Министерство связи и массовых коммуникаций Российской Федерации

Государственное образовательное учреждение
высшего профессионального образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

ЭЛЕКТРОННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА

Самара

Кафедра «Информатики и вычислительной техники»

«Сокрытие информации в звуковых WAV-файлах»

Методические указания на проведение лабораторных работ
по дисциплине «Информатика»,
специальности 210400…210406, 210302, 090106.

Авторы-составители:
доц., к.т.н. **Алексеев А.П., Аленин А.А.**
Под общей редакцией Алексеева А.П.

Самара, 2010

Введение

Интерес к стеганографии появился в последнее десятилетие и вызван широким распространением мультимедийных технологий. Методы стеганографии позволяют не только скрытно передавать данные, но и решать задачи помехоустойчивой аутентификации, защиты информации от несанкционированного копирования, отслеживания распространения информации по сетям связи, поиска информации в мультимедийных базах данных, охраны авторских прав. Стеганография – быстро и динамично развивающаяся наука, использующая методы и достижения криптографии, цифровой обработки сигналов, теории связи и информации.

Данные методические указания позволяют приобрести основные навыки работы с программой сокрытия и шифрования информации.

Для повышения криптостойкости использовано пространственное распределение информации по трем контейнерам. Контейнерами являются WAV-файлы.

Лабораторная работа
«Сокрытие информации в звуковых WAV-файлах»

1. Подготовка к работе

По указанной литературе и методическим указаниям изучить основные понятия стеганографии, ознакомиться с интерфейсом и основными возможностями программы Crypto 3A-001. Ответить на контрольные вопросы.

2. Контрольные вопросы

3.1. Какие основные цели и задачи стеганографии?
3.2. Какие основные цели и задачи криптографии?
3.3. Какое принципиальное отличие стеганографии от криптографии.
3.4. Какие типы файлов больше всего подходят для нужд стеганографии?
3.5. Наиболее распространенные методы сокрытия информации в файл-контейнерах.
3.6. Принципиальные отличия методов стеганографии.
3.7. Каким методом можно повысит стойкость скрытого сообщения к взлому?
3.8. Основные направления применения стеганографии.
3.9. Можно ли совместно использовать криптографию и стеганографию?
3.10. Предназначение программы Crypto 3A-001?
3.11. Какой метод сокрытия информации используется в программе Crypto 3A-001?
3.12. Каким образом задается ключ в программе Crypto 3A-001?

Задание 3.1. Сокрытие информации в файл-контейнере

В соответствии с номером своего варианта необходимо скрыть текстовую информацию в файлах формата WAV (табл. 3.1). Контейнеры находятся в папке Задание 1.

Таблица 3.1

Вариант	Имя фала	Скрываемый текст
1.	Вариант 1.1.wav Вариант 1.2.wav Вариант 1.3wav	Если человек отправляется от точки, в которой знание не помогает, он идет в направлении смысла. Мамардашвили М.
2.	Вариант 2.1.wav Вариант 2.2.wav Вариант 2.3.wav	Воля к смыслу - наиболее человеческий феномен, так как только животное не бывает озабочено смыслом своего существования. Франкл В.
3.	Вариант 3.1.wav Вариант 3.2.wav Вариант	Жизнь имеет в точности ту ценность, которой мы хотим ее наделить. Бергман И.

