Министерство образования Республики Беларусь

Белорусский государственный университет информатики и радиоэлектроники

Факультет информационных технологий и управления Кафедра интеллектуальных информационных технологий

Отчет по лабораторному практикуму

Дисциплина:
«Средства и методы защиты информации в интеллектуальных системах»

Выполнил

ст. гр. 121702 Промчук Д.В.

Проверил

Сальников Д.А.

Минск 2023

Вариант 3

Цель:

Разработать программу на языке C#, реализующую следующие функции:

1. Реализовать в виде программы шифр (зашифрование и расшифрование) в соответствии с вариантом 3.

2. Реализовать в виде программы атаку полным перебором ключа, используя для оценки правильности выбора ключа визуальный метод или исходный текст для автоматического сравнения результата дешифрования.

3. Оценить криптографическую стойкость реализованного шифра.

4. Предложить варианты усложнения шифра. Предложенные варианты оформить в виде алгоритма.

Задание 1

```
public static string Encrypt(string text, int diameter)
{
    var k:int = text.Length % diameter;
    if (k > 0)
    {
        text += new string(c:' ', count:diameter - k);
    }

    var columnCount:int = text.Length / diameter;
    var result = "";

    for (int i = 0; i < columnCount; i++)
    {
        for (int j = 0; j < diameter; j++)
        {
            result += text[i + columnCount * j].ToString();
        }
    }

    return result;
}
```

```
public static string Decrypt(string text, int diameter)
{
    var columnCount:int = text.Length / diameter;
    var symbols = new char[text.Length];
    int index = 0;

    for (int i = 0; i < columnCount; i++)
    {
        for (int j = 0; j < diameter; j++)
        {
            symbols[i + columnCount * j] = text[index];
            index++;
        }
    }

    return string.Join("", symbols);
}
```

- Реализация зашифрования и расшифрования шифра перестановки

Задание №2

```
private void FindKeyButton_Click(object sender, EventArgs e)
{
    for (int i = 1; i < 1000; i++)
    {
        FindKeyTextBox.Text += ($"{Environment.NewLine} Key {i} : {SkytaleCrypt.Decrypt(EncryptedTextBox.Text, i)}");
    }
}
```

- Реализация полного перебора ключей

Задание №3

Шифр перестановки Скитала — это довольно простой метод, который можно легко понять и реализовать. Его стойкость относительна, она зависит от размера таблицы, то есть от количества элементов в используемом алфавите и длины зашифрованного сообщения. Использование больших таблиц увеличивает стойкость.

Задание №4

Поскольку данный алгоритм в первую очередь относится к методам ручного шифрования сообщений, предлагаемый способ тоже будет для ручного шифрования.
Для каждого сообщения изготавливать конус с различными размерами.
Принцип шифрования тот же, но количество переменных, которые используются в процессе шифрования увеличивается, то расшифровка без ключа так же будет занимать больше времени.

Вывод: в ходе выполнения лабораторной работы были изучены некоторые методы шифрования и соответствующие им методы расшифровки сообщения, проанализирован алгоритм Скитала и выдвинуты предложения по его улучшению.