ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ САПР
Лабораторная работа №1

1. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

1.1. Проблемы защиты информации

В настоящее время во всем мире резко повысилось внимание к проблеме информационной безопасности. Это обусловлено процессами стремительного расширения потоков информации, пронизывающих все сферы жизни общества.

Информация давно перестала быть просто необходимым для производства вспомогательным ресурсом или побочным проявлением всякого рода деятельности. Она приобрела ощутимый стоимостной вес, который четко определяется реальной прибылью, получаемой при ее использовании, или размерами ущерба, с разной степенью вероятности наносимого владельцу информации. Однако создание индустрии переработки информации порождает целый ряд сложных проблем. Одной из таких проблем является надежное обеспечение сохранности и установленного статуса информации, циркулирующей и обрабатываемой в информационно-вычислительных системах и сетях.

Появление глобальных компьютерных сетей сделало простым получение доступа к информации, как для отдельных пользователей, так и для больших организаций. Но легкость и высокая скорость доступа к данным при помощи компьютерных сетей, таких как *Internet,* также сделали значительными следующие угрозы безопасности данных при отсутствии мер их защиты:

- неавторизованный доступ к информации;
- неавторизованное изменение информации;

– неавторизованный доступ к сетям и сервисам;

– другие сетевые атаки, например, повтор перехваченных ранее транзакций и атаки типа "отказ в обслуживании".

При обработке любой значимой информации при помощи отдельного компьютера, а тем более в сети, возникает вопрос о ее защите от несанкционированного доступа и использования. Наиболее распространенный в компьютерных системах способ защиты – использование паролей – более пригоден для защиты доступа к вычислительным ресурсам, нежели для защиты информации. Это своеобразный экран, отгораживающий законных пользователей системы от посторонних, пройдя сквозь который, квалифицированный пользователь получает доступ практически ко всей информации.

В настоящее время исключительно важное значение в разных областях приобрели вопросы, связанные с сохранением и передачей конфиденциальной информации. Возникающие при этом задачи решает *криптография* – наука о методах преобразования информации в целях ее защиты от незаконных пользователей.

Ретроспективный взгляд на историю развития криптографии, как специфическую область человеческой деятельности, позволяет выделить три основных периода. Первый, наиболее продолжительный, – это эпоха "ручной криптографии". Ее начало теряется в глубокой древности, а окончание приходится на 30-е годы XX века. Криптография прошла путь от магического искусства до вполне прозаической прикладной специальности чиновников дипломатических и военных ведомств.

Второй период – создание и широкое внедрение в практику сначала механических, затем электромеханических и электронных устройств шифрования, организация целых сетей засекреченной связи. Его началом

можно считать разработку Гилбертом Вернамом *(G.Vernam)* в 1917 году схемы телеграфной шифровальной машин, использующей *одноразовую гамму*, рис.1.1.

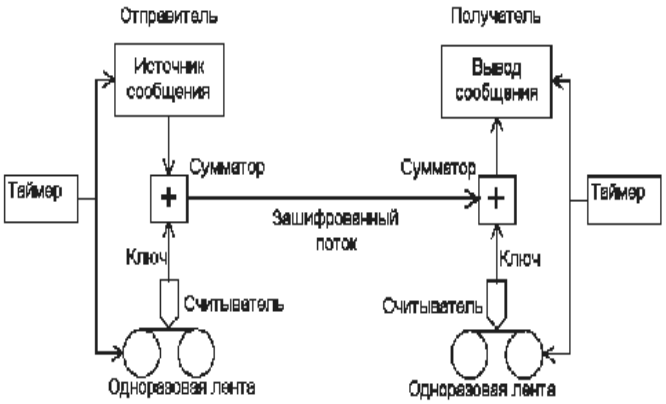


Рис. 1.1. Шифрование методом Вернама

К середине 70-х годов с развитием разветвленных коммерческих сетей связи, электронной почты и глобальных информационных систем на первый план вышли новые проблемы – проблемы снабжения ключами и проблемы подтверждения подлинности.

В 1976 году американские ученые Уитфилд Диффи *(W.Diffie)* и Мартин Хеллман *(M.Hellman)* предложили два новых принципа организации засекреченной связи без предварительного снабжения абонентов секретными ключами шифрования – принцип так называемого *открытого шифрования* и принцип *открытого распределения ключей*. Этот момент можно считать началом нового периода в развитии криптографии. В настоящее время это направление современной криптографии очень интенсивно развивается.

