

А. Н. Дробахина,

Новокузнецкий институт (филиал) Кемеровского государственного университета

ОСНОВЫ СИММЕТРИЧНОГО ШИФРОВАНИЯ В PASCAL.ABC

Аннотация

Для понимания школьниками важности вопросов, связанных с защитой информации, возникает необходимость их знакомства с элементами криптографии. В данной статье представлены сведения, позволяющие ознакомить школьников с некоторыми алгоритмами симметричного шифрования текста, описываются принципы шифрования и приводятся примеры реализации в среде программирования Pascal.ABC.

Ключевые слова: методы шифрования, программирование, Pascal, Pascal.ABC.

DOI: 10.32517/2221-1993-2019-18-3-52-54

В настоящее время информация играет большую роль во многих сферах жизнедеятельности человека. Она становится ресурсом не менее важным, чем, например, материальные, трудовые или природные ресурсы, и так же нуждается в защите.

Защита информации — достаточно сложная задача, над решением которой человечество задумалось еще в древние времена.

Отметим, что существуют различные направления защиты информации, в том числе засекречивание исходного сообщения с помощью шифра — шифрование. Шифрование информации является одним из разделов криптографии.

Используемые на практике методы шифрования достаточно многочисленны и разнообразны. Все их многообразие можно разделить на две большие группы: шифрование с открытым ключом (асимметричные методы), шифрование с закрытым ключом (симметричные методы).

Для симметричных методов шифрования характерно применение одного и того же ключа как при шифровании, так и при расшифровывании сообщений.

Асимметричные методы шифрования используют один (общедоступный) ключ для шифрования, а для расшифровывания — другой (секретный) ключ.

В рамках данной статьи ограничимся рассмотрением симметричных методов шифрования и их программной реализации.

Рассмотрим следующие популярные методы симметричного шифрования:

- замены (подстановки) — символы шифруемого текста заменяются другими символами, взятыми из одного (одно-, или моноалфавитная, подстановка) или нескольких (много-, или полиалфавитная, подстановка) алфавитов [2];
- перестановки — символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста.

Наиболее известными являются шифры замены, или подстановки, особенностью которых является замена символов исходного текста соответствующими символами, принадлежащими алфавиту шифротекста.

Шифр Цезаря относится к шифрам простой замены [1]. Как писал историк Древнего Рима Светоний в книге «Жизнь двенадцати цезарей», данный шифр использовался Гаем Юлием Цезарем для защиты военных сообщений. В нем для замены использовался тот же алфавит, но с определенным циклическим сдвигом относительно открытого алфавита (три символа). Этот сдвиг является ключом.

Применительно к русскому языку суть метода состоит в следующем. Выписывается исходный алфавит (А, Б, ..., Я), затем под ним выписывается тот же алфавит, но с циклическим сдвигом на три буквы влево (в данном случае число 3 — ключ шифра): символ А заменяется на Г, символ Б — на Д и т. д.

Данный шифр легко взламывается вручную. Это объясняется тем, что, во-первых, шифр Цезаря недостаточно хорошо маскирует стандартные частоты встречаемости букв в исходном тексте. Следовательно, зная

Контактная информация

Дробахина Анастасия Николаевна, канд. пед. наук, доцент, доцент кафедры информатики и общетехнических дисциплин факультета информатики, математики и экономики, Новокузнецкий институт (филиал) Кемеровского государственного университета; *адрес:* 654027, Кемеровская область, г. Новокузнецк, Пионерский пр-т, д. 13; *телефон:* (3843) 74-04-35; *e-mail:* drobakhina.kuzspa@gmail.com

A. N. Drobakhina,

Novokuznetsk Institute (branch) of Kemerovo State University

THE BASICS OF SYMMETRIC ENCRYPTION IN PASCAL.ABC

Abstract

To understand the importance of students issues related to the protection of information, there is a need to get acquainted with the elements of cryptography. This article provides information to familiarize students with some algorithms of symmetric text encryption, describes the principles of encryption and provides examples of implementation in the programming environment Pascal.ABC.

Keywords: encryption methods, programming, Pascal, Pascal.ABC.

частоту появления букв в тексте, можно определить соответствие букв открытого и зашифрованного алфавитов, т. е. узнать ключ. Во-вторых, шифр Цезаря имеет мало возможных ключевых комбинаций. Так как ключ — это величина сдвига символов алфавита, то количество возможных ключей ограничивается мощностью используемого алфавита.

