

Министерство общего и профессионального образования РФ

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
"САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ
УНИВЕРСИТЕТ имени академика С.П.КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)"

ПРОСТЕЙШИЕ МЕТОДЫ ШИФРОВАНИЯ ТЕКСТОВЫХ СООБЩЕНИЙ

Методические указания к
ЛАБОРАТОРНОЙ РАБОТЕ N 2

САМАРА 2021

Составители: К.Т.Н., доц. В.Н. Копенков

УДК 681.3

Простейшие методы шифрования текстовых сообщений:
Лабораторная работа N 2 / Самарский университет;
Самара, 2021. 22с.

В лабораторной работе изучается метод кодирования текста шифром простой подстановки и декодирования при помощи частотного анализа текстовой последовательности.

Лабораторная работа предназначена для студентов по курсу “Основы информационной безопасности” и для специалистов, проходящих курсы повышения квалификации.

Печатается по решению кафедры “Геоинформатика и информационная безопасность” Самарского государственного аэрокосмического университета имени академика С.П.Королева

Содержание:

1. Теоретические основы лабораторной работы.	4
1.1. Простейшие коды подстановки.	4
1.2. Простейшие коды перестановки.	5
1.3. Раскрытие кода подстановки.	7
1.4. Усложнение кода подстановки.	7
2. Применение частотного анализа для дешифрования.	10
3. Выполнение лабораторной работы.	12
3.1. Общий план выполнения работы.	12
3.2. Этапы выполнения.	12
3.3. Содержание отчета.	12
4. Контрольные вопросы.	13
5. Данные для выполнения лабораторной работы.	14
5.1. Общие данные:	14
5.2. Задание:	15
5.3. Варианты заданий:	16
6. Список используемой литературы	21

Цель работы – изучение простейших методов шифрования текстовых сообщений при помощи подстановки и перестановки, а также метода декодирования шифра простой замены на основе частотного анализа; получение навыков работы с шифрами.

1. Теоретические основы лабораторной работы.

Потребность шифровать и передавать зашифрованные сообщения возникла очень давно. Так, еще в V-IV вв. до н. э. *греки* применяли специальное шифрующее устройство. По описанию *Плутарха*, оно состояло из двух палок одинаковой длины и толщины. Одну оставляли себе, а другую отдавали отъезжающему. Эти палки называли *скиталами*. Когда правителям нужно было сообщить какую-нибудь важную тайну, они вырезали длинную и узкую, вроде ремня, полосу папируса, наматывали ее на свою скиталу, не оставляя на ней никакого промежутка, так чтобы вся поверхность палки была охвачена этой полосой. Затем, оставляя папирус на скитале в том виде, как он есть, писали на нем все, что нужно, а написав, снимали полосу и без палки отправляли адресату. Так как буквы на ней разбросаны в беспорядке, то прочитать написанное он мог, только взяв свою скиталу и намотав на нее без пропусков эту полосу.

Аристотелю принадлежит способ дешифрования этого шифра. Надо изготовить длинный конус и, начиная с основания, обертывать его лентой с зашифрованным сообщением, постепенно сдвигая ее к вершине. В какой-то момент начнут просматриваться куски сообщения. Так можно определить диаметр скиталы.

1.1. Простейшие коды подстановки.

A	B	C	D	E
F	G	H	I	J
K	L	M	N	O
P	Q	R	S	T
U	V	W	X	Y
Z				

В Древней Греции (II в. до н. э.) был известен шифр, называемый "*квадрат Полибия*". Это устройство представляло собой квадрат 5x5, столбцы и строки которого нумеровали цифрами от 1 до 5. В каждую клетку этого квадрата записывалась одна буква. В греческом варианте одна клетка оставалась пустой, в ла-

тинском – в одну клетку помещали две буквы i и j. В результате каждой букве отвечала пара чисел, и шифрованное сообщение превращалось в последовательность пар чисел.

В I в. н.э. Ю. Цезарь во время войны с галлами, переписываясь со своими друзьями в Риме, заменял в сообщении первую букву латинского алфавита (A) на четвертую (D), вторую (B) - на пятую (E), наконец, последнюю - на третью:

↑ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
↓ D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Сообщение об одержанной им победе выглядело так:

YHQL YLGL YLFL

Император Август (I в. н. э.) в своей переписке заменял первую букву на вторую, вторую - на третью и т. д., наконец, последнюю - на первую:

↑ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
↓ B C D E F G H I J K L M N O P Q R S T U V W X Y Z A

Его любимое изречение было:

"GFTUJOB MFOUF"

Квадрат Полибия, шифр Цезаря входят в класс шифров, называемых "подстановка" или "простая замена". Это такой шифр, в котором каждой букве алфавита соответствует буква, цифра, символ или какая-нибудь их комбинация.

1.2. Простейшие коды перестановки.

В другом классе шифров "перестановка" – буквы сообщения каким-нибудь способом переставляются между собой (шифр скитала). Классическим примером шифра "перестановка" является "маршрутная транспозиция" и его вариант "постолбцовая транспозиция". В каждом из них в данный прямоугольник [N×M] сообщение вписывается заранее обусловленным способом, а столбцы нумеруются или обычным порядком следования, или в порядке следования букв ключа. Так, ниже в 1-ом прямоугольнике столбцы нумеруются в обычном порядке следования, а во 2-ом - в порядке следования букв слова "Петербург".

