МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГУ»)

Факультет прикладной математики, информатики и механики Кафедра Системного анализа и управления

Лабораторная работа №1 «Шифрование перестановкой»

Выполнил: студент 4 к. 6 гр. ПМИ Бакаев Илья Игоревич

1. Описание задачи

Вариант усложненной перестановки. Для этого открытый текст записывается в матрицу по определенному ключу k1, определяющему порядок записи открытого текста в строки матрицы при шифровании. Шифр-текст образуется при считывании из этой матрицы по ключу k2, определяющему, в каком порядке записывается информация из столбцов матрицы. Для реализации такого варианта перестановки можно не использовать непосредственно матрицу, а осуществлять перерасчет коэффициентов.

Открытый текст:

ШИФРОВАНИЕ_ПЕРЕСТАНОВКОЙ

<u>Ключи</u>: k1: 5-3-1-2-4-6;

k2: 4-2-3-1.

Матрица:

k1/k2	1	2	3	4
1	И	E	-	Π
2	Е	P	Е	С
3	O	В	A	Н
4	Т	A	Н	O
5	Ш	И	Φ	P
6	В	К	O	Й

Запись по строкам осуществляется в соответствии с ключом k1, а чтение по столбцам - в соответствии с ключом k2

<u>Цель работы</u>: программно реализовать алгоритм перестановки.

```
PascalABC.NET
Файл Правка Вид Программа Сервис Модули Помощь

    Program1.pas* PABCSystem.pas

   e = 10;
 const
 const
   b = 4;
   txt, txt_i: string;
i, j, z, yardage: integer;
matrix: array[1..a, 1..b] of char;
k1, k2: array[1..e] of integer;
 begin
    writeln('Text to encrypt: ', #10); readln(txt);
 Файл Правка Вид Программа Сервис Модули Помощь
🗅 📂 💹 🕬 | X 🖦 🕵 🕑 (* 💯 🖳 ) 🕨 🗆 🕮 | 📮 🖅 🔟 🛢 | 🥡 🖫

    Program1.pas* PABCSystem.pas

    writeln('Text to encrypt: ', #10);readln(txt);
yardage := length(txt);
    if (yardage = a * b) then
       repeat
        epeat
writeln('Key to write line by line: ', #10);
readln(k1[1], k1[2], k1[3], k1[4], k1[5], k1[6]);
write(#10);z := 0;
for i := 1 to 5 do
    for j := i + 1 to 6 do
        if (k1[i] = k1[i]) then z := z + 1;

       if (z <> 0) then writeln('Key symbols are not unique', \#10) until z = 0;
Program1.pas* Program2.pas*
for j := 1 to 4 do
    for i := 1 to 6 do
        matrix[i, k2[j]] := txt_i[(j - 1) * a + i];txt := ' ';
for i := 1 to 6 do
    for j := 1 to 4 do
        txt := txt + matrix[k1[i], j];
writeln('Encrypted: ', #10, txt, #10);
end
    else write('Error!');
                                                                                                                                                                    ŢΧ
 Окно вывода
Text to encrypt:
ШИФРОВАНИЕ ПЕРЕСТАНОВКОЙ
Key to write line by line:
5
3
 1
2
 4
6
Encrypted:
пснорйерваик еанфоиеотшв
🔳 Окно вывода 🕞 Список ошибок 📳 Сообщения компилятора 🛭
```

Программа протестирована в Pascal ABC.NET сборка 2799