	3.3.wav	
4.	Вариант 4.1.wav Вариант 4.2.wav Вариант 4.3.wav	Человек нуждается не в разрядке напряжения любой ценой, но в возбуждении потенциального смысла, который он должен реализовать. Франкл В.
5.	Вариант 5.1.wav Вариант 5.2.wav Вариант 5.3.wav	Главная жизненная задача человека - дать жизнь самому себе, стать тем, чем он является потенциально. Самый важный плод его усилий - его собственная личность. Фромм Э.
6.	Вариант 6.1.wav Вариант 6.2.wav Вариант 6.3.wav	Я понял, что для того, чтобы понять смысл жизни, надо, прежде всего, чтобы жизнь была не бессмысленна и зла, а потом уже — разум для того, чтобы понять ее. Толстой Л. Н.
7.	Вариант 7.1.wav Вариант 7.2.wav Вариант 7.3.wav	Значение жизни открыто в сознании человека, как стремление к благу. Уяснение этого блага, более и более точное определение его, составляет главную цель и работу жизни всего человечества. Толстой Л. Н.
8.	Вариант 8.1.wav Вариант 8.2.wav Вариант 8.3.wav	Цель, и единственная цель, нашей жизни заключается в том, чтобы искоренить страсти и заменить их противоположными добродетелями. Варсонофий Оптинский
9.	Вариант 9.1.wav Вариант 9.2.wav Вариант 9.3.wav	Умирая, желал бы сказать: правда ли, что я думал о смысле жизни, что он в увеличении любви. Хоть головой мотнуть утвердительно или отрицательно. Толстой Л. Н.
10.	Вариант 10.1.wav Вариант 10.2.wav	Если я скажу, что вижу смысл жизни в борьбе за дело рабочего класса, то вы вряд ли поймете меня...

	Вариант 10.3.wav	Тельман Э.
11.	Вариант 11.1.wav Вариант 11.2.wav Вариант 11.3.wav	Даже если бы стремление к пониманию ...не было изначальной формой любви, не образовывало ее генезиса и кульминации, все равно следовало бы признать, что это стремление есть ее ярчайший признак. Ортега-и-Гассет Х.
12.	Вариант 12.1.wav Вариант 12.2.wav Вариант 12.3.wav	Цель жизни – жизнь!? Если глубоко всмотреться в жизнь, конечно, высшее благо есть само существование. Нет ничего глупее, как пренебречь настоящим в пользу грядущего. Настоящее есть реальная сфера бытия... Герцен А. И.
13.	Вариант 13.1.wav Вариант 13.2.wav Вариант 13.3.wav	Словами пользуются для выражения смысла. Постигнув смысл, забывают о словах. Где бы найти мне забывшего про слова человека, чтобы с ним поговорить! Фэн Юлань
14.	Вариант 14.1.wav Вариант 14.2.wav Вариант 14.3.wav	Человек не должен спрашивать, в чем смысл его жизни, но скорее должен осознать, что он сам и есть тот, к кому обращен вопрос. Франкл В.
15.	Вариант 15.1.wav Вариант 15.2.wav Вариант 15.3.wav	Я считаю специфически человеческим проявлением не только ставить вопрос о смысле жизни, но и ставить под вопрос существование этого смысла. Франкл В.
16.	Вариант 16.1.wav Вариант 16.2.wav Вариант 16.3.wav	Человек имеет в глубине души своей неизгладимое требование того, чтобы жизнь его была благом и имела разумный смысл. Толстой Л. Н.

Задание 3.2. Извлечение информации, скрытой в файл-контейнере

В соответствии со своим номером варианта необходимо извлечь текстовую информацию, которая скрыта в файлах формата WAV (табл. 3.2). Контейнеры находятся в папке Задание 2.

Таблица 3.2

Вариант	Имя фалов	Ключ
1.	Вариант 1.1.wav Вариант 1.2.wav Вариант 1.3.wav	1-2-3
2.	Вариант 2.1.wav Вариант 2.2.wav Вариант 2.3.wav	3-2-1
3.	Вариант 3.1.wav Вариант 3.2.wav Вариант 3.3.wav	2-3-1
4.	Вариант 4.1.wav Вариант 4.2.wav Вариант 4.3.wav	1-3-2
5.	Вариант 5.1.wav Вариант 5.2.wav Вариант 5.3.wav	3-2-1
6.	Вариант 6.1.wav Вариант 6.2.wav Вариант 6.3.wav	1-2-3
7.	Вариант 7.1.wav Вариант 7.2.wav Вариант 7.3.wav	2-3-1
8.	Вариант 8.1.wav Вариант 8.2.wav Вариант 8.3.wav	3-1-2
9.	Вариант 9.1.wav Вариант 9.2.wav Вариант 9.3.wav	1-2-3
10.	Вариант 10.1.wav Вариант 10.2.wav Вариант 10.3.wav	3-1-2
11.	Вариант 11.1.wav Вариант 112.wav Вариант 11.3.wav	2-3-1
12.	Вариант 12.1.wav Вариант 12.2.wav Вариант	3-2-1