Используя расположение букв этого ключа в алфавите, получим набор чисел [538461972]:

1	2	3	4	5	6	7	8	9
п	р	и	л	е	п	л	я	я
р	д	у	м	е	р	п	я	с
у	м	п	р	е	м	у	д	р
в	б	а	ь	ш	е	д	у	б

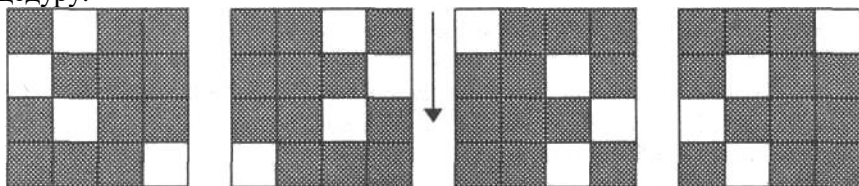
5	3	8	4	6	1	9	7	2
п	р	и	л	е	п	л	я	я
с	я	п	р	е	м	у	д	р
у	м	п	р	е	м	у	д	р
б	у	д	е	ш	ь	а	б	в

В первом случае шифрованный текст найдем, если будем выписывать буквы очередного столбца в порядке следования столбцов, во втором, - если будем выписывать буквы столбца в порядке следования букв ключа. Таким образом, будем иметь:

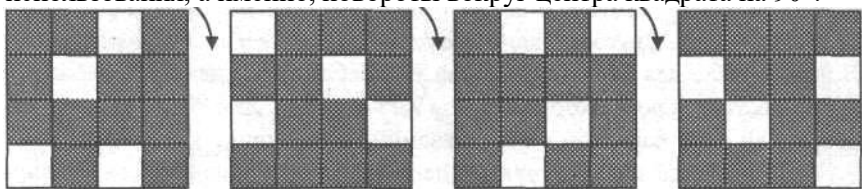
- 1) **прувр дмбиу палмр ьеееш прмел пудья дуясрб;**
- 2) **пмья ррвря мулрр епсуб еееша ддбип пдлууа;**

(Из послания Даниила Заточенаго к великому князю Ярославу Всеволодтию)

К классу "перестановка" принадлежит и шифр, называемый "решетка Кардано". Это прямоугольная карточка с отверстиями, которая при наложении на лист бумаги оставляет открытыми лишь некоторые его части. Число строк и столбцов в карточке четно. Карточка сделана так, что при ее последовательном использовании (поворачивании) каждая клетка лежащего под ней листа окажется занятой. Карточку сначала поворачивают вдоль вертикальной оси симметрии на 180° , а затем вдоль горизонтальной оси также на 180° . И вновь повторяют ту же процедуру:



Если решетка Кардано - квадрат, то возможен другой вариант использования, а именно, повороты вокруг центра квадрата на 90° :



1.3. Раскрытие кода подстановки.

Термин "шифр" арабского происхождения. В начале XV в. арабы опубликовали энциклопедию *"Шауба Аль-Аица"*, в которой есть специальный раздел о шифрах. В этой энциклопедии указан способ раскрытия шифра простой замены. Он основан на различной частоте повторяемости букв в тексте. В этом разделе есть перечень букв в порядке их повторяемости на основе изучения текста Корана. Заметим, что в русском тексте чаще всего встречается буква "О", затем буква "Е" и на третьем месте стоят буквы "И" и "А".

Неудобство шифров типа *"подстановка"* в случае использования стандартного алфавита очевидно. Таблица частот встречаемости букв алфавита позволяет определить один или несколько символов, а этого иногда достаточно для дешифрования всего сообщения (*"Пляшущие человечки"* Конан Дойля или *"Золотой жук"* Эдгара По).

1.4. Усложнение кода подстановки.

Для усложнения раскрываемости шифра простой подстановки цели используют *многобуквенную систему шифрования* - систему, в которой одному символу отвечает одна или несколько комбинаций двух и более символов. Другой прием - *использование нескольких алфавитов*. В этом случае для каждого символа употребляют тот или иной алфавит в зависимости от ключа, который связан каким-нибудь способом с самим символом или с его порядком в передаваемом сообщении.

В процессе шифрования (и дешифрования) используется таблица (*"таблица Виженера"*), которая устроена следующим образом: в первой строке выписывается весь алфавит, в каждой следующей осуществляется циклический сдвиг на одну букву. Так получается квадратная таблица, число строк которой равно числу столбцов и равно числу букв в алфавите. Ниже представлена таблица, составленная из 31 буквы русского алфавита (без букв Ё и Ъ). Чтобы зашифровать какое-нибудь сообщение, поступают следующим образом. Выбирается слово - лозунг (например, "монастырь") и подписывается с повторением над буквами сообщения.

