Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Кафедра Обчислювальна техніка та програмування

Звіт з лабораторної роботи з дисципліни « Реверсне програмування »

Лабораторна робота 7

Виконав ст.гр. КІТ–36

Надірян Г.О.

Перевірив

Челак В.В.

Харків 2019

**Лабораторна робота 7**

**Тема**: реверс-інжиніринг програм, що використовують технології CLR і JVM

**Мета**: набути практичних навичок в дослідженні програм, написані на

Мовах c # і java

**Постановка задачі**

Виконати завдання в кілька етапів:

1. Написати програми на С # і Java, які запитують пароль. Пароль необхідно зберігати в окремому класі. У окремого класу є поле fio, яке містить рядок ПІБ (Приклад «Челак Віктор Володимирович») і поле в якому зберігатися безпосередньо пароль (private). В конструкторі необхідно реалізувати алгоритм знаходження пароля (відповідно до індивідуального

завданням). У точках входу створювати об'єкти з паролями і запитувати пароль у користувача (в вигляді числа).

2. Провести дослідження (реверс-інжиніринг) .NET програми. Використовуючи dnSpy, отримати вихідний код, і експортувати в окремий проект. Змінити отриманий проект так, щоб програма замість введення пароля видавала вміст об'єкта (пароль). використовуючи змінену програму отримати доступ до оригінальної програми.

3. Повторити дії для програми, написаної на Java (вихідний файл - .jar)

**Завдання**

Відповідно до номером студента в групі вибрати варіант завдання і написати на С # і Java програму. Числа а є {a1, a2, a3, a4, ...,} - Це коди символів поля fio (масив - рядок).

12.bd + √a + c + e + f;

де b, c, d, e, f - За бажанням користувача (повинні бути оголошені як поля), числа а є {a1, a2, a3, a4} задані масивом (рядком).

Для парних варіантів операція об'єднання результатів складання, для непарних - виключає або.

