Львівський національний університет імені Івана Франка

**Звіт про виконання лабораторної роботи №2**

з навчальної дисципліни

«Основи інформаційної та кібербезпеки»

на тему:

**«Дослідження криптостійкості паролів»**

Студентки ІІ курсу

групи ПМО-21

Кравець О. Б.

Львів – 2022

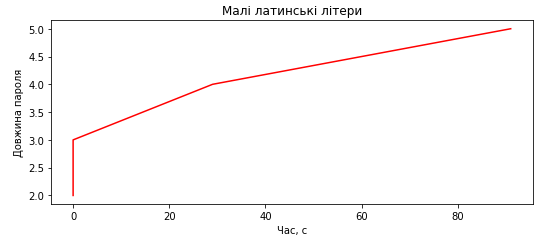
**Хід роботи**

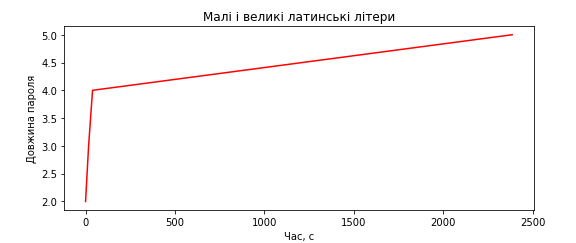
**Завдання А.** Розкриття закритих паролем архівів у програмі KRyLack ZIP Password Recovery.

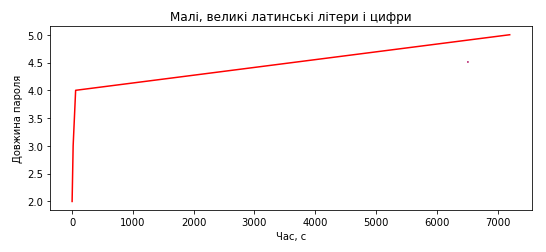
1. За допомогою програми архівації даних 7-zip було створено архівний файл zip і встановлено на нього пароль завдовжки 2 маленькі латинські літери.
2. Створений архів відкрито в програмі KRyLack ZIP Password Recovery і проведено перебір паролів за методом «грубої сили».
3. Вказані у пунктах 1-23 дії повторено для паролів різної довжини і різних наборів символів (мінімальну довжину для всіх випадків залишала 1).
4. Результати перебору паролів:

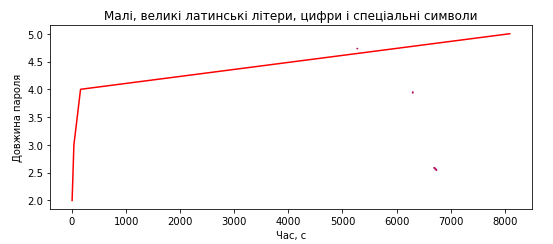
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № з/п | Набір  символів | Довжина пароля, символів | Час перебору,  с | Швидкість перебору,  паролів/c |
|  | Малі латинські літери (fg) | 2 | 0 |  |
|  | Малі латинські літери (dhl) | 3 | 0 |  |
|  | Малі латинські літери (kpsl) | 4 | 29 | 6013 |
|  | Малі латинські літери (adcfg) | 5 | 91 | 5036 |
|  | Малі і великі латинські літери (Wq) | 2 | 0 |  |
|  | Малі і великі латинські літери (Lkl) | 3 | 17 | 6155 |
|  | Малі і великі латинські літери (aBfF) | 4 | 39 | 4087 |
|  | Малі і великі латинські літери (bcDGK) | 5 | 2385  (39 хв, 45 с) | 6364 |
|  | Малі латинські літери і цифри (w5) | 2 | 0 |  |
|  | Великі латинські літери і цифри (Q5) | 2 | 0 |  |
|  | Малі, великі латинські літери і цифри (Xa6) | 3 | 17 | 5241 |
|  | Малі, великі латинські літери і цифри (aH8q) | 4 | 58 | 6538 |
|  | Малі, великі латинські літери і цифри (Bc2h3) | 5 | > 2 год (я вже не дочекалася) | 4054 |
|  | Малі, великі латинські літери і цифри (aaA11) | 5 | 14 (мінімальну довжину тут поставила 5, бо інакше дуже довго чекати) | 6979 |
|  | Малі латинські літери і спеціальні символи (g%) | 2 | 0 |  |
|  | Великі латинські літери і спеціальні символи (\_W) | 2 | 1 | 6584 |
|  | Цифри і спеціальні символи (7$) | 2 | 0 |  |
|  | Малі, великі латинські літери і спеціальні символи (Af#) | 3 | 34 | 7001 |
|  | Малі латинські літери, цифри і спеціальні символи (f6/) | 3 | 9 | 6564 |
|  | Великі латинські літери, цифри і спеціальні символи (J9)) | 3 | 58 | 6831 |
|  | Малі, великі латинські літери, цифри і спеціальні символи (aA1$) | 4 | 157 | 6988 |
|  | Малі, великі латинські літери, цифри і спеціальні символи (aA1$a) | 5 | >3 год (я вже не дочекалася) | 5086 |
|  | Малі, великі латинські літери, цифри і спеціальні символи (aA1$a) | 5 | 5385 (мінімальну довжину тут поставила 5, бо інакше дуже довго чекати) | 6941 |

1. Графіки залежності часу підбору пароля від довжини пароля для різних використаних наборів символів (де було по декілька варіантів часу для однієї довжини брала середнє значення)









**Завдання Б.** Написати програму, яка відновлює пароль з хеш-файлу.

Я ознайомився з тестом програми відновлення паролів зашифрованих за допомогою хеш-функції MD5.

Відповідно до номера залікової книжки мій варіант **25**.

За допомогою цієї програми підібрано пароль до його хешу:

**хеш : пароль**

**a1526a39242e120fb4efe081a5b87297 : CqeZj**

**Висновки:** Під час виконання цієї лабораторної роботи я навчилася розкривати закриті паролем архіви у програмі KRyLack ZIP Password Recovery та за допомогою програми на C++ відновлювати паролі зашифровані за допомогою хеш-функції MD5. Часу на виконання пішло не багато, єдине що сам підбір паролів займав багато часу, але в цей час я займалася іншими дз і це не створювало незручностей . Лабораторна робота була цікавою та потрібною для майбутнього, бо до цього я не займалася подібними речами. Мені сподобалося😊.