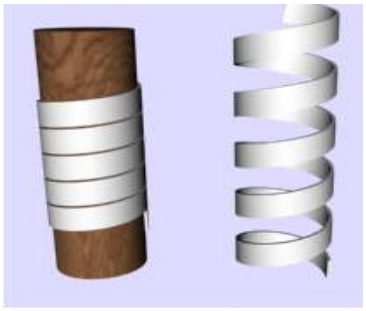
1.2. Из истории криптографии

Понятие “безопасность” охватывает широкий круг интересов, как отдельных лиц, так и целых государств. Во все исторические времена существенное внимание уделялось проблеме информационной безопасности, обеспечению защиты конфиденциальной информации от ознакомления, кражи, модификации, подмены. Решением этих вопросов занимается *криптография.*

Рис. 1.2. Джон Валлис

Криптография – тайнопись. Термин ввел Джон Валлис *(John Wallis)* (1616-1703), английский математик. Потребность шифровать и передавать шифрованные сообщения возникла очень давно. Так еще в V-VI вв до н.э. греки применяли специальное шифрующее устройство. По описанию Плутарха, оно состояло из двух цилиндрических стержней одинаковой длины и толщины. Один оставляли себе, а другой отдавали отъезжающему. Эти стержни называли *сциталами.* При необходимости передачи сообщения, длинную ленту папируса наматывали на сциталу, не оставляя на ней никакого промежутка.

Затем, оставляя папирус на сцитале, писали на нем все, что необходимо, а, написав, снимали папирус и без стержня отправляли адресату. Так как буквы оказывались разбросанными в беспорядке, то прочитать сообщение мог только тот, кто имел свою сциталу такой же длины и толщины, намотав на нее папирус.



. 1.3. Сцитала

Квадрат Полибия[1]

В Древней Греции (II в. до н.э.) был известен шифр, называемый "*квадрат Полибия"*.

Это устройство представляло собой квадрат 5*5, столбцы и строки которого нумеровали цифрами от 1 до 5. В каждую клетку записывалась одна буква (в греческом варианте одна клетка оказывалась пустой, а в латинском – в одну клетку помещали две буквы *I,J*). В результате каждой букве отвечала пара чисел по номеру строки и столбца.

1	2	3	4	5	
A	**B**	**C**	**D**	**E**	1
F	**G**	**H**	**I,J**	**K**	2
L	**M**	**N**	**O**	**P**	3
Q	**R**	**S**	**T**	**U**	4
V	**W**	**X**	**Y**	**Z**	5

13	**34**	**22**	**24**	**44**	**34**	**15**	**42**	**22**	**34**	**43**	**45**	**32**

Cogito ergo sum - лат. "Я мыслю, следовательно, существую" Р.Декарт

Код Цезаря

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.

[1] Полибий (200-120 гг. до н.э.) древнегреческий историк

ABCDEFGHIJKLMNOPQRSTUVWXYZ **DEFGHIJKLMNOPQRSTUVWXYZABC**

YHQL YLGL YLFL
Veni vidi vici - “Пришел, увидел победил"
Ю.Цезарь Донесение Сенату о победе над понтийским царем

Шифр Цезаря относится к так называемому классу *моноалфавитных подстановок* и имеет множество модификаций.

Решетка Кардано

Широко известны шифры, принадлежащие к классу *перестановка,* в частности “*решетка Кардано*”[2]. Это прямоугольная карточка с отверстиями, чаще всего квадратная, которая при наложении на лист бумаги оставляет открытыми лишь некоторые его части. Число строк и столбцов на карточке четно. Карточка сделана так, что при последовательном ее поворачивании каждая клетка лежащего под ней листа окажется занятой. Карточку поворачивают сначала вдоль вертикальной оси симметрии на 180°, а затем вдоль горизонтально оси также на 180°. И вновь повторяют ту же процедуру.