РЕВЕРС .NET ПРОГРАММИ

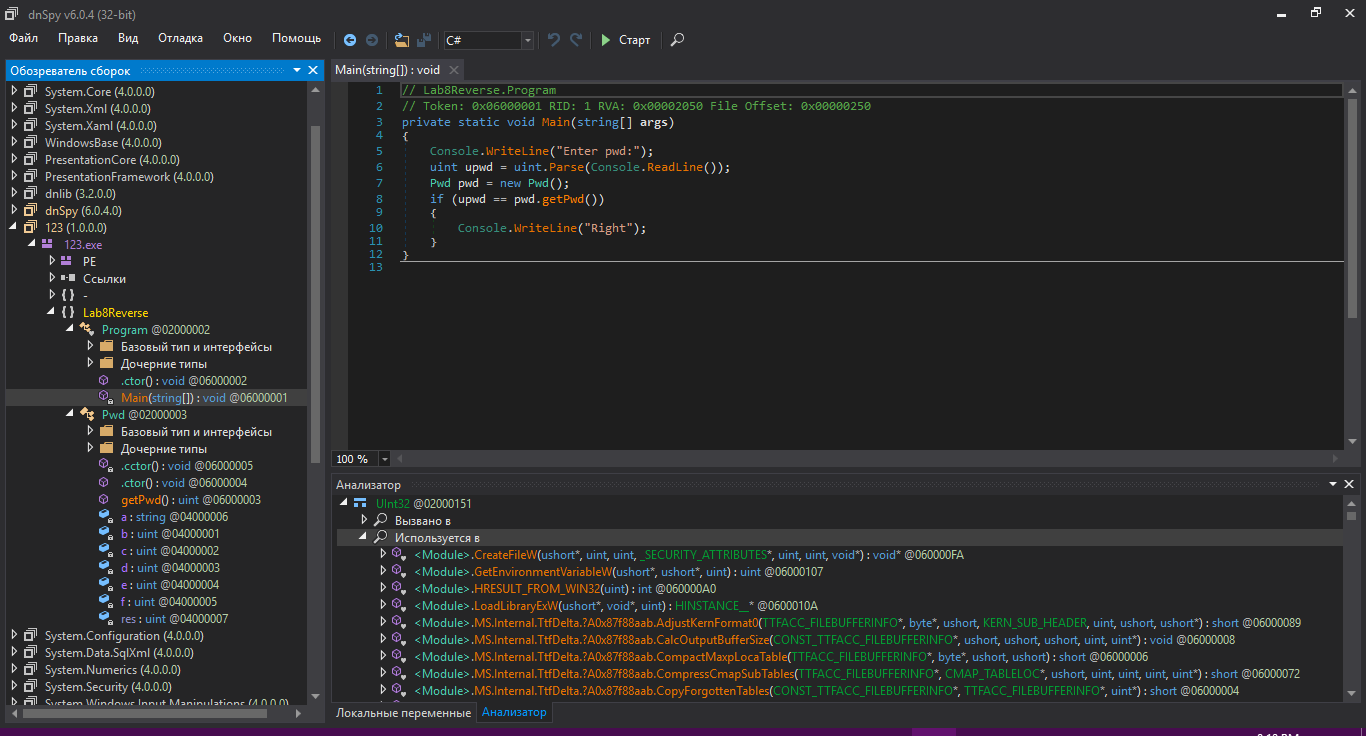


Рисунок 1 - Реверс .NET программи

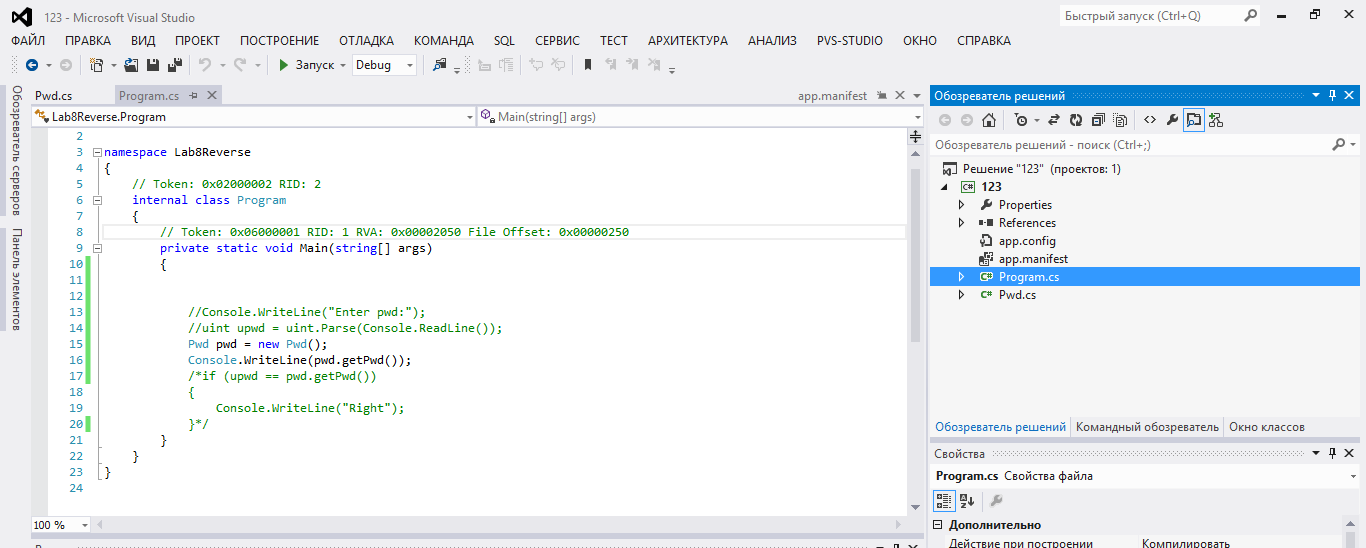


Рисунок 2 - exports to Visual Studio

**Код програми до реверсу**

using System;

namespace Lab8Reverse

{

class Program

{

static void Main(string[] args)

{

Console.WriteLine("Enter pwd:");

uint upwd = uint.Parse(Console.ReadLine());

Pwd pwd = new Pwd();

if (upwd == pwd.getPwd()) //685

Console.WriteLine("Right");

else

Console.WriteLine("Incorrect");

}

}

public class Pwd

{

uint b = 2, c = 3, d = 4, e = 5, f = 6;

private string a = "Nadirian Hamlet Ovikov";

private static uint res = 0;

public uint getPwd() { return res; }

public Pwd()

{

int i;

for (i = 0; i < a.Length; i++)

{

res += b \* d + (uint)Math.Sqrt((uint)a[i]) + c + e + f;

}

}

}}

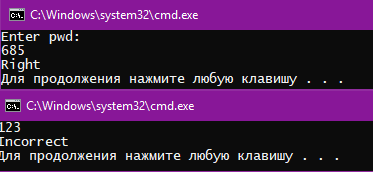


Рисунок 3 – результат роботи програми (до реверсу)

**Після реверсу**

using System;

namespace Lab8Reverse

{

// Token: 0x02000002 RID: 2

internal class Program

{

// Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250

private static void Main(string[] args)

{

//Console.WriteLine("Enter pwd:");

//uint upwd = uint.Parse(Console.ReadLine());