Чтобы получить зашифрованный текст, находят очередной знак лозунга, начиная с первого в вертикальном алфавите, а ему соответствующий знак сообщения в горизонтальном. В данном примере сначала находим столбец, отвечающий букве "м" лозунга, а затем строку, соответствующую букве "р" открытого текста. На пересечении выделенных столбца и строки находим букву "э". Так продолжая дальше, находим зашифрованный текст полностью:

М	О	Н	А	С	Т	Ы	Р	Ь	М	О	Н	А	С	Т	Ы	Р	Ь	М	О	Н
Р	А	С	К	И	Н	У	Л	О	С	Ь	М	О	Р	Е	Ш	И	Р	О	К	О
Э	О	Я	К	Щ	А	П	Ы	Ю	Й	Щ	О	В	Ч	Ф	Ш	Л	Ь	Ш	Ы	

Таблица Виженера

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

Аббат Тритемиус - автор первой печатной книги о тайнописи (1518 г.) - предложил несколько шифров и среди них шифр, который можно считать усовершенствованием шифра Цезаря. Этот шифр устроен так. Все буквы алфавита нумеруют по порядку (от 1 до 33 в русском варианте). Затем выбирают какое-нибудь слово, называемое "*ключом*", например "*Вологда*", и подписывают под сообщением с повторением, как показано ниже:

о п е р а ц и я н а ч и н а е т с я в в о с к р е с е н ь е
в о л о г д а в о л о г д а в о л о г д а в о л о г д а в о

Чтобы получить зашифрованный текст, складывают номер очередной буквы с номером соответствующей буквы ключа. Если полученная сумма больше 33, то из нее вычитают 33. В результате получают последовательность чисел от 1 до 33. Вновь заменяя числа этой последовательности соответствующими буквами, получают зашифрованный текст. Разбивая этот текст на группы одной длины (например, по 5), получают зашифрованное сообщение.

Если под ключом шифра понимать однобуквенное слово "В" (в русском варианте), то мы получим шифр Цезаря.

Появившийся в XVIII в. шифр "*по книге*" можно рассматривать как дальнейшее усовершенствование шифра Ю. Цезаря. Чтобы воспользоваться этим шифром, два корреспондента договариваются об определенной книге, имеющейся у каждого из них. В качестве *ключа* каждый из них может выбрать "слово" той же длины, что и передаваемое сообщение. Этот ключ кодируется парой чисел, а именно номером страницы и номером строки на ней, и передается вместе с зашифрованным сообщением.

2. Применение частотного анализа для дешифрования.

Пусть есть сообщение:

Д ЖТЦ БЦТ ЧКЙ ХТЖЙФЫССТ ХЙОФЙЦСТЙ ХТТЕЭЙСМЙ
СДР УФМЬПТХа ХИЙПДЦа ЙЗТ ИТХЦДЦТЫСТ ИПМС-
СЯРЮЩТЕЯ РТКСТ ЕЯПТ УФТИЙРТСХЦФМФТЖДЦа ФДЕТЦЧ
РЙЦТИДЫДХЦТЦСТЗТ ДСДПМЛД

Индекс частоты появления букв в стандартном тексте:	Индекс частоты появления букв в закодированном тексте:
О == 0.0886741	Т == 0.152866
И == 0.0653615	Ц == 0.082805
Е == 0.0650947	С == 0.076433
Т == 0.0601900	Й == 0.076433
А == 0.0570297	Д == 0.070063
С == 0.0461327	Х == 0.050956
Н == 0.0453323	Ф == 0.044589
В == 0.0381292	М == 0.031815
Р == 0.0321779	Р == 0.031815
Л == 0.0320343	П == 0.031815
М == 0.0311929	И == 0.031815
К == 0.0240719	Е == 0.025477
Д == 0.0231484	Ж == 0.019108
...	...

Попробуем заменить самую частую букву в шифротексте «Т» на «О» – самую частую букву в русском языке по собранным ранее сведениям.

Дешифрируем и получим сообщение:

Д ЖОЦ БЦО ЧКЙ ХОЖЙФЫССО ХЙОФЙЦСТЙ ХООЕЭЙСМЙ
СДР УФМЬПОХа ХИЙПДЦа ЙЗО ИОХЦДЦОЫСО ИПМС-
СЯРЮЩОЕЯ РОКСО ЕЯПО УФОИЙРОСХЦФМФОЖДЦа
ФДЕОЦЧ РЙЦОИДЫДХЦОЦСОЗО ДСДПМЛД

Теперь можно попробовать сменить «Д» на «И», но, посмотрев в таблицу, мы увидим, что вероятность «Д» в шифротексте несколько меньше и «Д» стоит на пятом месте, вместо положенного второго, а вот «А» стоит как раз на пятом месте.

Попробуем заменить:

А ЖОЦ БЦО ЧКЙ ХОЖЙФЬЙССО ХЙОФЙЦСТЙ ХООЕЭЙСМЙ
САР УФМЬПОХа ХИЙПАЦа ЙЗО ИОХЦАЦОЫСО ИПМС-
СЯРОЫЩОЕЯ РОКСО ЕЯПО УФОИЙРОСХЦФМФОЖАЦа
ФАЕОЦЧ РЙЦОИАБЯХЦОЦСОЗО АСАПМЛА

Теперь необходимо попробовать все известные союзы и предлоги, *пробуя делать* соответствующие замены. В результате фрагмент «ЖОЦ», замененный на «ВОТ», оказался верным решением. Аналогично «БЦО» получился замененным на «ЭТО» и так далее, пока не получилось вот это:

А ВОТ ЭТО УЖЕ ХОВЕФЬЕННО ХЕОФЕТНОЕ ХООЕЭЕНМЕ НАМ
УФМЬПОХа ХИЕПАТа ЕЗО ИОХТАТОЫНО ИПМННЯМОЫТОЕЯ
МОЖНО ЕЯПО УФОИЕМОИХТФМФОВАТа ФАЕОТУ МЕ-
ТОИАБЯХТОТНОЗО АНАПМЛА

Слова «ХОВЕФЬЕННО ХЕОФЕТНОЕ» есть не что иное как «СОВЕРШЕННО СЕКРЕТНОЕ». Осуществив замены новых, найденных букв, получим почти все сообщение:

А ВОТ ЭТО УЖЕ СОВЕРШЕННО СЕКРЕТНОЕ СООБЩЕНИЕ НАМ
ПРИШЛОСЬ СДЕЛАТЬ ЕГО ДОСТАТАЧНО ДЛИННЫМ ЧТОБЫ
МОЖНО БЫЛО ПРОДЕМОНСТРИРОВАТЬ РАБОТУ МЕТОДА ЧА-
СТОТНОГО АНАЛИЗА

Надо заметить, что, если бы у нас были большие словари, в которых бы находились все словоформы большинства русских букв на определенные тематики, мы могли бы подбирать слова для «отгадки» автоматически, проверяя всевозможные слова и выбирая наиболее «близкие» к словам с дешифрованными фрагментами.

3. Выполнение лабораторной работы.

3.1. Общий план выполнения работы.

1. Изучить метод частотного анализа.
2. Получить от преподавателя номер варианта задания.
3. Написать программу шифрования первой части задания.
4. Написать программу дешифровки второй части задания.
5. Составить отчет о выполненной работе.
6. Сдать отчет преподавателю, ответить на контрольные вопросы, получить зачет по работе.

3.2. Этапы выполнения.

1. Кодирование текста.

Придумать ключ подстановки и зашифровать им исходное сообщение. Сохранить в виде файлов исходное, закодированное сообщение и ключ шифрования.

2. Декодирование текста.

Используя метод частотного анализа расшифровать закодированное сообщение, воспользовавшись примером из части 2. Сохранить в виде файлов исходное, декодированное сообщение и найденный ключ шифрования.

3.3. Содержание отчета.

1. Результат выполнения первой части задания:
 - а) Исходный текст;
 - б) Зашифрованный текст;
 - в) последовательность ключа кодирования текста.
2. Результат выполнения второй части задания:
 - а) Исходный текст;
 - б) Дешифрованный текст;
 - в) найденный ключ кодирования текста.

В результате проделанной работы необходимо получить:

- 4 текстовых последовательности: 2 текста на русском языке, 2 текста закодированных шифром простой подстановки;
- 2 ключа простой подстановки (моноалфавитная замена);
- 2 программных модуля – кодирование и декодирование текста.

4. Контрольные вопросы.

1. Шифр простой подстановки – принцип работы.
2. Шифр простой подстановки – достоинства недостатки.
3. Шифр перестановки – принцип работы.
4. Усложнение шифра простой подстановки – примеры.
5. Метод частотного анализа – описание метода.

5. Данные для выполнения лабораторной работы.

5.1. Общие данные:

Алфавит: русский, все буквы большие, 33 символа (без Ё с пробелом):
АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ (пробел)

Индекс частот появления букв русского алфавита:

(пробел) = 0.128675

О = 0.096456

И = 0.075312

Е = 0.072292

А = 0.064841

Н = 0.061820

Т = 0.061619

С = 0.051953

Р = 0.040677

В = 0.039267

М = 0.029803

Л = 0.029400

Д = 0.026983

Я = 0.026379

К = 0.025977

П = 0.024768

З = 0.015908

Ы = 0.015707

Ь = 0.015103

У = 0.013290

Ч = 0.011679

Ж = 0.010673

Г = 0.009867

Х = 0.008659

Ф = 0.007249

Й = 0.006847

Ю = 0.006847

Б = 0.006645

Ц = 0.005034

Ш = 0.004229

Щ = 0.003625

Э = 0.002416

Ъ = 0.000000

5.2. Задание:

Задание 1:

Закодировать любой текст (не менее 500 символов), любым произвольным шифром простой подстановки (моноалфавитная замена) или перестановки.

Результат представить в виде 3-х файлов:

- 1) исходный текст;
- 2) зашифрованный текст;
- 3) ключ шифрования.

Задание 2:

Расшифровать текст, представленный во второй части задания (Дешифровка), закодированный шифром простой подстановки (моноалфавитная замена).

Алфавит открытого (исходного) текста – русский, все буквы большие 33 символа без буквы Ё, но с символом пробел.

Результат представить в виде 2-х файлов:

- 1) дешифрованный текст;
- 2) найденный ключ шифрования.

Написать отчет по результатам лабораторной работы.

