Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования „Санкт-Петербургский
государственный политехнический университет“

Институт информационных технологий и управления
Кафедра „Распределенные вычисления и компьютерные сети“

КУРСОВАЯ РАБОТА

по дисциплине: Информатика

на тему: Моноалфавитный подстановочный шифр и частотный анализ

Выполнил
студент гр. 13507/1 <подпись> Б.О Борисов

Руководитель
доцент <подпись> А.А Овчинников

Санкт-Петербург
2014

Содержание

1 Введение

1.1 Постановка задач

В данной курсовой работе необходимо:

- Реализовать моноалфавитный подстановочный шифр
- Реализовать частотный анализ

1.2 Описание области

Прежде чем мы будем говорить о моноалфавитном шифре и частотном анализе, сначала рассмотрим само понятие шифр и зачем он нужен.

Шифр (от фр. chiffre „цифра“) — какая-либо система преобразования текста с секретом (ключом) для обеспечения секретности передаваемой информации. Шифры применяются для тайной переписки дипломатических представителей со своими правительствами, в вооруженных силах для передачи текста секретных документов по техническим средствам связи, банками для обеспечения безопасности транзакций, а также некоторыми интернет-сервисами по различным причинам.

Шифр может представлять собой совокупность условных знаков (условная азбука из цифр или букв) либо алгоритм преобразования обычных цифр и букв. Процесс засекречивания сообщения с помощью шифра называется шифрованием. Наука о создании и использовании шифров называется криптографией. Криптоанализ — наука о методах получения исходного значения зашифрованной информации. Важным параметром любого шифра является ключ — параметр криптографического алгоритма, обеспечивающий выбор одного преобразования из совокупности преобразований, возможных для этого алгоритма. На сегодняшний день существует множество различных шифров, которые используются для засекречивания важной информации, но мы остановимся толька на моноалфавитном шифре. Моноалфавитный шифр является одним из четырех типов подстановочного шифра.

Подстановочным шифром называется шифр, который каждый символ открытого текста в шифротексте заменяет другим символом. Получатель инвертирует подстановку шифротекста, восстанавливая открытый текст. Как говорилось выше, в классической криптографии существует четыре типа подстановочных шифров:[3]

- **Простой подстановочный шифр** или **моноалфавитный шифр** - это шифр, который каждый символ открытого текста заменяет соответствующим символом шифротекста. Простыми подстановочными шифрами являются криптограммы в газетах.

- **Однозвучный подстановочный шифр** похож на простую подстановочную криптосистему за исключением того, что один символ открытого текста отображается на несколько символов шифротекста. Например, „A“ может соответствовать 5,13,25 или 56, „B“ - 7,19,31 и так далее.

- **Полиграммный подстановочный шифр** - это шифр, который блоки символов шифрует по группам. Например, „ABA“ может соответствовать „RTQ“, „ABB“ и так далее.

- **Полиалфавитный подстановочный шифр** состоит из нескольких простых подстановочных шифров. Например, могут быть использованы пять различных простых подстановочных фильтров; каждый символ открытого текста заменяется с использованием одного конкретного шифра.

Знаменитый **шифр Цезаря**, в котором каждый символ открытого текста заменяется символом, находящегося тремя символами правее по модулю 26 („A“ заменяется на „D“,“B“ - на „E“...“Z“ - на „C“), представляет собой простой подстановочный фильтр. Он действительно очень прост, так как алфавит шифротекста представляет собой смещенный, а не случайно распределенный алфавит открытого текста.[3] Осталось рассмотреть понятие частотного анализа.

Частотный анализ — один из методов криптоанализа, основывающийся на предположении о существовании нетривиального статистического распределения отдельных символов и их последовательностей как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и дешифрования.

Упрощённо, частотный анализ предполагает, что частота появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка. При этом в случае моноалфавитного шифрования если в шифротексте будет символ с аналогичной вероятностью появления, то можно предположить, что он и является указанной зашифрованной буквой.

