Міністерство освіти і науки України

Національний технічний університет «ХПІ»

Навчально-науковий інститут комп’ютерних наук та інформаційних технологій

Кафедра комп’ютерної інженерії та програмування

**ЗВІТ**

з лабораторної роботи № 5

з дисципліни «Сучасні технології безпечного програмування»

# **«[WINDOWS] ДОСЛІДЖЕННЯ ДИНАМІЧНИХ БІБЛІОТЕК»**

Виконав:

студент гр. КН-Н922б

Міщенко Д.С.

Перевірив:

Бульба С. С.

Харків – 2022

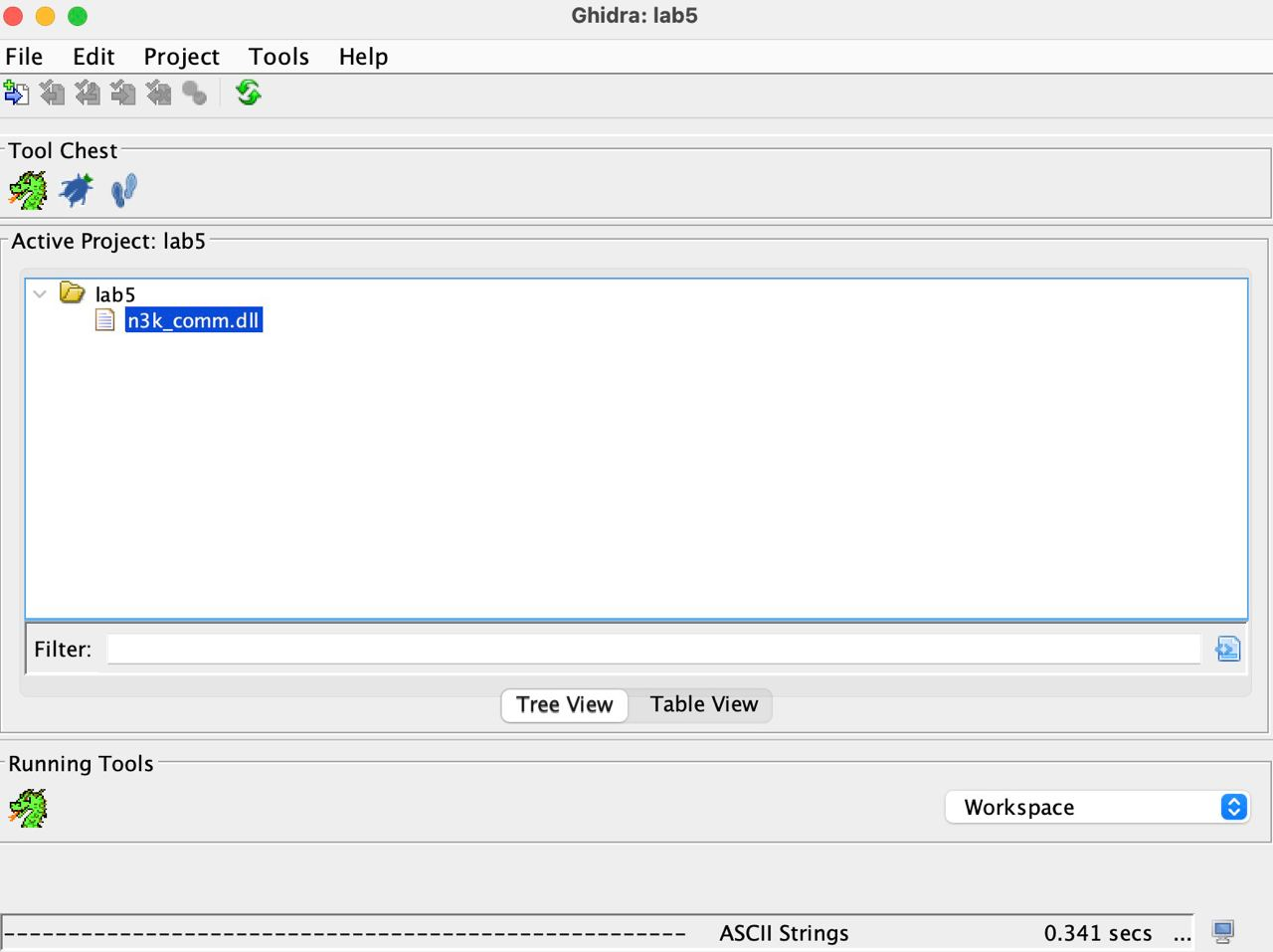
**Мета роботи:** Отримати навички основ реверс-інженірингу "на практиці"

