УДК 004.056.55

Реализация алгоритма шифрования перестановкой с помощью языка C++

Ленкин Алексей Викторович
Приамурский государственный университет имени Шолом-Алейхема
Студент

Аннотация
В данной статье рассмотрен алгоритм шифрования перестановкой. Описана реализация данного алгоритма с помощью языка программирования C++.
Ключевые слова: C++, шифрование перестановкой, шифрование, перестановка по таблице

Implementation of the encryption algorithm of permutation by using the C++ language

Lenkin Aleksei Viktorovich
Sholom-Aleichem Priamursky State University
Student

Abstract
This article discusses the encryption algorithm of the permutation. The implementation of this algorithm with the help of C++ programming language is described.
Keywords: C++, reshuffle, encryption, table reshuffle

Научный руководитель:
Лучанинов Дмитрий Васильевич
Приамурский государственный университет имени Шолом-Алейхема
старший преподаватель кафедры информационных систем, математики и методик преподавания

Проблема защиты информации всё чаще становится актуальной в наши дни в информационной среде. Одним из способов защиты данных стало шифрование. На данный момент известно огромное число алгоритмов кодирования информации, и с каждым днём их число растёт.

Одним из самых популярных является кодирование перестановкой.

Целью исследования является описать один из алгоритмов шифрования перестановкой и создать его программную реализацию на языке C++.

Исследованиями в данной теме занимались следующие авторы. А.А.Бабаев описал процедуры кодирования и декодирования перестановок[1]. Алгоритмы безызбыточного кодирования перестановок и их обоснование были показаны исследователями: Л.К.Бабенко, Т.А.Мазурова,

И.Д.Сидоров, А.Г.Чефранов [2]. А.С.Караханян, П.А.Румянцев была осуществлена модернизация схемы аппаратного кодирования методом перестановки [3].

Шифрование перестановкой возможно с помощью различных алгоритмов. Главное это переставлять символы по определенному правилу. Одним из самых простых методов перестановки является перестановка по таблице.

В этом методе производится запись исходного текста по строкам некоторой таблицы и чтение его по столбцам этой же таблицы. Последовательность заполнения строк и чтения столбцов может быть любой и задается ключом [4].

Приведём пример:

1. Возьмём фразу «А роза упала на лапу Азора» и определим ширину таблицы, пусть это будет 5.
2. Посимвольно занесём данные в таблицу 1, учитывая введенную ширину.

Таблица 1. Таблица для перестановки

А		р	о	з
а		у	п	а
л	а		н	а
	л	а	п	у
	А	з	о	р
а				

3. Для получения зашифрованного сообщения необходимо прочесть сообщение в таблице по столбцам сверху вниз, слева направо.
4. Полученный шифр будет таким «Аал а ал Ару аз опнпо зааур ».

Данный метод кодирования является довольно простым, но его расшифровка может занять довольно долгое время, если не будет известна размерность таблицы.

Реализуем данный алгоритм на языке C++. Разработанная программа состоит из двух функций «coder» и «decoder», которые соответственно кодируют и декодируют введённые сообщения, получая на вход кодируемую или закодированную фразу, а также ключ – ширину таблицы. Листинг представлен ниже:

```
#include <iostream>
#include <windows.h>
using namespace std;
string coder(string s, int w)
{
     int  h;
     if     (s.length()%w!=0)     h=s.length()/w+1;     else
h=s.length()/w;
     char a[h][w];
```

```
	int k=0;
	for (int i=0;i<h;i++)
	{
		for (int j=0;j<w;j++)
		{
			if (k<s.length())
			{
				a[i][j]=s[k];
				k++;
			}
			else a[i][j]=' ';
		}
	}
	string code;
	for (int i=0;i<w;i++)
	{
		for (int j=0;j<h;j++)
		{
			code+=a[j][i];
		}
	}
	return code;
}

string decoder(string s, int w)
{
	int h=s.length()/w;;
	char a[w][h];
	int k=0;
	for (int i=0;i<w;i++)
	{
		for (int j=0;j<h;j++)
		{
				a[i][j]=s[k];
				k++;
		}
	}
	string decode;
	for (int i=0;i<h;i++)
	{
		for (int j=0;j<w;j++)
		{
			decode+=a[j][i];
		}
	}
	return decode;
}

int main()
{
	setlocale(LC_ALL, "Russian");
	SetConsoleCP(1251);
	SetConsoleOutputCP(1251);
```

```
            string s;
            cout<<"Кодируемое слово:"<<endl;
            getline(cin,s);
            int w;
            cout<<"Ключ (ширина таблицы):"<<endl;
            cin>>w;
            cout<<"Закодированная                                    фраза:
"<<coder(s,w)<<endl<<"Декодированная                                    фраза:
"<<decoder(coder(s,w),w);
      }
```

Попробуем с помощью программы зашифровать фразу из примера выше. Результат на рисунке 1.