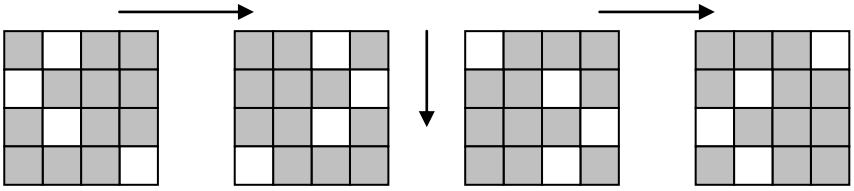


Рис. 1.4. Решетка Кардано

[2] Кардано Джероламо (1501-1576) - итальянский математик, философ и врач

Диск Альберти

Итальянец Альберти (XVI в.) впервые выдвинул идею "двойного шифрования" – текст, полученный в результате первого шифрования, подвергался повторному зашифрованию. В трактате Альберти был приведен его собственный шифр, который он назвал "шифром, достойным королей". Он утверждал, что этот шифр недешифруем. Реализация шифра осуществлялась с помощью шифровального диска, положившего начало целой серии *многоалфавитных подстановок*. Устройство представляло собой пару дисков – внешний, неподвижный (на нем были нанесены буквы в естественном порядке и цифры от 1 до 4) и внутренний – подвижный – на нем буквы были переставлены. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замену ее на соответствующую (стоящую под ней) букву шифрованного текста. После шифрования нескольких слов внутренний диск сдвигался на один шаг. Ключом данного шифра являлся порядок расположения букв на внутреннем диске и его начальное положение относительно внешнего диска.

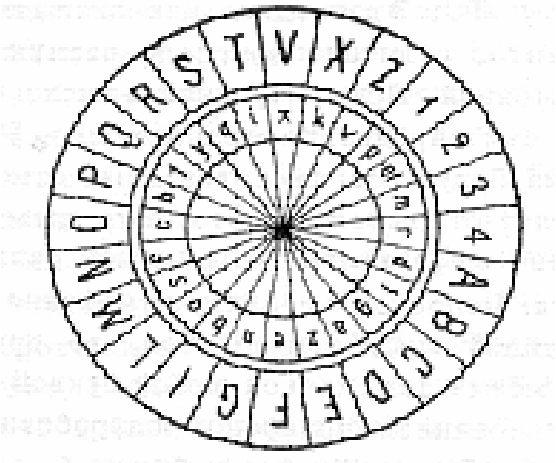


Рис. 1.5. Диск Альберти

Таблица Виженера

Неудобство рассмотренных выше шрифтов моноалфавитных подстановок очевидно, так как в случае использования стандартного алфавита таблица частот встречаемости букв алфавита позволяет определить один или несколько символов, а этого иногда достаточно для вскрытия шифра (“Плящущие человечки” Конан Дойля или “Золотой жук” Эдгара По). Поэтому использовались различные приемы для того чтобы затруднить дешифрование, например использование “*таблицы Виженера”*, которая представляет собой квадратную таблицу с числом строк и столбцов равным количеству букв алфавита. Чтобы зашифровать какое-либо сообщение выбирают слово – лозунг (например, “монастырь”) и надписывают его над сообщением с необходимым повторением.

Чтобы получить шифрованный текст, находят очередной знак лозунга, начиная с первого в вертикальном алфавите, а ему соответствующий знак сообщения в горизонтальном алфавите. На пересечении выделенных столбца и строки находим первую букву шифра. Очевидно, что ключом к такому шифру является используемый лозунг.

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[3]

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ
БВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯА
ВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБ
ГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВ
ДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯФБВГ
ЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯФБВГД
ЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯФБВГДЕ
ЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖ
ИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗ
ЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИ
КЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙ
ЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙК
МНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛ
НОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМ
ОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМН
ПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНО
РСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОП
СТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПР
ТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРС
УФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТ
ФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУ
ХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФ
ЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХ
ЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦ
ШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧ
ЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШ
ЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩ
ЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬ
ЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧЩШЬЫ
ЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭ
ЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮ

[3] Блез де Виженер (1523-1596) - французский посол в Риме, написал большой труд о шифрах. Квадратный шифр Виженера на протяжении почти 400 лет не был дешифрован, считался недешифруемым шифром

Одноразовый шифровальный блокнот

Примером нераскрываемого шифра может служить так называемый *одноразовый шифровальный блокнот* – шифр, в основе которого лежит та же идея, что в шифре Цезаря. Назовем *расширенным алфавитом* множество букв алфавита и знаков препинания **{** *. , : ; ! ? () – “ <пробел>*}, число символов расширенного кириллического алфавита в данном варианте будет равно *44*. Занумеруем символы расширенного алфавита числами от *0* до *43*. Тогда любой передаваемый текст можно рассматривать как последовательность $\{a_n\}$ чисел множества $A=\{0,1,2,\ldots,43\}$.

