Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут ім. Ігоря Сікорського»

Факультет інформатики та обчислювальної техніки

Кафедра обчислювальної техніки

**ЛАБОРАТОРНА РОБОТА № 3**

з дисципліни «Системне програмування» на тему

«Дослідження структури програм формату EXE»

Виконав: Перевірив:

Студент 2 курсу ФІОТ-у доц. Павлов В. Г.

групи ІМ-12

Креславський Михайло Олегович

номер у списку групи - 11

Київ 2023

**Мета роботи:** ознайомлення із специфікацією COFF та вивчення прийомів дослідження структури файлу РЕ-формату.

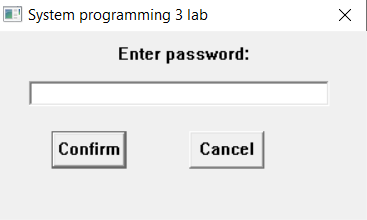
**Структура програм формату ЕХЕ:**

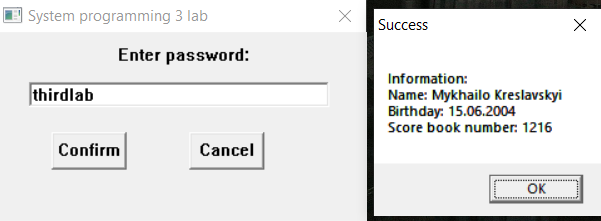
.ехе (executable - виконуваний) - це розширення виконуваного файлу, що застосовується в системах DOS, Microsoft Windows, та інших.

Файл EXE складається з двох частин: заголовок (інформація до завантажувача програми) та модуль завантаження. Заголовок займає перші 25 рядків файлу, та містить, зокрема інформацію про довжину файлу, розмір пам’яті, що потрібно виділити.

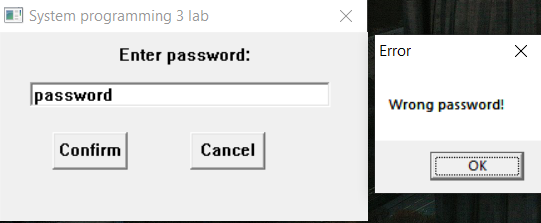
Після нього записана таблиця налаштування адрес, що складається з елементів, що мають два двобайтових поля - зміщення та адресу. що потрібно налаштувати на місце пам’яті в яке завантажується конкретна задача.

**Скріншоти виконання програми:**

Вікно для введення паролю:  


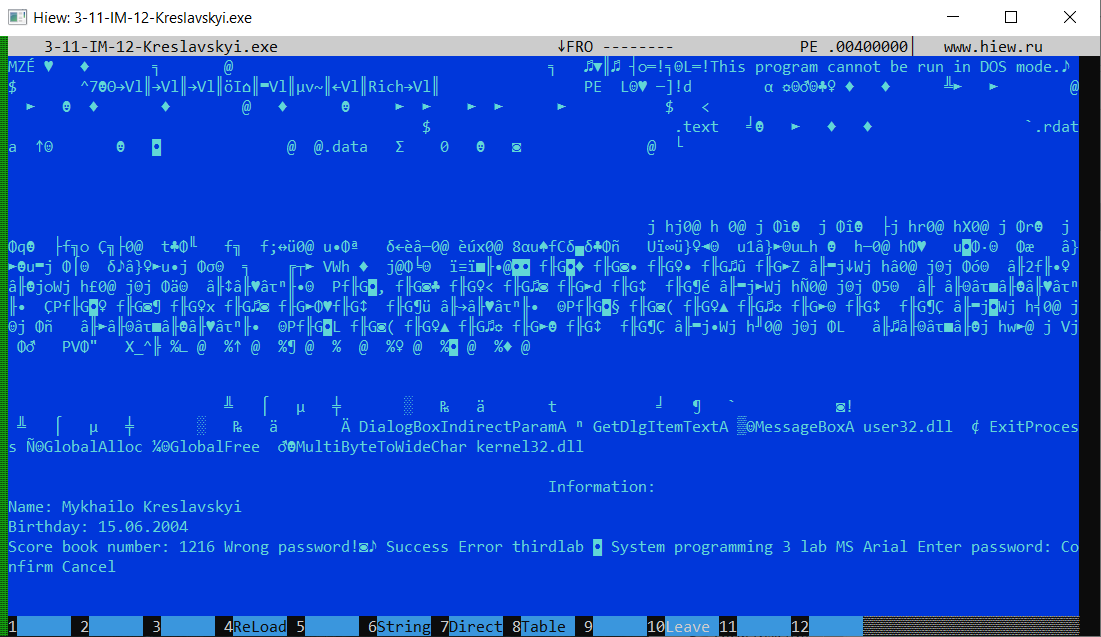
Якщо ввести правильний пароль:  