Pwd pwd = new Pwd();

Console.WriteLine(pwd.getPwd());

/\*if (upwd == pwd.getPwd())

{

Console.WriteLine("Right");

}\*/

}

}

}

using System;

namespace Lab8Reverse

{

// Token: 0x02000003 RID: 3

public class Pwd

{

// Token: 0x06000003 RID: 3 RVA: 0x000020A0 File Offset: 0x000002A0

public uint getPwd()

{

return Pwd.res;

}

// Token: 0x06000004 RID: 4 RVA: 0x000020B8 File Offset: 0x000002B8

public Pwd()

{

for (int i = 0; i < this.a.Length; i++)

{

Pwd.res += this.b \* this.d + (uint)Math.Sqrt(this.a[i]) + this.c + this.e + this.f;

}

Console.WriteLine("Key:" + Pwd.res);

}

// Token: 0x04000001 RID: 1

private uint b = 2u;

// Token: 0x04000002 RID: 2

private uint c = 3u;

// Token: 0x04000003 RID: 3

private uint d = 4u;

// Token: 0x04000004 RID: 4

private uint e = 5u;

// Token: 0x04000005 RID: 5

private uint f = 6u;

// Token: 0x04000006 RID: 6

private string a = "Nadirian Hamlet Ovikov";

// Token: 0x04000007 RID: 7

private static uint res = 0u;

}

}

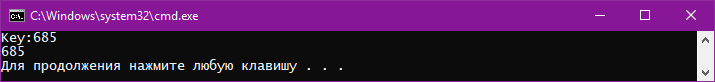


Рисунок 4 – результат роботи програми (Післяреверсу)

РЕВЕРС JAVA-ПРОГРАМИ

/\*\*

\*

\*/

package Nadirian07;

import java.util.Scanner;

/\*\*

\* @author Ham

\*

\*/

public class Lab08 {

/\*\*

\* @param args

\*/

public static void main(String[] args) {

// TODO Auto-generated method stub

System.out.print("Input password: ");

Scanner in = new Scanner(System.in);

int upwd = in.nextInt();

PWD pwd = new PWD();

// System.out.println(pwd.getPwd());

if(upwd==pwd.getPwd())

System.out.println("Right");

else

System.out.println("Incorrect");

}

}

**package** Nadirian07;

**public** **class** PWD {

**int** b=2,c=3,d=4,e=5,f=6;

**private** **static** String *a* = "Nadirian Hamlet Ovikov";

**private** **static** **int** *res* = 0;

**public** **int** getPwd() {**return** *res*;}

**public** PWD() {

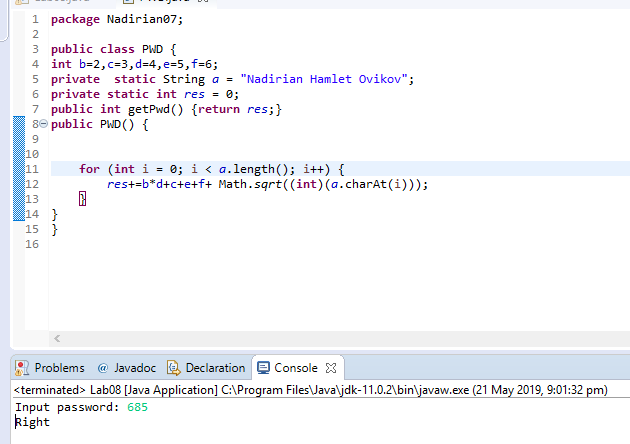
**for** (**int** i = 0; i < *a*.length(); i++) {

*res*+=b\*d+c+e+f+ Math.*sqrt*((**int**)(*a*.charAt(i)));

}

}

}



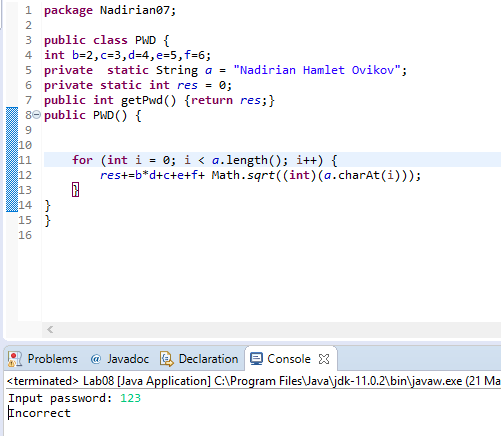


Рисунок 5 – результат роботи програми (до реверсу)

