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 безопасностм” 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:

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 шифрованные 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 шифрованным 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* (П 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 [NxM] 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

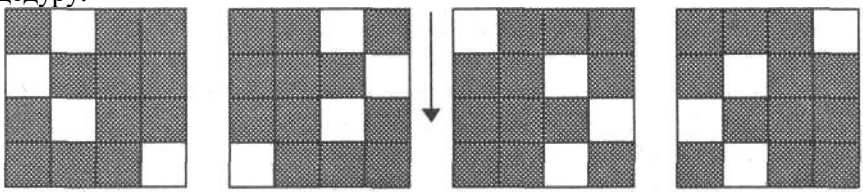
5	3	8	4	6	1	9	7	2
п	р	и	л	е	п	л	я	я
с	я	п	р	е	м	у	д	р
у	м	п	р	е	м	у	д	р
б	у	д	е	ш	ь	а	б	в

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:

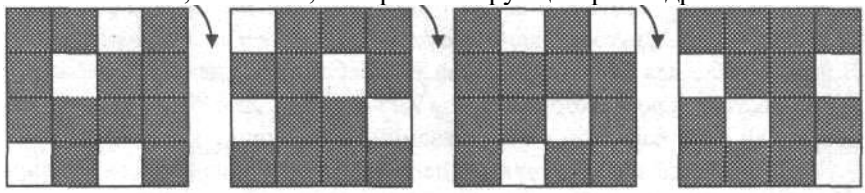
1) прувр дмбиу палмр ьееешпрмел пудяя дуясрб;
2) пммья ррвря мулрр епсуб ееешя ддбип пдлууа;

(Из послания Даниила Заточенаго к великому князю Ярославу Всеволодтю)

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 Алъ-Аща",* 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 шифрованный 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 шифрованный 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	Й	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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	Ь	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
Ь	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	Ь
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	Ь	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	Ь	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	Ь	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 шифрованный 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 шифрованный текст. Разбивая этот текст на группы одной длины (например, по 5), получают шифрованное 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 шифрованным сообщением.

2. Применение частотного анализа для дешифрования.

Пусть есть сообщение:

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

Индекс частоты появления букв в стандартном тексте:

```
О == 0.0886741
И == 0.0653615
Е == 0.0650947
Т == 0.0601900
А == 0.0570297
С == 0.0461327
Н == 0.0453323
В == 0.0381292
Р == 0.0321779
Л == 0.0320343
М == 0.0311929
К == 0.0240719
Д == 0.0231484
...
```