Предположим, что имеем случайную последовательность $\{c_n\}$ из чисел множества *A* той же длины, что и передаваемый текст – *ключ*. Складывая по модулю *44* число из передаваемого текста a_n с соответствующим числом из множества ключа c_n:

$$a_n + c_n \equiv b_n \ (mod\ 44),\ 0<=b_n<=43$$

получим последовательность $\{b_n\}$ знаков шифрованного текста. Чтобы получить передаваемый текст, можно воспользоваться тем же ключом:

$$a_n \equiv b_n - c_n \ (mod\ 44),\ 0<=a_n<=43$$

У двух абонентов, находящихся в секретной переписке, имеются два одинаковых блокнота. В каждом из них на нескольких листах напечатана случайная последовательность чисел множества *A*. Отправитель свой текст шифрует, указанным выше способом, при помощи первой страницы блокнота. Зашифровав сообщение, он уничтожает использованную страницу и отправляет текст сообщения второму абоненту, получатель шифрованного текста расшифровывает его и также уничтожает

использованный лист блокнота. Нетрудно видеть, что одноразовый шифр не раскрываем в принципе, так как символ в тексте может быть заменен любым другим символом и этот выбор совершенно случаен.

1.3. Методы шифрования

1.3.1.Одноалфавитный метод

Данный метод, пожалуй, самый древний из всех известных методов. В его основе лежит простой способ шифрования: отправитель и получатель зашифрованного документа заранее договариваются об определенном смещении букв относительно их обычного местоположения в алфавите. Например, для кириллицы, если смещение равно 1, то “А” соответствует букве “Б”, “Б” – “В”, и так далее, а когда алфавит подходит к концу, то начинают брать буквы из начала списка. И выходит, например, следующее: из слова “КОДИРОВАНИЕ” получается “ЛПЕЙСПГБОЙЖ”.

Частным случаем данного метода является ранее рассмотренный шифр Цезаря. Очевидно, что произвольный шифр из класса одноалфавитных методов не является шифром Цезаря (если мощность алфавита текста равна n, то число шифров Цезаря равно n, а число всех одноалфавитных шифров равно $n!$).Однако и для таких методов легко предложить способы дешифрования, основанные на статистических свойствах шифрованных текстов поскольку открытый и закрытый тексты имеют одинаковые статистические характеристики.

В лабораторной работе № 1 рассматриваются два варианта одноалфавитного метода с фиксированным смещением и с произвольным (задаваемым) смещением.

1.3.2.Шифрование методом перестановки символов

Суть этого метода заключается в том, что символы текста переставляются по определенным правилам, при этом используются только символы исходного (незашифрованного) текста.

Перестановки в классической криптографии обычно получаются в результате записи исходного текста и чтения шифрованного текста по разным путям геометрической фигуры.

Простейшим примером перестановки является запись исходного текста по строкам некоторой матрицы и чтение его по столбцам этой матрицы.

Последовательность заполнения строк и чтения столбцов может быть любой и задается ключом. Таким образом, для матрицы размером 8*8 (длина блока 64 символа) возможно $1.6*10^{9}$ ключей, что позволяет на современных компьютерах путем перебора дешифровать заданный текст. Однако для матрицы размером 16*16 (длина блока 256 символов) имеется $1.4*10^{26}$ ключей, и перебор их с помощью современных вычислительных средств весьма затруднителен.

Примером применения метода перестановки может быть также восьмиэлементная таблица, обладающая совокупностью маршрутов, носящих название маршрутов Гамильтона. Последовательность заполнения таблицы каждый раз соответствует нумерации ее элементов. Если длина шифруемого текста не кратна числу элементов, то при последнем заполнении в свободные элементы заносится произвольный символ. Выборка из таблицы для каждого заполнения может выполняться по своему маршруту, при этом маршруты могут использоваться как последовательно, так и в порядке, задаваемом ключом.

Для методов перестановки характерны простота алгоритма, возможность программной реализации и низкий уровень защиты, так

как при большой длине исходного текста в его зашифрованном варианте проявляются статистические закономерности ключа, что и позволяет его быстро раскрыть. Другой недостаток этих методов – легкое раскрытие, если удается направить в систему для шифрования несколько специально подобранных сообщений. Так, если длина блока в исходном тексте равна *K* символам, то для раскрытия ключа достаточно пропустить через шифровальную систему *K-1* блоков исходного текста, в которых все символы, кроме одного, одинаковы.

1.3.3.Шифрование инверсными символами (по дополнению до 255)

Данный метод шифрования, является частным случаем одноалфавитной замены в алфавите мощности 256. Суть метода заключается в замене символа *ASCII*-кодировки с номером *i* на символ с номером *255-i.* Аналогично проводится и операция расшифрования.

1.3.4.Многоалфавитные методы шифрования

Многоалфавитное шифрование (многоалфавитная замена) заключается в том, что для последовательных символов шифруемого текста используются одноалфавитные методы с различными ключами.