2 Основная часть

2.1 Описание алгоритма

Шифр представляет собой программу, которая работает с пятью файлами. Это файлы - key.txt,crypt.txt,input.txt,result.txt,text.txt.

- В файле key.txt - программа случайным образом генерирует ключ из 161 символов таблицы ASCII.
- В файле text.txt - находится текст для частотного анализа
- В файле input.txt - находится исходный текст, который программа будет считывать и шифровать.
- В файл crypt.txt - программа будет записывать шифротекст.
- В файл result.txt - программа запишет результат взлома зашифрованного сообщения в файле crypt

2.1.1 Генерирование ключа

При запуске программы,в первую очередь происходит генерирование ключа. Для этого нам понадобятся библиотека <fstream>- для работы с файлами и оператор srand(time(NULL))- для того чтобы обнулить время и чтобы функция rand() возвращала каждый раз новые значения. Потом заводим несколько массивов, которые генерируют все строчные и прописные буквы русского и английского языка,арабские числа и знаки препинания и заполняем их индексами. Затем делаем еще один массив и 161 раз меняем случайно сгенерированный элемент с очередным.

2.1.2 Шифрование

После генерирования ключа программа непосредственно шифрует исходный текст. Здесь нам потребуется функция int get(), которая позволит нам побайтово считать каждый символ исходного текста, а дальше заносим символ из сгенерированного ключа по индексу считанного символа.

2.1.3 Дешифрование

После шифрования, программа расшифрует шифротекст и запишет другой фаил. Здесь нам также понадобится побайтовое считывание,чтобы считать каждый символ шифротекста и еще массив, который будет считать сколько раз встречается очередной символ в тексте и в шифре.

2.2 Описание реализации

Цель программы - выполнить шифрование открытого текста, дешифрование шифротекста и частотный анализ.

2.2.1 Используемые програмные средства

Программа написана на языке C++ с помощью Microsoft Visual Studio - линейка продуктов компании Microsoft, включающих интегрированную среду разработки програмного обеспечения и ряд других инструментальных средств.

2.2.2 Спецификация

1. При запуске программы выводится консоль, в которой ничего вводить не надо. Программа работает непосредственно с текстовыми файлами. На саму консоль выводится время работы программы.

2. В файле „input.txt“, где располагается исходный текст, написать можно любую последовательность цифр и букв.

2.2.3 Реализация

При запуске программы выполняются следующие действия:

- Генерирование ключа 161 элементов
- Побайтовое считывание каждого символа исходного текста
- Записываем символ из сгенерированного ключа по индексу считанного символа
- Побайтовое считывание каждого символа шифротекста

- Используем индексы шифротекста и исходного текста, взламываем шифр

2.2.4 Функции и библиотеки

Подключенные библиотеки:

- <iostream>
- <fstream>
- <time.h>

Функции:

- void keygen() - генерирует ключ и записывает его в файл key.txt;
- void inkey(int *array) - считывает ключ из файла key.txt для дальнейшего использования в программе;
- void encryption(int *key, int *array) - с помощью ключа шифрует текст;
- void decryption(int *icrypt, int *itext, int *order) - расшифровывает текст;
- void counting(int *array, bool b, int *order) - функция подсчета частоты каждого символа текста.

2.3 Тестирование

Требуется протестировать программу на различных тестах. Результатом программы должен быть взлом зашифрованного сообщения и результат запишется в фаил result.txt. Фаил result.txt должен полностью или частично совпасть с файлом input.txt.

2.3.1 Первый запуск программы:

Программа шифровала первый текст
INTRODUCTION TO A LEGEND OF MONTROSE
Шифротекст
лFJмX)7'JлXFpJXрзрицхцF)рXйргXFJмX:ц
Результат взлома с помощью частотного анализа
RTNIODCLNROT NO S AEUETD OM GOTNIOFE

2.3.2 Второй запуск программы:

