Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра интеллектуальных информационных технологий

**Отчет по лабораторной работе №1**

**по курсу «СиМОИБ»**

**на тему: «Генерация паролей»**

|  |  |
| --- | --- |
| Выполнил студентк  группы 821703: | Веренич К.О. |
| Проверил: | Захаров В.В. |

**МИНСК**

2020

**Задание 1 :** Написать программу генерации пароля

Требования к генерируемому паролю:

1. Пароль - текстовая строка длиной 1, 2, 3, 4, 6, 8, 10 символов.
2. Для генерации использовать функции rand, srand.
3. Пароль должен состоять из следующих наборов символов:

f) цифры , латиница строчные.

Оценить качество генерации.

**Задание 2:** Написать программу подбора пароля, сгенерированного в задании 1. Программа должна выводить время, затраченное на подбор пароля. Оценить зависимость времени, затраченного на подбор паролей от длины и использованных символов. Вместе с программой представить отчет, в котором описаны реализованные в программе методы и оценки времени.

**Оценка генерации:** На вход ГПСЧ подается системное время, после чего генерируется псевдослучайный набор символов. Сгенерированные подобным образом пароли хороши тем, что не являются осмысленными словами и никак не связаны с личными данными пользователя. Минус состоит в сложности запоминания. Также если злоумышленнику известно время создания пароля, перебирать становится проще. При желании в алфавит пароля можно добавить больше элементов, например, символы, что увеличит время, необходимое на атаку.

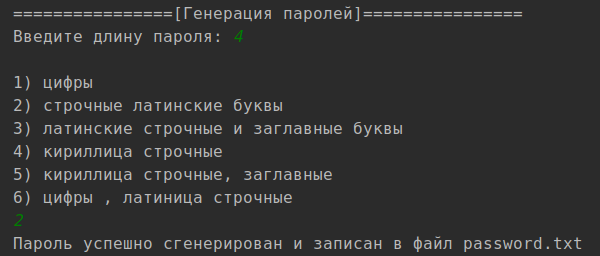
**Результат подбора:**

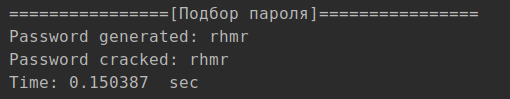
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 1 попытка | 2 попытка | 3 попытка | 4 попытка | 5 попытка | Среднее время |
| 1 элемент | c  < 0.00001 сек | 7  < 0.00001 сек | h  < 0.00001 сек | w  < 0.00001 сек | j  < 0.00001 сек | < 0.00001 сек |
| 2 элемента | Jz  0.000929 сек | ip  < 0.000624 сек | e9  < 0.00022 сек | bf  < 0.00041 сек | xd  < 0.00038 сек | 0.0005106 сек |
| 3 элемента | 5tr  0.024 сек | 10z  0.011 сек | gie  0.010 сек | 6we  0.014 сек | c8x  0.23 сек | 0.082 сек |
| 4 элемента | cb8e  0.417 сек | tbj5  0.137 сек | in1n  0.669 сек | e90l  0.631 сек | wchx  0.975 сек | 0.5658 сек |
| 5 элементов | ximj  19.31 сек | zqs05  5.21 сек | k5vln  22.64 сек | fa2mh  18.03 сек | Hw7rc  14.73 сек | 15.954 сек |
| 6 элементов | 66fwfa  349 сек | 0col1y  1146 сек | 3l6suc  453 сек | pn10et  335 сек | 07haqt  1020 сек | 660 сек |

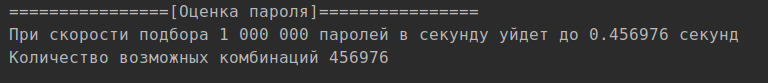
Время на подбор остальных паролей рассчитывается вручную, т.к. оно слишком велико.

|  |  |
| --- | --- |
| 7 элементов | 10 часов |
| 8 элементов | 16 дней |
| 9 элементов | 1,6 года |
| 10 элементов | 57 лет |

**Выполнение программы:**







**Оценка подбора:**

Время необходимое на подбор пароля экспоненциально зависит от мощности алфавита и длины пароля. В данном алгоритме подбора пароля дольше всего будет подбираться пароль, состоящий полностью из последней буквы в алфавите, быстрее всего – из первой.

В условиях сильно ограниченного времени, 150 секунд должно хватить на подбор пароля по модели «скринсейвера», когда оператор машины временно за ней отсутствует, при условии, что пароль состоит из 6 строчных латинских букв.

Пароль рекомендуется делать не меньше 8-ми символов, содержащий строчные и заглавные буквы, цифры, символы.

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