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
«___» _____ 2015 г.

КРИПТОАНАЛИЗ ШИФРА ТАБЛИЧНОЙ ПЕРЕСТАНОВКИ

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 шифра табличной перестановки: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2015. 12 с.: табл. 1. Библиогр.: с. 12.

Содержат основные сведения о криптоанализе сообщений, зашифрованных с помощью шифра табличной перестановки, с использованием таблицы частот диграмм русского языка. 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 - дешифровать криптограмму, зашифрованную методом табличной перестановки, получить ключ шифрования.

2. ЗАДАНИЕ

Ознакомиться с руководством пользователя и с теоретическим материалом. Пользуясь таблицей вероятностей следования строк друг за другом, и таблицей диграмм русского языка, переставить строки рабочей таблицы до получения осмысленного текста. Пользоваться при этом вероятностями диаграмм в отдельных столбцах. Расшифровать криптограмму и получить ключ шифрования.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание.
2. Изучить теоретическую часть.
3. Переставить строки рабочей таблицы.
4. Расшифровать криптограмму.
5. Получить ключ шифрования.
6. Получить таблицу вероятностей следования строк друг за другом.
7. Составить отчет.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Описание процесса дешифрования криптограммы.
4. Подробное описание получения ключа шифрования и таблицы вероятностей следования строк.
5. Вывод.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

5.1 Введение

Шифр перестановки — это один из древнейших шифров. Основная идея шифра — переставить буквы в тексте так, чтобы, не зная правил этой перестановки, нельзя было прочитать его. При шифровании перестановкой символы шифруемого текста переставляются по определенному правилу в пределах блока этого текста. Шифры перестановки являются самыми простыми и, вероятно, самыми древними шифрами.

С начала эпохи Возрождения (конец XIV столетия) начала возрождаться и криптография. Наряду с традиционными применениями криптографии в политике, дипломатии и военном деле появляются и другие задачи - защита интеллектуальной собственности от преследований инквизиции или заимствований злоумышленников. В разработанных шифрах перестановки того времени применяются шифрующие таблицы, которые в сущности задают правила перестановки букв в сообщении.

В качестве ключа в шифрующих таблицах используются:

• размер таблицы;

• слово или фраза, задающие перестановку;

• особенности структуры таблицы.

5.2 Криптоанализ перестановок. Метод диграмм

В общем случае, при использовании перестановок с длиной блока N, существует N! вариантов ключа. Поэтому при малой длине ключа N, для вскрытия шифра достаточен простой перебор всех вариантов перестановок. При больших значениях N перебор становится невозможен. Использование маршрутов Гамильтона упрощает дешифрацию перестановок, т.к. из всего множества возможных ключей используются только пути Гамильтона. Однако, при больших значениях N, это преимущество становится незаметным.

Знание частот встречаемости в тексте пар букв - диграмм - позволяет легко вскрывать шифры табличной перестановки. Оказывается, рассматривая маловероятные сочетания букв, можно восстановить истинный порядок строк в таблице. Кроме того, с

помощью вероятностей появления диграмм можно рассчитать вероятность следования одной строки за другой.

Рассмотрим шифр табличной перестановки, для которого текст M = $m_1m_2\ldots m_{n\times m}$ выписывается по столбцам в таблицу размером n×m, а затем строки переставляются в соответствии с ключом и, в результате, получается криптограмма E:

$e_{1,1}$	$e_{1,2}$	…	$e_{1,m}$
…	…	…	…
$e_{i,1}$	$e_{i,2}$	…	$e_{i,m}$
…	…	…	…
$e_{j,1}$	$e_{j,2}$	…	$e_{j,m}$
…	…	…	…
$e_{n,1}$	$e_{n,2}$	…	$e_{n,m}$

Обозначим вероятность того, что в исходном тексте встретится диграмма “ab”, как p (a, b). Тогда вероятность следования в исходном тексте j-ой строки за i-ой строкой можно записать так:

$$p(i,j) = \prod_{k=1}^{m} p(e_{i,k}, e_{j,k}) \qquad (1)$$

Пользуясь формулой 1 можно вычислить вероятности следования друг за другом всех возможных пар строк, вычислить p(i, j) для всех i ≠ j : i,j [1,m]. Если в исходном тексте за i-ой строкой стоит строка j, то вероятность p(i,j) должна быть, в принципе, больше вероятностей p(i,k), где k ≠ j, и p(k,j), где k ≠ i. Руководствуясь этим соображением, для таблиц небольшого размера легко восстановить истинный порядок следования строк. В общем случае для расшифровки криптограммы необходимо решить оптимизационную задачу нахождения наиболее вероятного порядка строк в таблице (задача коммивояжера).

