**Лабораторная работа №5**

**Тема:** Метод поворотной решётки.

**Задание:** Разработать программу для шифрации и дешифрации по методу поворотной решётки.

**Пояснения:**

*Шифр «Поворотная решетка».*

Для использования шифра, называемого поворотной решеткой, изготавливается трафарет из прямоугольного листа клетчатой бумаги размером 2*m* × 2*n* клеток. В трафарете вырезано *m* × *n* клеток так, что при наложении его на чистый лист бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа.

Буквы сообщения последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырех его возможных положений в заранее установленном порядке.

Рассмотрим процесс шифрования на примере. Пусть в качестве ключа используется решетка 6 × 10, приведенная на рисунке 5, *а*. Зашифруем с ее помощью текст

ШИФРРЕШЕТКАЯВЛЯЕТСЯЧАСТНЫМСЛУЧАЕМШИФРАМАРШРУТНОЙПЕРЕСТАНОВКИ.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| а)   |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | | б)   |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | Ш |  |  |  |  |  |  |  |  | | И |  |  |  | Ф |  | Р | Р |  |  | |  | Е |  |  |  | Ш |  |  |  | Е | |  |  |  | Т |  |  |  | К |  |  | |  | А |  |  |  |  |  |  |  |  | |  |  | Я |  |  | В | Л |  |  | Я | |
| в)   |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Е | Ш |  | Т | С |  |  | Я |  |  | | И |  |  |  | Ф |  | Р | Р | Ч |  | |  | Е | А |  |  | Ш | С |  |  | Е | |  |  |  | Т | Н |  |  | К | Ы |  | |  | А | М | С |  | Л |  |  |  | У | |  |  | Я |  |  | В | Л |  | Ч | Я | | г)   |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Е | Ш | А | Т | С | Е | М | Я |  | Ш | | И | И |  |  | Ф |  | Р | Р | Ч |  | |  | Е | А | Ф |  | Ш | С | Р |  | Е | | Т | А |  | Т | Н | М |  | К | Ы | А | | Р | А | М | С | Ш | Л | Р | У |  | У | |  | Т | Я |  |  | В | Л |  | Ч | Я | |
| д)   |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Е | Ш | А | Т | С | Е | М | Я | Н | Ш | | И | И | О | Й | Ф | П | Р | Р | Ч | Е | | Р | Е | А | Ф | Е | Ш | С | Р | С | Е | | Т | А | Т | Т | Н | М | А | К | Ы | А | | Р | А | М | С | Ш | Л | Р | У | Н | У | | О | Т | Я | В | К | В | Л | И | Ч | Я | | |
| *Рис. 5.* Пример шифрования текста методом поворотной решетки. | |

Наложив решетку на лист бумаги, вписывается первые 15 (по числу вырезов) букв сообщения. Результат после снятия решетки изображен на рисунке 5, *б*. Повернув решетку на 180 градусов и вписав следующие 15 букв, получаем лист, изображенный на рисунке 5, *в*. Перевернув лист и проделав то же самое, шифруется остаток текста (рисунок 5, *г* и *д*).

Получатель сообщения, имеющий точно такую же решетку, без труда прочтет исходный текст, наложив решетку на шифртекст по порядку четырьмя способами.

Число трафаретов, то есть количество ключей шифра «решетка», составляет *T* = 4*mk*. Этот шифр предназначен для сообщений длины *n* = 4*mk*. Уже при размере трафарета 8 × 8 число возможных решеток превосходит 4 миллиарда.

**Контрольные вопросы:**

1. Алгоритм шифрации.
2. Алгоритм дешифрации.
3. Как осуществляется поворот решётки?
4. Что является в данном методе ключом?
5. Какое соотношение между размерностью решётки, числом окон и длиной сообщения?
6. Программа допускает изменение размерности решётки?
7. Анализ метода.

**Содержание отчета:**

1. Цель работы.
2. Алгоритм шифрации и дешифрации по заданному методу, который реализует разработанная программа.
3. Описание программы (исходный код с комментариями).
4. Анализ ограничений возможности применения разработанной программы.
5. Анализ ограничений возможности применения данного метода.
6. Заключение.