МИНОБРНАУКИ РОССИИ

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

Кафедра защиты информации и систем связи

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«15» _____ 2015 г.

КРИПТОАНАЛИЗ БЛОЧНЫХ ШИФРОВ

Методические указания по выполнению лабораторной работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01

Курск 2015

УДК 004.056.55 (076.5)

Составитель: М.А. Ефремов

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

Криптоанализ блочных шифров: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2015. 12 с.: ил. 3, табл. 1.

Содержат основные теоретические и практические сведения о сущности криптоанализа сообщений зашифрованных с помощью блочных шифров. 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 специальностей 10.05.03, 10.05.02, 10.03.01 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. . Уч.-изд.л. . Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Цель лабораторной работы - расшифровать криптограммы, зашифрованные методом перестановок, получить ключ шифрования.

2. ЗАДАНИЕ

Ознакомьтесь с руководством пользователя и с теоретическим материалом. Запустите исполняемый файл и выберите необходимый номер варианта. Требуется расшифровать криптограммы, зашифрованные методом перестановок и методом перестановок по путям Гамильтона, получить ключи шифрования.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание.
2. Изучить теоретическую часть.
3. Определить индекс соответствия.
4. На основе частотного анализа отдельных групп криптограммы получить ключ.
5. Составить отчет.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Краткий протокол криптоанализа.
4. Расшифрованный исходный текст и ключи шифрования.
5. Вывод.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

5.1 Блочные и поточные шифры. Перестановки

Все шифры замены, которые были рассмотрены выше, относятся к т.н. *поточным* шифрам. В поточных шифрах шифрование происходит посимвольно. Если уподобить поточные шифры - а, вернее, шифраторы - черному ящику и подавать на вход поток символов открытого текста, то на выходе практически без задержек будут появляться соответствующие им символы криптограммы.

Кроме поточных, существуют еще *блочные* шифры. При использовании блочных шифров текст предварительно разбивается на блоки и шифрование происходит поблочно. 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 8 х 8) возможны 1,6 х 10^9 комбинаций ключа. Для блока длиной 256 символов (матрица размерностью 16 х 16) число возможных ключей достигает 1,4 х 10^{26}. Решение задачи перебора ключей в последнем случае даже для современных ЭВМ представляет существенную сложность.

Перестановки относятся к блочным шифрам. Текст делится на блоки по N символов, и в каждом блоке символы переставляются в соответствии с некоторым правилом (ключом). Таким образом ключ задает порядок символов в блоке. Кроме того, известны т.н. табличные перестановки. Например, исходный текст вписывают в таблицу по столбцам, а затем строки таблицы переставляются в

соответствии с ключом. Размер таблицы оговаривается заранее. Существует два способа использования ключа.

Пусть

Ключ K $= k_1 k_2 \ldots k_i \ldots k_N$

Текст M $= m_1 m_2 \ldots m_i \ldots m_N$

K_i - целое число: $k_i \in [1,N]$.

Способ 1.

Чтобы зашифровать текст M, нужно i-ый символ текста поставить на k_i-ое место. При расшифровке на i-ое место ставим k_i-ый символ криптограммы.

N = 5; Ключ 3-1-5-4-2

Исходный Текст : ИНФОР | МАЦИЯ

Криптограмма : НРИОФ | АЯМИЦ

Способ 2.

При шифровке на i-ое место ставим k_i-ый символ текста. При расшифровке i-ый символ криптограммы ставится на k_i-ое место.

N = 5; Ключ 3-1-5-4-2

Исходный Текст : ИНФОР | МАЦИЯ

Криптограмма : ФИРОН | ЦМЯИА

В нашем лабораторном практикуме для простой перестановки используется способ 2, а для случая табличной перестановки - способ 1.

5.2 Пути Гамильтона

Любую перестановку можно представить в виде графа G = < V,E >, где V - вершины, а E - ребра графа. В этом случае перестановки получают, записывая открытый текст и читая зашифрованный текст по всевозможным путям этого графа.

Для этих целей удобно пользоваться путями Гамильтона. Гамильтонов путь в графе - это путь, проходящий в точности один раз через каждую вершину данного графа.

Таким образом, заранее выбирается некоторый граф, и затем один из путей Гамильтона используется в качестве ключа перестановки. 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. Расшифрование производится в обратном порядке. В соответствии с ключом выбирается маршрут и заполняется таблица согласно этому маршруту.

6. ВЫПОЛНЕНИЕ РАБОТЫ

6.1 Запуск программы

1 Дешифровать криптограмму, зашифрованную методом простой перестановки.