Якщо ввести неправильний пароль:



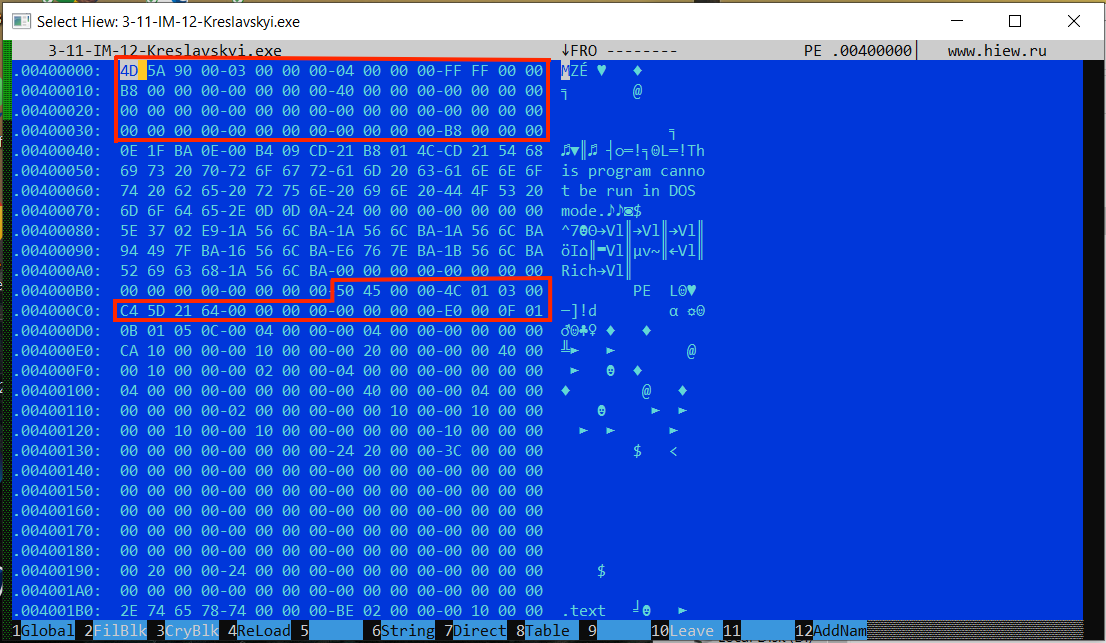
**Дослідження файлу в HIEW32:**

Текстовий формат:



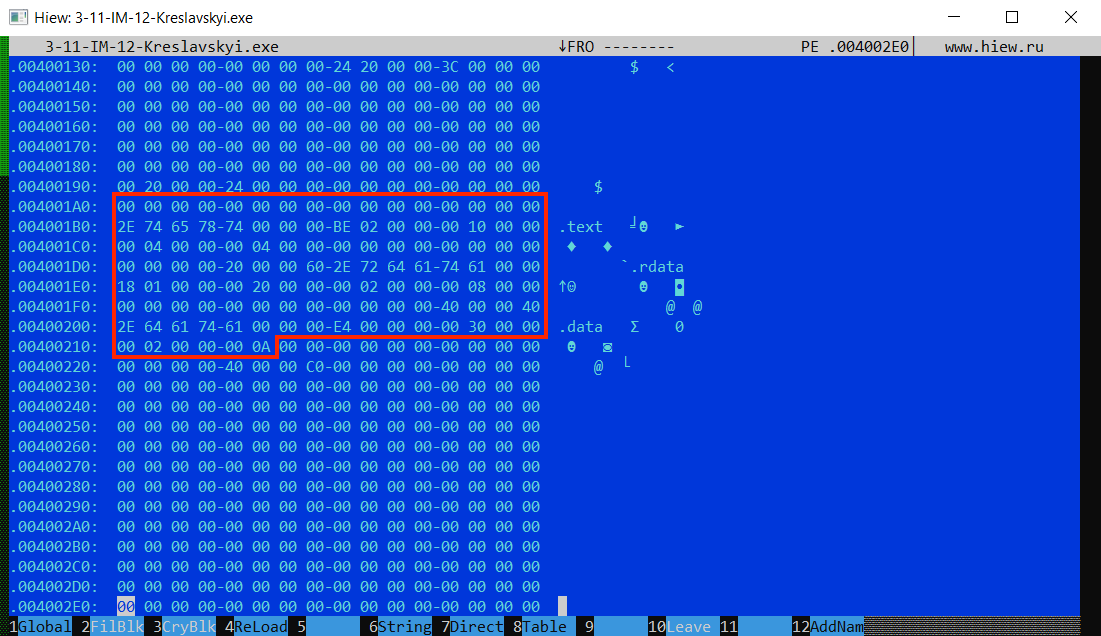
Шістнадцятковий формат:

1. DOS Header
2. PE Header
3. Section headers



2

1

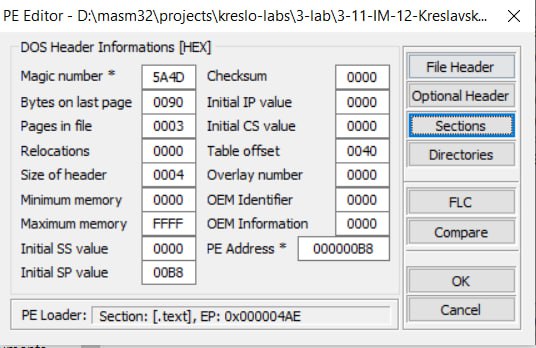


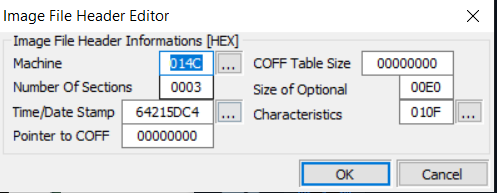
3

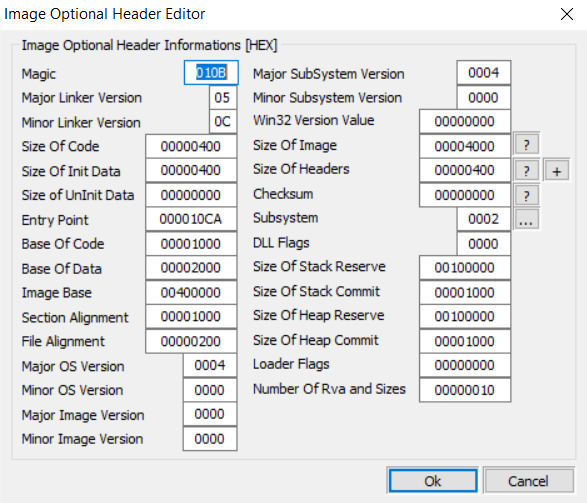
**Таблиця параметрів файлу:**

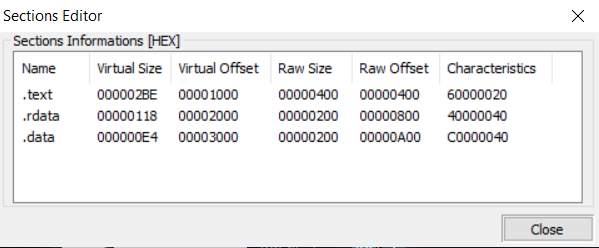
|  |  |  |  |
| --- | --- | --- | --- |
| Поле | Значення | Опис поля | Опис значення поля |
| Machine type | 014С | Тип машини (CPU) | Intel 386 або пізніша, та інші схожі процесори |
| Optional Header standard fields | | | |
| Magic | 5A 4D | Число типу unsigned integer, що ідентифікує стан файлу | Ідентифікатор нормального файлу типу .ехе |
| Major linker version | 05 | Номер версії основного лінкера | |
| Minor linker version | 0С | Номер версії меншого лінкера | |
| Size Of Code | 0000-0400 | Розмір секції коду | |
| Size Of Init Data | 0000-0400 | Розмір секції ініціалізованих змінних | |
| Size Of UnInit Data | 0000-0000 | Розмір секції неініціалізованих змінних | |
| Entry Point | 000010CA | Адреса вхідної точки в програму, початкова адреса програми | |
| BaseOfCode | 0000-1000 | Адреса початку секції коду, коли завантажено в пам’ять | |
| BaseOfData | 0000-2000 | Адреса початку секції змінних, коли завантажено в пам’ять | |
| Section Table (Section Headers) | | | |
| Name | text | Назва секції - 8 бітний стрінг ASCII | |
| Virtual Size | 0000-02BE | Розмір секції, завантаженої в пам’ять | |
| Virtual Offset | 0000-1000 | Адреса першого байту секції | |
| Raw Size | 0000-0400 | Розмір секції | |
| Pointer To Raw  Data |  | Пойнтер до першої сторінки секції у файлі COFF | |
| Pointer To  Relocations | 0 | Пойнтер до початку входжень релокацій в секцію (для файлів .ехе рівний 0) | |
| Pointer To  Linenumbers |  | Пойнтер до початку входжень в секцію чисел | |
| Number Of  Relocations | 0 | Кількість релокаційних входжень в секцію (для файлів .ехе рівний 0) | |
| NumberO  fLinenumbers |  | Кількість числових входжень у секцію | |
| Characteristics | 6000-0020 | Прапори опису характеристики секції | |