5.3. Варианты заданий:

Вариант №1

1) Зашифровать текст

2) Дешифровка: cod1.txt

r2Я Ь9К>>К2ЙЬБt ЪрДЫt12<Д>>tr82tМ<КЫIХО>12>t<rБЧ82ЯК КБrtАД-
ХО>12ЯБ2ЙЬБЪrБ<02Я Ь>О
ДЫ>Or02ЬЕК>ЯKatrД12r2Е0Б0сК<2Ф..КЙOtrЫЬК2ЯБ2r К<КЫt2БКЙЬБt
ЪрДЫtК2>ЛДОЬАЬ2ОКЙ>ОД2ЫЬ2r<К>ОК2>2tМ<КЫКЫtК<2
Д>ЯЬЧЬЛКЫt12ЬО КМЙЬr2>ЬЬOrКО>Or0Хct32>t<rБЧД<2r2ЙЬБЪrБ<2Я
Ь>О ДЫ>OrК2tМ<КЫIКО>12ОДЙЛК2t2Я
КБ>ОДrЧКЫt12>ЛДО832>t<rБЧЪr2Об2К>О,2r2ЫДЬt32ОК <tЫД32bt.
БЕЬМЫДаКЫt1?2ЫДЯ t<К 2ЯК
КБrtЫ0r2>t<rБЧr2tМ2ЙЬЫ9Д2ЙЬБЪrБАЬ2Я Ь>О
ДЫ>OrД2r2ЫДаДЧЬ2ЙЬБt
0ХсКК2МЫДаКЫtК2<ЬЛКО2r8АЧ1БКО,2ЫК2ЙДЙ2МДЯЧДЫt
ЪрДЫЫЬК2tМЫДаДЧ,ЫЬ2Д2ЯЬБ
0АЬ<02>ЬЬOrКО>OrКЫЫЬ2<КЫIХО>12t2EtО82ЙЬБt 0ХctК2ЫДЬК2
КМ0Ч,От 0ХсКК2МЫДаКЫtК2rБЬЕДrЫЙ2ДБДЯOtrЫЬ<2ДЧАЬ
tО<К2r>К2<КЫIКО>12БtЫД<taК>Йt2ЯЬ>ЧК2tМ<КЫКЫt12ЙДЛБЬАЬ2>t<r
БЧД

Вариант №2

1) Зашифровать текст

2) Дешифровка: cod2.txt

>P>ОХ2Х>ДЕ2rА2Х>РОЕ7О1Аа>Х29аФ7Е2РО17аХ> РФ аAr
>2Ма1УО>PaЕ2 А12rА7>Д2 РФа17 >УОб9232>r7ХР2ФО>АО0Ф7МО>PaЕ2
А12rАа8>Д2 РФа17 >УОб9232>r7ХР2ФО>2r12РО11О
>1О>Д29rtaАа>tOrА2А>7Л>PrАЕatОaХ2rА7>1Ос<РОaAr
>Х29аФЫЯ>ДаЕР232>ДЕ70Ф7ba17 >7Ф7>аЙа>ДаЕР232>Д2Е
9УО>АО0Ф7МО>Бt7А<РОЯЙО
>02Фаа>rФ2b1<a>сОР7r7Х2rА7>1ОДЕ7ХаЕ>Д2
РФа17а>291232>r7ХР2ФО>Д2rФа>УОУ232А2>9ЕБ3232>7ХаЯА>r22АPaAr
АPa112>РА2Е28>7>02Фаа>Д2Е 92У>r>Д2Х2ЙЫЯ>ЬА7Л>PaЕ2
А12rАа8>Х2baА>0<АЫ>P<t7rФа1О>Ы1АЕ2Д7
>7>Д2rАЕ2a1>92rАОА2t12>ЬККаУА7Р1<8>У29>Д2сР2Ф
ЯЙ78>rBOАЫ>АaУrА>1О7ФБtИО >rEa91
>9Ф71О>У29О>7>r22АPaArАPa112>rАaДa1Ы>rBOА7 >92rА73ОaAr >Х29аФ
Х7>P>У2А2Е<Л>2Ма1У7>PaЕ2 А12rА7>УОУ>Х2b12>02Фаа>А2t1<

Вариант №3

1) Зашифровать текст

2) Дешифровка: cod3.txt

7OY8cr8ЛБ8ЧХОДХЛМтсбЛrAc<MAcPcMAEс<ХЛД8сХсБAc5MA1с
БКX<Xr8сКД8cr8сБК87ЛМОРДб8МЛбсАБМХЕОД4r
ЕсОД>АКХМЕАЕсЛУОМХб?сБАЛ2АД42tcArcr8сХЛБАД4Фt8McrX2
O2A1сХrИАКЕОЧХХсAcЛУХЕО8ЕАЕсМ82ЛМ8?с<МАП
сBArbM4с2O2сБАХЛЙА7ХМсЛУОМХ8сХЛБАД4Фтаb88сФrOrXbc
AcM82ЛМ8сP8Kr8ЕЛбс2сBArbMXbEc5rMKAбХХсХсХrИАКЕОМХР
rАЛМХсМ82ЛМОсcЛPbФ4сЕ8У7tcP8KAбMrАЛМbEXсХс2A7OEXсX
Фt<O8МЛбсPсОД>8ПКОХ<8Л2A1сМ8AKXXс2A7ХКАPOrXbcАЛrA
PrA1сМ8AKX81с2АМАКА1cbPДб8МЛбсrX2MAcXrA1с2O2с2ДА7с5
ДPт7сЫ8rrArc8>AcM8AK8E
с2A7ХКАPOrXbcХЛМА<rX2OcХЛБАД4ФтаМЛбсA<8r4сO2MXPrAc
ХсФ78Л4

