Лабораторная работа № 10

«Шифрование информации методом перестановок с использованием маршрутов Гамильтона»

Цель работы:

1. Закрепление теоретического материала по изучению метода перестановок.
2. Получение шифротекста по исходным данным.
3. Получение исходного текста по заданному шифротексту, маршрутам и ключу.

Пояснения к работе:

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).

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 (рис. 19).

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.

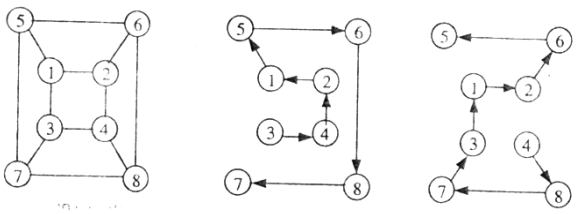


Таблица **Маршрут № 1** **Маршрут № 2**

Расшифрование производится в обратном порядке. В соответствии с ключом выбирается маршрут и заполняется таблица согласно этому маршруту.

Из таблицы символы считываются в порядке следования номеров элементов.

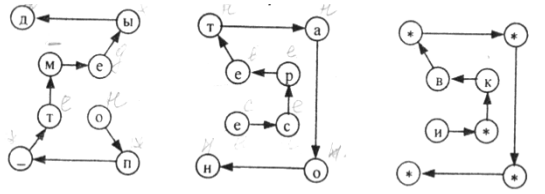
Пример использования маршрутов Гамильтона для шифрования текста

Пусть требуется зашифровать исходный текст

То = <МЕТОДЫ_ПЕРЕСТАНОВКИ>.

Ключ и длина зашифрованных блоков соответственно равны: К=<2.1,1>, L=4.

Для шифрования используются таблица и два маршрута, представленные на рис.6. Для заданных условий маршруты с заполненными матрицами имеют следующий вид:



Маршрут № 2 ***Маршрут № 1*** ***Маршрут № 2***

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.

Т, = <ОП ТМЕЫДЕСРЕТАОНИ*КВ****>.

Шаг 4. Разбиение на блоки шифртекста

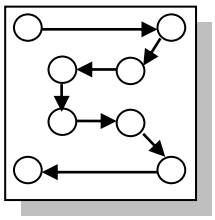
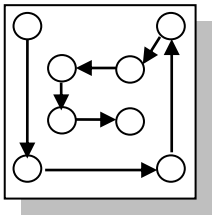
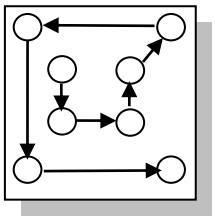
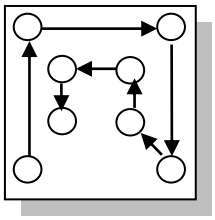
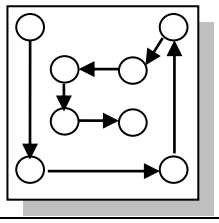
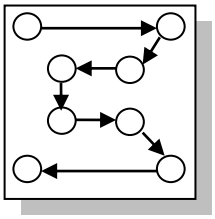
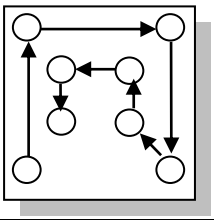
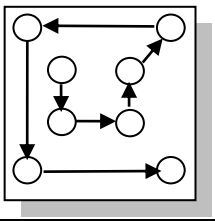
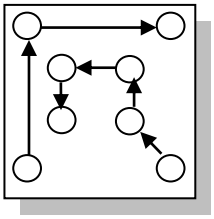
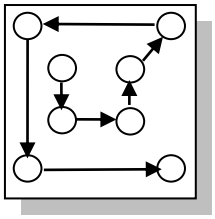
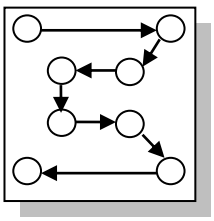
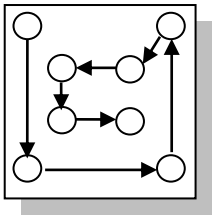
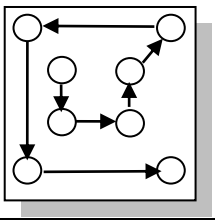
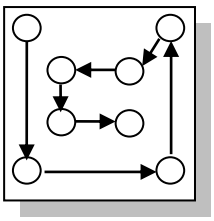
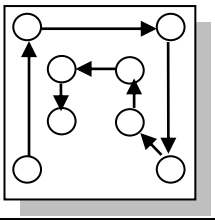
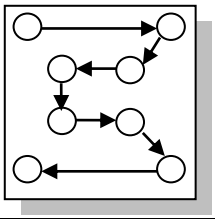
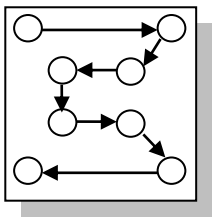
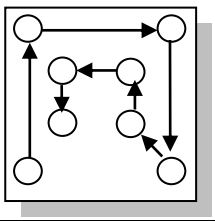
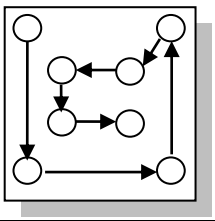
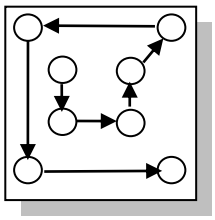
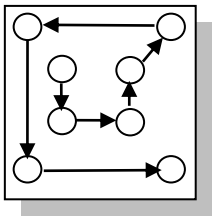
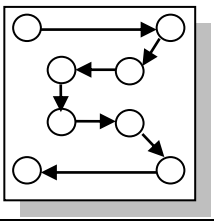
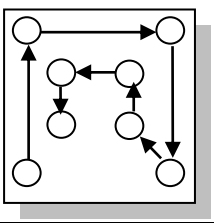
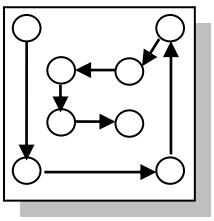
Т] = <ОП_Т МЕЫД ЕСРЕ ТАОН И*КВ ****>.

Ход выполнения лабораторной работы:

1. Изучить приведенные в методическом описании к лабораторной работе материал и пример шифрования.

2. Получить у преподавателя исходный текст, маршруты и ключ для шифрования.
3. Выполнить по шагам процедуру шифровании, полученный шифротекст представить в виде блоков информации.
4. Представить результаты преподавателю.
5. Получить у преподавателя шифротекст, маршруты и ключ для расшифрования.
6. Выполнить по шагам процедуру расшифрования, полученный исходный текст представить преподавателю для проверки.
7. Оформить отчет в установленной форме.
8. Представить результаты работы преподавателю.

Варианты маршрутов:

№ варианта	**Маршрут № 1**	**Маршрут № 2**	**Маршрут № 3**	**Маршрут № 4**
1				
2				
3				
4				
5				
6				

Контрольные вопросы:

1. Понятие криптостойкости. Условия, предъявляемые к криптостойкости.
2. Понятие метода перестановок.
3. Понятие замены с помощью маршрутов Гамильтона.
4. Перечислите достоинства и недостатки методов перестановок.