В таблице 1 диграмм русского языка приведены не вероятности диграмм, а их логарифмы. Поэтому, для оценки вероятности следования строк друг за другом, необходимо складывать значения логарифмов вероятностей необходимых диграмм (таблица 1).

Таблица 1 – Таблица диграмм русского языка

i\j	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	–
А	2	7	8	6	7	7	7	4	7	7	7	8	8	3	7	6	7	8	2	6	6	7	7	5	5	0	0	0	0	6	7	9
Б	7	1	1	0	1	6	2	2	6	0	5	6	3	5	7	2	7	5	0	7	0	5	4	1	0	5	5	7	2	2	0	3	5
В	8	0	5	0	4	8	0	3	7	1	6	7	5	6	8	4	6	6	6	6	0	3	0	1	3	0	0	8	2	0	0	4	8
Г	6	0	1	1	6	5	0	0	6	0	4	5	4	4	8	0	7	0	0	6	0	0	1	2	0	0	0	0	0	0	0	0	4
Д	8	1	6	3	4	8	1	0	7	0	4	7	1	7	8	4	6	5	2	7	1	3	3	3	4	0	0	6	4	0	4	5	7
Е	5	5	6	7	8	6	6	6	4	7	7	8	8	9	6	5	8	8	9	3	3	6	5	6	5	6	0	0	1	1	5	5	9
Ж	6	0	0	0	6	7	2	1	7	0	5	0	2	7	1	0	1	2	1	3	0	0	0	0	0	0	0	0	2	0	0	0	2
З	8	4	6	2	6	4	1	1	6	1	5	5	6	6	7	1	5	0	0	6	0	0	2	1	0	0	2	6	2	0	0	4	6
И	6	6	7	6	6	8	5	7	7	7	7	6	8	8	5	5	7	8	8	1	5	7	7	7	6	3	0	1	0	0	6	7	9
Й	0	0	3	0	3	0	0	0	0	0	3	6	5	4	0	0	0	6	6	0	0	0	1	2	3	0	0	0	0	0	0	0	8
К	8	1	5	1	1	6	5	2	7	1	2	7	0	5	8	0	7	6	6	7	0	0	6	0	1	0	0	0	0	0	0	0	7
Л	8	4	1	2	1	8	6	1	8	0	4	4	1	6	7	0	0	3	3	6	3	0	0	3	1	1	0	6	8	0	7	8	6
М	7	5	7	2	2	8	0	1	7	0	4	4	7	6	8	5	1	3	1	6	1	0	0	0	0	0	0	7	3	0	0	6	8
Н	9	0	3	3	6	8	1	1	9	0	6	0	1	7	8	0	0	5	7	6	5	2	5	3	0	0	0	8	5	0	4	6	7
О	2	8	8	8	8	6	7	7	6	8	7	8	8	7	6	7	8	8	8	3	2	5	6	7	6	5	0	0	1	5	2	5	9
П	7	0	0	0	0	8	0	4	7	0	3	6	1	4	8	4	9	4	5	6	2	0	1	0	0	0	0	4	5	3	0	4	4
Р	9	1	6	4	4	8	6	0	8	0	5	2	6	6	8	4	2	6	6	7	3	5	4	2	4	2	0	7	4	0	1	6	7
С	6	4	6	2	5	7	2	0	7	0	7	8	6	6	8	7	5	6	9	6	3	5	1	5	5	0	0	5	6	1	3	8	7
Т	8	2	7	1	4	8	0	0	8	0	6	4	5	6	9	3	8	8	4	6	0	0	0	4	0	2	1	7	8	0	1	5	8
У	3	4	4	6	6	7	6	5	3	3	6	5	5	6	0	6	7	7	7	1	5	5	0	6	3	6	0	0	0	0	7	4	8
Ф	6	0	0	0	0	5	0	0	6	0	0	2	2	0	6	0	4	0	3	5	4	0	0	0	0	0	0	1	0	0	0	0	2
Х	4	3	3	0	0	4	0	0	3	0	1	1	0	5	6	0	5	3	1	3	0	0	2	0	0	0	1	0	0	0	0	0	8
Ц	5	0	6	0	0	6	0	0	7	0	0	0	0	0	3	0	0	0	0	4	0	0	0	0	0	0	0	5	0	0	0	0	5
Ч	7	0	1	0	0	8	0	0	7	0	6	1	0	6	2	0	1	0	7	3	0	0	0	1	3	0	0	1	3	0	0	0	4
Ш	5	0	0	0	0	6	0	0	7	0	3	3	0	3	4	0	3	0	3	4	0	0	0	0	0	0	0	0	4	0	0	0	5
Щ	6	0	0	0	0	7	0	0	6	0	0	0	0	2	0	0	2	0	0	4	0	0	0	0	0	0	0	0	4	0	1	0	1
Ъ	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	2	
Ы	1	4	7	3	5	7	1	5	1	7	5	5	6	2	1	5	5	5	6	0	0	7	0	5	4	1	0	1	0	0	0	1	8
Ь	0	1	0	0	0	3	0	7	1	0	6	0	4	7	1	0	0	6	4	0	0	0	0	1	6	1	0	0	0	6	2	8	
Э	0	0	4	0	0	1	0	0	0	2	6	5	2	1	0	2	0	1	7	0	4	3	0	0	0	0	0	0	0	0	0	0	1
Ю	0	5	0	0	2	0	1	2	0	4	1	0	0	0	0	0	0	3	7	0	0	0	0	6	1	7	0	0	1	0	3	0	7
Я	0	1	5	2	5	6	2	5	0	2	2	3	6	5	0	1	4	4	7	0	0	4	4	3	0	4	0	0	0	6	4	9	
-	7	8	9	7	8	7	5	8	8	3	8	6	8	9	9	9	8	9	8	7	7	6	7	8	5	1	1	2	1	8	2	6	0