**Індивідуальне завдання**

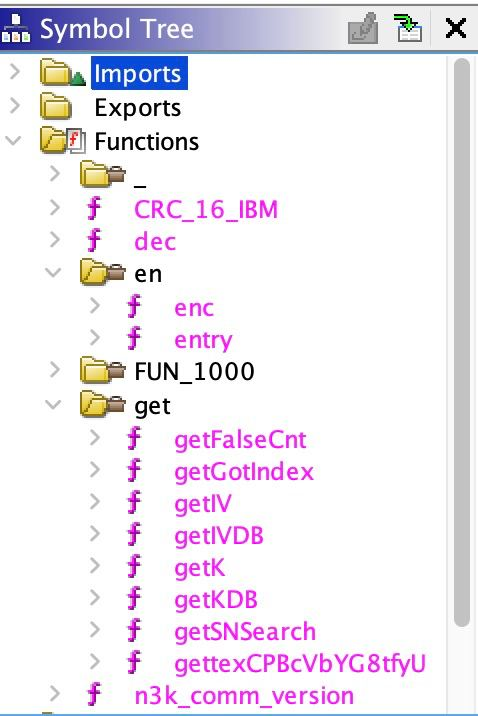
1. Визначити мову програмування, на якої була написана бібліотека (C/C++, C#, Deplhi, Java). Визначення мови програмування дозволить найбільш ефективно використовувати "декомпілятор". При цьому, рекомендуються наступні декомпілятори:
   * для Java - jdgui, або нативний декомпілятор від Intellij IDEA
   * для C# - dotPeek
   * для Delphi - DeDe
   * для C/C++ - Ghidra, IDA Pro
2. Визначити функції та їх прототипи, з яких складається динамічна бібліотека.
3. Створити додаток, що підключає дану бібліотеку та визначити, що роблять функції getIV,getK.
4. Декомпілювати функцію CRC\_16\_IBM. Судячи з її назви Вам буде не важко це зробити (бо її алгоритм завідомо відомий), але треба бути підібрати кректні коефіцієнти. Необхідно довести коректність реалізованого алгоритму через порівняння результатів з результатами роботи функції динамічної бібліотеки.
5. Декомпілювати та переписати функції dec та enc. Який алгоритм вони використовують? Підсказка - це скорочення від encode, decode. Більшість алгоритмів шифрування використовують табличні дані, на базі яких використовується кодування. Знавши це - найбільш швидкий для вас варіант - визначити таблицю, що використовується, та знайти алгоритм, що її використовує. Реалізувати алгоритм на мові високого рівня, та довести коректність реалізованого алгоритму через порівняння результатів з результатами роботи функції динамічної бібліотеки.