Вариант №4

1) Зашифровать текст

2) Дешифровка: cod4.txt

X4MEOb1сХЛЫIX>7McOXAMETbOEratKrME1rX>МД4PY><X
ЙМ4Уb1Д>rФ1aMEП4r>ЛМ5OPM21rОДАМЕМ4с42r>aX
Ф>М>MEr4r><OE8>Ф>МФ1сОУЛФ>М2ДOcEr4aУOX>ЛMc4XX
ЙМ>ЙМаЕОМФ1ПХ1МД4P5>rAMX4MXO2ОДОЕО84Кь>ОЕЛМ8У4
ЕЕ М>У>МЕОФО7Era4М21ME21E15tM81с>Д1a4X>ЛMc4XX
ЙМ84Пс1ОМЕОФО7Era1М2Д>Pa4X1MEП4rAMrO8ErM12ДOcOУOX
X17MErДt8rtД
MEM12ДOcOУOXX17MErO2OXAKMBИИO8r>aX1Er>М>M5
ErД1сO7Era>ЛMaMP4a>Е>Ф1Er>M1rMr1b1M<r1Ma4ПХООMaM2Д>
У1ПОХ>>ME81Д1ErAM>У>M81БИИ>Ч>OXrMEП4r>Л

Вариант №5

1) Зашифровать текст

2) Дешифровка: cod5.txt

И7У24>2 >МР4ДД >М2ЕПЧЙМД48
О4ЙАИЛМrEt48ДЕ2ЧММИЙtЕХ4МШ4Ф1МЙ>ХИЙМУ1УМРОЕУ<Д >МР4ДД
>МУ1УМЕЪУШtЕО4ДД ФМИ-
УПД41МИИЙЕ<ХУМ8t>ДУЛМЙ>EtУУМrt>PrЕ14П4>ЙИЛМ<ЙЕМР4ДД
>MrtЕУ8ОЕРЛЙИЛМУИЙЕ<ДУХЕ2МУМrt>РЕИЙ4О1ЛКЙИЛМХЕ2rt>ИИЕтЧМОМ
ОУР>МИУ2ОЕ14МД4РМД>ХЕЙEt
2М41Ш4ОУЙЕ2Мt4ДАЫ>МО>ИАМrtЕЪ>ИИМИ74ЙУЛМД48
О41УМХЕРУtЕО4ДУ>2МУИЙЕ<ДУХ4МrЕИХЕ1АХЧМЕДЕМrtУ8О4ДЕМЧР41УЙ
АМУ85 ЙЕ<ДЕИЙАМОМР4ДД
ЩМД4МЕИДЕО>МУЩМrt>РИХ48Ч>2ЕИЙУМrЧЙ>2МУДЕПЕМrt>РИЙ4О1>ДУЛ
МР4ДД
ЩММЙЕМ>ИЙАМУЩМХЕРУtЕО4ДУЛМ84МРО4MrЕИ1>РДУЩМР>ИЛЙУ1>ЙУ
ЛМХ4tЙУД4МД>ИХЕ1АХЕМУ82>ДУ14ИАМr>tОЕФМ14ИЙЕ<ХЕФМИЙ414МУР>
ЛМt48Р>1УЙАМrtЕЪ>ИИМИ74ЙУЛМД4МРО4МО84У2ЕИОЛ84ДД
ЩMrtЕЪ>ИИ4МХЕРУtЕО4ДУ>МД>rЕИt>РИЙО>ДДЕМОЕИrtЕУ8ОЕРЛЪ>>МИ74Й
ФMrЕЙЕХ-
МИУ2ОЕ1ЕОМУМ2ЕР>1УtЕО4ДУ>Mrt>РЕИЙ4О1ЛКЪ>>МОИКМД>Е5ЩЕРУ2ЧК
МР1ЛМХЕРУtЕО4ДУЛМУДШEt24ЪУК