Программа шифровала второй текст
Our subject leads us to talk of deadly feuds, and we must begin with one still more ancient than that to which our story relates. During the reign of James IV., a great feud between the powerful families of Drummond and Murray divided Perthshire. The former, being the most numerous and powerful, cooped up eight score of the Murrays in the kirk of Monivaird, and set fire to it. The wives and the children of the ill-fated men, who had also found shelter in the church, perished by the same conflagration. One man, named David Murray, escaped by the humanity of one of the Drummonds, who received him in his arms as he leaped from amongst the flames. As King James IV. ruled with more activity than most of his predecessors, this cruel deed was severely revenged, and several of the perpetrators were beheaded at Stirling. In consequence of the prosecution against his clan, the Drummond by whose assistance David Murray had escaped, fled to Ireland, until, by means of the person whose life he had saved, he was permitted to return to Scotland, where he and his descendants were distinguished by the name of Drummond-Eirinich, or Ernoch, that is, Drummond of Ireland; and the same title was bestowed on their estate.

Шифротекст
EOlбaOTэAo5б]Ал<aбOaб52б5л]Шб2 < <]AO<aЩблz<б!АбшOa5бTАна
zб!a5й2zAбa5a]]бш2lAблzoaAz5б5лzб5л5б52б!aоб2Olба52lЛбlA]л5Aa*бyOlaz
ний5АбlAанzб2$raET * l$5AO<бTA5!AAzб5АбY2!Al]лша]aAай2$l2z < z <
$qll < < < > l5al*G$2lшAlЩбTAazнб5Абш2a5йzOшAl2Oаблz<бY2!Al]22$Y <
$Y5a2l$2б5АбqOllлЛабazб5АбШalШй2$q2zl < z < a$5alАб52ба5*бGАб!ааблz<б5
Абоа]<lAzб25]]л5A<бшAzЩб!2бл<бл]а2б2$z < a$]5lz5lYla < 5a2z]лнlл5a2z*бE
zАбшлzЩбzлшA<бул<бqOllлЛЩбAaолYA<бTЛб5АбOшлza5Лй22z2б5АбylO

шш2z<аЩб!2блАоАа<башбazбааблшаблабАб]АлYА<б$l22za55$]лшАа*бпаб?az нбглшАабЕТ*блО]А<б!а5бш2lАбло5а5Лб5лzбш2а5й2$aYl < aa2la5al] < < !$aal]lz < z < al$]2б5АбYАlYА5лл52lаб!АlАбТААл<А<бл5б05al]azн*бЕzбо2za A_{z2}б5АйYl2аАоО5а2zблнлаza5бааб0]лzЩб5АбylОшш2z<бТЛб!2аАблаааа5лzо Абул<йqОllлЛбл<бАаолYА<Щб] < 52El]z < z5]za2б5АбYАla2zб!2аАй]a < a < !aYl55 < 52$l5lz$52025]z < !lz < a < az < z5a!l < a5za < 5z2бylОшш2z<ыXа lazaоЩб2lйXlz2оЩб5л5бааЩбylОшш2z<б2El]z < z < 5a55]!aa52! < 2z5la55∗

Результат взлома с помощью частотного анализа

Sur subPect leads us to talk of deadly feuds, and we must begin with one still more ancient than that to which our story relates. During the reign of Tames M-., a great feud between the powerful families of Drummond and Iurray divided Aerthshire. Vhe former, being the most numerous and powerful, cooped up eight score of the Iurrays in the kirk of Ionivaird, and set fire to it. Vhe wives and the children of the illEfated men, who had also found shelter in the church, perished by the same conflagration. Sne man, named David Iurray, escaped by the humanity of one of the Drummonds, who received him in his arms as he leaped from amongst the flames. js King Tames M-. ruled with more activity than most of his predecessors, this cruel deed was severely revenged, and several of the perpetrators were beheaded at Jtirling. Mn conse;uence of the prosecution against his clan, the Drummond by whose assistance David Iurray had escaped, fled to Mreland, until, by means of the person whose life he had saved, he was permitted to return to Jcotland, where he and his descendants were distinguished by the name of DrummondEOirinich, or Ornoch, that is, Drummond of Mrelandq and the same title was bestowed on their estate.