**Хід роботи**

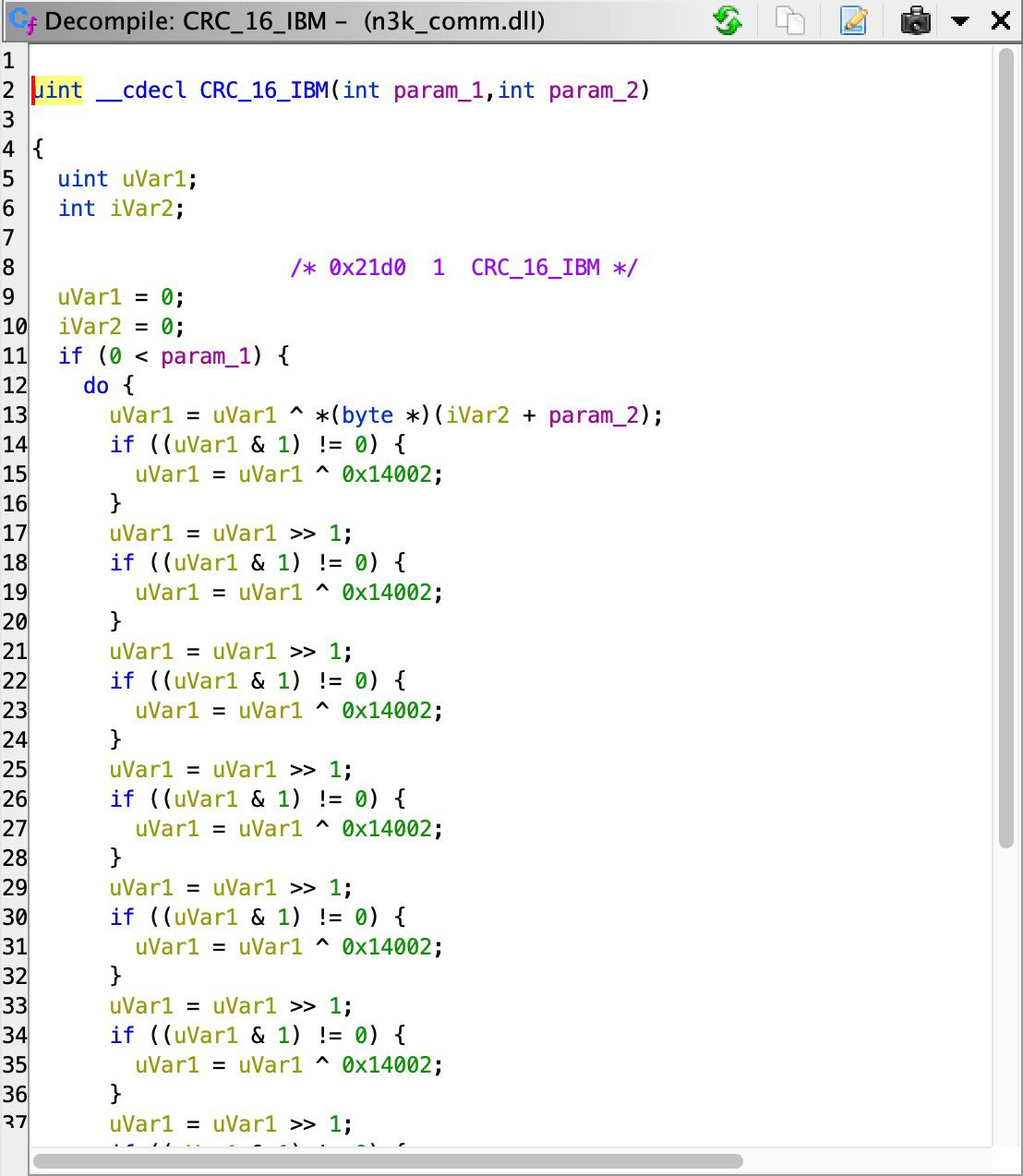
Встановлено Ghidra для декомпіляції бібліотеки