Например, первый символ заменяется по методу Цезаря со смещением 14, второй – со смещением 10, и так далее до конца заданного ключа. Затем процедура продолжается периодически. Более общей является ситуация, когда используется не шифр Цезаря, а последовательность произвольных подстановок, соответствующих одноалфавитным методам.

Более наглядным примером подобного шифрования является метод гаммирования. Данный способ преобразования заключается в том, что символы закрываемого текста последовательно складываются с символами

некоторой специальной последовательности именуемой гаммой. Такое преобразование иногда называют наложением гаммы на открытый текст.

Собственно процедура наложения может осуществляться одним из двух способов:

1) Символы закрываемого текста и гаммы заменяются цифровыми эквивалентами а затем складываются по модулю K, где K – количество символов алфавита,

$$T_ш = (T_o \oplus T_г) \bmod K$$

где $T_ш$ – шифротекст,

T_o – открытый текст,

$T_г$ – гамма.

2) Символы текста и гаммы представляются в двоичных кодах, а затем каждая пара двоичных разрядов складывается по модулю 2.

Стойкость шифрования методом гаммирования определяется, главным образом, качеством гаммы, которое определяется двумя характеристиками: длиною периода и случайностью распределения по периоду.

Длиною периода гаммы называется минимальное количество символов, после которого последовательность начинает повторяться. Случайность распределения символов по периоду означает отсутствие закономерностей между появлением различных символов в пределах периода.

В лабораторной работе № 1 рассматриваются три варианта многоалфавитного метода – с фиксированным ключом, с ключом фиксированной длины и с ключом произвольной длины.

1.3.5. Основные требования, которые предъявляются к методам шифрования информации

1) Сложность и трудоемкость процедур шифрования и расшифрования должны определяться в зависимости от степени секретности защищаемых данных.
2) Надежность закрытия должна быть такой, чтобы секретность не нарушалась даже в том случае, когда злоумышленнику известен способ закрытия.
3) Способ закрытия и набор используемых служебных данных (ключевых установок) не должны быть слишком сложными. Затраты на защитные преобразования должны быть приемлемые при заданном уровне сохранности информации.
4) Выполнение процедур прямого и обратного преобразования должно быть формальным и как можно проще.
5) Процедуры прямого и обратного преобразования не должны зависеть от длины сообщения.
6) Ошибки, возникающие в процессе преобразования, не должны распространяться по системе и вызывать потерю информации. Из-за появления ошибок передачи зашифрованного сообщения по каналам связи не должна исключаться возможность надежной расшифровки текста на приемном конце.
7) Избыточность сообщений, вносимая закрытием должна быть как можно меньшей.
8) Объем ключа не должен затруднять его запоминание и пересылку.

1.3.6. Гистограмма текста

Одним из наиболее известных методов криптоанализа является изучение статистических характеристик шифрованных текстов. Графическое отображение совокупности частот встречаемости символов в тексте называют гистограммой этого текста.

Предположим, что мы имеем дело с методом одноалфавитного шифрования. Зная частоту встречаемости букв в алфавите, можно предположить, какая буква была заменена на данную. Например, часто встречаемая буква “О” заменена на редко встречающуюся букву “Щ”.

Для наглядности, в лабораторной работе № 1 используются двойные гистограммы, отображающие частоту встречаемости символов в исходном и зашифрованном текстах.

Следует иметь в виду, что вид гистограммы для стандартного распределения зависит от вида исходного текста следующим образом: если исходный текст содержит символы кириллицы и латинского алфавита, то выводится статистическое распределение для кириллицы и латиницы, если только кириллицы (латиницы) то выводится статистическое распределение для кириллицы (латиницы).

ЛАБОРАТОРНАЯ РАБОТА №1

ИСПОЛЬЗОВАНИЕ КЛАССИЧЕСКИХ КРИПТОАЛГОРИТМОВ ПОДСТАНОВКИ И ПЕРЕСТАНОВКИ ДЛЯ ЗАЩИТЫ ТЕКСТОВОЙ ИНФОРМАЦИИ

Цель работы: Изучение классических криптографических алгоритмов моноалфавитной подстановки, многоалфавитной подстановки и перестановки для защиты текстовой информации. Использование гистограмм, отображающих частоту встречаемости символов в тексте для криптоанализа классических шифров.