1.1 Запустить на выполнение файл rela12.exe и выбрать из главного меню опцию “Метод перестановок”. На вопрос “Метод перестановок по маршруту?” ответьте “Нет”.

1.2 Нажмите на клавишу Enter и выберите в появившемся списке свой вариант.

1.3 На рисунке 1 представлен интерфейс программы. Задайте длину ключа. Это можно сделать, нажав клавишу F9. Вам

будет предложено несколько возможных длин ключа. Выберите наиболее вероятную.

1.4 Укажите способ порождения ключа: автоматическая генерация или Вы будете вводить ключ вручную. Переключение режимов осуществляется по клавише F8.

1.5 Если возникло предположение, что какое-либо слово или его часть присутствует в тексте, можно его проверить, воспользовавшись клавишей F5. В появившееся окно ввода введите Ваше вероятное слово, и программа попытается найти такое значение ключа, при котором это слово присутствовало бы в тексте.

1.6 Проверяя различные значения ключей, расшифруйте криптограмму.

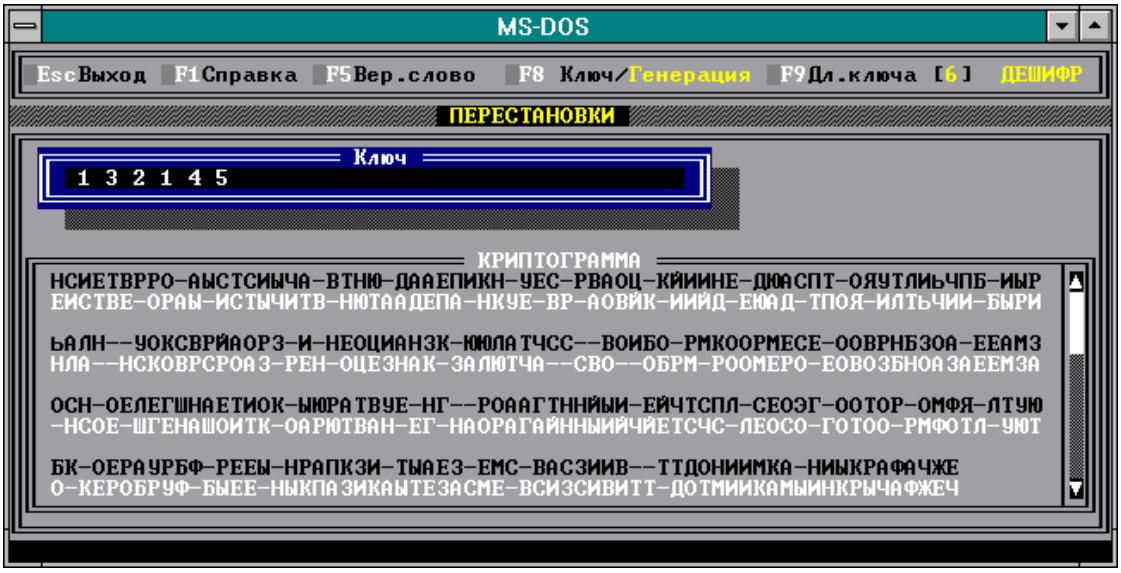

Рисунок 1 – Интерфейс программы

2 Дешифровать криптограмму, зашифрованную с использованием путей Гамильтона.

2.1 Запустить на выполнение файл rela12.exe и выбрать из главного меню опцию “Метод перестановок”. На вопрос “Метод перестановок по маршруту?” ответьте “Да”.

2.2 Введите число вершин и заполните матрицу смежности для графа, выданного Вам преподавателем. Вершина не

считается смежной сама себе. Программа вычислит все пути Гамильтона для этого графа (см. рисунок 2).

2.3 Нажмите на клавишу Enter и выберите в появившемся списке свой вариант.

2.4 Перед Вами на экране текст криптограммы. Процесс дешифрации аналогичен описанному выше случаю простой перестановки. Исключение составляет добавившаяся возможность просмотра путей Гамильтона, один из которых и является ключом. Просмотреть пути Гамильтона можно по клавише F9.

2.5 Расшифровать криптограмму.