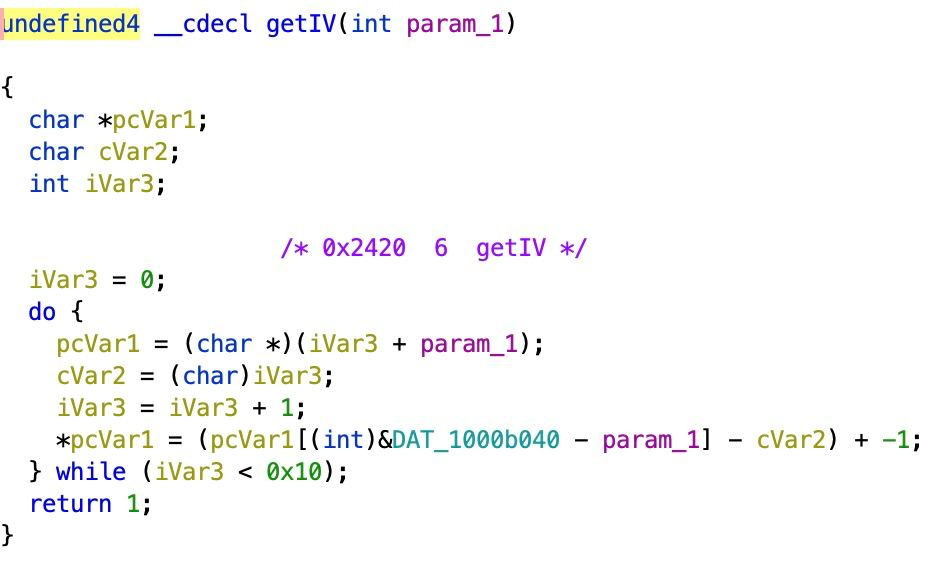
**Рисунок 1 –** Ghidra



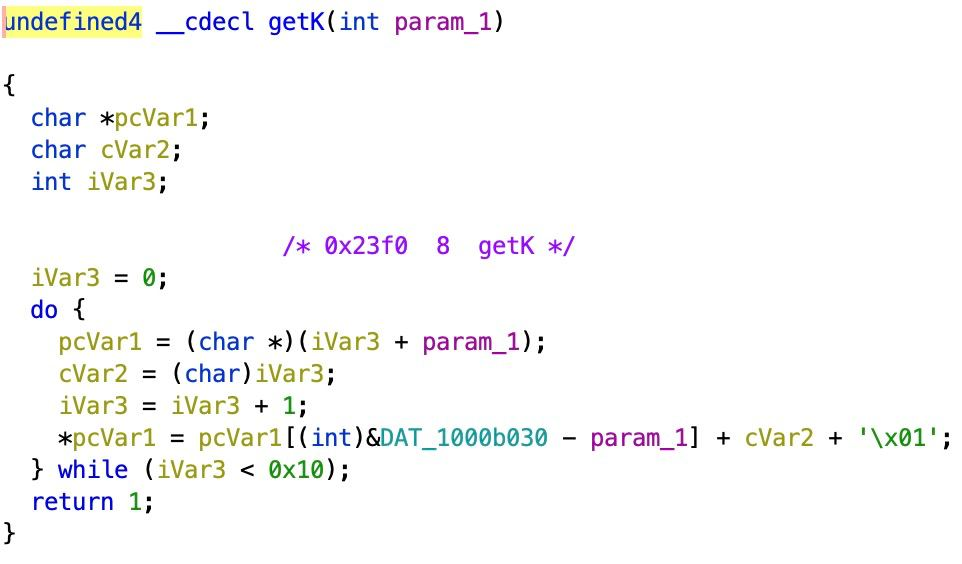
**Рисунок 2 –** Знайдені функції бібліотеки