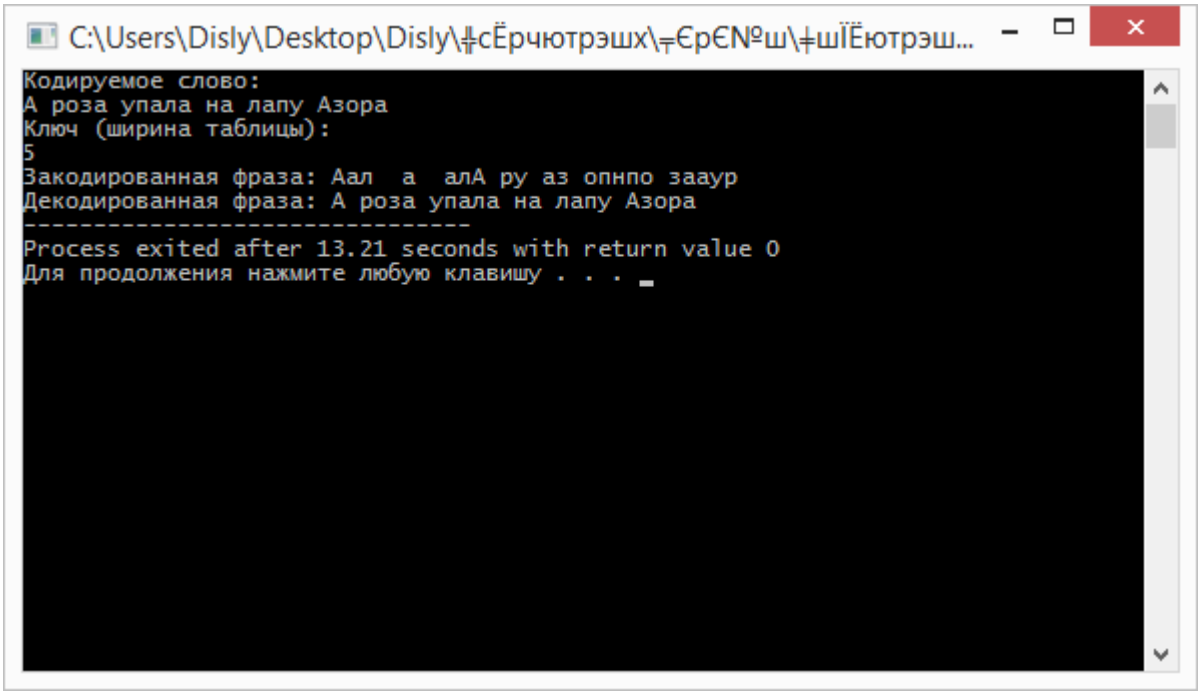

Рисунок 1. Программа для кодирования перестановкой на основе таблицы

По результату видно, что полученный код не отличается от зашифрованного вручную, и также, что декодирование прошло верно.

Таким образом, можно сказать, что кодирование перестановкой на основе таблицы является легким алгоритмом для шифрования, и кодированные фразы имеют некоторую крипто устойчивость, увеличивающуюся с размером сообщения, но использовать его необходимо только в совокупности с другими методами шифрования, так как это существенно повысит защиту информации.

Библиографический список

1. Простейшие методы шифрования с закрытым ключом. Методы перестановки [Электронный ресурс] URL: https://www.intuit.ru/studies/courses/691/547/lecture/12373?page=5 (дата

обращения 30.01.2018)
2. Бабаев А.А. Процедуры кодирования и декодирования перестановок // Кибернетика и системный анализ. 1984. Т. 20. № 6. С. 75-76.
3. Бабенко Л.К., Мазурова Т.А., Сидоров И.Д., Чефранов А.Г. Алгоритмы безызбыточного кодирования перестановок и их обоснование // Известия ЮФУ. Технические науки. 2003. № 4 (33). С. 259-262.
4. Караханян А.С., Румянцев П.А. Модернизация схемы аппаратного кодирования методом перестановки // В сборнике: ОБЩЕСТВО, НАУКА И ИННОВАЦИИ Сборник статей Международной научно-практической конференции. Ответственный редактор: Сукиасян Асатур Альбертович. 2015. С. 27-30.