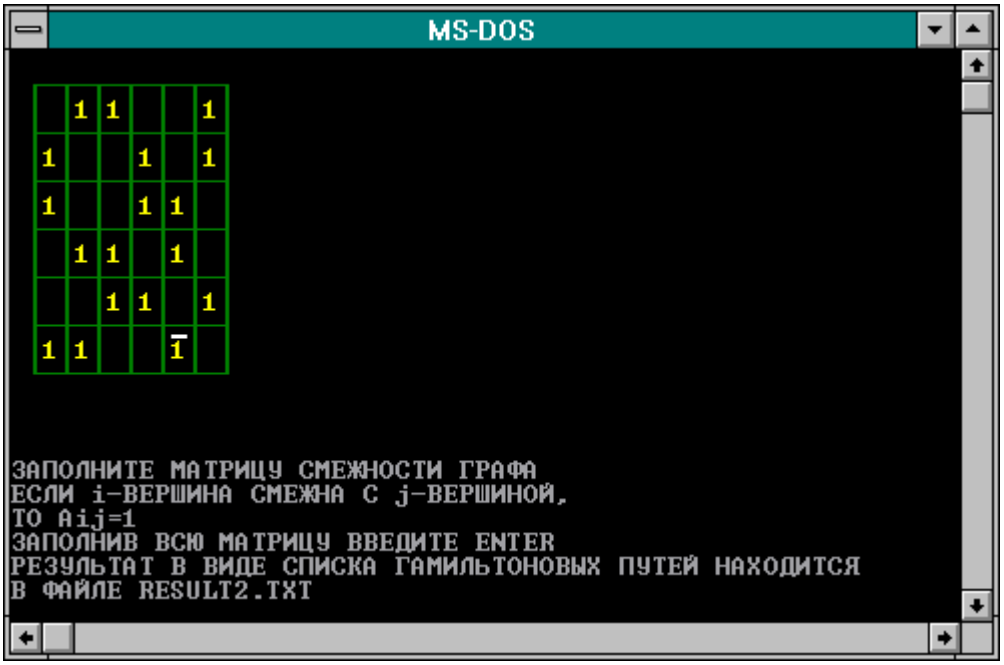

Рисунок 2 – Матрица смежности

6.2 Пример дешифрации криптограммы, зашифрованной простой перестановкой

Криптограмма:

```
 ЮЛЧЕКЕ_ОЗВЧАЕНН_ЕДЛИС_БАЯНАСИЛВОАНРСОТИН
ЫРНК_Ц_ЕНАХЫ_БНАМГ_УЕМЕТИБОЕС_ЧЕ_ЕНП_ЕЖИИВД
НКТСИ_ОКИВИЛЫНЙ_ДНЬЮКРАХРА_ТРЖЕУТСЗУ_ЗКЯ_МР
АИЫРВОЗМ_ЕЖМ_УЦЕ_ДЙО_ПНДОАВР_АИ_ЦНЕОЙЦОПКУ_
ТАЕЛПН_ЕБЯЬЛШИО_ИКОМБЕАНЛМЯИ_ИНЕ_ОЦС_ДЕТИК_
КЛД_СЕЛ_ЕЛИКИВДНКТСЬ_ОМЕ_ВТЕШ_ЧЫ_МБОЕШЬЕ_ЛА
ЧСГУКИОВНРПОД_ИЖЕМА
```

Определим длину ключа. Программа предлагает следующие варианты: 5,11. Предположим, длина ключа равна 5.

Установим автоматический режим генерации ключей. При значении ключа, равном 3-1-5-4-2, возникло предположение, что в тексте присутствует слово "ЗНАЧЕНИЕ":

```
ЮЛЧЕКЕО_ЗВЧАЕНН_ЕДЛИС_БАЯНАСИЛВОАНРС...
ЛКЮЕЧОВЕЗ_АНЧНЕЕИ_ЛД_ЯСАБАЛНИСОРВНАО...
```

Введем его как вероятное слово. В результате перебора ключей программа выдала следующее:

```
ЮЛЧЕКЕО_ЗВЧАЕНН_ЕДЛИС_БАЯНАСИЛВОАНРСОТИ...
КЛЮЧЕВОЕ_ЗНАЧЕНИЕ_ДЛЯ_СБАЛАНСИРОВАННОСТ...
```