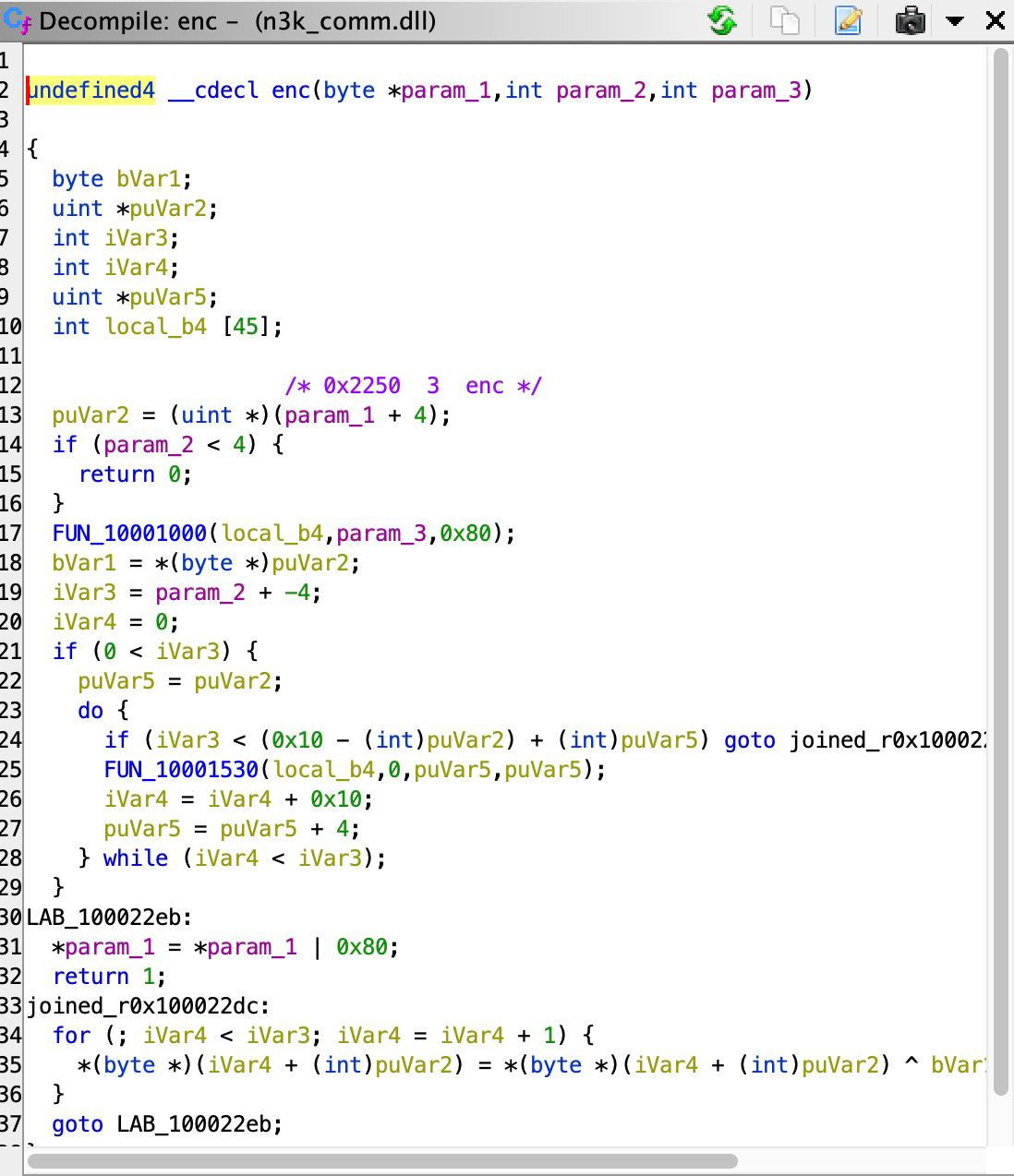
**Рисунок 3 –** Декомпільована функція CRC\_16\_IBM



