Лабораторная работа №1.

Простейшие шифры.

Цель работы – изучение простейших шифров подстановки и перестановки; получение навыков программной реализации алгоритмов шифрования.

1. Теоретические основы лабораторной работы.

1.1. Простейшие (одноалфавитные) коды подстановки.

Криптография — тайнопись. Термин ввел *Д. Валлис.* 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.

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:

Y H Q L Y L G L Y L F L

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

⇑ 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"

Шифр *Цезаря* входит 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.

Одним из простейших шифров перестановки является так называемый шифр блочной перестановки. Суть его заключается в следующем. Пусть длина блока выбрана равной N. Для шифрования выбирается ключевая последовательность целых чисел от 1 до N, случайным образом «перемешанная» для N = 8 примером такой последовательности будет [5 3 8 4 6 1 9 7 2]). Далее, текст шифруемого сообщения разделяется на блоки размера N так, чтобы одной букве текста соответствовало одно число из ключевой последовательности. Для шифрования буквы первого блока выписываются в порядке , задаваемом ключевой последовательностью (то есть первым выписывается буква, которой соответствует 1 ключевой последовательности и т.д.). После того как все буквы первого блока выписаны, аналогично выписывается второй блок и все последующие.

Для расшифровки текста первый блок зашифрованного текста выписывается в соответствии с ключевой последовательностью таким образом, чтобы первая буква зашифрованного текста оказалась на позиции, соответствующей 1 ключевой последовательности и т.д.

К классу *"перестановка"* принадлежит и шифр, называемый *"решетка Кардано"*. Для шифрования используется специальное приспособление - квадратная карточка с отверстиями, разделенная на клетки, которая при наложении на лист бумаги оставляет открытыми лишь ¼ клеток. Число строк и столбцов в карточке является четным числом. Процедура шифрования состоит в следующем. Решетка накладывается поверх бумаги и текст последовательно (слева направо, сверху вниз) вписывается в открытые клетки решетки. Далее, решетка поворачивается на 90° градусов и следующая часть текста вписывается в открытые клетки (при этом уже написанные буквы не оказываются в открытых клетках). Аналогично процедура повторяется, пока решетка не будет повернута на 360 градусов (рис. 1). После чего текст, написанный на бумаге, может быть прочитан только с помощью аналогичной решетки.

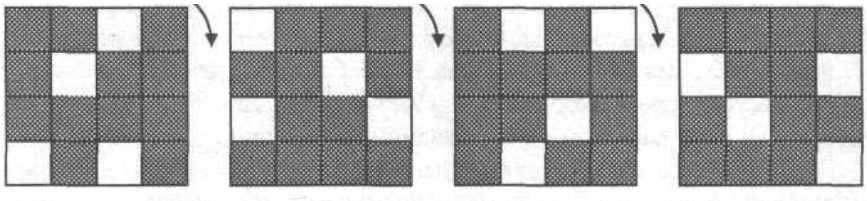

Рисунок 1. Пример использования квадратной решетки Кардано для шифрования (последовательный поворот на 90°)

1.3. Усложненные (многоалфавитные) шифры подстановки.

Для усложнения раскрываемости шифра простой подстановки цели используют *многоалфавитную систему шифрования* - систему, в которой для шифрования каждого символа употребляют тот или иной способ подстановки (алфавит подстановки) в зависимости от ключа, или от номера шифруемого символа в передаваемом сообщении.

Одним из первых способов шифрования, основанных на многоалфавитной подстановке, был так называемый шифр Вижинера. Простой вариант шифра Вижинера (*шифр Вижинера с ключевым словом*) описывается следующим образом. Для шифрования (и дешифрования) используется специальным образом составленная таблица символов *("таблица Виженера")*. При создании данной таблицы используется следующее правило: в первой строке выписывается весь алфавит, во второй строке осуществляется циклический сдвиг алфавита на одну позицию, в третьей – на две позиции и т.д.. Так получается квадратная таблица, число строк которой равно числу столбцов и равно числу букв в алфавите. На рисунке 2 представлена таблица, составленная для английского алфавита (первая строка и первый столбец выделены для удобства и не являются частью создаваемой таблицы Вижинера). Чтобы зашифровать сообщение, поступают следующим образом. Выбирается ключевое слово, известное только отправителю и получателю сообщения, (например, "монастырь") и записывается с повторением над буквами сообщения.