В большинстве случаев при шифровании пробелы между словами удаляются, чтобы не выдавать информацию о длине зашифрованного слова.

Ниже представлена программа на Pascal.ABC, реализующая шифрование исходного текста шифром Цезаря. Если величина сдвига больше нуля, то будет выполнено шифрование сообщения, если меньше нуля — дешифрование. В качестве алфавита используются прописные буквы русского языка.

```
program Caesar;
const
  alfavit='абвгдежзийклмнопрстуфхцчшщъыьэя';
var
  s0, s1: string;
  key: integer;

procedure Shifrovanie(s: string; k: integer;
  var ss: string);
var
  l, ll, i, p: integer;
  c: char;
begin
  l:=length(s);
  ll:=length(alfavit);
  ss:=s;
  for i:=1 to l do
  begin
    c:=s[i];
    p:=pos(c, alfavit);
    p:=p+k;
    if p>ll then p:=p-ll;
    ss[i]:=alf[p];
  end;
end;

procedure DeShifrovanie(s: string; k: integer;
  var ds: string);
var
  l, ll, i, p: integer;
  c: char;
begin
  l:=length(s);
  ll:=length(alfavit);
  k:=1;
  ds:=s;
  for i:=1 to l do
  begin
    c:=s[i];
    p:=pos(c, alfavit)-k;
    if p<=0 then p:=p+ll;
    ds[i]:=alfavit[p];
  end;
end;

begin
  write('Введите сообщение');
  readln(s0);
  write('Введите ключ: ');
  readln(key);
  if key>0
  then Shifr(s0, key, s1)
  else DeShifr(s0, -key, s1);
  writeln(s1);
end.
```

На рисунке 1 представлены результаты работы программы, реализующей шифрование текста шифром Цезаря.

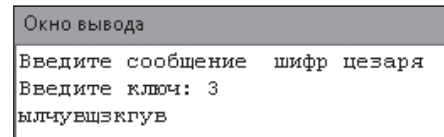


Рис. 1. Демонстрация работы программы

Еще один метод симметричного шифрования — **шифрование методом перестановки**. Суть метода заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов [2].

Самый простой вариант перестановки — написание исходного текста в обратном порядке с одновременным разделением текста на блоки, например, по шесть букв. Перед началом шифрования необходимо убедиться, что исходный текст можно будет разбить на блоки одинаковой длины. Если последний блок окажется короче, то его исходный текст дополняют незначащими символами.

Например, исходный текст «шифрование методом перестановки» разобьем на блоки по шесть символов и зашифруем. Для выравнивания последнего блока добавим символ «Ю».

```
program Perestанovka;
var
  i, h: integer;
  str: string;
  c: char;
begin
  writeln('Введите исходный текст');
  readln(str);
  for i:=length(str) downto 1 do
    if str[i]=' ' then delete(str, i, 1);
  writeln('Введите размер блока');
  readln(h);
  for i:=1 to length(str) div 2 do
  begin
    c:=str[i];
    str[i]:=str[length(str)-i+1];
    str[length(str)-i+1]:=c;
  end;
  while length(str) mod h <> 0 do
    str:=str+'Ю';
  for i:=1 to length(str) div h do
    write(copy(str, (i-1)*h+1, h), ' ');
  end.
```

На рисунке 2 представлены результаты работы программы, реализующей шифрование текста методом перестановки.

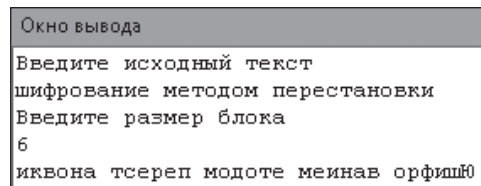


Рис. 2. Демонстрация работы программы

Отметим, что в зависимости от уровня подготовки учащихся можно рассматривать более сложные методы шифрования.

Так, можно рассмотреть более сложный вариант перестановки — **перестановку с ключом**, например, маршрутное шифрование. Данный способ шифрования разработал французский математик и криптограф Франсуа Виет.

Суть этого метода в том, что исходное сообщение записывают в некоторую геометрическую фигуру (обычно прямоугольник) по некоторому пути, а затем, выписывая символы по другому пути, получают зашифрованный текст.