6. ВЫПОЛНЕНИЕ РАБОТЫ

6.1 Запуск программы

Запустить на выполнение исполняемый файл crypto64.exe. Выберите свой вариант из предложенного списка (NN).

Перед Вами на экране три таблицы: таблица с криптограммой, рабочая таблица - в ней отражаются изменения, вносимые пользователем в процессе криптоанализа. В результате расшифровки в рабочей таблице должен появиться исходный текст криптограммы. Строки этих двух таблиц перенумерованы: слева - красными цифрами, справа - зелеными. Красные цифры означают номер строки в таблице («позицию» строки), а зеленые - номер самой строки (“идентификатор” строки). Чтобы поменять местами две строки рабочей таблицы, необходимо в окне ввода, расположенном в нижней части экрана, ввести номера их позиций (красные цифры). В третьей таблице содержится оценки вероятностей следования строк друг за другом. Кроме того, по клавише F2 можно просмотреть таблицу диграмм русского языка и вызвать помощь по клавише F1.

6.2 Дешифрация криптограммы

Пользуясь таблицей вероятностей следования строк друг за другом, и таблицей диграмм русского языка, переставьте строки рабочей таблицы таким образом, чтобы в ней получился осмысленный текст. Не забудьте, что текст нужно читать по столбцам.

Если использование таблицы вероятностей p(i,j) не дает результата, можно сделать следующее:

- проверка не только максимальной вероятности следования строк друг за другом, но и семантического смысла получающихся сочетаний;
- пользоваться не вероятностями следования строк друг за другом, а вероятностями диграмм в отдельных столбцах;
- использовать не вероятности p(i,j), а суммы p(i,j)+p(j,k). Т.е. вероятностями следования строк i,j и k друг за другом.

Расшифруйте криптограмму и получите ключ шифрования.