**Дослідження в PE Tools:**



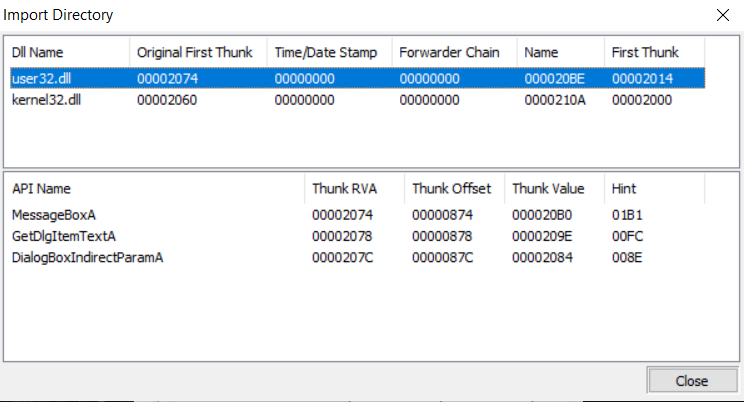


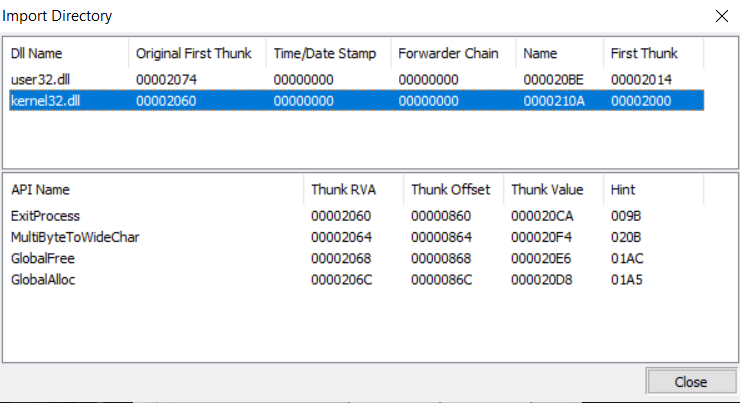




**Дослідження таблиці імпорту:**

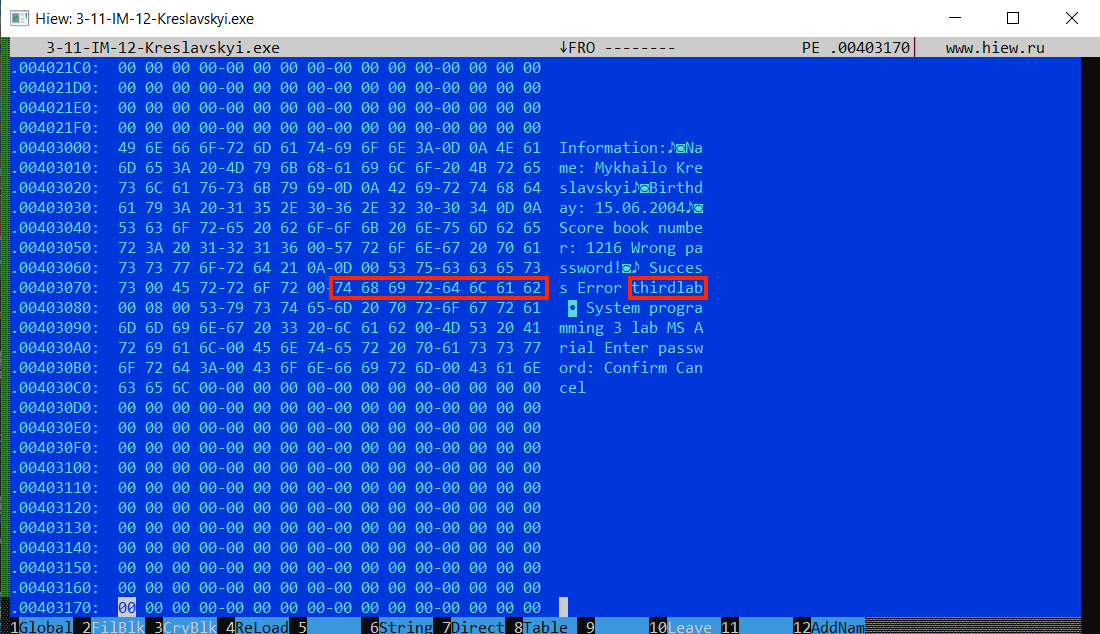
У програмі використовуються дві бібліотеки: user32.dll та kernel32.dll. Нижче наведено список функцій цих бібліотек, які використовуються в програмі і який було знайдено за допомогою PE Tools.





