Основи інформаційної безпеки

ПЗ №2

Тема: “Реалізація шифру Вернама”

Підготував:

Студент групи МІТ-21

Міхальський Владислав

using System;

using System.IO;

using System.Linq;

using System.Security.Cryptography;

using System.Text;

namespace lab2

{

class Program

{

static void Main(string[] args)

{

byte[] decData;

decData = File.ReadAllBytes("file.txt").ToArray();

Console.Write("Зчитуємо наше число й виводимо його побайтово: ");

foreach (byte i in decData)

{

Console.Write(i);

Console.Write(" ");

}

Console.WriteLine();

var rndNumberGenerator = new RNGCryptoServiceProvider();

byte[] key = new byte[decData.Length];

rndNumberGenerator.GetBytes(key);

Console.Write("Генеруємо ключi для шифрацiї байтiв: ");

foreach (byte i in key)

{

Console.Write(i);

Console.Write(" ");

}

Console.WriteLine();

Console.Write("Шифруємо й виводимо нашi байти: ");

byte[] encData = new byte[decData.Length];

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

{

encData[i] = (byte)(decData[i] ^ key[i]);

Console.Write(encData[i]);

Console.Write(" ");

}

File.WriteAllBytes("ex.dat", encData);

Console.WriteLine();

Console.Write("Розшифровуємо нашi зашифрованi байти й виводимо їх: ");

byte[] newEncData = File.ReadAllBytes("ex.dat").ToArray();

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

{

newEncData[i] = (byte)(encData[i] ^ key[i]);

Console.Write(newEncData[i]);

Console.Write(" ");

}

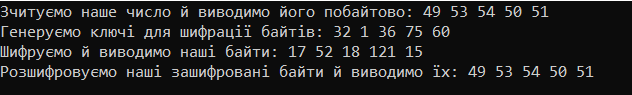
Console.WriteLine();

}

}

}

Результат виконання:



Посилання на репозиторій гітхабу: <https://github.com/vmikhalskyi/Security-basics-2021.git>

Висновок: У ході лабораторної роботи я навчився, генерувати рандомні ключі для шифрації байтів, шифрувати й розшифровувати числа. Опанував шифрування методом Вернама.