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.

**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.

**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.

#include <iostream>

#include <string>

#include <ctime>

#include <fstream>

using namespace std;

void main(void)

{

setlocale(LC\_ALL, "Russian");

char alphabet[] = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ";

int n; cout << "Введите количество символов: "; cin >> n;

string out = "";

srand(time(0));

for (int i = 0; i < n; i++) {

out += alphabet[(rand() % 52)];

}

cout << "Ваш пароль: " << out << endl;

const char \*finout = out.c\_str();

double start\_time = clock();

for (int j = 0; j < pow(sizeof(alphabet)-1, strlen(finout)); j++) {

char generated[10];

int k = 0;

for (int i = strlen(finout) - 1; i >= 0; i--) {

generated[k] = alphabet[(j / int(pow(sizeof(alphabet)-1, i))) % (sizeof(alphabet)-1)];

k++;

}

generated[k] = '\0';

if (strcmp(generated, finout) == 0) {

double end\_time = clock();

cout << "Время взлома: " << (end\_time - start\_time) / 1000 << " секунд" << endl;

break;

}

}

}

**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 дополнительные символы, например, цифры, что увеличит время, необходимое на атаку.

**Результат подбора:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 1 попытка | 2 попытка | 3 попытка | 4 попытка | 5 попытка | Среднее время |
| 1 элемент | i  < 0.001 сек | H  < 0.001 сек | g  < 0.001 сек | w  < 0.001 сек | J  < 0.001 сек | < 0.001 сек |
| 2 элемента | qQ  0.001 сек | AU  < 0.001 сек | us  < 0.001 сек | ib  < 0.001 сек | cz  < 0.001 сек | < 0.001 сек |
| 3 элемента | drv  0.003 сек | lNU  0.011 сек | Njz  0.041 сек | emx  0.004 сек | EmM  0.036 сек | 0.019 сек |
| 4 элемента | GJNk  2.066 сек | aiRo  0.013 сек | OBCg  2.499 сек | jgcC  0.566 сек | GEPL  2.032 сек | 1.4352 сек |
| 5 элементов | sBgFU  73 сек | KFIRa  150 сек | RbdUL  170 сек | UktOS  184 сек | hiZxe  28 сек | 121 сек |

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.

