УДК 004.021

РАЗРАБОТКА СИСТЕМЫ ДЛЯ СКРЫТИЯ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ШИФРА ПЕРЕСТАНОВКИ

А.И. СМОЛЯК
(Представлено: канд. физ.-мат. наук, доц. Д.Ф. ПАСТУХОВ)

В данной статье рассматриваются: алгоритм скрытия данных с использованием шифра перестановки и основные функции разрабатываемого программного продукта.

Ключевые слова: *информационные технологии, скрытие информации, криптография, шифр перестановки, C#.*

Введение. Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптографии – ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры.

Основной раздел. Для разработки программного средства организации и функционирования программы необходимо выбрать среду разработки, с помощью которой будет производиться проектирование.

Для разработки этого приложения был выбран язык C#.

Основными функциями разрабатываемого программного продукта являются шифрование и дешифрование данных.

Шифр перестановки – это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы (самый распространенный случай), пары букв, тройки букв, комбинирование этих случаев и так далее.

Алгоритм шифра перестановки

Исходное сообщение разбивается на блоки длины m, где m – это длина ключа.

Ключ в шифре перестановки имеет следующий вид:

1	2	3	4
2	4	1	3

Шифр перестановки: ключ

В первой строке таблицы указаны номера символов блока по порядку, а во второй строке указаны номера позиций, которые должны занимать указанные символы в зашифрованном блоке текста.

Кодирование осуществляется перестановкой букв. Таким образом первый символ из исходного блока должен быть переставлен на второе место, второй на четвертое, третий на первое, четвертый на третье.

Если данным ключом зашифровать слово кофе, то получится слово фкео.

Дешифрование производится в обратном порядке. На примере указанного ключа: второй символ из зашифрованного блока ставим на первое место, четвертый на второе, первый на третье, третий на четвертое.

При использовании любого блочного шифра (шифр перестановки не исключение), может возникнуть ситуация, когда текст не делится на равные блоки длины m. То есть остаток от деления длины текста n на длину ключа m не равен нулю.

В таких случаях длину исходного сообщения увеличивают на m – (n % m) символов, чтобы оно делилось на равные блоки длины m.

Листинг 1 – Шифр перестановки

```
1::   class Transposition
2::   {
3::   private int[] key = null;
4::   public void SetKey(int[] _key)
5::   {
6::   key = new int[_key.Length];
7::   for (int i = 0; i < _key.Length; i++)
8::   key[i] = _key[i];
9::   }
10::  public void SetKey(string[] _key)
```

```
11::  {
12::  key = new int[_key.Length];
13::  for (int i = 0; i < _key.Length; i++)
14::  key[i] = Convert.ToInt32(_key[i]);
15::  }
16::  public void SetKey(string _key)
17::  {
18::  SetKey(_key.Split(' '));
19::  }
20::  public string Encrypt(string input)
21::  {
22::  for (int i = 0; i < input.Length % key.Length; i++)
23::  input += input[i];
24::  string result = "";
25::  for (int i = 0; i < input.Length; i += key.Length)
26::  {
27::  char[] transposition = new char[key.Length];
28::  for (int j = 0; j < key.Length; j++)
29::  transposition[key[j] - 1] = input[i + j];
30::  for (int j = 0; j < key.Length; j++)
31::  result += transposition[j];
32::  }
33::  return result;
34::  }
35::  public string Decrypt(string input)
36::  {
37::  string result = "";
38::  for (int i = 0; i < input.Length; i += key.Length)
39::  {
40::  char[] transposition = new char[key.Length];
41::  for (int j = 0; j < key.Length; j++)
42::  transposition[j] = input[i + key[j] - 1];
43::  for (int j = 0; j < key.Length; j++)
44::  result += transposition[j];
45::  }
46::  return result;
47::  }
48::  }
```

Заключение. В данной статье был рассмотрен алгоритм сокрытия информации с использованием шифра перестановки, а также основные функции разрабатываемого программного продукта.

ЛИТЕРАТУРА

1. А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. Основы криптографии. – Гелиос АРВ, 2002. – ISBN 5-85438-137-0.
2. А. В. Бабаш, Г. П. Шанкин. Криптография. – М. СОЛОН-ПРЕСС, 2007. – ISBN 5-93455-135-3.
3. Фред Б. Риксон. Коды, шифры, сигналы и тайная передача информации. – Астрель, 2011. – ISBN 978-5-17-074391-9.
4. Дориченко С. А., Ященко В. В. 25 этюдов о шифрах: Популярно о современной криптографии. – Теис, 1994. – ISBN 5-7218-0014-3.