МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

ШИФРОВАНИЕ МЕТОДОМ ПЕРЕСТАНОВОК

Методические указания по выполнению лабораторной работы для студентов направлений 02.03.03, 09.03.01, 09.03.02, 09.03.03, 09.03.04, 10.03.01, 10.05.02, 38.03.01, 38.03.03, 38.03.05, 38.05.01, 40.05.01, 43.03.02, 43.03.03, 45.03.03

Курск 2019

УДК 004.056.55 (076.5)

Составители: М.А. Ефремов, С.И. Егоров

Рецензент
Кандидат технических наук, доцент *М.О. Таныгин*

Шифрование методом перестановок: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов, С.И. Егоров. Курск, 2019. 9 с.: ил. 2, табл. 1. Библиогр.: с. 9.

Рассматриваются основные практические и теоретические положения этапов шифрования сообщений с помощью шифров перестановки на примере маршрутов Гамильтона. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по образованию в области информационной безопасности (УМО ИБ).

Предназначены для студентов направлений 02.03.03, 09.03.01, 09.03.02, 09.03.03, 09.03.04, 10.03.01, 10.05.02, 38.03.01, 38.03.03, 38.03.05, 38.05.01, 40.05.01, 43.03.02, 43.03.03, 45.03.03 очной и заочной формы обучения.

Текст печатается в авторской редакции

Подписано в печать 04.04.19. . Формат 60х84 1/16.
Усл.печ. л.0,4 . Уч.-изд.л. 0,3 Тираж 30 экз. Заказ.299 Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1 ЦЕЛЬ РАБОТЫ

Цель лабораторной работы - изучить и получить практические навыки в сокрытии информации с помощью шифрованиея методом перестановок при помощи маршрутов Гамильтона.

2 ЗАДАНИЕ

Ознакомиться с теоретическим материалом. Произвести шифрование буквенной последовательности методом перестановок, на основе маршрутов Гамильтона, расшифровать полученную криптограмму, проанализировать алгоритм выполнения работы.

3 ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание.
2. Изучить теоретическую часть.
3. Зашифровать сообщение.
4. Расшифровать криптограмму.
5. Составить отчет.

4 СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Описание процесса выполнения работы.
4. Вывод.

5 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Суть методов перестановки заключается в разделении исходного текста на блоки фиксированной длины и последующей перестановке символов внутри каждого блока по определенному алгоритму.

Перестановки получаются за счет разницы путей записи исходной информации и путей считывания зашифрованной информации в пределах геометрической фигуры. Примером простейшей перестановки является запись блока исходной информации в матрицу по строкам, а считывание - по столбцам. Последовательность заполнения строк матрицы и считывания зашифрованной информации по столбцам может задаваться ключом. Криптостойкость метода зависит от длины блока (размерности матрицы). Так для блока длиной 64 символа (размерность матрицы 8x8) возможны $1{,}6 \times 10^9$ комбинаций ключа. Для блока длиной 256 символов (матрица размерностью 16x16) число возможных ключей достигает 1×10^{26}. Решение задачи перебора ключей в последнем случае даже для современных ЭВМ представляет существенную сложность.

Перестановки используются также в методе, основанном на применении *маршрутов Гамильтона.* Этот метод реализуется путем выполнения следующих шагов.

Шаг 1. Исходная информация разбивается на блоки. Если длина шифруемой информации не кратна длине блока, то на свободные места последнего блока помещаются специальные служебные символы-заполнители (например, *).

Шаг 2. Символами блока заполняется таблица, в которой для каждого порядкового номера символа в блоке отводится вполне определенное место

Шаг 3. Считывание символов из таблицы осуществляется по одному из маршрутов. Увеличение числа маршрутов повышает криптостойкость шифра. Маршруты выбираются либо последовательно, либо их очередность задается ключом К.

Шаг 4. Зашифрованная последовательность символов разбивается на блоки фиксированной длины L. Величина L может отличаться от длины блоков, на которые разбивается исходная информация на шаге 1. Расшифровывание производится в обратном порядке. В соответствии с ключом выбирается маршрут и заполняется таблица согласно этому маршруту.

