UDC 004.223.2

DEVELOPING A SYSTEM FOR HIDDEN INFORMATION USING A TRANSPOSITION CIPHER

A. SMALIAK, D. PASTUKHOV
Polotsk State University, Belarus

This article discusses: an algorithm for hiding data using a permutation cipher and the main functions of the developed software product.

Introduction. The problem of protecting information by transforming it, excluding it from being read by an outsider, has worried the human mind since ancient times. The history of cryptography is the same age as the history of human language. Moreover, in the beginning, writing itself was a cryptographic system, since in ancient societies only the elite owned it. The sacred books of Ancient Egypt, Ancient India are examples of this.

Main section. To develop a software tool for the organization and functioning of the program, you must select the development environment with which the design will be carried out.

To develop this application, C # was chosen.

The main functions of the developed software product are data encryption and decryption.

A permutation cipher is a symmetric encryption method in which elements of the original plaintext are interchanged. Elements of the text can be individual characters (the most common case), pairs of letters, triples of letters, a combination of these cases and so on.

Permutation cipher algorithm:

The original message is divided into blocks of length m, where m is the key length.

The key in the permutation cipher is as follows:

1	2	3	4
2	4	1	3

Permutation Cipher: Key

The first line of the table shows the numbers of the block characters in order, and the second line shows the numbers of the positions that these characters should occupy in the encrypted text block.

Coding is carried out by permutation of letters. Thus, the first character from the source block should be rearranged in second place, second in fourth, third in first, fourth in third.

If you encrypt the word coffee with this key, you get the word phkeo.

Decryption is performed in reverse order. Using the specified key as an example: put the second character from the encrypted block in first place, fourth in second, first in third, third in fourth.

When using any block cipher (permutation cipher is no exception), a situation may arise when the text is not divided into equal blocks of length m. That is, the remainder of dividing the length of the text n by the length of the key m is not equal to zero.

In such cases, the length of the original message is increased by m - (n% m) characters so that it is divided into equal blocks of length m.

Listing 1 – Transposition cipher

```
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::  }
}
```

Conclusion. This article examined the information hiding algorithm using a permutation cipher, as well as the main functions of the software product being developed.

REFERENCES

1. А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черёмушкин. 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.