

Міністерство освіти та науки України
Харківський національний університет радіоелектроніки
Кафедра програмної інженерії

Лабораторна робота №3
з дисципліни: «Безпека програм та даних»
На тему: «ПРОГРАМНА РЕАЛІЗАЦІЯ ХЕШ-Функцій

Виконав:
ст. гр. ПЗП 20-5
Середа Ілля

Перевірив:
Олійник О. О.

ЛАБОРАТОРНА РОБОТА №3

Мета: Ознайомитись з можливостями криптографічних хеш-функцій при організації контролю цілісності цифрових об'єктів та отримати навички їх використання

Хід роботи:

Код програми(C#):

```
using System;
using System.IO;

namespace Practice
{
    class Program
    {
        static void Main(string[] args)
        {
            string message = "";
            int hashLen;
            Console.Write("Вкажіть початкову строку: ");
            message = Console.ReadLine();
            Console.Write("Вкажіть довжину хеша(2, 4 або 8): ");
            hashLen = Convert.ToInt32(Console.ReadLine());

            Console.WriteLine("\nЙде обробка початкової строки");
            Console.WriteLine("Початковий хеш строки: {0}", GetHashCode(message,
hashLen));

            Console.WriteLine("\nЙде спроба знайти колізії:");
            int col = SearchCollisions(message, hashLen);
            if (col > 0)
                Console.WriteLine("Було знайдено колізій: {0}", col);
            else
                Console.WriteLine("Колізії не знайдені");

            message += "dd";
            Console.WriteLine("\nЙде обробка зміненої строки: ");
            Console.WriteLine("Нова строка: \"{0}\"", message);
            Console.WriteLine("Хеш нової строки: {0}", GetHashCode(message, hashLen));

            Console.Write("\nЙде робота з зображеннями: ");
            string image = @"image.png";
            Console.WriteLine("Хеш зображення: {0}", GetHashCode(GetBytes(image),
hashLen));

            Console.Write("\nЙде робота з файлом csproj: ");
            string file = @"Lab3.csproj";
            Console.WriteLine("Хеш csproj: {0}", GetHashCode(GetBytes(file), hashLen));

            Console.Write("\nЙде робота з текстовим файлом: ");
            string docx = @"Lab3.docx";
            Console.WriteLine("Хеш docx: {0}", GetHashCode(GetBytes(docx), hashLen));
        }

        private static string GetHashCode(string message, int value)
        {
            string messageToByte = "";
            for (int i = 0; i < message.Length; i++)
            {
```

```

2);
        messageToByte += "0" + Convert.ToString(Convert.ToInt64(message[i]),
    }

    int size = messageToByte.Length / 8;
    byte[] blockArray = new byte[size];
    for (int i = 0; i < size; ++i)
    {
        blockArray[i] = Convert.ToByte(messageToByte.Substring(8 * i, 8), 2);
    }

    byte resultInByte = 0;
    foreach (byte b in blockArray) resultInByte ^= b;
    int result = resultInByte >> ((value == 8) ? 0 : value);

    return Convert.ToString(result, 2);
}

private static string GetBytes(string path)
{
    byte[] data = File.ReadAllBytes(path);
    return BitConverter.ToString(data).Replace("-", string.Empty);
}

private static string GetRandomString(int len, int iter)
{
    Random rnd = new Random(iter);
    byte[] rndBytes = new byte[len];
    rnd.NextBytes(rndBytes);
    return System.Text.Encoding.ASCII.GetString(rndBytes);
}

private static int SearchCollisions(string message, int value)
{
    int totalIterations = 100000;
    int collisionsCount = 0;
    while (totalIterations >= 0)
    {
        string randomString = GetRandomString(message.Length,
totalIterations);
        string randomStringHash = GetHash(randomString, value);
        if (randomStringHash == GetHash(message, value))
        {
            Console.WriteLine($"Була знайдена колізія в повідомленні:
{randomString} \n Її хеш: {randomStringHash}");
            collisionsCount++;
        }
        totalIterations--;
    }
    return collisionsCount;
}
}
}

```

Приклад виконання:

```

Вкаж?ть початкову строку: Ilya Sereda
Вкаж?ть довжину хеша(2, 4 або 8): 8


Йде обробка початкової строки
Початковий хеш строки: 11110111

Йде спроба знайти кол?з?ї:
Була знайдена кол?з?я в пов?домленн?: ??S!P]?u?X
  Її хеш: 11110111
Була знайдена кол?з?я в пов?домленн?: с? ???&0Д/?
  Її хеш: 11110111
Була знайдена кол?з?я в пов?домленн?: ??0??UQ???Y
  Її хеш: 11110111
Була знайдена кол?з?я в пов?домленн?: ]ЅI???`9[?#
  Її хеш: 11110111
Була знайдена кол?з?я в пов?домленн?: ?q4????r?o
  Її хеш: 11110111
Була знайдена кол?з?я в пов?домленн?: k6??*ЅG?~сw
  Її хеш: 11110111
Була знайдена кол?з?я в пов?домленн?: C??♦6?!?rYA
  Її хеш: 11110111
Була знайдена кол?з?я в пов?домленн?: ?@QDTw'?kE?
  Її хеш: 11110111
Була знайдена кол?з?я в пов?домленн?: ??{??g????1
  Її хеш: 11110111
Була знайдена кол?з?я в пов?домленн?: ?T?y?I?§ o?
  Її хеш: 11110111
Була знайдена кол?з?я в пов?домленн?: Kt?_=Id♦?R?
  Її хеш: 11110111
Була знайдена кол?з?я в пов?домленн?: ?"????????

