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

Вариант №7

по дисциплине

Средства и методы защиты информации в интеллектуальных системах

Выполнил: А. С. Терлеев

Студент группы

121703

Проверил: В. В. Захаров

Минск 2023

Тема: Генерация паролей

Задача: 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.

Листинг программы:

```cpp
#include "RandomDevice.h"


RandomDevice::RandomDevice(unsigned long n) : rand_seed(n), engine(n){ }

int RandomDevice::randInt(int min, int max){
    std::uniform_int_distribution<int> distribution(min, max);
    return distribution(engine);
}

char RandomDevice::randChar(const std::string& alphabet) {
    return alphabet.at(randInt(0,  int(alphabet.length()) - 1));
}

std::string RandomDevice::randString(const std::string& alphabet, int length) {
    std::string result;
    for (int i = 0; i < length; i++)
        result += randChar(alphabet);
    return result;
}
```

```cpp
#include <chrono>

namespace ch = std::chrono;

template <typename duration = ch::seconds, typename clock = ch::high_resolution_clock>
class Timer
{
    typename clock::time_point m_start, m_stop;

public:
    void start() { m_start = clock::now(); }
    const Timer& stop()  { m_stop = clock::now(); return *this; }

    typename clock::rep get_time() const
    {
        return ch::duration_cast<duration>(m_stop - m_start).count();
    }
};
```

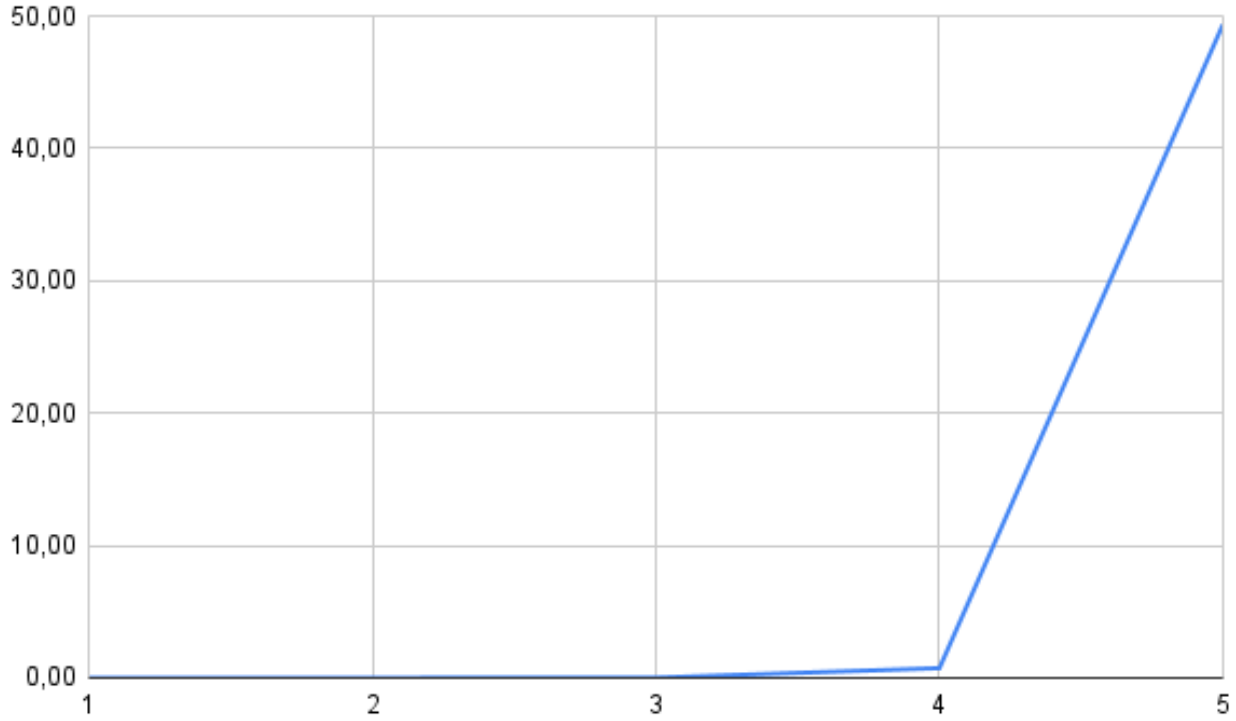
```cpp
#include "iostream"
#include "src/RandomDevice.h"
#include "src/Timer.cpp"

bool brute(const std::string& text, const std::string& pass, const std::string& alphabet) {
    if (text.length() == pass.length()) {
        if (text == pass) {
            return true;
        }
        return false;
    }
    for (const char &ch: alphabet) {
        if (brute(text + ch, pass, alphabet)){
            break;
        }
    }
}


void test(RandomDevice& randomDevice) {
    std::string alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789";
    Timer<std::chrono::milliseconds> aTimer;
    std::chrono::high_resolution_clock::rep sumTime;
    for (int i = 1; i < 6; i++) {
        std::cout << "---- Length: " << i << " ----\n";
        sumTime = 0;
        for (int j = 0; j < 5; j++) {
            std::string randString = randomDevice.randString(alphabet, i);
            std::cout << "\tString: " << randString << "\n";
            aTimer.start();
            brute("", randString, alphabet);
            aTimer.stop();
            std::cout <<"\tTime: " << aTimer.get_time() << "ms \n\n";
            sumTime += aTimer.get_time();
        }
        std::cout <<"\tAverage time: " << sumTime / 5 << "ms \n\n";
    }
}


int main(){
    unsigned long seed = time(nullptr);
    RandomDevice my_rand(seed);
    test(my_rand);
}
```

График зависимости среднего времени подбора пароля от его длины (на ASUS VivoBook S15):



Дальнейшие расчеты проведем вручную

- При 6 элементах - 1.5 ч
- При 7 элементах - 3.8 дней
- При 8 элементах - 260 дней
- При 9 элементах - 50 лет
- При 10 элементах - 3100 лет

Вывод:

В данной лабораторной работе была разработана программа на языке C++, которая выполняет несколько функций, связанных с генерацией и подбором паролей.

Рекомендации по выбору пароля:

- Используйте пароли достаточной длины (минимум 10 символов). Более длинные пароли обычно сложнее подобрать методами перебора. По результатам проверки на ASUS Vivobook S15 подбор пароля длинной в 10 сиволов будет длиться 3100 лет

- Разнообразьте пароль, включая в него различные типы символов, такие как буквы (в разных регистрах), цифры и специальные символы. Это усложнит процесс подбора пароля. Добавление одного символа в алфовит увеличивает время подбора (имеется логарифмическая зависимость).
- Избегайте использования очевидных паролей, таких как "123456"или "password". Такие пароли являются первыми кандидатами для атакующих.