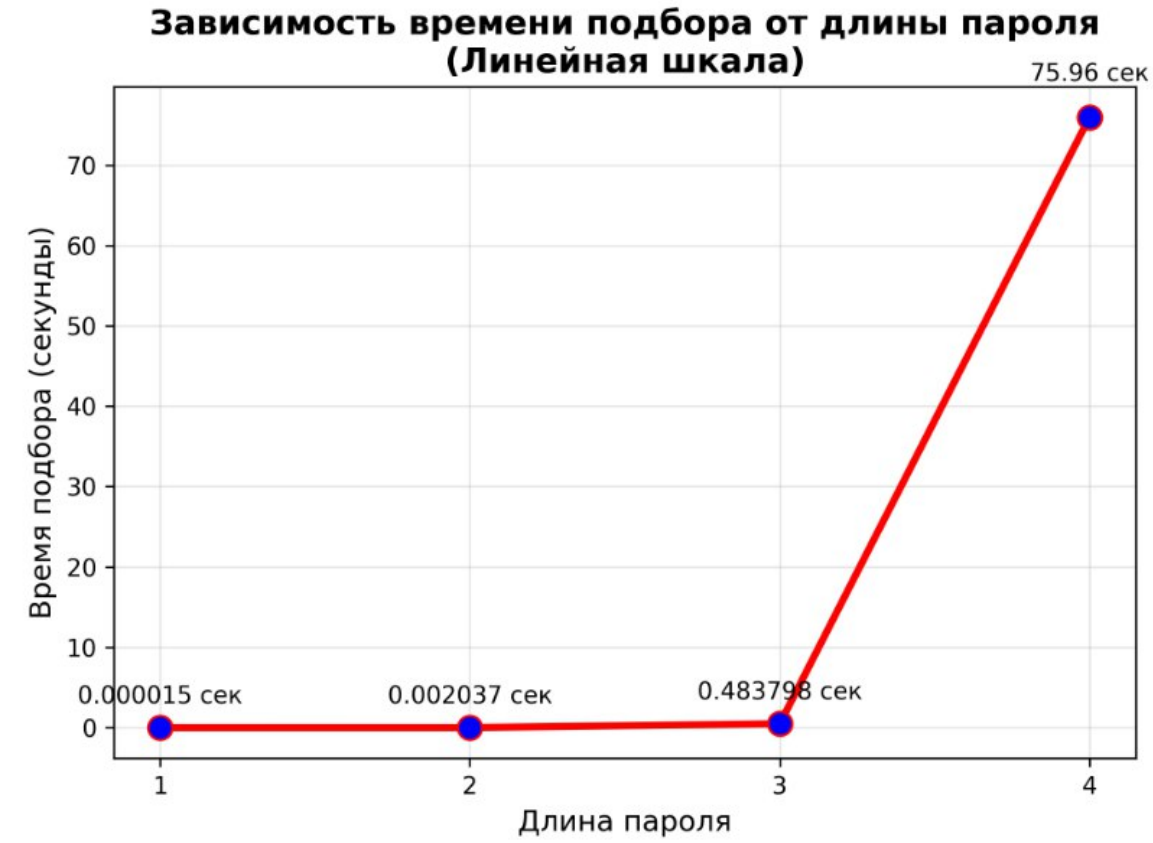
1) Пример работы программы:

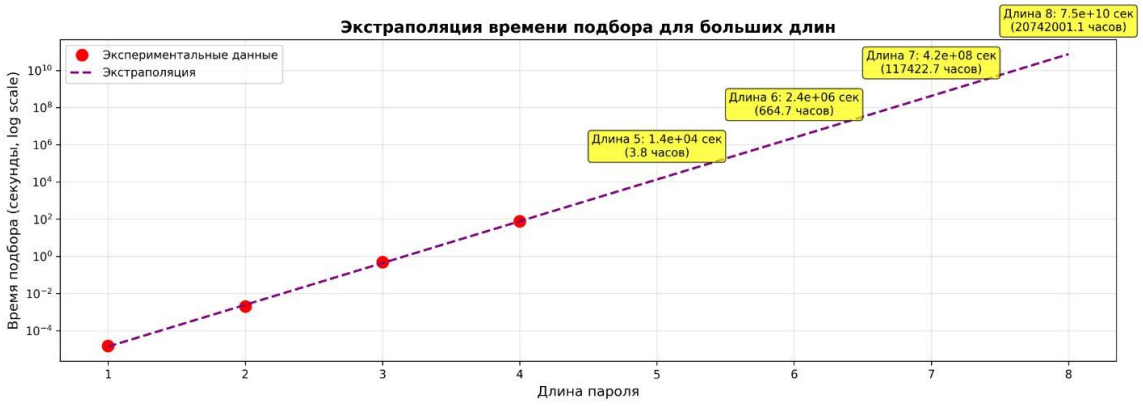
```
(myvenvv) artem@artem-ASUS-TUF-Gaming-A15-FA507RE-FA507RE:~/Рабочий стол$ "/home/artem/Рабочий стол/SIMZIS/myvenvv/bin/python" "
Введите длину пароля 24
абвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
Сгенерированный пароль: УЮбхДпШЦрЬФтфелъДкЙНхЁдЙ
dict_values([1, 1, 1, 2, 2, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 1, 1, 1])
dict_keys(['У', 'Ю', 'б', 'х', 'Д', 'п', 'Ш', 'Ц', 'р', 'Ь', 'Ф', 'т', 'ф', 'е', 'л', 'ъ', 'к', 'Й', 'Н', 'Ё', 'д'])
(myvenvv) artem@artem-ASUS-TUF-Gaming-A15-FA507RE-FA507RE:~/Рабочий стол$
```

Частотное распределение:



Построить график зависимости среднего времени подбора пароля от его длины





Рекомендации:

1. Используйте длинные пароли-фразы**.** С ростом длины пароля количество возможных комбинаций (энтропия) растёт **экспоненциально**.
2. Используйте разный регистр
3. Для сильно длинных паролей можно использовать ассоциативный ряд: часть имени + фамилии + любимый цвет и т.п.
4. **Низкая ценность** (одноразовая регистрация на форуме): достаточно пароля из **10-12 символов**.

- **Средняя ценность** (почта, соцсети): необходим надёжный пароль из **14-16+ символов**.
- **Высокая ценность** (банк, основная почта, аккаунт на работе): **обязательно используйте менеджер паролей** для генерации и хранения максимально длинных и сложных паролей (20+ символов), **и двухфакторную аутентификацию (2FA)**.

Вывод: Разработал программу для генерации пароля, а так же для его перебора. Проверил эффективность перебора для различной длины паролей, построил графики зависимости, а так же построил график равномерности распределения символов. Дал практические рекомендации по выбору пароля исходя из предположений об алфавите пароля.