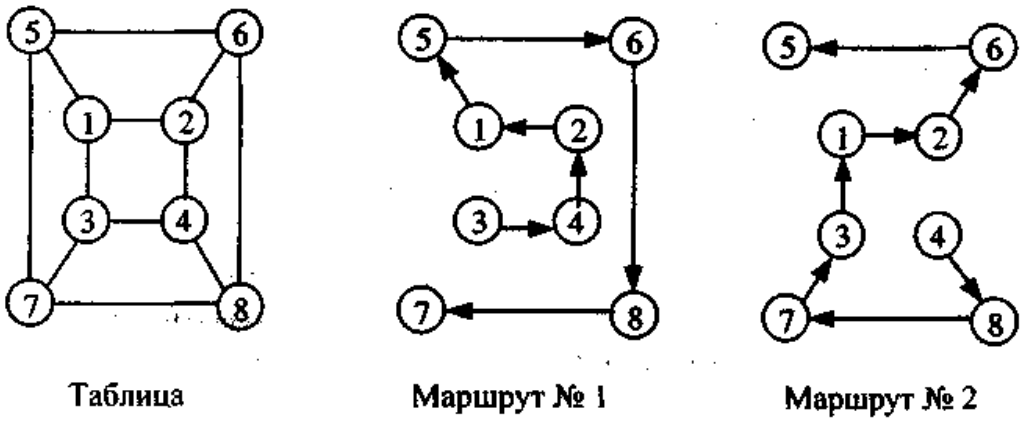

Рисунок 1 — Таблица символов и маршруты Гамильтона

Из таблицы символы считываются в порядке следования номеров элементов. Ниже приводится пример шифрования информации с использованием маршрутов Гамильтона.

Пусть требуется зашифровать исходный текст T_0 = <МЕТОДЫ_ПЕРЕСТАНОВКИ>. Ключ и длина зашифрованных блоков соответственно равны: К=<2,1,1>, L=4. Для шифрования используются таблица и два маршрута, представленные на рисунке. Для заданных условий маршруты с заполненными матрицами имеют вид, показанный ниже:

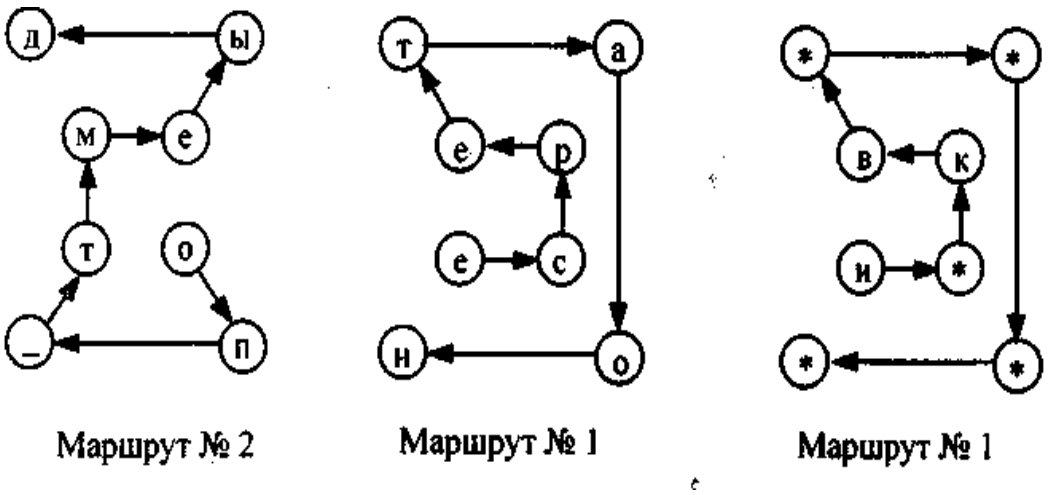

Рисунок 2 — Маршруты Гамильтона для заданной буквенной последовательности

Шаг 1. Исходный текст разбивается на три блока:

Б1 = <МЕТОДЫ_П>;

Б2 = <ЕРЕСТАНО>;

БЗ = <ВКИ*****>.

Шаг 2. Заполняются три матрицы с маршрутами 2,1,1.

Шаг 3. Получение шифртекста путем расстановки символов в соответствии с маршрутами.

T_1= <ОП_ТМЕЫДЕСРЕТАОНИ*КВ****>.

6 ИНДИВИДУАЛЬНЫЕ ВАРИАНТЫ ЗАДАНИЙ

Требуется получить шифртекст R и расшифрированный текст T, используя соответствующие маршруты Гамильтона и ключ K.

Таблица 1 – Варианты заданий

№ п/п	Исходный текст T	Ключ K
1.	Отговорила роща золотая	211
2.	Я полон дум о юности	112
3.	Но никого не может он согреть	1211
4.	Стая галок и ворон	111
5.	Заунывный ветер гонит	221
6.	Не обгорят рябиновые кисти	2221
7.	За листком летит листок	212
8.	Ель надломленная стонет	121
9.	С криком в воздухе кружится	2111
10.	Под нависшею скалою	221
11.	Сгребёт их в один ненужный ком	1122
12.	Листья в поле пожелтели	121
13.	Стремленье всех надземных сил	1112
14.	У они хлещут пеною кипучей	2212
15.	Глухо шепчет тёмный лес	122

7 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Назовите основные преимущества шифрования методом перестановок?
2. Назовите основные недостатки шифрования методом перестановок?
3. В чем отличие методов перестановки от методов подстановки?
4. Перечислите основные этапы получения шифрограммы методом перестановок по маршрутам Гамильтона?

8 СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Н. Смарт . Криптография [текст] Издательство: М.: Техносфера, 2005. – 528 с.
2. С. Баричев Криптография без секретов [текст] Издательство: Горячая Линия – Телеком. 2004.- 43 с.
3. Нильс Фергюсон, Брюс Шнайер. Практическая криптография [текст] Издательство: Вильямс. 2005.- 416 с.