	12.3.wav	
13.	Вариант 13.1.wav Вариант 13.2.wav Вариант 13.3.wav	1-2-3
14.	Вариант 14.1.wav Вариант 14.2.wav Вариант 14.3.wav	3-1-2
15.	Вариант 15.1.wav Вариант 15.2.wav Вариант 15.3.wav	2-1-3
16.	Вариант 16.1.wav Вариант 16.2.wav Вариант 16.3.wav	1-3-2

Методические указания

Программа Crypto 3A-001 (см. рисунок 1) предназначена для скрытой передачи сообщений в файл-контейнерах, с использованием принципов стеганографии. В частности в данной программе применяется метод замены наименьшего значащего бита (LSB). Этот метод является наиболее приемлемым для звуковых файлов, так как самый последний бит не воспринимается органами слуха человека, что позволяет использовать эти биты для передачи различной информации.

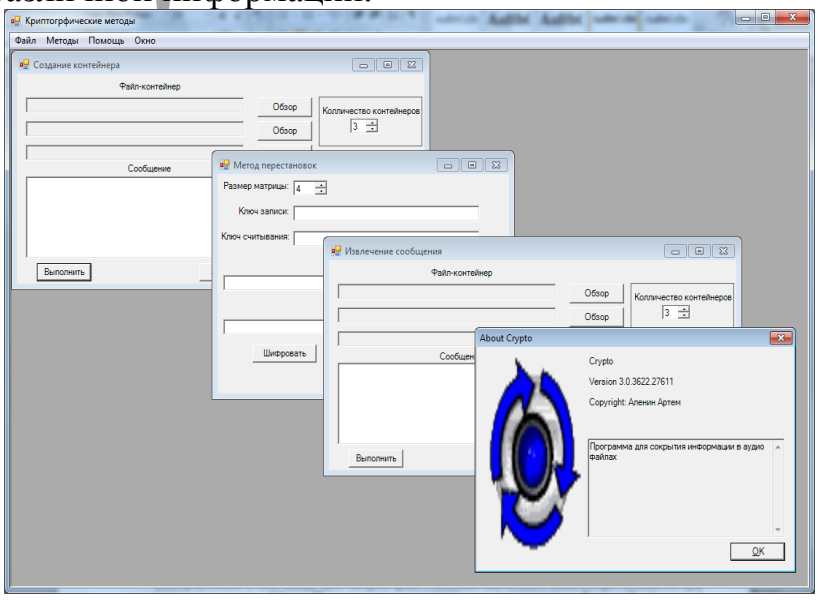


Рисунок 1 - Главное окно программы Crypto 3A-001

В программе в качестве файла-контейнера используется не сжатый файл формата WAV. Для повышения степени защиты скрываемой информации сообщение разделено на части (фрагменты) и сохраняется в нескольких контейнерах (от одного до десяти, по выбору пользователя). Ключом для извлечения сообщения служит последовательность файлов, в которых были скрыты фрагменты сообщения. Для повышения степени защиты информации скрываемое сообщение можно предварительно зашифровать с использованием следующих алгоритмов: шифр Цезаря, шифр Атбаш, квадрат Полибия, прямоугольник Плейфейра, метод перестановок, метод гаммирования, аффинные криптосистемы, таблица Виженера. Все перечисленные методы реализованы в данной программе.

Методические указания к пункту 3.1.

Для сокрытия сообщения необходимо выполнить следующие действия. В окне создания контейнера (см. рисунок 2) выбрать желаемое количество файл-контейнеров. Появляются соответствующие поля для ввода пути и имени файлов, в которых будет скрываться сообщение. Путь можно ввести с помощью диалогового окна, которое появляется при нажатии на кнопку «Обзор». По-умолчанию используется три файл-контейнера. В поле «Сообщение» с клавиатуры вводится сообщение, которое необходимо скрыть в выбранных звуковых файлах.