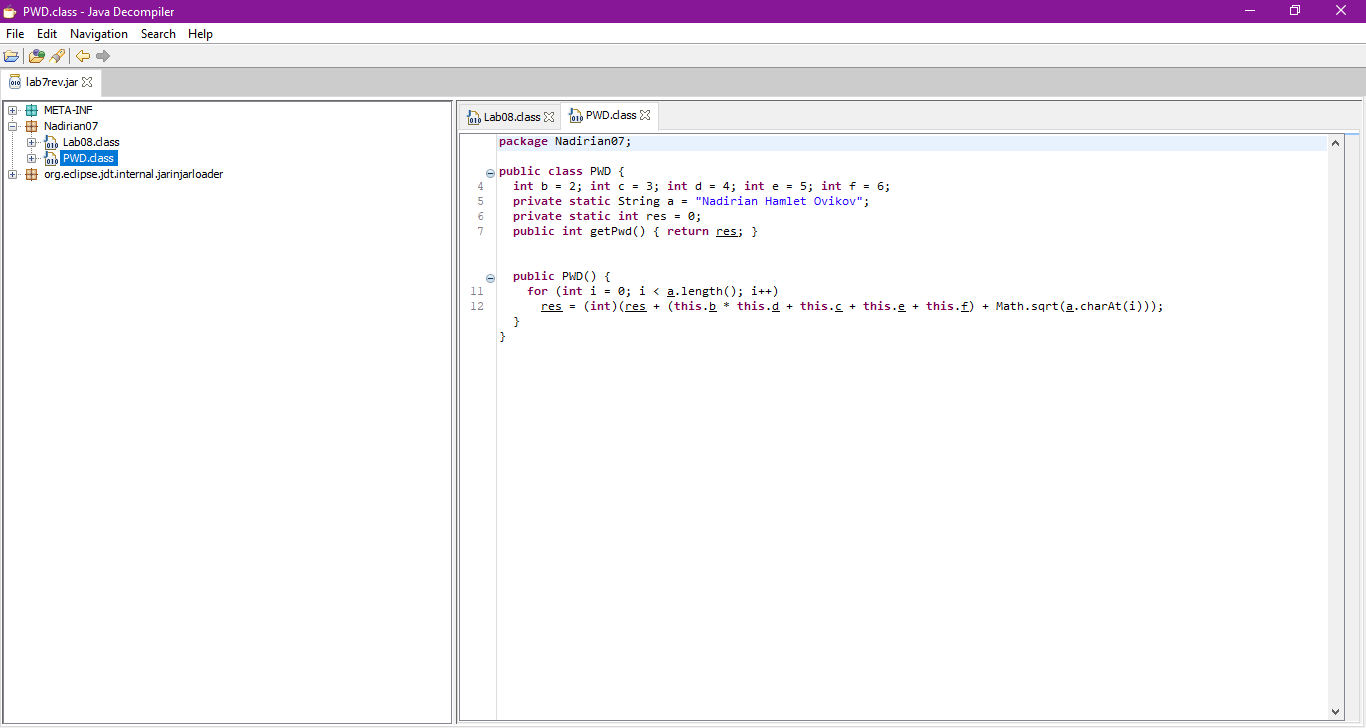
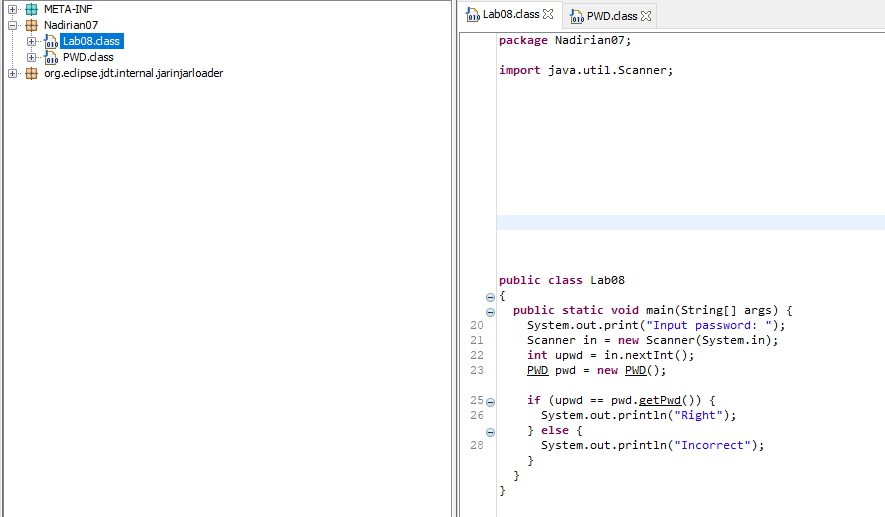


