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
«ЮЗГУ» декабря 2015 г.

КРИПТОАНАЛИЗ ШИФРА МОНОАЛФАВИТНОЙ ПОДСТАНОВКИ

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 моноалфавитной подстановки: методические указания по выполнению лабораторной работы / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2015. 13 с.: ил. 1, табл. 7. Библиогр.: с. 13.

Рассматриваются основные практические и теоретические положения этапов дешифрования криптограмм, зашифрованных методом моноалфавитной подстановки, используя частотный анализ. 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

Используя частотный анализ, дешифровать криптограмму, зашифрованную методом моноалфавитных подстановок.

2. ЗАДАНИЕ

Ознакомиться с руководством пользователя и с теоретическим материалом. Для дешифровки криптограммы, зашифрованной моноалфавитной подстановкой, необходимо произвести замену символов. Учесть, что замена символов производится в соответствии с значениями частот букв русского языка, а также частоты встречаемости символов для данной криптограммы.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

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

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Описание процесса дешифрования криптограммы.
4. Описание получения ключ (в данном случае ключом является таблица замен).
5. Вывод.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

5.1 Введение

Шифр моноалфавитной подстановки - это один из самых древних шифров. Частным случаем этого шифра для закрытия секретных сообщений пользовался еще Гай Юлий Цезарь. Данная лабораторная работа посвящена изучению криптоанализа моноалфавитных подстановок.

Рассмотрим, как используют этот шифр. Прежде всего, выбирается нормативный алфавит, т.е. набор символов, которые будут использоваться при составлении сообщений, требующих зашифровки. Допустим, это будут прописные буквы русского алфавита (исключая буквы “Ё” и “Ъ”) и пробел. Таким образом, наш нормативный алфавит состоит из 32 символов. Затем выбирается алфавит шифрования и устанавливается взаимно однозначное соответствие между символами нормативного алфавита и символами алфавита шифрования. Алфавит шифрования может состоять из произвольных символов, в том числе и из символов нормативного алфавита. Чтобы зашифровать исходное сообщение, необходимо каждый символ открытого текста заменить соответствующим ему символом алфавита шифрования (таблица 1).

Таблица 1 – Соответствие символов исходного и шифрующего алфавитов

Нормативный алфавит	А	Б	В	Г	Д	Е	Ж	З	….
Алфавит шифрования	Н	К	А	Л	З	Т	П	И	….

Зашифруем, например, слово “звезда”. Если использовать алфавиты, приведенные в таблице 1, то получится следующее:

Таблица 2 – Пример шифрования

Исходное сообщение	З	В	Е	З	Д	А
Шифрованный текст	И	А	Т	И	З	Н

Метод моноалфавитной подстановки можно представить как числовые преобразования символов исходного текста. Для этого каждой букве нормативного алфавита ставится в соответствие некоторое число, называемое числовым эквивалентом этой буквы. Например, для букв русского алфавита и пробела это выглядит так, как показано в таблице 3.

Моноалфавитные подстановки можно описать выражением:

$$E_i = (M_i + S_i) \bmod L, \quad (1)$$

где E_i, M_i - числовые эквиваленты символов алфавита шифрования и нормативного алфавита соответственно, S_i - коэффициент сдвига, L - мощность алфавита.

Таблица 3 – Числовые эквиваленты

Нормативный алфавит	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Числовые эквиваленты	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Нормативный алфавит	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	“_“
Числовые эквиваленты	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

5.2. Шифр Цезаря

Простейшим примером моноалфавитных подстановок является шифр Цезаря. В этом шифре каждый символ открытого текста заменяется третьим после него символом в алфавите, замкнутом в кольцо, т.е. после пробела следует буква “А”. Таким образом, шифр Цезаря описывается так:

$$E_i = (M_i + S) \bmod L, \quad (2)$$

где S - коэффициент сдвига, одинаковый для всех символов. Цезарь использовал величину сдвига $S=3$, но, конечно, можно использовать любое целое S: $1 \leq S \leq (L-1)$. Зашифруем, например, текст “ШИФР_ЦЕЗАРЯ”, используя коэффициент сдвига $S=2$ (Таблица 4).