6.3 Пример дешифрации криптограммы, зашифрованной табличной перестановкой

Криптограмма:

0	В	Ь	В	Г	Л	О	Р		0
1	Р	С	А	Н	С	Е	М	Л	1
4	А	А	Л	Е	П	_	У	Л	2
3	З	Л	С	_	_	Е	_	С	3
2	И	У	_	И	Й	О	И	_	4
6	Е	_	К	Е	_	Ф	Ю	А	5
7	Л	Н	О	М	И	В	_	О	6
5	_	С	И	В	И	К	Г	У	7

Программа вычислила оценки вероятностей следования строк друг за другом и поместила их в таблицу:

i\j	0	1	2	3	4	5	6	7
0		43	40	33	41	42	54	46
1	40		57	47	52	49	41	43
2	40	51		49	35	53	62	58
3	53	55	65		52	36	50	54
4	47	56	40	63		56	56	52
5	37	56	44	47	41		52	42
6	45	46	62	43	63	44		48
7	47	50	51	59	60	42	39	

Из таблицы видно, что максимальные вероятности у пар строк 0-6, 0-7, 1-2, 2-6, 2-7, 3-2, 4-3, 5-1, 6-2, 7-4.

Попробуем поставить строку 3 после 4-ой, 2-ую после 3-ей, 7-ую после 2-ой:

0	В	Ь	В	Г	Л	О	Р	Ш	0
1	Р	С	А	Н	С	Е	М	Л	1
2	И	У	_	И	Й	О	И	_	4
3	З	Л	С	_	_	Е	_	С	3
4	А	А	Л	Е	П	_	У	Л	2
5	_	С	И	В	И	К	Г	У	7
6	Е	_	К	Е	_	Ф	Ю	А	5
7	Л	Н	О	М	И	В	_	О	6

Во втором столбце “..УЛАС..”. Похоже, что здесь глагол, оканчивающийся на “..УЛАСЬ ..”. Т.е. строку 0 после 7-ой и 5-ую после 0-ой.

0	Л	Н	О	М	И	В	_	О	6
1	Р	С	А	Н	С	Е	М	Л	1
2	И	У	_	И	Й	О	И	_	4
3	З	Л	С	_	_	Е	_	С	3
4	А	А	Л	Е	П	_	У	Л	2
5	_	С	И	В	И	К	Г	У	7
6	В	Ь	В	Г	Л	О	Р	Ш	0
7	Е	_	К	Е	_	Ф	Ю	А	5

Теперь текст очевиден. Поставим 1-ую строку после 5-ой:

0	Л	Н	О	М	И	В	_	О	6
1	И	У	_	И	Й	О	И	_	4
2	З	Л	С	_	_	Е	_	С	3
3	А	А	Л	Е	П	_	У	Л	2
4	_	С	И	В	И	К	Г	У	7
5	В	Ь	В	Г	Л	О	Р	Ш	0
6	Е	_	К	Е	_	Ф	Ю	А	5
7	Р	С	А	Н	С	Е	М	Л	1

Криптограмма расшифрована.

Исходный текст:

ЛИЗА-ВЕРНУЛАСЬ-СО-СЛИВКАМИ-ЕВГЕНИЙ-ПИЛ-СВОЕ-КОФЕ-И-УГРЮМО-СЛУШАЛ

Ключ: 6-4-3-2-7-0-5-1.

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. К какому виду шифров относится шифр табличной перестановки?
2. С помощью какой формулы можно вычислить вероятности следования друг за другом всех возможных пар строк?
3. Дайте определение термину «диграмма».
4. Что необходимо для оценки вероятности следования строк друг за другом?
5. Какую задачу необходимо решить для расшифровки криптограммы в общем случае?
6. Какую роль выполняет таблица вероятностей?
7. Что необходимо предпринять, если использование таблицы вероятностей не дает результата?

8. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Нильс Фергюсон, Брюс Шнайер. Практическая криптография. Издательство: Вильямс. 2005. – 416 с.

2. Н. Смарт. Криптография. Издательство: М.: Техносфера. 2005. – 528 с.

3. С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. Основы современной криптографии издание 1.3 исправленное. Издательство: Горячая Линия Телеком. 2004. – 152 с.