Вариант №6

1) Зашифровать текст

2) Дешифровка: cod6.txt

tАЪЧХАЫ151Ъ1ХЯ Ч<tЫФБ7Х1ЪЕЪ ЧБ<ХЩ ЧЯБЪЕ 1ЛЧ5tАЩЪЕЪХЯ tЪ2
1ЙЪД1ЫЧФХr1ЫЫ>МХБЪХЫЩ1ИtБАФХ5БЪХ1ЪЕЪ
ЧБ<ХАИ1БЧФХЫtХ<ЪИtБХ8ЛЛtЩБЧДЫБХ 12БЪ1Б7ХЫ1ХОЧЛ
БЪtЩАБ1МХМЪ БОЧМХЩ ЧЯБЪ1ЪЕЪ ЧБ<ЪДХАИ1Б7ХОЧЛ
БЪtЩАБХДtА7<1ХБФИтЪБХЯЪХБЫШХЯ ЪАБЫШХЯ Ч5ЧЫtХ5БЪХЩ ЧЯ-
БЪЕ
1ЛЧ5tАЩ1ФХАЧАБt<1ХrЪЫИЫ1ХЪУ2><ЧХrЪАБКЯЫ><ЧХАЯЪАБ21<ЧХ
ЧЙ21ДЪФБ7ХОЧЛ ЪБtЩАБХЪБХЪ5tДЧrЫ>МХДЫКБ
tЫЫЧМХЙ1ДЧАЧ<ЪАБtШХ1ХЯБЪБ<КХtЕЪХ8ЫБ
БЯЧФХ2КrtБХДtА7<1ХД>АБЩЫШХЧХКИХБЪ5ЫБХЫ1<ЫЪЕЪХД>ОтХ5t<
ХКХЪБЩ >БЪЕЪХБtЩАБ1ХЯ trАБ1ДЧБ7ХАt2tХ1ЪЕЪ
ЧБ<ХАИ1БЧФХЩЪБЪ >ШХ2>ХМЪ
БОбХАИЧ<1ЪХЙ1ОК<ЪtЫЫ>tХr1ЫЫ>tХrЪДЪЪ7ЫБХБФИтЪБХДtr7Хr1Ит
ХЧЫБКЧБЧДЫБХЯЪЫФБЫБХ5БЪХАИ1БЧtХДAt4tЪБХ21ЙЧ
КtБАФХЫ1ХЧЙ2>БЪ5ЫЪАБЧХЧЫЛЪ <14ЧЧХДХБtЩАБtХОЧЛ

БД1ЫЧтХ8БКХЧЙ2>БЬ5ЫЬАБ7ХКАБ 1ЫФтБХ1ХД<тАБтХАХЫтШХКАБ
1ЫФтБХЧХДЬЙ<БИЫЬАБ7ХАИ1Б7ХБЩАБ

Вариант №7

1) Зашифровать текст

2) Дешифровка: cod7.txt

КwЧ5Д>ЫХЧ1ЬЕт Й2>ХИЬЧЙ ФХ 1 ХБЧБХЫПЫХЪ-
ЕЩЕтФЙХБЕ2тЫИИ ХrЕЯЩЕ1ФУЙХДЫХЙЕ17БЕХ8ЛЫБЙ
ЩДЕХМтЧД Й7ХБЕДЛ wЫД4 Ч17Д>ЫХwЧДД>ЫХДЕХ ХДЧrt
2ЫтХЯДЧ5 ЙЫ17ДЕХК2ЫД7О
Й7ХтЧЯ2ЫтХrtЕЬтЧ22>ХБЕЙЕтКУХЯЧХЕw ДХrt
Ы2Х2ЕБДЕХЯЧЪтКЯ Й7ХЩХrЧ2ФЙ7Х Х ИрЕ1Д
Й7ХИКПЫИЙЩКЫЙХДЫХ2ЫД7ОЫХwУЬ Д>ХтЧЯ1
5Д>МХKrЧБЕЩП БЕЩХ ИрЕ1Д 2>МХЛЧА1ЕЩХДЫБЕЙЕт>ЫХ
ЯХД МХИЕwЫтЬЧЙХЫЧ1 ЯЧ4 ХЧ1ЬЕт Й2ЕЩХО ЛтЕЩЧД
ФХИХ4Ы17УХКИ1ЕБД Й7ХЬ яД7ХrЕЙЫД4
Ч17Д>2ХМЧБЫтЧ2ХДЕХД ХЩХЕwДЕАХ ЯХД МХЧ1ЬЕт Й2ХО
ЛтЕЩЧД ФХД БЧБХДЫХИЩФЯЧДХИХЧ1ЬЕт Й2Е2ХИЬЧЙ ФХЕД
ХтЫЧ1 ЯЕЩЧД>ХБЧБХЕЙwЫ17Д>ЫХЧ1ЬЕт Й2>Х Х
ИрЕ17ЯКУЙИФХтЧЯwЫ17ДЕ

Вариант №8

1) Зашифровать текст

2) Дешифровка: cod8.txt

БЯОД КЪМ4ИЯЕtrMtЯЛМ41тДЯr 2 ХтЯМДЯЬБКЬЫРПЬ-
ЯПР4КЪЯ5ОтЛтPtБМЩЛтЯЙ ЙЯМ 5ОтЛДОЯr 2 Х Яr ЦтТО4Б
MtЬЯ42М414ЯТ ИК Я4ХДМЪЯХ
ПР4ЯРОДА>ДРПЪЯМДЯР4КЪЙ4ЯтЯМДПР4КЪЙ4Яr ЦтТО4Б РЪЯ2
ММЩДЯМ4ЯДЧДЯтЯП2ДК РЪЯтУЯУО МДМтДЯтЯ5ДОД2 Х>ЯЙ
ЙЯЛ4ЕМ4ЯА4КДДЯwТТДЙPtБМДДЯБЯ5О41О
ЛЛМЩУЯ5ОтК4ЕДМтЬУЯБ4БПЫЯтП54КЪr>ЫРПЪЯ
К14ОтРЛЩЦПЕ РЪЯ Я5ДОтДОтИМЩДЯ>ПРО4ИПРБ ЯМ Я 55 О
РМ4ЛЯ>О4БМДЯ5422ДОЕтБ ЫРЯО
А4Р>ЯЛДР424БЯ4АДП5ДХДМтЬЯФДК4ПРМ4ПРтЯУО
МтЛЩУЯтЯ5ДОД2 Б ДЛЩУЯ2 ММЩУ?