Пусть n и m — целые положительные числа, большие 1. Исходное сообщение разбивается на блоки равной длины, состоящие из числа символов, равного произведению $m \cdot n$. Если последний блок получится меньше остальных, то в него следует дописать требуемое количество произвольных символов. Затем составляется таблица размера $m \times n$. Блоки вписываются построчно в эту таблицу. Зашифрованное сообщение получается выписыванием букв из таблицы в соответствии с некоторым маршрутом. Ключом такой криптограммы является маршрут и числа m и n . Обычно буквы выписывают по столбцам, которые упорядочивают согласно паролю: внизу таблицы приписывается слово из n неповторяющихся букв и столбцы нумеруются по алфавитному порядку букв пароля.

Например, для шифрования текста методом перестановки сначала удалим все пробелы, а затем разобьем текст на блоки длиной $n = 6$. Блоков получится $m = 5$. К последнему блоку припишем произвольную букву, например букву А. В качестве пароля выберем слово «пароль».

Теперь будем выписывать буквы по столбцам в соответствии с алфавитным порядком букв пароля и получим зашифрованный текст: «инорооммтиреоскшатенфидеввепаа».

Ниже представлен листинг программы, реализующий данный метод шифрования.

```
program Perestankovka2;
var
  A:array [1..100,1..100] of string;
  n,m,i,j,s,k:integer;
  ch:char;
  str,pass,pass_cipher:string;

begin
  writeln('Введите m и n:');
  readln(m,n);
  repeat
    writeln('Введите исходный текст из ',n*m,'
символов:');
    readln(str);
    until length(str)=n*m;
  repeat
    writeln('Введите пароль из ',n,' символов:');
    readln(pass);
    until length(pass)=n;
    for j:=1 to n do A[m+1,j]:=pass[j];
    pass_cipher:=pass;
    for i:=1 to length(pass_cipher)-1 do
      begin
        for j:=i+1 to length(pass_cipher) do
          if pass_cipher[j]<pass_cipher[i] then
            begin
              ch:=pass_cipher[i];
              pass_cipher[i]:=pass_cipher[j];
              pass_cipher[j]:=ch;
            end;
        end;
      end;
    end;
```

```
for j:=1 to n do A[m+2,j]:=pass_cipher[j];
k:=1;
for i:=1 to m do
  for j:=1 to n do
    begin
      A[i,j]:=str[k];
      inc(k);
    end;
  writeln('Зашифрованный текст:');
  s:=0;
  j:=1;
  k:=1;
  repeat
    if A[m+1,j]=pass_cipher[k] then
      begin
        for i:=1 to m do write(A[i,j]);
        inc(s);
        j:=1;
        inc(k);
      end
    else inc(j);
  until s=n;
end.
```

На рисунке 3 представлены результаты работы программы, реализующей шифрование текста с помощью метода маршрутного шифрования.

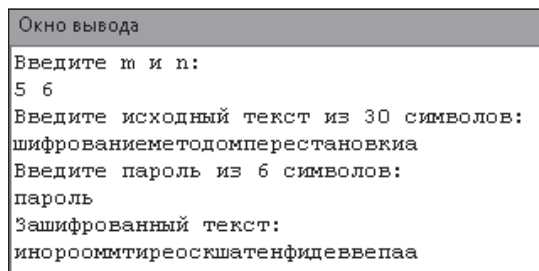


Рис. 3. Демонстрация работы программы

Отметим, что предложенный способ решения данной задачи не оптимальный, а является «отправной точкой» и открывает простор для повторения различных разделов изученного курса программирования. Так, можно предложить ученикам иначе организовать ввод исходного текста (программное удаление пробелов, определение длины текста, добавление незначащих символов и др.). Также для решения данной задачи можно использовать файлы, в которых будут храниться исходный и зашифрованный тексты.

В заключение отметим, что в настоящее время разработано множество алгоритмов защиты информации, основанных на применении различных схем и методов шифрования. Изложенный материал не претендует на полное и всестороннее освещение тем, связанных с защитой информации посредством шифрования, однако позволит школьникам понять важность вопросов, связанных с защитой информации, освоить и реализовать на практике некоторые алгоритмы шифрования, а также совершенствовать знания языка программирования Pascal.

Список использованных источников

1. Введение в криптографию / под общ. ред. В. В. Яшенко. 4-е изд., доп. М.: МЦНМО, 2012.
2. Партыка Т. Л., Попов И. И. Информационная безопасность: учебное пособие. 3-е изд., перераб. и доп. М.: ФОРУМ, 2010. (Профессиональное образование.)