**Виявлення паролю у тексті файлу:**

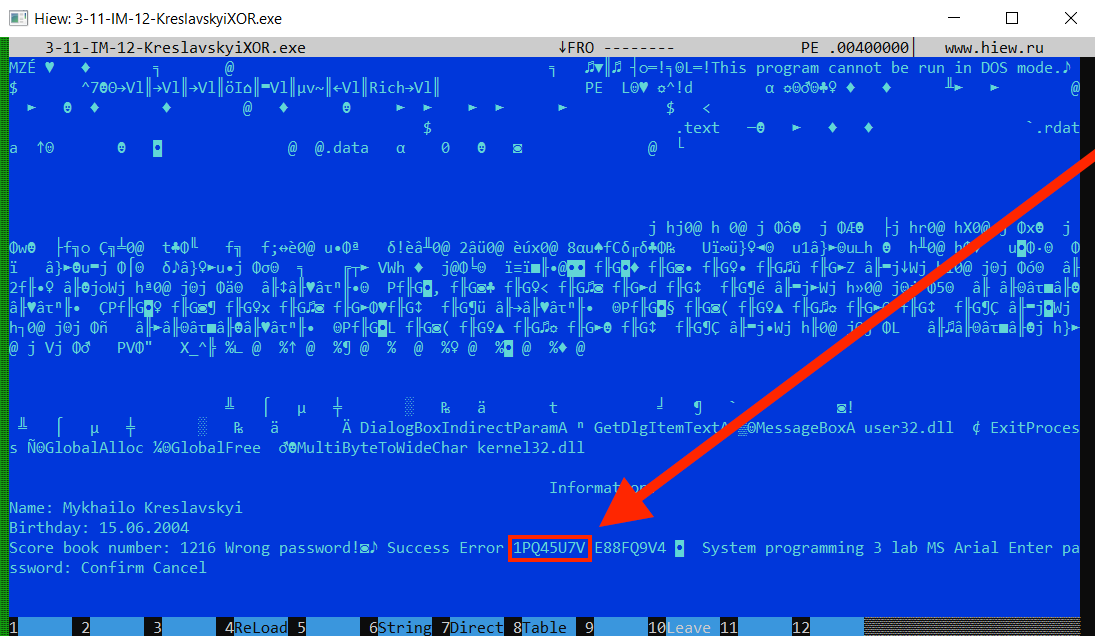
Як можна побачити, пароль явно зберігається у файлі:



