Лабораторная работа 4. Исследование классических криптоалгоритмов подстановки и перестановки для защиты информации

Цель и содержание: Исследование свойств классических криптографических алгоритмов многоалфавитной подстановки, многоалфавитной подстановки и перестановки для защиты текстовой информации. Использование в исследовании гистограмм, отображающих частоту встречаемости символов в тексте для криптоанализа классических шифров.

1. Теоретическая часть

Метод подстановки, 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 шифр 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. Шифр Цезаря относится к так называемому классу *одноалфавитных подстановок* и имеет множество модификаций.

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.

Суть этого перестановки 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.

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”.

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).

2. Задания к лабораторной работе

Для выполнения лабораторной работы необходимо запустить программу L_LUX (выдает преподаватель). На экране дисплея появится окно с размещенным в его центре текстовым редактором. В верхней строке окна расположено главное меню, позволяющее пользователю выполнить требуемое действие. Чуть ниже основного меню расположена панель инструментов, 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, не обходимо нажать клавишу F10. Передвижение по главному меню осуществляется мышью.

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.

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.

Гистограмма

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

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.

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 до20).
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.

Дешифрование

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

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

После этого в окно редактора будет выдан дешифрованный текст.

При правильном дешифровании, полученный текст совпадает с исходным.

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 программеCtrl+F11').

Пример работы с программой. Рассмотрим одноалфавитное шифрование с фиксированным ключом.

Загрузите в окно редактора исходный текст (любой) длиной от 10 до 15 предложений. Сохраните его, это необходимо для последующей работы с этим файлом. Затем вызовите пункт меню ШИФРОВАНИЕ, выберите одноалфавитный метод (с фиксированным смещением). В появившемся окне нажмите клавишу ЗАШИФРОВАТЬ. После того как шифрование выполнено, можно в редакторе просмотреть зашифрованный текст.

Перейдите к пункту меню ГИСТОГРАММА. Выберите тип гистограмм, отображающий гисторраммы исходного и шифрованного текста. Проанализируйте гистограммы. Они должны иметь примерно одинаковый вид.

Чтобы узнать ключ шифра (смещение второго алфавита относительно первого), необходимо по гистограммам найти 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 дешифровать. Вызвав меню ДЕШИФРОВАНИЕ, можно провести те же действия в автоматическом режиме.

Примечание. При шифровании и дешифровании 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 159, а 223, аналогично П не 175, а 239.

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

Задание 1. Ознакомиться с описанием лабораторной работы и заданиями.

Задание 2. Для одноалфавитного метода с фиксированным смещением определить установленное в программе смещение. Для этого следует:

- 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, в чем отличаются) и определить, с каким смещением было выполнено шифрование;

- расшифровать зашифрованный текст:

С помощью гистограммы, после чего проверить в редакторе правильность расшифрования;

Вручную с помощью гистограмм, описать и объяснить процесс дешифрования.

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

В отчет предоставить ход проделанной работе и все использованные и созданные файлы.

Задание 3. Для одноалфавитного метода с заданным смещением (шифр Цезаря) следует:

- выполнить шифрование с произвольным смещением для своего исходного текста;

- просмотреть и описать гистограммы исходного и зашифрованного текстов, определить смещение для нескольких символов;

- расшифровать текст с помощью программы;

- дешифровать зашифрованный шифром Цезаря текст с помощью программы методом перебора смещения; указать в отчете с каким смещением был зашифрован файл.

Задание 4. Для метода перестановки символов дешифровать зашифрованный файл. Для этого необходимо определить закон перестановки символов открытого текста. Создайте небольшой файл длиной в несколько символов с известным вам текстом, зашифруйте его. Посмотрите гистограммы, опишите их, ответьте можно ли извлечь из них полезную для дешифрования информацию. Сравните с помощью редактора ваш исходный текст и зашифрованный текст и определите закон перестановки символов.

Дешифруйте файл:

- вручную и объясните ваши действия;

- с помощью программы.

Задание 5. Для инверсного кодирования (по дополнению до 255)

- выполните шифрование для своего произвольного файла;

- посмотрите гистограммы исходного и зашифрованного текстов, опишите гистограммы и определите смещение для нескольких символов;

- дешифруйте зашифрованный текст, проверьте в редакторе правильность дешифрования.

Задание 6. Для многоалфавитного шифрования с фиксированным ключом определите, сколько одноалфавитных методов и с каким смещением используется в программе. Для этого нужно создать свой файл, состоящий из строки одинаковых символов, выполнить для него шифрование и по гистограмме определить способ шифрования и набор смещений.

Задание 7. Для многоалфавитного шифрования с ключом

фиксированной длины:

- выполните шифрование и определите по гистограмме, какое смещение получает каждый символ для файла, состоящего из строки одинаковых символов;

- выполните шифрование и расшифрование для файла произвольно текста;

- просмотрите и опишите гистограммы исходного и зашифрованного текстов; ответьте, какую информацию можно получить из гистограмм.

Задание 8. Для многоалфавитного шифрования с произвольным паролем задание полностью аналогично п. 7.

Отчет должен содержать:

- наименование работы;

- цель работы;

- рабочие схемы, основные соотношения и расчетные формулы, таблицы;

- выводы по работе.

Задания для самостоятельной работы

1. Укажите в письменной форме, какова стойкость шифра перестановки.

2. Укажите в письменной форме, какова стойкость шифра подстановки.

3. Укажите в письменной форме, какую информацию можно получить из гистограмм.

Вопросы к лабораторной работе

1. В чем преимущества и недостатки одноалфавитных методов?

2. Если необходимо зашифровать текст, содержащий важную информацию, какой метод вы выберете?

3. Целесообразно ли повторно применять для уже зашифрованного текста: а) метод много алфавитного шифрования; б) метод Цезаря?