Таблица 4 – Пример шифрования

Открытый текст	Ш	И	Ф	Р	_	Ц	Е	З	А	Р	Я
Шифрованный текст	Ы	К	Ц	Т	Б	Ш	З	Й	В	Т	А

5.3. Частотный анализ

Все естественные языки имеют характерное частотное распределение символов. Например, буква “О” - встречается в русском языке чаще других, а буква “Ф” - самая редкая (см. таблицу 5). Моноалфавитные подстановки обладают важным свойством: они не нарушают частот появления символов, характерных для данного языка. Это позволяет криптоаналитику легко получить открытый текст при помощи частотного анализа. Для этого нужно сопоставить частоты появления символов шифра с вероятностями появления букв используемого алфавита (в данном случае русского). После этого наиболее частые символы криптограммы заменяются наиболее вероятными символами алфавита, остальные замены производятся на основе вероятных слов и знания синтаксических правил используемого языка.

5.4. Вероятности встречаемости букв русского языка

Таблица 5 – Частотные характеристики символов

Символ	Вероят-ность	Символ	Вероят-ность	Символ	Вероят-ность
Пробел	0.175	К	0.028	Ч	0.012
О	0.089	М	0.026	Й	0.010
Е	0.072	Д	0.025	Х	0.009
А	0.062	П	0.023	Ж	0.007
И	0.062	У	0.021	Ю	0.006
Н	0.053	Я	0.018	Ш	0.006
Т	0.053	Ы	0.016	Ц	0.004
С	0.045	З	0.016	Щ	0.003
Р	0.040	Ь	0.014	Э	0.003
В	0.038	Б	0.014	Ф	0.002
Л	0.035	Г	0.013		

6. ВЫПОЛНЕНИЕ РАБОТЫ

6.1. Руководство пользователя

- Запустить на выполнение файл rela12.exe.
- Выбрать в меню пункт “Моноалфавитные подстановки”.
- Нажать на клавишу Enter и выбрать в появившемся списке свой вариант.
- Теперь экран выглядит как это показано на рисунке 1. На данном этапе вы можете:

1. Вывести на экран таблицу частот встречаемости символов криптограммы и вероятностей символов русского языка (по клавише F4);
2. Заменить символ криптограммы на символ нормативного алфавита (прописные буквы русского языка и пробел);
3. Получить помощь (по клавише F1);
4. Выйти в главное меню (по клавише F10 или Esc).

- Пользуясь описанными возможностями, расшифруйте криптограмму. Результат вашей работы покажите преподавателю.

Если Вы ошибочно заменили какой-либо символ криптограммы и хотите это исправить, замените этот символ на служебный символ “-”.