Чтобы зашифровать первую букву текста, необходимо выбрать столбец таблицы Вижинера, соответствующий первой букве ключевого слова, и строку, соответствующую первой букве текста. Буква, находящаяся на пересечении выделенных столбца и строки, записывается как буква зашифрованного сообщения. Аналогично шифруются все последующие буквы сообщения.

Расшифровать данное сообщение можно следующим образом. Над зашифрованным текстом сообщения, записанным в одну строку, записывается повторяющееся ключевое слово. Далее, в таблице Вижинера выбирается столбец, соответствующий первой букве ключевого слова, и в данном столбце находится буква, соответствующая первой букве зашифрованного сообщения. Строка, в которой данная буква найдена, и определяет первую букву расшифрованного текста. Аналогично процесс повторяется для всех последующих букв.

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

Рисунок 2. Пример таблицы Вижинера для английского алфавита

Кроме того, существуют более сложные варианты шифра Вижинера (*шифры Вижинера с «самоключом»*), не требующие использования ключевого слова. Шифрование в данном случае осуществляется аналогично предыдущему случаю, но в качестве буквы ключевого слова используется *предыдущая буква самого сообщения* (для шифрования первой буквы сообщения предыдущей буквой считается буква «а»).

К многоалфавитной системе шифрования можно также отнести *диграммную (биграммную) подстановку*. Данный способ шифрования предполагает, что отправителю и получателю сообщения известна специальным образом созданная таблица подстановки. В данной таблице каждый столбец соответствует первой букве диграммы (двухбуквенной последовательности), а каждая строка – второй букве диграммы. В клетках таблицы вписаны случайным образом все возможные диграммы (двухбуквенные сочетания). При шифровании текст разбивается на диграммы и каждая диграмма заменяется соответствующей диграммой из таблицы. Вместо подстановки диграмм можно использовать подстановку трех букв (триграмм) и т.д.

Шифр *Плейфер.* Этот шифр является частным видом диграммной подстановки, которая производится с помощью перемешанного алфавита, записанного в виде квадрата. Например, для латинского алфавита заполняется квадрат размером 5 x 5. (Буква J опускается (аналогично русской “й”), так как она встречается реже остальных. В тех случаях, когда она встречается, ее можно заменить буквой I.) Предположим, что ключевой квадрат записывается следующим образом:

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

В этом случае диграмма AC, например, заменяется на пару букв, расположенных в противоположных углах прямоугольника, определенного буквами A и C, т.е. на LO, причем L взята первой, так как она выше A.

Если буквы диграммы расположены на одной горизонтали, то используются стоящие справа от них буквы. Таким образом, RI заменятся на DF,RF заменяется на DR. Если буквы расположены на одной вертикали, то используются буквы, стоящие под ними. Таким образом, PS заменяется на UW. Если обе буквы диграммы совпадают, то можно использовать для их разделения нуль или же первую из букв опустить и т.д.

Порядок выполнения лабораторной работы.

Общий план выполнения работы.

1. Изучить методы шифрования, представленные в данном пособии.
2. Получить от преподавателя номер варианта задания .
3. Написать программу шифрования и дешифрования текстовых файлов (конкретный метод шифрования определяется вариантом задания).
4. Сдать отчет преподавателю, ответить на контрольные вопросы, получить зачет по работе.

Контрольные вопросы.

1. Шифр простой подстановки – принцип работы.

2. Шифры перестановки – принцип работы, пример работы шифра (блочная пере- становка или решетка Кардано).

3.Шифры многоалфавитной подстановки – принцип работы, пример работы шифра (шифр Вижинера, диграммная подстановка).

Требования к программам шифрования и дешифрования.

Входными данными являются текстовый файл, содержащий сообщение (открытое – для программы шифрования, зашифрованное – для программы дешифрования) и текстовый файл, содержащий ключ шифрования.

В текстовом файле с сообщением могут содержаться только строчные буквы русского (или английского, на выбор) алфавита, разделенные пробелами и символами конца строки.