Индекс частоты появления букв в закодированном тексте:

```
Т == 0.152866
Ц == 0.082805
С == 0.076433
Й == 0.076433
Д == 0.070063
Х == 0.050956
Ф == 0.044589
М == 0.031815
Р == 0.031815
П == 0.031815
И == 0.031815
Е == 0.025477
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 ХОЖЙФЬЙССО ХЙОФЙЦСТЙ ХООЕЭЙСМЙ СДР УФМЬПОХа ХИЙПДЦа ЙЗО ИОХЦДЦОЫСО ИПМС-СЯРОЫЦОЕЯ 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 ИПМССЯРОЫЦОЕЯ РОКСО ЕЯПО УФОИЙРОСХЦФМФОЖАЦа ФАЕОЦЧ РЙЦОИАЫАХЦОЦСОЗО 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 УФОИЕМОНХТФМФОВАТа ФАЕОТУ МЕТОИАЫАХТОТНОЗО 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 ЧАСТОТНОГО 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 дешефрированными 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):
АБВГДЕЖЗИЙКЛМОПРСТУФХЦЧШЩЪЫЬЭЮЯ (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 ЬrДЫt12<Д>>tr82tM<КЫ1ХО>12>t<rЬЧ82ЯК КБrtАД-
ХО>12ЯЬ2ЙЬББrЬ<02Я Ь>О
ДЫ>Or02ЬЕК>ЯКatrД12r2Е0Б0cК<2Ф..КЙОtrЫЬК2ЯЬ2r К<КЫt2БКЙЬБt
ЬrДЫtК2>ЛДОЬАЬ2ОКЙ>ОД2ЫЬ2r<К>ОК2>2tM<КЫКЫtК<2
Д>ЯЬЧЬЛКЫt12ЬО КМЙЬr2>ЬЬОrКО>Or0Xct32>t<rЬЧД<2r2ЙЬББrЬ<2Я
Ь>О ДЫ>OrК2tM<КЫ1КО>12ОДЙЛК2t2Я
КБ>ОДrЧКЫt12>ЛДО832>t<rЬЧЬr2ОЬ2К>О,2r2ЫДbt32ОК <tЫД32bt.
ЬЕЬМЫДаКЫt1?2ЫДЯ t<К 2ЯК
КБrtЫ0r2>t<rЬЧ2r2tM2ЙЬЫ9Д2ЙЬББrЬАЬ2Я Ь>О
ДЫ>OrД2r2ЫДаДЧЬ2ЙЬБt
0ХсКК2МЫДаКЫtК2<ЬЛКО2r8АЧ1БКО,2ЫК2ЙДЙ2МДЯЧДЫt
ЬrДЫЫЬК2tMЫДаДЧ,ЫЬ2Д2ЯЬБ
0АЬ<02>ЬЬОrКО>OrКЫЫЬ2<КЫ1ХО>12t2EtO82ЙЬБt 0XctК2ЫДbК2
КМ0Ч,Ot 0ХсКК2МЫДаКЫtК2rБЬЕДrЬЙ2ДБДЯОtrЫЬ<2ДЧАЬ
tO<К2r>К2<КЫ1КО>12БtЫД<taК>Йt2ЯЬ>ЧК2tM<КЫКЫt12ЙДЛБЬАЬ2>t<r
ЬЧД

Вариант №2

1) Зашифровать текст

2) Дешифровка: cod2.txt

>Р>rОХ2Х>ДЕ2rА2Х>РОЕ7О1Аа>Х29аФ7Е2РО17аХ> РФ аАr
>2Ма1УО>РаЕ2 А12rА7>Д2 РФа17 >УОb9232>r7ХР2ФО>АО0Ф7МО>РаЕ2
А12rАа8>Д2 РФа17 >УОb9232>r7ХР2ФО>2r12РО11О
