

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

Воронеж – 2021

1. Описание задачи

Вариант усложненной перестановки. Для этого открытый текст записывается в матрицу по определенному ключу k_1 , определяющему порядок записи открытого текста в строки матрицы при шифровании. Шифр-текст образуется при считывании из этой матрицы по ключу k_2 , 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

Ключи: k_1 : 5-3-1-2-4-6;

k_2 : 4-2-3-1.

Матрица:

k_1/k_2	1	2	3	4
1	И	Е	-	П
2	Е	Р	Е	С
3	О	В	А	Н
4	Т	А	Н	О
5	Ш	И	Ф	Р
6	В	К	О	Й

Запись по строкам осуществляется в соответствии с ключом k_1 , а чтение по столбцам - в соответствии с ключом k_2

Цель работы: программно реализовать алгоритм перестановки.