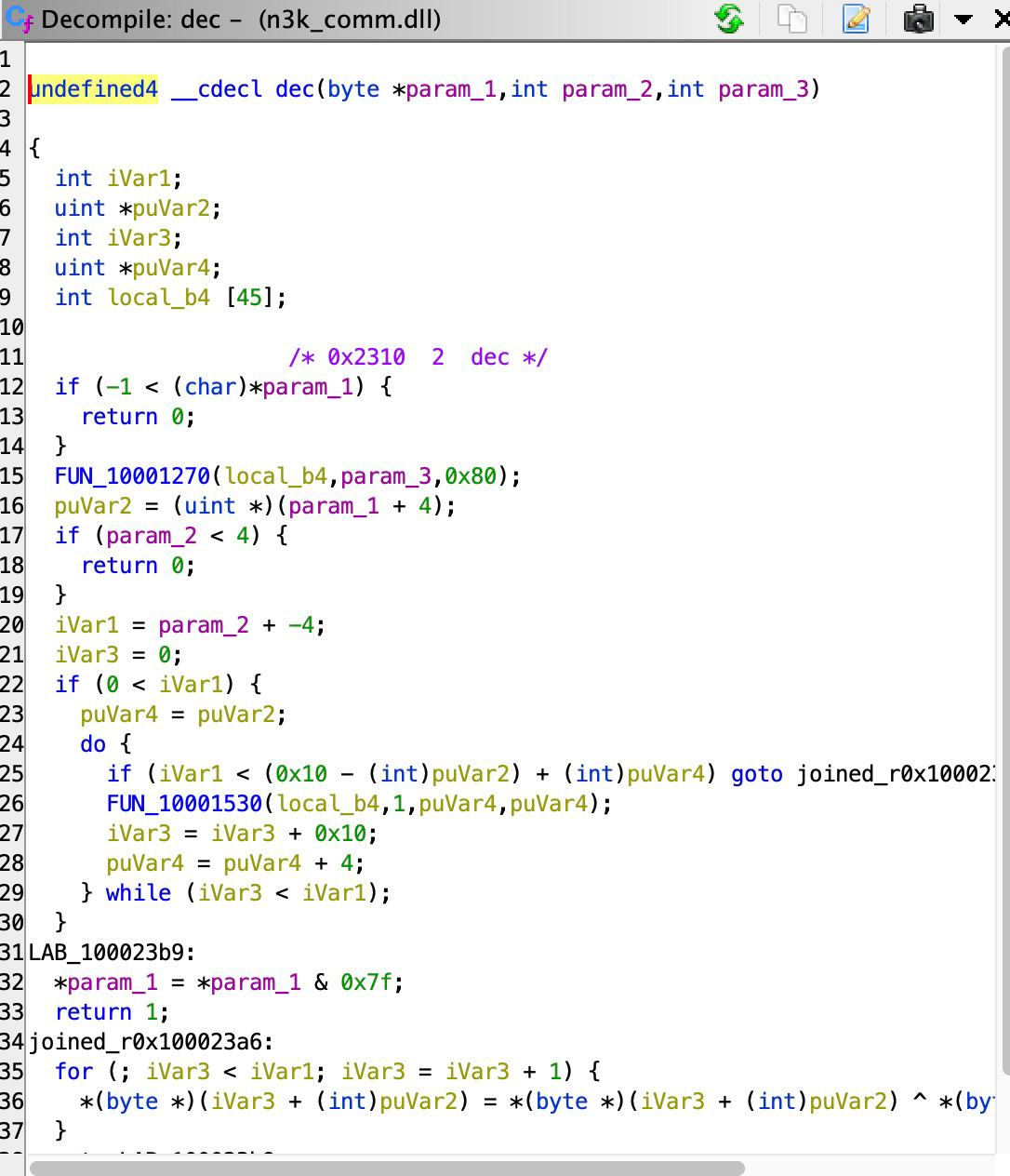
**Рисунок 4 –** Декомпільована функція getIV