Криптограмма расшифрована. Исходный текст:

```
 КЛЮЧЕВОЕ_ЗНАЧЕНИЕ_ДЛЯ_СБАЛАНСИРОВАННОСТИ
_РЫНКА_ЦЕННЫХ_БУМАГ_ИМЕЕТ_ОБЕСПЕЧЕНИЕ_ЛИКВИД
НОСТИ_ЛИКВИДНЫЙ_РЫНОК_ХАРАКТЕРИЗУЕТСЯ_УЗКИМ_
РАЗРЫВОМ_МЕЖДУ_ЦЕНОЙ_ПРОДАВЦА_И_ЦЕНОЙ_ПОКУП
АТЕЛЯ_НЕБОЛЬШИМИ_КОЛЕБАНИЯМИ_ЦЕН_ОТ_СДЕЛКИ_
К_СДЕЛКЕ_ЛИКВИДНОСТЬ_ТЕМ_ВЫШЕ_ЧЕМ_БОЛЬШЕ_УЧА
СТНИКОВ_ПРОДАЖИЕМ
```

Ключ: 3-2-4-5-1

6.3 Пример дешифрации криптограммы, зашифрованной перестановкой по маршрутам Гамильтона

Криптограмма:

Л_ЯПДОЕВРРИН_АКИИЧЯЛВРЕО_ТОНГЯ_ЛСООАК_РВПОТАИАИЛ ТНКВ_ЫИИАТЕЧ_ГЕОТИ_ЗШ_ФОРВИНОНГА_ЕТКОТ_АПС_ОМДОЛ_Ю КУВ_ОВ_Е_ХВСЗОМЖОЫ_ХПНЗЦИИОХЫЮХЯ

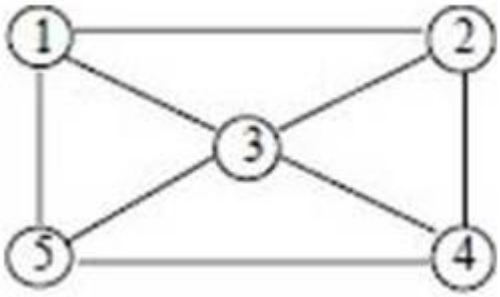

Рисунок 3 – Граф

Матрица смежности для данного графа выглядит следующим образом (таблица 1).

Таблица 1 – Матрица смежности

	1	1		1
1		1	1	
1	1		1	1
	1	1		1
1		1	1	

Программа вычислит по матрице смежности пути Гамильтона для нашего графа:

1 2 3 4 5 цикл
1 2 3 5 4
1 2 4 3 5
1 2 4 5 3 цикл
1 3 2 4 5 цикл
1 3 5 4 2 цикл
1 5 3 2 4
1 5 3 4 2 цикл
1 5 4 2 3 цикл
1 5 4 3 2 цикл

Будем испытывать пути Гамильтона в качестве ключей перестановки.

Применение перестановок 1 2 3 4 5 (цикл). 1 2 3 5 4, 1 2 4 3 5 не

дало результата. Для пути Гамильтона 2 4 3 5 1 программа выдала следующее:

```
Л_ЯПДОЕВРРИН_АКИИЧЯЛВРЕО_ТОНГЯ_ЛСООАК_РВП
ДЛЯ_ПРОВЕРКИ_НАЛИЧИЯ_ВЕРОЯТНОГО_СЛОВА_КРИ

ОТАИАИЛТНКВ_ЫИИАТЕЧ_ГЕОТИ_ЗШ_ФОРВИНОНГА_
ПТОАНАЛИТИК_ВЫЧИТАЕТ_ЕГО_ИЗ_ШИФРОВАННОГО

ЕТКОТ_АПС_ОМДОЛ_ЮКУВ_ОВ_Е_ХВСЗОМЖОЫ_ХПНЗ
_ТЕКСТА_ПО_МОДУЛЮ_К_ВО_ВСЕХ_ВОЗМОЖНЫХ_ПО

ЦИИОХЫЮХЯ
ЗИЦИЯХЮЫХ
```

Криптограмма расшифрована.

Исходный текст:

```
ДЛЯ_ПРОВЕРКИ_НАЛИЧИЯ_ВЕРОЯТНОГО_СЛОВА_КРИ
ПТОАНАЛИТИК_ВЫЧИТАЕТ_ЕГО_ИЗ_ШИФРОВАННОГО_ТЕКСТА_ПО
_МОДУЛЮ_К_ВО_ВСЕХ_ВОЗМОЖНЫХ_ПОЗИЦИЯХЮЫХ
```

Ключ: 2-4-3-5-1.

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. В чем отличие блочных от поточных шифров?
2. От чего зависит криптостойкость выбранного метода?
3. К каким шифрам относятся шифры перестановки?
4. Сколько всевозможных ключей может быть бля блока длинной 8, 10 символов?
5. В чем отличие простых перестановок от путей Гамильтона, где больше ключей шифрования?