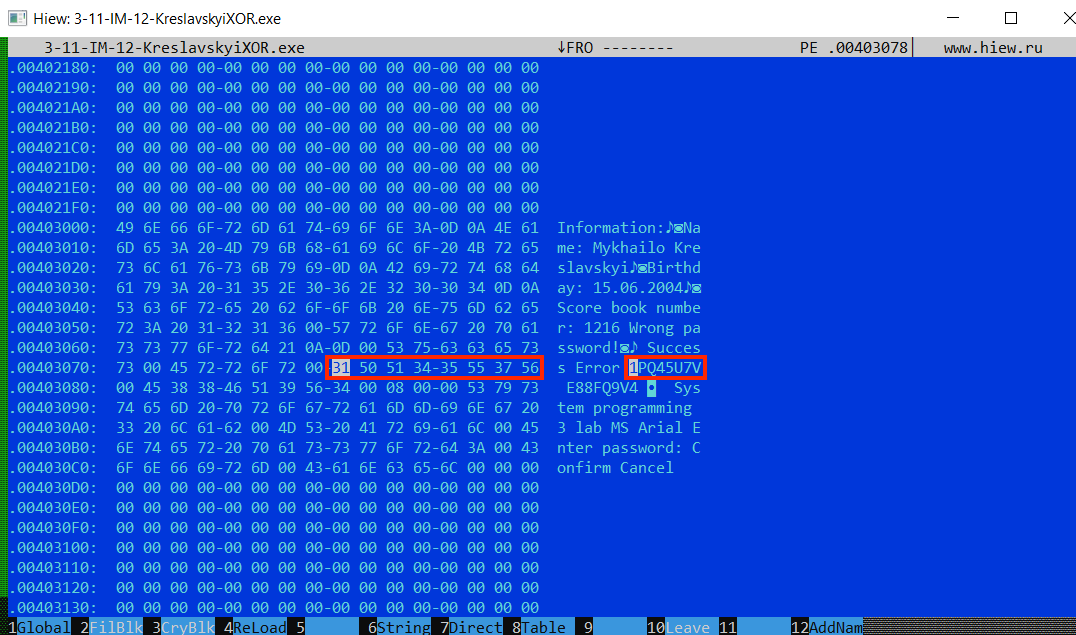
**Дослідження файлу, де пароль зашифрований методом XOR:**

Обидві версії програми використовували однаковий пароль, але в другій версії пароль не був збережений явно, а був зашифрований за допомогою простого методу XOR-шифрування. У цьому методі кожна буква пароля переводиться в двійкове число за таблицею ASCII, потім кожен біт цього числа побітово «XOR-иться» з певним числом. Отримані біти конкатенуються в байт, який потім переводиться в символ ASCII. Зашифровані символи зберігаються в рядку «1PQ45U7V». Щоб дешифрувати пароль, потрібно застосувати той самий алгоритм до зашифрованого рядка. Хоча цей метод є одним із найпростіших, він забезпечує деякий захист даних, кращий, ніж відсутність шифрування. У скріншотах показано, де у файлі зберігається зашифрований пароль у текстовому та шістнадцятковому режимах.

Режим «text»:

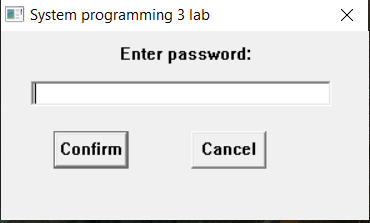


Режим «hex»:

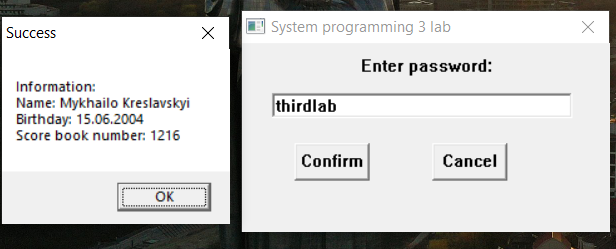


Також додаю скріншоти виконання програми, в якій пароль зашифрований методом XOR:

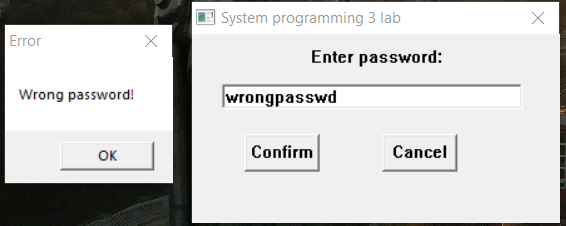
Вікно для введення паролю:



Якщо ввести правильний пароль:



Якщо ввести неправильний пароль:



**Висновок:**

Під час лабораторної роботи я вивчав структуру файлів із розширенням .exe, які використовуються в операційних системах DOS і Microsoft Windows для запуску програм.

Файл EXE складається з двох частин: заголовка (інформація для завантажувача програми) і модуля завантаження. Я вивчив деякі параметри файлу і способи їх знаходження та зміни, використовуючи програму PE Tools. Також я використовував цю програму для вивчення імпортованих бібліотек і функцій, які використовуються у файлі.

Під час роботи було написано дві програми, суть обох полягала у введенні пароля і, якщо він правильний, то програма дає доступ до інформації, якщо ні - видає помилку. У першій програмі пароль було задано явно в коді, що небезпечно. У другій програмі пароль зашифровано методом XOR, а в коді міститься тільки зашифрований пароль і ключ. Таке рішення є більш безпечним, ніж перше.