>1О>Д29rtаАа>tОrА2А>7Л>РrАЕatОаХ2rА7>1Ос<РОаАr
>Х29аФЫЯ>ДаЕР232>ДЕ70Ф7bа17 >7Ф7>аЙа>ДаЕР232>Д2Е
9УО>АО0Ф7МО>Бt7А<РОЯЙО
>02Фаа>rФ2b1<а>сОР7r7Х2rА7>1ОДЕ7ХаЕ>Д2
РФа17а>291232>r7ХР2ФО>Д2rФа>УОУ232А2>9ЕБ3232>7ХаЯА>r22АРаАr
АРа112>РА2Е28>7>02Фаа>Д2Е 92У>r>Д2Х2ЙЫЯ>ЬА7Л>РаЕ2
А12rАа8>Х2bаА>0<АЫ>Р<t7rФа1О>Ь1АЕ2Д7
>7>Д2rАЕ2а1>92rАОА2t12>ЬККаУА7Р1<8>У29>Д2сР2Ф
ЯЙ78>rbОАЫ>АаУrА>1О7ФБtИО >rЕа91
>9Ф71О>У29О>7>r22АРаАrАРа112>rАаДа1Ы>rbОА7 >92rА73ОаАr >Х29аФ
Х7>Р>У2А2Е<Л>2Ма1У7>РаЕ2 А12rА7>УОУ>Х2b12>02Фаа>А2t1<

Вариант №3

1) Зашифровать текст

2) Дешифровка: cod3.txt

7ОУ8cr8ЛБ8ЧХОДХЛМtcbJrAc<МАcPcМАЕc<ХЛД8cХcБАc5МА1c
БКХ<Xr8cКД8cr8cБК87ЛМОРДb8МЛbcАБМХЕОД4r
ЕcОД>АКХМЕАЕcЛУОМХb?cБАЛ2АД42tcArcr8cХЛБАД4Фt8McrX2
О2А1cXrИАКЕОЧХХcАcЛУХЕО8ЕАЕcМ82ЛМ8?c<МАП
cБArbМ4c2О2cБКАХЛЙА7ХМcЛУОМХ8cХЛБАД4ФtaЬ88cФrOrXbc
АcМ82ЛМ8cР8Кr8ЕЛbc2cБArbМХbЕc5rМКАБХХcХcXrИАКЕОМХР
rАЛМХcМ82ЛМОccЛРbФ4cЕ8У7tcР8КАbMrАЛМbЕХcХc2А7ОЕХcХ
Фt<О8МЛbcРcОД>8ПКОХ<8Л2А1cМ8АКХХc2А7ХКАРОrXbcАЛrА
РrА1cМ8АКХ81c2АМАКА1cbРДb8МЛbcrX2МАcXrA1c2О2c2ДА7c5
ДРt7cЫ8rrArc8>АcМ8АК8Е
c2А7ХКАРОrXbcХЛМА<rX2ОcХЛБАД4ФtaМЛbcА<8r4cО2МХРrАс
ХcФ78Л4

Вариант №4

1) Зашифровать текст

2) Дешифровка: cod4.txt

Х4МЕОb1cХЛЫХ>7МcОХАМЕtЬОЕratKrМЕ1rX>МД4РУ><Х
ЙМ4Уb1Д>rФ1aМЕП4r>ЛМ5ОРМ21rОДАМЕМ4c42r>aХ
Ф>М>МЕr4r><ОЕ8>Ф>МФ1cОУЛФ>М2ДОcЕr4aУОХ>ЛМc4ХХ
ЙМ>ЙМaЕОМФ1ПХ1МД4Р5>rАМХ4МХО2ОДОЕО84КЬ>ОЕЛМ8У4
ЕЕ М>У>МЕОФО7Era4М21МЕ21Е15tМ81c>Д1a4Х>ЛМc4ХХ
ЙМ84Пc1ОМЕОФО7Era1М2Д>Pa4Х1МЕП4rАМrО8ЕrМ12ДОcОУОХ
Х17МЕrДt8rtД
МЕМ12ДОcОУОХХ17МЕrО2ОХАКМБИИО8r>aХ1Er>М>М5
ЕrД1cО7Era>ЛМaМР4a>Е>Ф1Er>М1rМr1b1М<r1Ма4ПХООМаМ2Д>
У1ПОХ>>МЕ81Д1ЕrАМ>У>М81БИИ>Ч>ОХrМЕП4r>Л

Вариант №5

1) Зашифровать текст

2) Дешифровка: cod5.txt

И7У24>2 >МР4ДД >М2ЕПЧЙМД48
О4ЙАИЛМrEt48ДЕ2ЧММИЙtEX4МШ4Ф1МЙ>ХИЙМУ1УМРОЕУ<Д >МР4ДД
>МУ1УМЕЪУШtЕО4ДД ФМИ-