Вариант №9

1) Зашифровать текст

2) Дешифровка: cod9.txt

36-w0n/e/s/e-ren\05w2t-50n`i2\0i21-im07e86w2`-/-2wpemq6f2ewwe1-
703er6nweni2-noc0ni80wwe-23q0w2\2ns-5e-w6k6\6-d2me/e9e-2nre\s3e86w2`-
68ieq6i232me86ww;t-n2ni0q-e7m67ei/2-56ww;t-703er6nwenis-2wpemq6f22-
5eni296\6ns-2n\zk2i0\swe-p232k0n/2q2-2-65q2w2nim6i28w;q2-q0m6q2-n-
re`8\0w20q-/eqrszi0me8-ni6\6-ek0825we1-w0e7te52qenis-2nre\s3e86w2`-
68ieq6i2k0n/2t-nm05ni8-36c2i;-p61\e8-56ww;t-2-rme9m6qqwe1-nm05;-
n\05ozc21-xi6r-m6382i2`-68ieq6i2k0n/2t-nm05ni8-36c2i;-n8`36w-n-re`8\0w20q-
m6nrm050\0ww;t-n2ni0q-e7m67ei/2-56ww;t-2-/eqrszi0mw;t-n0i01-8-/eiem;t-
nm05ni86-n0i08e1-703er6nweni2-2nre\s3ozin`-8-r0m8oz-ek0m05s-5\`-36c2i;-
r0m056860q;t-re-n0i`q-56ww;t-8-w627e\00-re\we1-im6\ie8/0-re5-nm05ni86q2-
n0i08e1-703er6nweni2-q;-7o50q-2q0is-8-825o-q0m;-rm05ei8m6c0w2`-
w6mod0w21-703er6nweni2-/eiem;0-8e3w2/6zi-rm2-r0m056k0-2wpemq6f22-re-
n0i`q-6-i6/40-q0m;-re38e\`zc20-erm050\`is-kie-i6/20-w6mod0w2`-703er6nweni2-
2q0\2-q0nie?

Вариант №10

1) Зашифровать текст

2) Дешифровка: cod10.txt

m291tPE2/69xz-
tPzt\00P193`z1Pt2Q\OP3t`zd962PR/t`z9z1Q2QW/R/t`zd962PR/OO;Qz3PP\cQO
9xzRP8O9mN/zPkQO`zW/ROPzQcQzWPzO/dQ0z-
2;zE2Qm9z129IQOxN9z31Q49/N`OPQzd962fscQQzf3t?2P03tRPz1PzP193/O9sz
1Nft/25/zPOPz3P3tPxNPz98zWRf5z1/NPmzPW9O/mPRP0zWN9O;z9ztPnc9O;
zPWOzfzP3t/RNxN9z3Q\Qz/zW2fEfszPtW/R/N9zPtvQ87/scQIfz-
t9z1/Nm9zO/8;R/N9z3m9t/N/I9zmPEW/z12/R9tQNxIzOf7OPz\;NPz3PP\c9t`zm/
mfs?O9\fw`zR/7Ofsz/0OfzPO9zR;2Q8/N9zWN9OOfsz9zf8mfszR2PWQz2QIO
xz1PNP?3fz1/192f3/zO/I/t;R/N9zQQzO/z3RPs3m9t/NfzOQzP3t/RNxxzO/zOQ0
zO9m/mPEPz12PIQ?7ftm/zt/mzktP\;zR3xz1PRQ25OP3t`z1/Nm9z\;N/zP5R/kQO/
z-
tP0z1PNP3P0z8/tQIzP3?t/RNxxz1/192f3zO/z3m9t/NQzRztPIzR9WQzm/mzPOz
Q3t`z193/N9zO/zOQIzR3QzktPzOf7OPz/zO/193/Rz3O9I/N9z1PNP3fz9z\Q8z1/
Nm9zPt12/RNxN9z/W2Q3/tfzt/mzm/mz\fm?R;zO/zOQ0z2/8\2P3/O;zRz\Q31P2x
WmQztPz12Pk9t\`zO/193/OOPQzPOzIPEztPN`mPzR8xRz3RPs3m9t/Nfz9zO/I
Pt/RzO/zOQQz\Q8z12P1f3mPRz-tfz1PNP3f?

Прим. У преподавателя можно получить варианты текстов для дешифрования в электронном виде.

6. Список используемой литературы

Введение в криптографию / Под общ. ред. Яценко В.В. – М. МЦНМО, «ЧеРо», 1998. – 272 с.

Баричев С.Г. и др. Основы современной криптографии. Учебный курс. 2-е изд., пер. и доп., ГЛТ

Нечаев В.И. Элементы криптографии (Основы теории защиты информации). Учебное пособие для ун-тов и вузов/ М.: Высшая школа , 1999.

Учебное издание

**ИСПОЛЬЗОВАНИЕ ЧАСТОТНОГО АНАЛИЗА
ДЛЯ ДЕКОДИРОВАНИЯ ТЕКСТА**

Методические указания

Составитель *Копенков Василий Николаевич*

Самарский университет
443086 Самара, Московское шоссе, 34.