1. Описание лабораторной работы

Для выполнения лабораторной работы необходимо запустить программу *L_LUX.EXE.* На экране дисплея появляется окно, с размещенным в его центре текстовым редактором (для отображения зашифрованных и расшифрованных текстов), в верхней строке окна расположено главное меню, позволяющее пользователю выполнить требуемое действие, чуть ниже основного меню расположена панель инструментов (для управления быстрыми командными кнопками и другими “горячими” элементами управления), а в самом низу окна, под текстовым редактором, находится строка состояния, в которой указывается подсказка и выводится дополнительная информация. Клавиши панели инструментов, для удобства, снабжены всплывающими подсказками.

Для того чтобы попасть в основное меню, необходимо нажать клавишу *F10.* Передвижение по главному меню осуществляется клавишами перемещения курсора. Чтобы вызвать пункт меню, нужно нажать клавишу “ENTER”, вернуться в главное меню или вовсе выйти из него – “ESC”.

А теперь более подробно рассмотрим каждый из пунктов главного меню.

1.1. Редактор

Данный пункт основного меню содержит подпункты: создать документ, открыть файл, сохранить файл, выход из программы.

Предварительно, сразу после запуска программы, текстовый редактор недоступен, также недоступными являются почти все пункты главного меню (кроме создания документа, открытия файла, выхода из программы, информации о программе) и большая часть клавиш панели управления (за исключением создания документа, открытия файла и выхода из программы).

Создать документ (Ctrl+N) – данный подпункт делает доступным для работы тестовый редактор (пользователь получает право создать свой текстовый файл, который впоследствии можно будет использовать при работе с программой), также появляется возможность использовать все недоступные до этого пункты основного меню и клавиши панели управления.

Открыть файл (Ctrl+L) – при выборе этого пункта появляется диалоговое окно, предоставляющее возможность выбора файла для загрузки. При этом содержимое файла будет отображено в окне редактора текстов.

Аналогично пункту “Создать документ” доступным для работы становится текстовый редактор с отображаемым текстом, а также появляется возможность использовать все недоступные до этого пункты основного меню и клавиши панели управления.

Сохранить файл (Ctrl+S) - при выборе этого пункта появляется диалоговое окно, позволяющее сохранить на диск содержимое редактора текстов.

Выход из программы (Ctrl+X) - при выборе этого пункта появляется диалоговое окно, позволяющее выйти из программы.

1.2. Гистограмма

Вывод на экран двух гистограмм, отображающих частоту встречаемости символов в тексте.

> ***Внимани !*** *До выполнения шифрования и дешифрования вызывать гистограмму не имеет смысла, так как еще не сформированы тексты, для которых будет просматриваться гистограмма.*

Имеется возможность просмотра следующих сочетаний гистограмм:

- гистограммы исходного и зашифрованного файла,
- гистограммы зашифрованного и расшифрованного файла,
- гистограммы стандартного распределения и зашифрованного текста,
- гистограммы стандартного распределения и расшифрованного текста.

В гистограммах с целью масштабирования используются левая и правая клавиши мыши.

Например, после шифрования текста большого объема пользователь хочет посмотреть гистограммы исходного и зашифрованного файла. Поскольку размеры текста достаточно большие, то на экран будут выведены две гистограммы с большим количеством столбцов в каждой (столбец соответствует одному символу текста), однако трудно будет сказать, какой из этих столбцов соответствует тому или иному символу текста, и какова частота встречаемости данного символа. Поэтому у пользователя есть возможность увеличить масштаб любой из двух гистограмм с целью более точного определения требуемого значения частоты встречаемости конкретного символа. Для этого необходимо навести указатель мыши на левую границу того участка гистограммы, который требуется увеличить, затем нажать левую клавишу мыши, и не отпуская ее растянуть прямоугольник так, чтобы его нижний правый угол совпал с правой границей увеличиваемого участка гистограммы. После

этого следует отпустить левую клавишу мыши и на экране появится увеличенное изображение нужного участка.

Причем, нажав и не отпуская правую клавишу мыши, можно перемещать гистограмму в любом направлении с целью изучения всего полученного распределения в увеличенном масштабе.

Для того, чтобы от увеличенного масштаба вернуться к исходному виду, нужно навести указатель мыши на гистограмму, затем нажать левую клавишу мыши, и, не отпуская ее, снизу вверх растянуть небольшой по размерам прямоугольник, после этого следует отпустить левую клавишу мыши и на экране появится исходное изображение гистограммы.

1.3.Шифрование

Выполнение шифрования текстового файла осуществляется одним из семи методов, рассматриваемых в лабораторной работе.