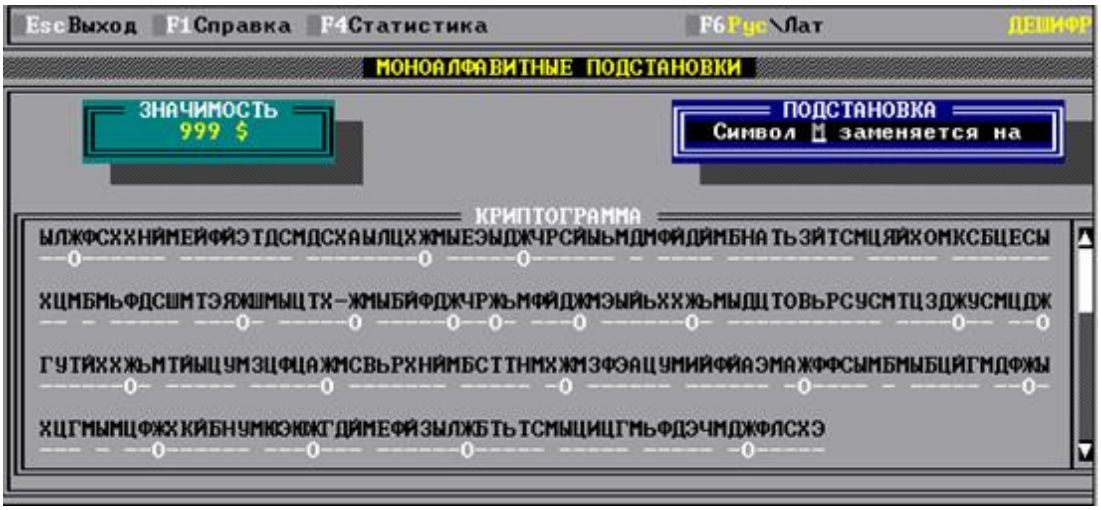

Рисунок 1 – Интерфейс программы

6.2. Пример дешифрации криптограммы, зашифрованной моноалфавитной подстановкой

Текст криптограммы:

```
КЩРНСЙШЩХДТАРБУТЦПФЮСНЫАШЙАЬЙЛБАНСЙСТНСТОБНДЩМЩАЙШЙ
----------------------------------------------------
ЖТЛЙАСБДНСЙАШЩАСЩЖЕДЩАБНЖТАЩШАРЩНСЙСЩОШЩАРЖТШШИГ
----------------------------------------------------
```

В таблице находятся результаты статистического анализа данной криптограммы. Сюда включены значения частот букв русского языка, а также частоты встречаемости символов для данной криптограммы.

Таблица 6 – Статистика криптограммы

Криптограмма		Русский язык	
Символ	Частота	Буква	Вероятность
А	0.121	Пробел	0.175
Щ	0.11	О	0.090
С	0.101	Е	0.072
Й	0.091	А	0.062

Таблица 6 (продолжение)

Н	0.081	И	0.062
Ш	0.081	Н	0.053
Т	0.071	Т	0.053
Б	0.051	С	0.045
Р	0.040	Р	0.040
Д	0.040	В	0.038
Ж	0.040	Л	0.035
И т.д.		И т.д.	

Исходя из полученной статистики, сделаем первые замены: “А”-“ ”, “Щ”“О”.

Реакция программы:

```
КЩРНСЙШЩХДТАРБУТЦПФЮСНЫАШЙАЬЙЛБАНСЙСТНСТОБНДЩМЩАЙШЙ
-О-----О--- ---------- -- ---- ----------О-О ---

ЖТЛЙАСБДНСЙАШЩАСЩЖЕДЩАБНЖТАЩШАРЩНСЙСЩОШЩАРЖТШШИГ
---- ------ -О -О---О ---- О- -О----О--О -------
```

Обратим внимание на 8-ое и 12-ое слова: “ШЩ” и “ЩШ”. Т.к. мы предположили, что “Щ” заменяет “О” в открытом тексте, то буква “Ш” может быть только буквой “Н” или буквой “Т”. Попробуем сделать замену “Ш” - “Н”.

Можно предположить, что 5-ое слово - оканчивается на “ОГО” и является, стало быть, прилагательным или причастием. Замена “М” - “Г”. Слово, следующее за прилагательным или причастием, скорее всего является существительным и оканчивается на “А”. Отсюда следует замена “Й” - “А”.

Теперь имеем следующую картину:

```
КЩРНСЙШЩХДТАРБУТЦПФЮСНЫАШЙАЬЙЛБАНСЙСТНСТОБНДЩМЩАЙШЙ
-О---АНО--- ---------- НА -А-- --А---------ОГО АНА

ЖТЛЙАСБДНСЙАШЩАСЩЖЕДЩАБНЖТАЩШАРЩНСЙСЩОШЩАРЖТШШИГ
---А -----А НО -О---О ---- ОН -О--А-О-НО ---НН--
```

Четвертым словом является предлог “НА”, поэтому следующее слово оканчивается, скорее всего, на букву “Е”. Заменяем “Б” - “Е”.

Шестое слово имеет вид “АНА---А”. Это очень похоже на слово “АНАЛИЗА”. Заменим “Ж” - “Л”, “Т” - “И”, “Л” - “З”.

Реакция программы:

```
КЩРНСЙШЩХДТАРБУТЦПФЮСНЫАШЙАЬЙЛБАНСЙСТНСТОБНДЩМЩАЙШЙ
-О---АНО--И -Е-И------- НА -АЗЕ --А-И--И-Е--ОГО АНА

ЖТЛЙАСБДНСЙАШЩАСЩЖЕДЩАБНЖТАЩШАРЩНСЙСЩОШЩАРЖТШШИГ
ЛИЗА -Е---А НО -ОЛ--О Е-ЛИ ОН -О--А-О-НО -ЛИНН--
```

Словосочетание “НА -АЗЕ” означает, видимо, слова “НА БАЗЕ”, слово “Е-ЛИ” является словом “ЕСЛИ”, а последнее слово криптограммы “ЛИНН--” похоже на слово “ДЛИННЫЙ”. Сделаем соответствующие замены: “Ь” - “Б”, “Н” - “С”, “Р” - “Д”, “И” - “Ы”, “Г” - “Й”.