```

При довжині хешу 2 або 4 в консолі буде дуже багато виводів, тому скріншоти роблю для довжини 8, але і для 2, і для 4 все працює

Приклад виконання для зображення і двох файлів:

 Консоль отладки Microsoft Visual Studio

```

  Її хеш: 11110111
Була знайдена кол?з?я в пов?домленн?: ?7A??P♦?UG?
  Її хеш: 11110111
Була знайдена кол?з?я в пов?домленн?: ?*BG♥????A
  Її хеш: 11110111
Була знайдена кол?з?я в пов?домленн?: <????C?C? ?
  Її хеш: 11110111
Була знайдена кол?з?я в пов?домленн?: <?/ "?E??9?
  Її хеш: 11110111
Було знайдено кол?з?й: 414

Йде обробка зм?неної строки:
Нова строка: "Ilya Seredadd"
Хеш нової строки: 1111101

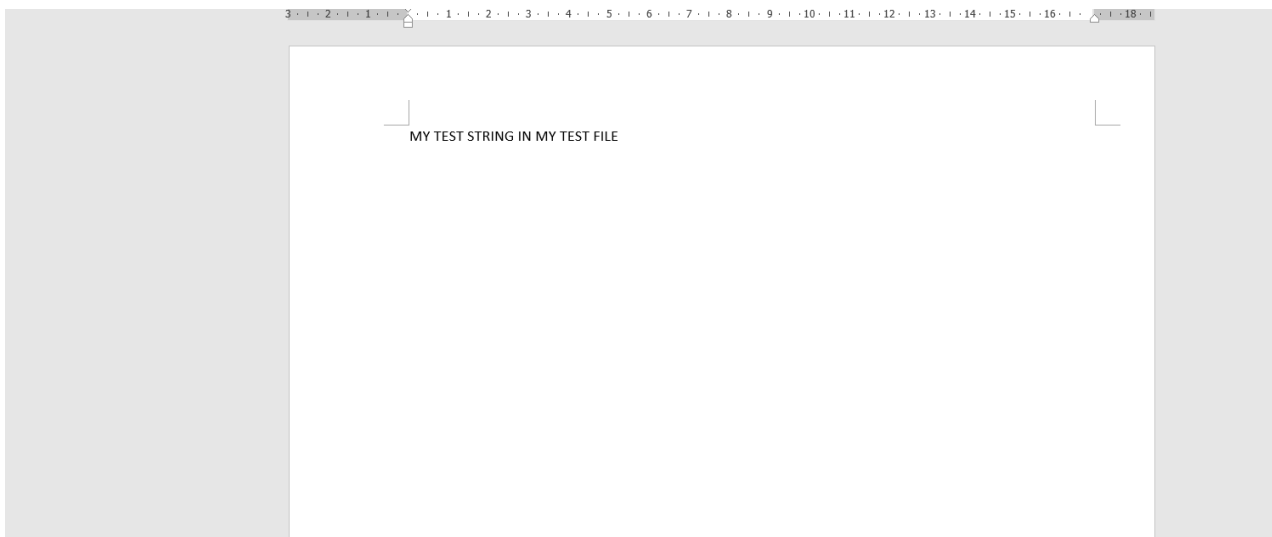
Йде робота з зображеннями: Хеш зображення: 1011001

Йде робота з файлом csproj: Хеш csproj: 111111

Йде робота з текстовим файлом: Хеш docx: 1101100

```

Файл Lab3.docx:



Файл Lab3.csproj

```
Lab3.csproj X
D: > Программирование > Учеба > BPTD > Lab3 > Lab3 > bin > Debug > net8.0 > Lab3.csproj
1  <Project Sdk="Microsoft.NET.Sdk">
2
3      <PropertyGroup>
4          <OutputType>Exe</OutputType>
5          <TargetFramework>net8.0</TargetFramework>
6          <ImplicitUsings>enable</ImplicitUsings>
7          <Nullable>enable</Nullable>
8      </PropertyGroup>
9
10 </Project>
11
```

Висновки

Я ознайомився з можливостями криптографічних хеш-функцій при організації контролю цілісності цифрових об'єктів та отримав навички їх використання