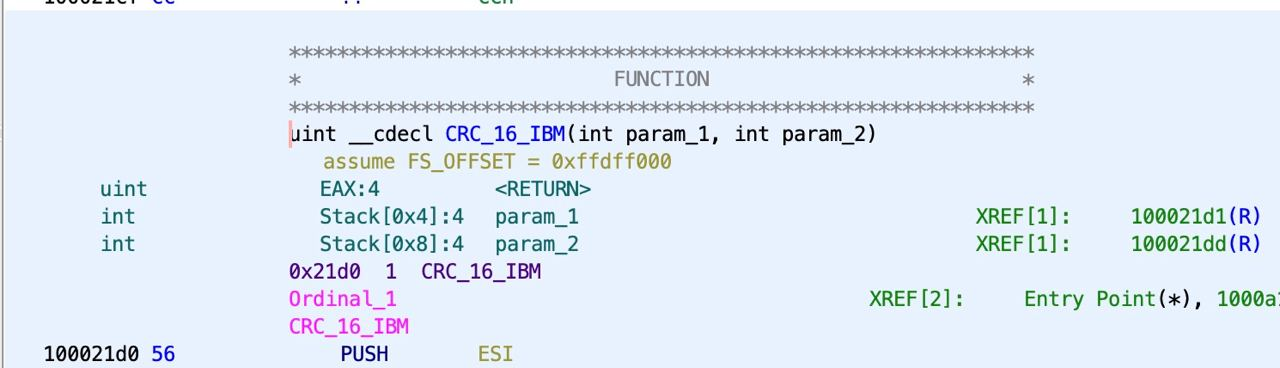
**Рисунок 5 –** Декомпільована функція getK



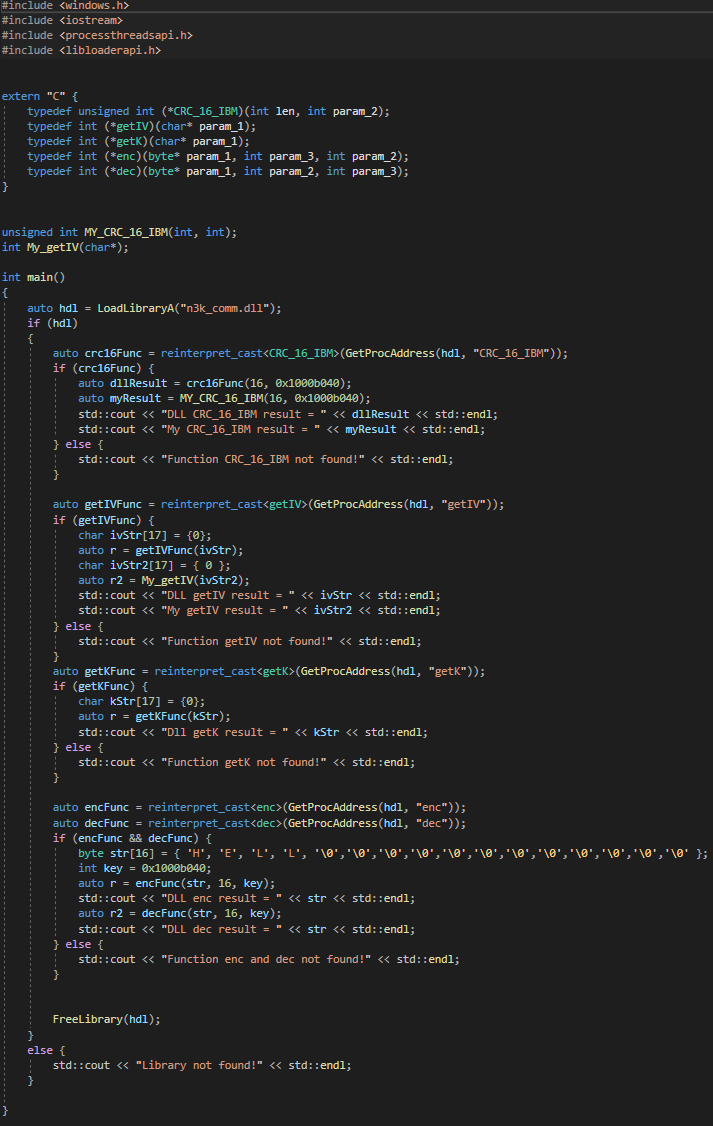
**Рисунок 6 –** Декомпільована функція enc