Реакция программы:

```
КЩРНСЙШЩХДТАРБУТЦПФЮСНЫАШЙАЬЙЛБАНСЙСТНСТОБНДЩМЩАЙШЙ
-ОДС-АНО--И ДЕ-И-----С- НА БАЗЕ С-А-ИС-И-ЕС-ОГО АНА

ЖТЛЙАСБДНСЙАШЩАСЩЖЕДЩАБНЖТАЩШАРЩНСЙСЩОШЩАРЖТШШИГ
ЛИЗА -Е-С-А НО -ОЛ--О ЕСЛИ ОН ДОС-А-О-НО ДЛИННЫЙ
```

Слово “ С-А-ИС-И-ЕС-ОГО” (АНАЛИЗА) похоже на слово «СТАТИСТИЧЕСКОГО”. Замены: “С” - “Т”, “О” - “Ч”, “Д” - “К”.

Реакция программы:

```
КЩРНСЙШЩХДТАРБУТЦПФЮСНЫАШЙАЬЙЛБАНСЙСТНСТОБНДЩМЩАЙШЙ
-ОДСТАНО-КИ ДЕ-И----ТС- НА БАЗЕ СТАТИСТИЧЕСКОГО АНА

ЖТЛЙАСБДНСЙАШЩАСЩЖЕДЩАБНЖТАЩШАРЩНСЙСЩОШЩАРЖТШШИГ
ЛИЗА ТЕКСТА НО ТОЛ-КО ЕСЛИ ОН ДОСТАТОЧНО ДЛИННЫЙ
```

Последующие замены не вызывают затруднений.

Исходный текст:

ПОДСТАНОВКИ ДЕШИФРУЮТСЯ НА БАЗЕ СТАТИСТИЧЕСКОГО АНАЛИЗА ТЕКСТА НО ТОЛЬКО ЕСЛИ ОН ДОСТАТОЧНО ДЛИННЫЙ

В таблице 7 приведены замены (ключ) между символами нормативного алфавита и символами алфавита шифрования. Прочерки в таблице соответствуют буквам, ни разу не встретившимся в исходном тексте криптограммы.

Таблица 7 – Замены символов алфавита

Нормальный Алфавит	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Алфавит шифрования	Й	Ь	Х	М	Р	Б	-	Л	Т	Г	Д	Ж	-	Ш	Щ	К
Нормальный Алфавит	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	_
Алфавит шифрования	П	Н	С	Ф	Ц	-	-	О	У	-	И	Е	-	Ю	Ы	А

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что понимается под моноалфавитными подстановками?
2. Приведите примеры моноалфавитных подстановок.
3. Что такое коэффициент сдвига?
4. Что такое мощность алфавита?
5. Что такое частотные характеристики символов?
6. Какова криптостойкость шифра моноалфавитной подстановки?

8. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Ж. Брассар. Современная криптология. Издательство: Полимед. 1999. - 176 с. 11. Секреты и ложь. Безопасность данных в цифровом мире / Б.Шнайер. – СПб.: Питер, 2003. – 368 с. : ил.

2. Начала криптологии. Методические указания к выполнению лабораторного практикума по курсу “ИНФОРМАЦИОННЫЙ ОБМЕН В СЕТЯХ”. МГИФИ. Москва. 1999 г.

3. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: От примитивов к синтезу алгоритмов. Издательство: "БХВ-Петербург" . 2004. – 446 с.

4. Нильс Фергюсон, Брюс Шнайер. Практическая криптография. Издательство: Вильямс. 2005.- 416 с.

6. Баричев С. Криптография без секретов. Издательство: Горячая Линия – Телеком. 2004.- 43 с.

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

9. Ященко В.В., Варновский Н.П., Нестеренко Ю.В. и др. Введение в криптографию. Издательство: ЧеРо. 1999. – 272 с.