Основи інформаційної безпеки

ПЗ №2

Тема: “Реалізація шифру Вернама”

Підготував:

Студент групи МІТ-21

Пономаренко Владислав

(КОД)

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 = File.ReadAllBytes("data.txt").ToArray();

foreach (byte i in decData)

{

Console.Write(i);

Console.Write(" ");

}

Console.WriteLine();

Console.WriteLine();

var genPassword = new RNGCryptoServiceProvider();

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

genPassword.GetBytes(password);

foreach (byte i in password)

{

Console.Write(i);

Console.Write(" ");

}

Console.WriteLine();

Console.WriteLine();

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

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

{

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

}

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

byte[] Text = File.ReadAllBytes("encdata.dat").ToArray();

byte[] decText = new byte[Text.Length];

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

{

decText[i] = (byte)(Text[i] ^ password[i]);

}

Console.Write(Encoding.UTF8.GetString(decText));

Console.WriteLine();

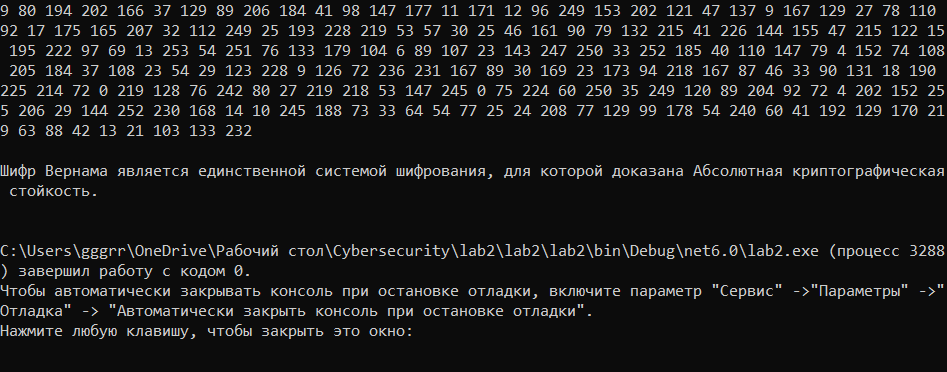
Console.WriteLine();

}

}

}

(РЕЗУЛЬТАТ)



(Посилання на репозиторій гітхабу)

<https://github.com/VladPonomarenkoi/Cybersecurity>

(Висновок)

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