УПД41МИМЙЕ<ХУМ8t>ДУЛМЙ>EtУУМrt>PrE14П4>ЙИЛМ<ЙЕМР4ДД
>MrtEУ8ОЕРЛЙИЛМУИЙЕ<ДУХЕ2МУМrt>РЕИЙ4О1ЛКЙИЛМХЕ2rt>ИИЕtЧМОМ
ОУР>МИУ2ОЕ14МД4РМД>ХЕЙEt
2М41Ш4ОУЙЕ2Mt4ДАЫ>МО>ИАМrtЕЪ>ИИМИ74ЙУЛМД48
О41УМХЕРУtЕО4ДУ>2МУИЙЕ<ДУХ4МrЕИХЕ1АХЧМЕДЕМrtУ8О4ДЕМЧР41УЙ
АМУ85 ЙЕ<ДЕИЙАМОМР4ДД
ЩМД4МЕИДЕО>МУЩМrt>РИХ48Ч>2ЕИЙУМrЧЙ>2МУДЕПЕМrt>РИЙ4О1>ДУЛ
МР4ДД
ЩММЙЕМ>ИЙАМУЩМХЕРУtЕО4ДУЛМ84МРО4МrЕИ1>РДУЩМР>ИЛЙУ1>ЙУ
ЛМХ4tЙУД4МД>ИХЕ1АХЕМУ82>ДУ14ИАМr>tОЕФМ14ИЙЕ<ХЕФМИЙ414МУР>
ЛМt48Р>1УЙАМrtЕЪ>ИИМИ74ЙУЛМД4МРО4МО84У2ЕИОЛ84ДД
ЩМrtЕЪ>ИИ4МХЕРУtЕО4ДУ>МД>rЕИt>РИЙО>ДДЕМОЕИrtЕУ8ОЕРЛЬ>>МИ74Й
ФМrЕЙЕХ-
МИУ2ОЕ1ЕОМУМ2ЕР>1УtЕО4ДУ>Mrt>РЕИЙ4О1ЛКЬ>>МОИКМД>Е5ЩЕРУ2ЧК
МР1ЛМХЕРУtЕО4ДУЛМУДШЕt24ЪУК

Вариант №6

1) Зашифровать текст

2) Дешифровка: cod6.txt

tАЪЧХАЫI151Ъ1ХЯ Ч<tЫФБ7Х1ЪЕЬ ЧБ<ХЩ ЧЯБЬЕ 1ЛЧ5tАЩЬЕЬХЯ tЬ2
1ЙЬД1ЫЧФХr1ЫЫ>МХБЬХЬЩ1ИtБАФХ5БЬХ1ЪЕЬ
ЧБ<ХАИ1БЧФХЫtХ<ЬИtБХ8ЛЛtЩБЧДЫЬХ 12ЬБ1Б7ХЫ1ХОЧЛ
ЬБtЩАБ1МХМЬ ЬОЧМХЩ ЧЯБЬ1ЪЕЬ ЧБ<ЬДХАИ1Б7ХОЧЛ
ЬБtЩАБХДtА7<1ХБФИtЪЬХЯЬХБЬШХЯ ЬАБЬШХЯ Ч5ЧЫtХ5БЬХЩ ЧЯ-
БЬЕ
1ЛЧ5tАЩ1ФХАЧАБt<1ХrЬЪИЫ1ХЪУ2><ЧХrЬАБКЯЫ><ЧХАЯЬАЬ21<ЧХ
ЧЙ21ДЪФБ7ХОЧЛ ЬБtЩАБХЬБХЬ5tДЧrЫ>МХДЫКБ
tЫЫЧМХЙ1ДЧАЧ<ЬАБtШХ1ХЯЬБЬ<КХtЕЬХ8ЫБ
ЬЯЧФХ2КrtБХДtА7<1ХД>АЬЩЬШХЧХКИХБЬ5ЫЬХЫ1<ЫЬЕЬХД>ОtХ5t<
ХКХЬБЩ >БЬЕЬХБtЩАБ1ХЯ trАБ1ДЧБ7ХАt2tХ1ЪЕЬ
ЧБ<ХАИ1БЧФХЩЬБЬ >ШХ2>ХМЬ
ЬОЬХАИЧ<1ЪХЙ1ОК<ЪtЫЫ>tХr1ЫЫ>tХrЬДЬЪ7ЫЬХБФИtЪЬХДtr7Хr1Ит
ХЧЫБКЧБЧДЫЬХЯЬЫФБЫЬХ5БЬХАИ1БЧtХДАt4tЪЬХ21ЙЧ
КtБАФХЫ1ХЧЙ2>ББ5ЫЬАБЧХЧЫЛЬ <14ЧЧХДХБtЩАБtХОЧЛ

ЬД1ЫЧtХ8БКХЧЙ2>ББ5ЫЬАБ7ХКАБ 1ЫФtБХ1ХД<tАБtХАХЫtШХКАБ 1ЫФtБХЧХДЬЙ<ЬИЫЬАБ7ХАИ1Б7ХБtЩАБ

Вариант №7

1) Зашифровать текст

2) Дешифровка: cod7.txt

KwЧ5Д>ЫХЧ1ЪEt Й2>ХИЬЧЙ ФХ 1 ХБЧБХЫПЫХЪ-
ЕЩЕtФЙХБЕ2rtЫИИ XrЕЯЩЕ1ФУЙХДЫХЙЕ17БЕХ8ЛЛЫБЙ
ЩДЕХМtЧД Й7ХБЕДЛ wЫД4 Ч17Д>ЫХwЧДД>ЫХДЕХ ХДЧrt
2ЫtХЯДЧ5 ЙЫ17ДЕХК2ЫД7О
Й7XtЧЯ2ЫtXrtЕЪtЧ22>ХБЕЙЕtКУХЯЧХЕw ДХrt
Ы2Х2ЕЬДЕХЯЧЪtКЯ Й7ХЩХrЧ2ФЙ7Х Х ИrЕ1Д
Й7ХИКПЫИЙЩКЫЙХДЫХ2ЫД7ОЫХwУЬ Д>ХtЧЯ1