1. Одноалфавитный метод (с фиксированным смещением).
2. Одноалфавитный метод с задаваемым смещением (от 2 до 20).
3. Перестановка символов.
4. По дополнению до 255 (инверсный метод).
5. Многоалфавитный метод (с фиксированным ключом).
6. Многоалфавитный метод с ключом фиксированной длины.
7. Многоалфавитный метод с ключом произвольной длины.

Выбор метода шифрования производится как мышкой, так и клавишами перемещения курсора и клавишей “ENTER”.

Затем появляется окно в котором в зависимости от метода шифрования требуется указать те или иные параметры, и либо подтвердить процесс

кодировки, либо отказаться от него. После этого в окне редактора будет выдан зашифрованный текст.

1.4. Расшифрование

Аналогично предыдущему пункту выбирается метод расшифрования (должен соответствовать методу, которым был зашифрован файл).

Снова появляется окно, в котором в зависимости от метода расшифрования требуется указать те или иные параметры, и либо подтвердить процесс расшифрования, либо отказаться от него.

После этого в окно редактора будет выдан расшифрованный текст. При правильном расшифровании, полученный текст совпадает с исходным.

1.5. Дополнительная информация

Программа предусматривает возможность посмотреть дополнительную информацию ('Помощь Ctrl+F9'), справочную информацию об используемых методах шифрования ('О методах Ctrl+F10'), сведения о программе ('О программе Ctrl+F11').

Пример работы с программой

В качестве примера рассмотрим одноалфавитное шифрование с фиксированным ключом.

Нажав клавиши Ctrl+L, либо выбрав в меню пункт «Открыть файл», загрузите в окно редактора исходный текст.

Затем вызовите пункт меню «Шифрование», выберите одноалфавитный метод (с фиксированным смещением). В появившемся окне нажмите клавишу «Зашифровать». После того, как шифрование выполнено, можно также просмотреть в редакторе зашифрованный текст.

Перейдите к пункту меню «Гистограмма». Выберите тип гистограмм, отображающий гистограммы исходного и шифрованного файлов. Проанализируйте гистограммы. Они должны иметь примерно одинаковый вид.

Чтобы узнать ключ шифра, (смещение второго алфавита относительно первого), необходимо найти по гистограммам символы, имеющие одинаковую частоту встречаемости. Например, самый частый символ в первой гистограмме при шифровании должен перейти в самый частый символ во второй гистограмме.

Таким образом, найдя два самых часто встречаемых символа в обеих гистограммах, можно по стандартной таблице *ASCII* кодов вычислить смещение.
Зная смещение и таблицу кодировки символов, текст можно легко расшифровать.
Вызвав пункт меню «Дешифрование», можно провести те же действия в автоматическом режиме.

Примечание: при шифровании и расшифровании из таблицы кодировки не используются символы с кодами: 176 – 223 и 240 – 255. То есть при ручной расшифровке эти символы следует пропускать, и считать, что, например, символ « Я » имеет код не 159, а – 223, аналогично « п » не 175, а – 239.

Иногда в гистограммах под столбцами, показывающими частоту встречаемости символов, изображены не сами символы, а их табличные коды в квадратных скобках.

Описание "горячих клавиш":

Shift+F10 - ‘О программе’
Ctrl+X - ‘Выход из программы’
Ctrl+N - New - ‘Файл\Создать’
Ctrl+L - Load - ‘Файл\Открыть’
Ctrl+S - Save - ‘Файл\Сохранить’

Шифрование:

Ctrl+F1 - ‘Одноалфавитный метод (с фиксированным смещением)’

Ctrl+F2 - ‘Одноалфавитный с задаваемым смещением (от 2 до 20)’

Ctrl+F3 - ‘Перестановка символов’

Ctrl+F4 - ‘По дополнению до 255 (инверсный метод)’

Ctrl+F5 - ‘Многоалфавитный метод с фиксированным ключом’

Ctrl+F6 - ‘Многоалфавитный метод с ключом фиксированной длины‘

Ctrl+F7 - ‘Многоалфавитный метод с ключом произвольной длины ‘

Расшифрование:

Shift+F1 - ‘Одноалфавитный метод (с фиксированным смещением)’

Shift+F2 - ‘Одноалфавитный с задаваемым смещением (от 2 до 20)’

Shift+F3 - ‘Перестановка символов’

Shift+F4 - ‘По дополнению до 255 (инверсный метод)’

Shift+F5 - ‘Многоалфавитный метод с фиксированным ключом’