Выходными данными является текстовый файл, содержащий выходное сообщение (открытое – для программы дешифрования, зашифрованное – для программы шифрования). Все пробелы и символы конца строки, содержавшиеся во входном файле с сообщением, должны присутствовать и в выходном файле (без их шифрования).

ВАРИАНТЫ ЗАДАНИЙ

Легкий

1. Реализовать программу шифрования и дешифрования для метода простой подстановки (шифр Цезаря). Ключ – число (смещение при шифровании).
2. Реализовать программу шифрования и дешифрования для метода Вижинера с ключевым словом. Ключ – слово фиксированной длины (8 символов, только русский или английский алфавит)
3. Реализовать программу шифрования и дешифрования для метода блочной перестановки. Ключ – последовательность из 18 целых чисел, разделенная пробелами.

Средний

4. Реализовать программу создания решеток Кардано заданного размера (8 на 8 ячеек). Входных данных не требуется, выходные данные – текстовый файл с записанной решеткой. В выходном файле 8 строк, разделенных символом конца строки, в каждой строке 8 символов 1 и 0 без разделения (1 – есть отверстие в решетке, 0 – нет отверстия).
5. Реализовать программу шифрования и дешифрования для решетки Кардано. Ключ – файл с записанной решеткой из варианта 4.
6. Реализовать программу шифрования и дешифрования для метода Вижинера с «самоключом» (в качестве буквы ключа используется предыдущая буква открытого текста).
7. Реализовать программу шифрования и дешифрования для метода Вижинера с «самоключом» (в качестве буквы ключа используется предыдущая буква уже зашифрованного текста)
8. Реализовать программу шифрования и дешифрования для метода диграммной подстановки. Ключ – файл с записанной таблицей диграммных подстановок, строки таблицы разделены символами конца строки, диграммы в строке разделены пробелами.
9. Реализовать программу шифрования и дешифрования для метода триграммной подстановки. Ключ – файл с записанной таблицей триграммных подстановок, строки таблицы разделены символами конца строки, триграммы в строке разделены пробелами.
10. Реализовать программу шифрования и дешифрования для метода Плейфер. Ключ – файл с записанной таблицей подстановок. Строки таблицы разделены символами конца строки, столбцы – пробелами.

Сложный

11. Реализовать программу шифрования и дешифрования для сложной блочной перестановки (для шифрования последовательно применяются две блочные перестановки с разным периодом ключа N). Ключ – текстовый файл, первой строке последовательность из 18 целых чисел, разделенных пробелами (ключ первой перестановки), во второй строке последовательность из 7 целых чисел, разделенных пробелами (ключ второй перестановки).

12. Реализовать программу создания решеток Кардано произвольного размера. Входных данных не требуется, выходные данные – текстовый файл с записанной решеткой.

13. Реализовать программу создания решеток Кардано заданного размера (8 на 8 ячеек). Реализовать программу шифрования и дешифрования для случайно сгенерированной решетки.

14. Реализовать программу шифрования для метода простой подстановки (шифр Цезаря). Ключ шифрования – произвольное число. Реализовать программу дешифрования без знания ключа. Для определения ключа дешифрования реализовать атаку полного перебора (brute force attack).

15. Реализовать программу шифрования для метода Вижинера с «самоключом» (в качестве буквы ключа используется предыдущая буква открытого текста). Реализовать программу дешифрования без знания ключа. Для определения ключа дешифрования реализовать атаку полного перебора (brute force attack).

16. Реализовать программу шифрования для метода Вижинера с «самоключом» (в качестве буквы ключа используется предыдущая буква уже зашифрованного текста). Реализовать программу дешифрования без знания ключа. Для определения ключа дешифрования реализовать атаку полного перебора (brute force attack).

17. Реализовать программу шифрования для метода простой подстановки (шифр Цезаря). Ключ шифрования – произвольное число. Реализовать программу дешифрования без знания ключа (с применением частотного анализа).

18. Реализовать программу шифрования и дешифрования для метода *n*-граммной подстановки. На вход подается число n - количество символов подстановки. Например, для диграммной подстановки n=2, для триграммной – n=3.