|  |  |  |
| --- | --- | --- |
| Министерство науки и высшего образования  Российской Федерации | | |
| Федеральное государственное бюджетное  образовательное учреждение высшего образования | | |
| «Новосибирский государственный технический университет» | | |
|  | | |
|  | | |
|  | | |
| Практическое задание №6 | | |
| по дисциплине «Методы построения и анализа алгоритмов» | | |
|  | | |
| **кафедра теоретической и прикладной информатики** | | |
|  | | |
|  | Факультет: | ПМИ |
| Группа: | ПМИ-03 |
| Бригада: | Место для ввода текста. |
| Студенты: | Сидоров Даниил, |
|  | Малыгин Сергей |
|  |  |
| Преподаватели: | Щукин Георгий Анатольевич |
|  |  |
|  | | |
| Новосибирск | | |
| 2021 | | |

**1.Результаты замеров:**

|  |  |  |
| --- | --- | --- |
| Размер алфавита | Длина пароля | Время |
| 4 | 5 | 0.0076351 sec |
| 6 | 0.0295074 sec |
| 7 | 0.127023 sec |
| 8 | 0.500663 sec |
| 9 | 2.05471 sec |
| 10 | 7.93639 sec |
|  | | |
| 5 | 5 | 0.0221585 sec |
| 6 | 0.111989 sec |
| 7 | 0.583728 sec |
| 8 | 2.49788 sec |
| 9 | 14.191 sec |
| 10 | 72.1044 sec |
|  | | |
| 6 | 5 | 0.0557124 sec |
| 6 | 0.346583 sec |
| 7 | 2.05278 sec |
| 8 | 10.6752 sec |
| 9 | 72.7289 sec |
| 10 | 446.803 sec |

**2.Программа:**

**Main.cpp**

#define CATCH\_CONFIG\_RUNNER

#include "catch.hpp"

#include<iostream>

#include "bruteforce.h"

#include "sha256.h"

using namespace std;

int main(int argc, char \*argv[])

{

int result = Catch::Session().run(argc, argv);

setlocale(LC\_ALL, "rus");

auto t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("bacab"), "abcd", 5);

auto t2 = std::chrono::high\_resolution\_clock::now();

auto seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 4,длина 5 " << ": " << "Time: " << seconds << " sec." << endl;

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("bacada"), "abcd", 6);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 4,длина 6 " << ": " << "Time: " << seconds << " sec." << endl;

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("bacabdc"), "abcd", 7);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 4,длина 7 " << ": " << "Time: " << seconds << " sec." << endl;

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("bacbaccd"), "abcd", 8);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 4,длина 8 " << ": " << "Time: " << seconds << " sec." << endl;

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("baccaddaa"), "abcd", 9);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 4,длина 9 " << ": " << "Time: " << seconds << " sec." << endl << endl;

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("baccaddaab"), "abcd", 10);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 4,длина 10 " << ": " << "Time: " << seconds << " sec." << endl << endl;

//////////////////

//////////////////

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("baeed"), "abcde", 5);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 5,длина 5 " << ": " << "Time: " << seconds << " sec." << endl;

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("baeead"), "abcde", 6);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 5,длина 6 " << ": " << "Time: " << seconds << " sec." << endl;

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("bacebda"), "abcde", 7);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 5,длина 7 " << ": " << "Time: " << seconds << " sec." << endl;

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("becbadea"), "abcde", 8);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 5,длина 8 " << ": " << "Time: " << seconds << " sec." << endl;

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("baccedead"), "abcde", 9);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 5,длина 9 " << ": " << "Time: " << seconds << " sec." << endl << endl;

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("baccedeadb"), "abcde", 10);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 5,длина 10 " << ": " << "Time: " << seconds << " sec." << endl << endl;

//////////////////

//////////////////

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("bafea"), "abcdef", 5);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 6,длина 5 " << ": " << "Time: " << seconds << " sec." << endl;

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("bafead"), "abcdef", 6);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 6,длина 6 " << ": " << "Time: " << seconds << " sec." << endl;

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("bacefde"), "abcdef", 7);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 6,длина 7 " << ": " << "Time: " << seconds << " sec." << endl;

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("bedfaced"), "abcdef", 8);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 6,длина 8 " << ": " << "Time: " << seconds << " sec." << endl;

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("bacfefead"), "abcdef", 9);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 6,длина 9 " << ": " << "Time: " << seconds << " sec." << endl;

t1 = std::chrono::high\_resolution\_clock::now();

bruteforce(sha256("bacfefeadb"), "abcdef", 10);

t2 = std::chrono::high\_resolution\_clock::now();

seconds = std::chrono::duration<double>(t2 - t1).count();

cout << "Алфавит 6,длина 10 " << ": " << "Time: " << seconds << " sec." << endl;

return result;

}

**Bruteforce.cpp**

string bruteforce(const string &password\_hash, const string &alphabet, int max\_length) {

int max\_set = 0, j = 0, size\_alphabet = alphabet.size();

string password = "";

for (int i = 0; i < max\_length; ++i)

{

password.resize(i + 1, alphabet[0]);

j = password.size() - 1;

max\_set = 0;

for (int i = 0; i < password.size() - 1; ++i)

{

password[i] = alphabet[alphabet.size() - 1];

}

while (max\_set != pow(alphabet.size(), i + 1))

{

password[j] = alphabet[size\_alphabet - 1];

++max\_set;

size\_alphabet--;

if (sha256(password) == password\_hash)

{

return password;

}

if (size\_alphabet == 0)

{

size\_alphabet = alphabet.size();

if (password[password.size() - 1] <= alphabet[0])

{

password[password.size() - 1] = alphabet[alphabet.size() - 1];

if (password.size() > 1) --password[password.size() - 2];

}

for (int k = i - 1; k > 0; k--)

{

if (password[k] < alphabet[0])

{

password[k] = alphabet[alphabet.size() - 1];

--password[k - 1];

}

}

}

}

}

return "";

}