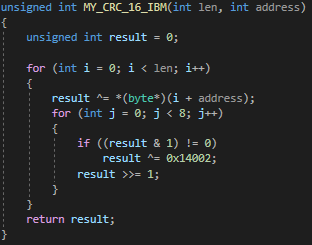


**Рисунок 7 –** Декомпільована функція dec

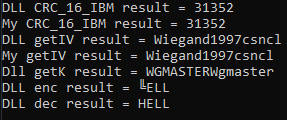


**Рисунок 8 –** Адреса функції CRC\_16\_IBM

  
**Рисунок 9 –** Код мовою С++ для виклику функції з dll

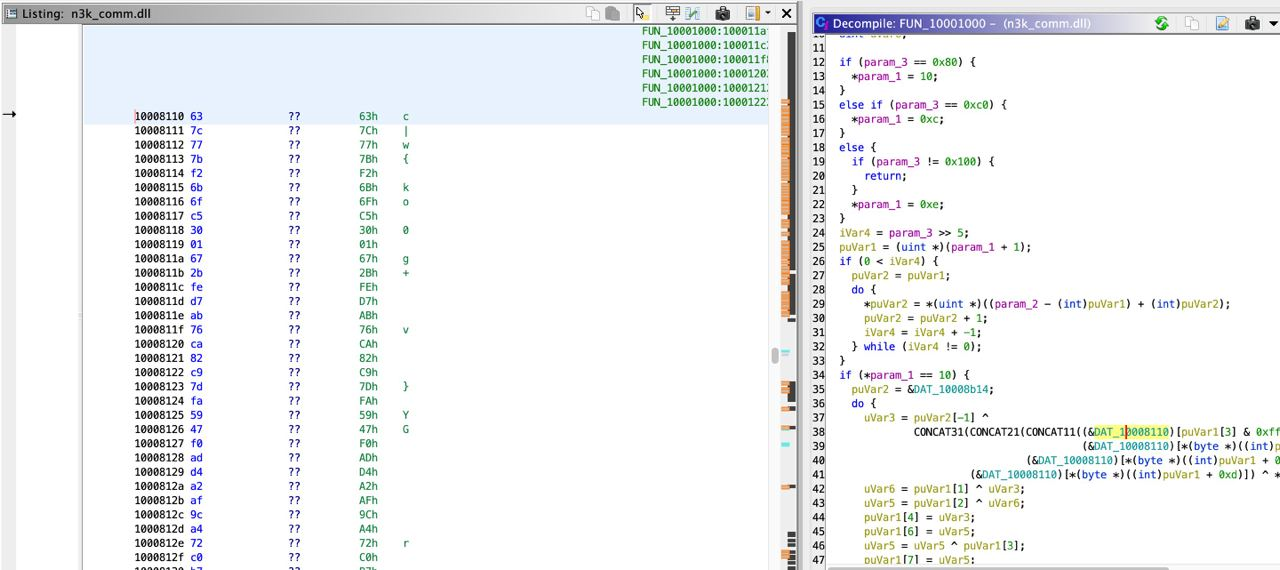


**Рисунок 10 –** Реалізована функція CRC\_16\_IBM



**Рисунок 11 –** Результат виконання програми

Функції dec та enc викликають підпрограми що мають вбудовані таблиці даних. Таблиця нижче співпадає з таблицею AES S-Box алгоритму AES розробленого у 2 лабораторній роботі.



 **Рисунок 12 –** Таблиця S-Box для AES алгоритму

**Висновки:** в результаті виконання лабораторної роботи було отримано навичок основ реверс-інженірингу "на практиці".