2.3.3 Третий запуск программы:

Программа шифровала третий текст

Гостиная Анны Павловны начала понемногу наполняться. Приехала высшая знать Петербурга, люди самые разнородные по возрастам и характерам, но одинаковые по обществу, в каком все жили; приехала дочь князя Василия, красавица Элен, заехавшая за отцом, чтобы с ним вместе ехать на праздник посланника. Она была в шифре и бальном платье. Приехала и известная, как la femme la plus s?duisante de P?tersbourg 1, молодая, маленькая княгиня Болконская, прошлую зиму вышедшая замуж и теперь не выезжавшая в большой свет по причине своей беременности, но

ездившая еще на небольшие вечера. Приехал князь Ипполит, сын князя Василия, с Мортемаром, которого он представил; приехал и аббат Морио и многие другие.

Шифротекст

ВраЫЕ,с7ЭШ„йЭ/сЙЬрЙ,йЭ,сВсЬсЭУр,Кж,р6RЭ,сУрЬ,7Ы‘а7ЧЭ/LЕКфс ЬсЭЙйа|с7Э2,сЫ‘Э/КЫKLRL6суЭЬтцЕЭасжйКЭLс2,рLрц,йКЭУрЭЙр2Lса ЫсжЭЕЭфсLс"ЫKLсжуЭ,рЭрцЕ,с"рЙйКЭУрЭраЫЙRуЭЙЭ"с"ржЭЙаКЭf ЕЬЕ$_{YLcc‘\ 727ca7y”Lcacicm,y2cc|c72ciy}a, ac‘, cYLc2, ”Yac, , ”c−, cc|xLc‘, Yc‘/Lcc2a, c7y ”c”l!kkl!qlgssEg < s! > kEkkMs; wgMjyc7yc, ‘”c7 76, 7A”, a”c7yYL|R2R||c72c RfYL‘, 2fc|c7‘|aYYL, aL, , ay, 2|c7, c, ‘|Lc/Lc 72‘YYya, 727ca7yaNLcLy”L6 , YLac$_{YLcc}$cNL, 6LR6$

Результат взлома с помощью частотного анализа

boятинас fнны еавловны начала понекногу наполнстьяс. ериехала выябас знать еетердурга, лdши яакые разнорошные по возраятак и харамтерак, но ошинамовые по одтеятву, в мамок вяе жилищ приехала шочь мнсзс ;аяилис, мраяавиюа Глен, заехавбас за отюок, чтоды я ник вкеяте ехать на празшним пояланнима. Ана дыла в би1ре и дальнок платье. ериехала и извеятнас, мам ua iП??П ua nuls sMцlфsaРВП цП ОМВПйsИрlйg o, колошас, каленьмас мнсгинс Болмонямас, проблyd зику выбешбас закуж и теперь не выезжавбас в дольбor явет по причине явоer дерекенноляти, но езшивбас ete на недольбие вечера. ериехал мнсзь Эпполит, яын мнсзс ;аяилис, я mортекарок, моторого он прешятавилщ приехал и аддат морио и кногие шругие.

2.4 Анализ работы

Исходя из полученных данных можно сказать, что программа шифрует текст по ключу и взламывает его. По проделанным тестам можно увидеть, что результат взлома частично совпадает с исходным текстом.

2.4.1 Время работы программы

Время подсчета 3 запусков программы

№	Время работы	количество символов
1 текст	0.34 seconds	36
2 текст	2.3 seconds	437
3 текст	3.82 seconds	694

Чем больше символов, тем дольше времени программа выполняет свою работу.

3 Заключение

Поставленная задача выполнена. Алгоритм реализован на языке C++. Проделаны 3 теста с разными по объему символов текстовыми файлами, посчитано время работы программы. В ходе проделанной работой был также освоен текстовый редактор [2]

Список литературы

[1] Кнут Д. Искусство программирования.Т.1. Основные алгоритмы, М.: Вильямс, 2007

[2] Львовский С. Latex: Подробное описание.Электронное издание

[3] Шнайер Б. Подстановочные шифы. Прикладная криптография. 2-е изд. Протоколы, алгоритмы и исходные тексты на языке Си.