Shift+F6 - ‘Многоалфавитный метод с ключом фиксированной длины‘

Shift+F7 - ‘Многоалфавитный метод с ключом произвольной длины‘

Гистограммы:

Shift+Ctrl+F1 - ‘Исходного и шифрованного файла‘

Shift+Ctrl+F2 - ‘Шифрованного и расшифрованного файла‘

Shift+Ctrl+F3 - ‘Стандартного распределения и шифрованного текста‘

Shift+Ctrl+F4 - ‘Стандартного распределения и расшифрованного текста‘

Помощь:

Ctrl+F9 - 'Помощь'

Ctrl+F10 - 'О методах'

Ctrl+F11 - 'О программе'

2. Задание

1. Ознакомиться с описанием лабораторной работы и заданием.
2. Для одноалфавитного метода с фиксированным смещением определить установленное в программе смещение.

   Для этого:

   – просмотреть предварительно созданный с помощью редактора свой текстовый файл;

- выполнить для этого файла шифрование;
- просмотреть в редакторе зашифрованный файл;
- просмотреть гистограммы исходного и зашифрованного текстов,
- описать гистограммы (в чем похожи, чем отличаются) и определить, с каким смещением было выполнено шифрование;
- расшифровать зашифрованный текст:
  1) с помощью программы, после чего проверить в редакторе правильность расшифрования;
  2) вручную с помощью гистограмм; описать и объяснить процесс дешифрования.

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов, описываются полученные гистограммы, указывается найденное смещение, описывается процесс дешифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные и созданные файлы.

3. Для одноалфавитного метода с задаваемым смещением (шифр Цезаря):
   - для своего исходного текста выполнить шифрование с произвольным смещением;
   - просмотреть и описать гистограммы исходного и зашифрованного текстов, определить смещение для нескольких символов;
   - расшифровать текст с помощью программы;
   - имеется зашифрованный шифром Цезаря текст; дешифровать его с помощью программы методом подбора смещения; указать, с каким смещением был зашифрован файл.
4. Для метода перестановки символов дешифровать зашифрованный файл.

Для этого необходимо определить закон перестановки символов открытого текста. Создайте небольшой файл длиной в несколько слов с известным вам текстом, зашифруйте его, просмотрите гистограммы (опишите их; ответьте, можно ли извлечь из них полезную для дешифрации информацию). Сравните (с помощью редактора) ваш исходный и зашифрованный тексты и определите закон перестановки символов.

Дешифруйте файл:

1) вручную (объясните ваши действия);

2) с помощью программы.

5. Для инверсного кодирования (по дополнению до 255):
   - для своего произвольного файла выполните шифрование;
   - просмотрите гистограммы исходного и зашифрованного текстов, опишите гистограммы и определите смещение для нескольких символов;
   - дешифруйте зашифрованный текст, проверьте в редакторе правильность дешифрования.

6. Привести в отчете ответы на контрольные вопросы, в соответствии с номером варианта, указанным преподавателем.

Номер варианта	**Контрольные вопросы**
1,5,7, 3,9,18,28	Какие вы знаете методы криптографической защиты файлов?
2,4,6,8, 20,22,24, 26,30	В чем преимущества и недостатки одноалфавитных методов?
11,13,15, 10,17,19, 27	Если вам необходимо зашифровать текст, содержащий важную информацию, какой метод, из рассмотренных, вы выберете? Обоснуйте свой выбор.
12,14,16 21,23.25, 29	Целесообразно ли повторно применять для уже зашифрованного текста: а) метод многоалфавитного шифрования? б) метод Цезаря?

Список литературы

1. Бабаш А.В., Шанкин Г.П. Криптография. / Под редакцией В.П.Шерстюка, Э.А. Применко. – М.: СОЛОН-Р, 2007. – 512 с.
2. Бабаш А.В. Криптографические и теоретико-автоматные аспекты современной защиты информации. Криптографические методы защиты. – М.: Изд.центр ЕАОИ, 2009. – 414 с.
3. Баранова Е.К. Эффективное кодирование и защита информации: Текст лекций для студентов специальности 510200. – М.: МГУЛ, 2002. – 88 с.
4. Башлы П.Н., Бабаш А.В., Баранова Е.К. Информационная безопасность: учебно-практическое пособие – М.: Изд.центр ЕАОИ, 2010. – 376 с.
5. Мельников В.В. Защита информации в компьютерных системах. М.: Финансы и статистика; Электроинформ, 1997. 368 с.
6. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001. – 376 с.
7. Смарт Н. Криптография. – М.: Техносфера, 2006. – 528 с.