5Д>МХКrЧБЕЩП БЕЩХ ИrЕ1Д 2>МХЛЧА1ЕЩХДЫБЕЙЕt>ЫХ
ЯХД МХИЕwЫtЬЧЙХtЫЧ1 ЯЧ4 ХЧ1ЪEt Й2ЕЩХО ЛtЕЩЧД
ФХИХ4Ы17УХКИ1ЕЬД Й7ХЬ ЯД7ХrЕЙЫД4
Ч17Д>2ХМЧБЫtЧ2ХДЕХД ХЩХЕwДЕАХ ЯХД МХЧ1ЪEt Й2ХО
ЛtЕЩЧД ФХД БЧБХДЫХИЩФЯЧДХИХЧ1ЪEt Й2Е2ХИЬЧЙ ФХЕД
ХtЫЧ1 ЯЕЩЧД>ХБЧБХЕЙwЫ17Д>ЫХЧ1ЪEt Й2>Х Х
ИrЕ17ЯКУЙИФХtЧЯwЫ17ДЕ

Вариант №8

1) Зашифровать текст

2) Дешифровка: cod8.txt

БЯОД КЪМ4ИЯЕtrМtЯЛМ41tДЯr 2 ХtЯМДЯЬБКЬЫРПЬ-
ЯПР4КЪЯ5ОtЛtРtБМЩЛtЯЙ ЙЯМ 5ОtЛДОЯr 2 Х Яr ЦtТО4Б
МtЬЯ42М414ЯТ ИК Я4ХДМЪЯХ
ПР4ЯРОДА>ДРПЬЯМДЯР4КЪЙ4ЯtЯМДПР4КЪЙ4Яr ЦtТО4Б РЪЯ2
ММЩДЯМ4ЯДЧДЯtЯП2ДК РЪЯtУЯУО МДМtДЯtЯ5ДОД2 Х>ЯЙ
ЙЯЛ4ЕМ4ЯА4КДДЯwТТДЙРtБМДДЯБЯ5О41О
ЛЛМЩУЯ5ОtК4ЕДМtЬУЯБ4БПЫЯtП54КЪr>ЫРПЬЯ
К14ОtРЛЩЯПЕ РtЬЯ Я5ДОtТДОtИМЩДЯ>ПРО4ИПРБ ЯМ Я 55 О
РМ4ЛЯ>О4БМДЯ5422ДОЕtБ ЫРЯО
А4Р>ЯЛДР424БЯ4АДП5ДХДМtЬЯФДК4ПРМ4ПРtЯУО
МtЛЩУЯtЯ5ДОД2 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/0OP193`z1Pt2Q\OP3t`zd962PR/t`z9z1Q2QW/R/t`zd962PR/OO;Qz3PP\cQO9xzRP8O9mN/zPkQO`zW/ROPzQcQzWPzO/dQ0z-2;zE2Qm9z129IQOxN9z31Q49/N`OPQzd962fscQQzf3t?2P03tRPz1PzP193/O9sz1Nft/25/zPOPz3P3tPxNPz98zWRf5z1/NPmzPW9O/mPRP0zWN9O;z9ztPNc9O;zPWOfzP3t/RNxN9z3Q\Qz/zW2fEfszPtW/R/N9zPtvQ87/scQIfz-t9z1/Nm9zO/8;R/N9z3m9t/N/I9zmPEW/z12/R9tQNxIzOf7OPz\;NPz3PP\c9t`zm/mfs?O9\fW`zR/7Ofszt/0OfzPO9zR;2Q8/N9zWN9OOfsz9zf8mfszR2PWQz2QIOxz1PNP?3fz1/192f3/zO/I/t;R/N9zQQzO/z3RPsz3m9t/NfzOQzP3t/RNxxzO/zOQ0zO9m/mPEPz12PIQ?7ftm/zt/mzktP\;zR3xz1PRQ25OP3t`z1/Nm9z\;N/zP5R/kQO/z-tP0z1PNP3P0z8/tQIzP3?t/RNxxz1/192f3zO/z3m9t/NQzRztPIzR9WQzm/mzPOzQ3t`z193/N9zO/zOQIzR3QzktPzOf7OPz/zO/193/Rz3O9I/N9z1PNP3fz9z\Q8z1/Nm9zPt12/RNxN9z/W2Q3/tfzt/mzm/mz\fm?R;zO/zOQ0z2/8\2P3/O;zRz\Q31P2xWmQztPz12Pk9t/t`zO/193/OOPQzPOzIPEztPN`mPzR8xRz3RPsz3m9t/Nfz9zO/IPt/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. Ященко 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.