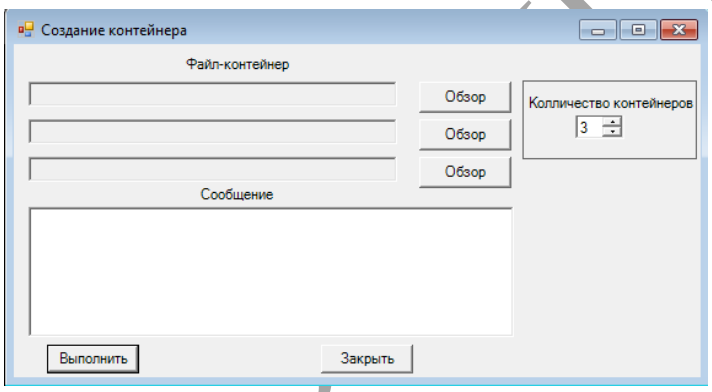


Рисунок 2 - Окно создания контейнера

Данное сообщение можно предварительно зашифровать. Для этого необходимо нажать на кнопку

ниспадающего меню главного окна программы. В результате появится список доступных методов шифрования (см. рисунок 3). Выбрать нужный метод шифрования. В открывшемся окне нужно ввести в поле «Входная строка» сообщение и ключ в поле «Ключ», если он необходим для выбранного метода, и нажать на кнопку «Шифровать». В поле «Выходная строка» появится зашифрованное сообщение. Его необходимо скопировать и вставить в поле «сообщение» в окне создания файл-контейнера. По нажатию на кнопку «Выполнить» происходит сокрытие сообщения в файл-контейнерах. Файлы со

скрытым сообщением помещаются в ту же папку, где находится исполняемый файл программы – Crypto.exe. Они называются соответственно: o1.wav, o2.wav, o3.wav и так далее.

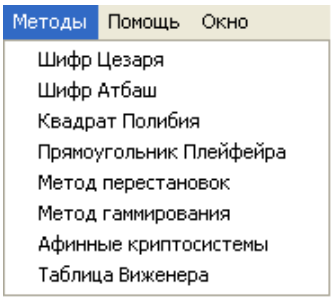


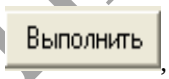
Рисунок 3 - Список методов шифрования

Методические указания к пункту 3.2.

Для извлечения сообщения необходимо выполнить следующие действия.

В окне извлечения сообщения выбрать требуемое количество файл-контейнеров. Появляются соответствующие поля для ввода пути и имени файлов, из которых будет извлекаться сообщение. Путь можно ввести с помощью диалогового окна, которое появляется при нажатии на кнопку «Обзор». Файлы вводить в поля необходимо в той последовательности, в которой они вводились при сокрытии сообщения.

По-умолчанию используется три файл-контейнера. При нажатии кнопки «Выполнить»



происходит извлечение сообщения из файлов. Извлеченное сообщение выводится в поле «Сообщение». Если оно было предварительно зашифровано, то его надо дешифровать. Для этого можно использовать возможности, предоставляемые данной программой. Для дешифрации необходимо нажать на кнопку ниспадающего меню

главного окна программы, появится список доступных методов шифрования и дешифрования (см. рисунок 3). Выбрать нужный метод дешифрования. В открывшимся окне ввести в поле «Входная строка» извлеченное сообщение и ключ, если он необходим для выбранного метода, и нажать на кнопку «Дешифровать». В поле «Выходная строка» появится дешифрованное сообщение.

Рекомендуемая литература

1. Алексеев А.П. Информатика 2007. – М.: СОЛОН-ПРЕСС.- 2007.- 608 с.
2. Алексеев А.П. Введение в Web-дизайн. Учебное пособие.- М.: СОЛОН-ПРЕСС, 2008.- 184 с.
3. Алексеев А.П., Орлов В.В., Сухова Е.Н. Изучение стеганографии на уроках информатики //Информатика и образование, № 8, 2007, стр. 65…72.
4. Алексеев А.П., Алексеев П.А., Мартяшина О.М., Сухова Е.Н. Изучение криптографии на уроках информатики //Информатика и образование, № 4, 2003, стр. 33…42.