Рисунок 6 - Реверс Java-программы



Рисуеок 7 - Реверс Java-программы

**Після реверсу**

/\* \*/ **package** Nadirian07;

/\* \*/

/\* \*/ **import** java.util.Scanner;

/\* \*/ **public** **class** Lab08

/\* \*/ {

/\* \*/ **public** **static** **void** main(String[] args) {

/\* 20 \*/ //System.***out***.print("Input password: ");

/\* 21 \*/ //Scanner in = **new** Scanner(System.***in***);

/\* 22 \*/ **int** upwd = in.nextInt();

/\* 23 \*/ PWD pwd = **new** PWD();

/\* \*/

/\* 25 \*/ **if** (upwd == pwd.getPwd()) {

/\* 26 \*/ System.***out***.println("Right");

/\* \*/ } **else** {

/\* 28 \*/ System.***out***.println("Incorrect");

/\* \*/ }

/\* \*/ }

/\* \*/ }

/\* Location: C:\Revers\7\Lab07Rev\lab7rev.jar!\Nadirian07\Lab08.class

\* Java compiler version: 11 (55.0)

\* JD-Core Version: 1.0.1

\*/

/\* \*/ **package** Nadirian07;

/\* \*/

/\* \*/ **public** **class** PWD {

/\* 4 \*/ **int** b = 2; **int** c = 3; **int** d = 4; **int** e = 5; **int** f = 6;

/\* 5 \*/ **private** **static** String *a* = "Nadirian Hamlet Ovikov";

/\* 6 \*/ **private** **static** **int** *res* = 0;

/\* 7 \*/ **public** **int** getPwd() { **return** *res*; }

/\* \*/

/\* \*/

/\* \*/ **public** PWD() {

/\* 11 \*/ **for** (**int** i = 0; i < *a*.length(); i++)

/\* 12 \*/ *res* = (**int**)(*res* + (**this**.b \* **this**.d + **this**.c + **this**.e + **this**.f) + Math.*sqrt*(*a*.charAt(i)));

/\* \*/ }

/\* \*/ }

/\* Location: C:\Revers\7\Lab07Rev\lab7rev.jar!\Nadirian07\PWD.class

\* Java compiler version: 11 (55.0)

\* JD-Core Version: 1.0.1

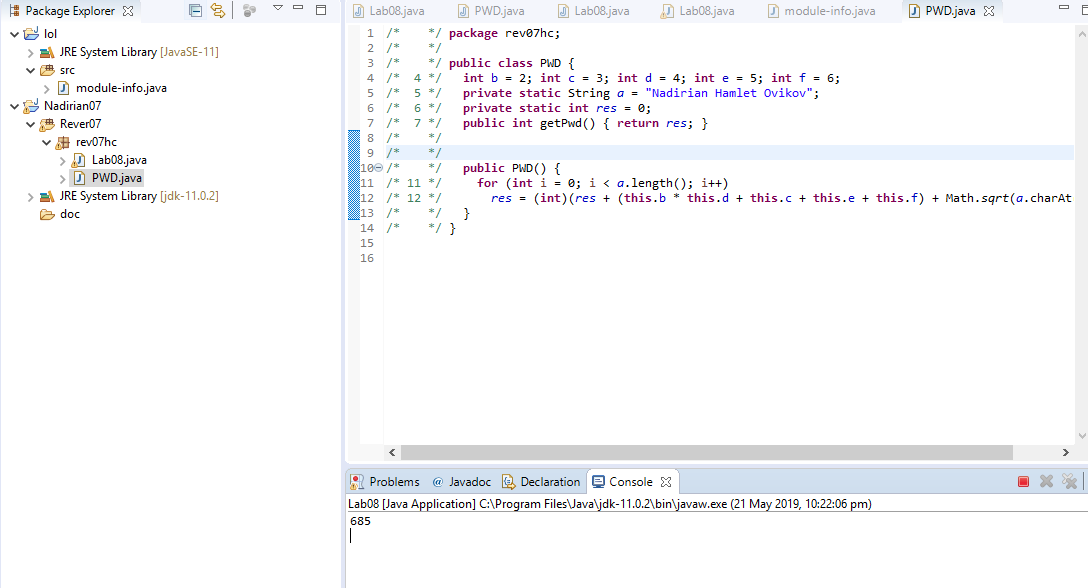


Рисунок 8 - результат роботи програми (Післяреверсу)

**Висновок**

Провели дослідження (реверс-інжиніринг) .NET програми та .Java програми. Використовуючи dnSpy та Java decompiler, отримали вихідний код, і експортувати в окремий проект. Змінили отриманий проект так, щоб програма замість введення пароля видавала вміст об'єкта (пароль).