

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**Український державний університет науки і технологій**

Кафедра «Комп’ютерні інформаційні технології»

**Лабораторна робота №6**

**з дисципліни «Безпека програм та даних»**

**на тему: «Кількісна оцінка стійкості парольного захисту»**

Виконав: ???

Прийняв: ???

Дніпро, 2023

**Тема**: Кількісна оцінка стійкості парольного захисту.

**Мета**: Реалізація найпростішого генератора паролів, що володіє необхідною стійкістю до злому.

**Завдання**:

Реалізувати програму для генерації паролів користувачів. Програма повинна формувати випадкову послідовність символів довжини L, при цьому повинен використовуватися алфавіт з A символів.

|  |  |  |  |
| --- | --- | --- | --- |
| Варіант | *P* | *V* | *T* |
| 11 | 10-6 | 11 паролів/хвилину | 2 неділі |

**Короткі теоретичні відомості:**

Підсистеми ідентифікації і аутентифікації користувача відіграють важливу роль в системах захисту інформації. Стійкість підсистеми ідентифікації і аутентифікації користувача в системі захисту інформації (СЗІ) багато в чому визначає стійкість до злому самої СЗІ. Дана стійкість визначається гарантією того, що зловмисник не зможе пройти аутентифікацію, присвоївши чужий ідентифікатор або вкравши його.

Парольні системи ідентифікації / аутентифікації є одними з основних і найбільш поширених в СЗІ методами користувальницької аутентифікації. В даному випадку інформацією, аутентифікуючою користувача, є певний секретний пароль, відомий тільки легальному користувачеві.

Парольна аутентифікація користувача, як правило, передній край оборони СЗІ. У зв'язку з цим модуль аутентифікації по паролю найбільш часто піддається атакам з боку зловмисника. Мета останнього в даному випадку - підібрати аутентифікуючу інформацію (пароль) легального користувача.

**Обчислення необхідних даних**

Обчислення за формулою (1) нижньої межі S\*

Формула 1:  *S*\* = [*V ∙ P / T*],

S\* = 11\*60\*24\*10-6/14= 1 131 \* 10-6

Отримання мінімальної довжини пароля L, при якому виконується умова.

Умові S \* ≤ AL задовольняють, наприклад, такі комбінації A і L, A = 52, L = 8 (пароль складається з восьми символів, серед яких можуть бути малі латинські букви і довільні цифри).

**Текст програми:**

#include <iostream>

#include <ctime>

std::string alphabet = "";

char random\_symvol()

{

return alphabet[rand() % alphabet.length()];

}

int main()

{

srand(time(0));

for (char i = 'a'; i <= 'z'; i++)

{

alphabet += i;

}

for (char i = 'A'; i <= 'Z'; i++)

{

alphabet += i;

}

for (char i = '0'; i <= '9'; i++)

{

alphabet += i;

}

std::string password = "";

for (int i = 0; i < 8; i++)

{

password += random\_symvol();

}

std::cout << "Random password: " << password << std::endl;

system("pause");

return 0;

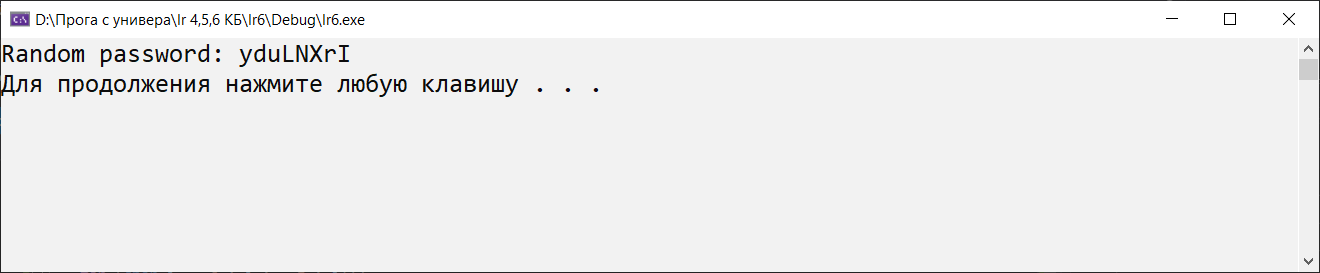
}

**Результати виконання програми:**

1) Перший запуск програми



2) Другий запуск програми



**Висновок**: під час виконання лабораторної роботи я навчився реалізовувати найпростіший генератор паролів, що володіє необхідною стійкістю до злому.