Лабораторная работа № 8
Сокрытие информации в файлах формата WAV

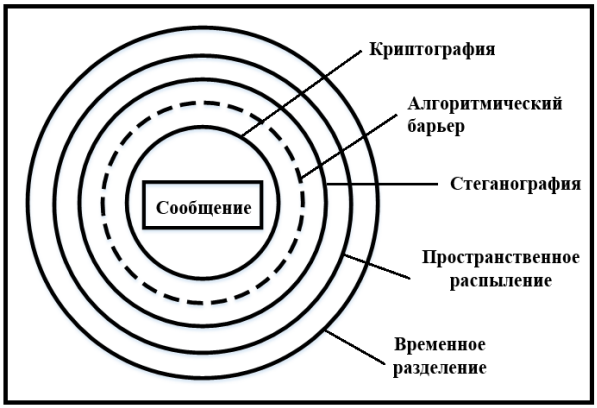
1. Цель работы

Изучить основные принципы скрытой передачи информации в звуковых контейнерах, получить навыки работы с программой стеганографического сокрытия информации Crypto 3A-001.

2. Общие сведения

Защита передаваемой и хранимой информации в настоящее время базируется на принципах, разработанных в криптографии и стеганографии. С помощью криптографических методов защищаемое сообщение преобразуется в набор символов, нечитаемый без ключа. Приёмы стеганографии позволяют создать скрытый канал связи, который сложно обнаружить даже с помощью специальных методов обработки информации. Размещение скрываемой информации в контейнерах также происходит по ключу.

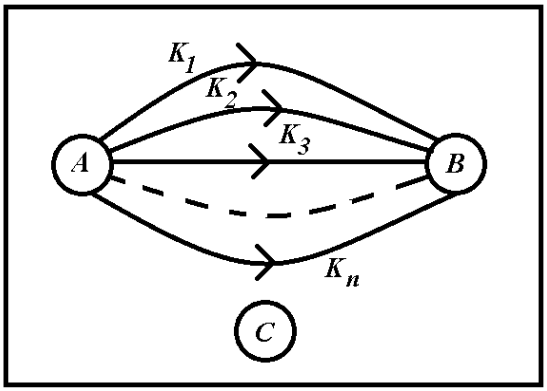
Специалистами проведено большое число результативных криптографических атак на известные шифры и на стеганографические методы защиты. Наличие успешно проведённых атак говорит о имеющейся уязвимости существующих принципов защиты информации.



Процесс разработки средств защиты информации и средств атаки на шифры и методы сокрытия сообщений носит соревновательный (итерационный) характер. Как правило, через несколько лет после создания широко распространённого шифра появляется эффективная атака на этот шифр и его использование постепенно затухает. Мозговой штурм по разработке новых алгоритмов защиты стимулируется проведением международных конкурсов.

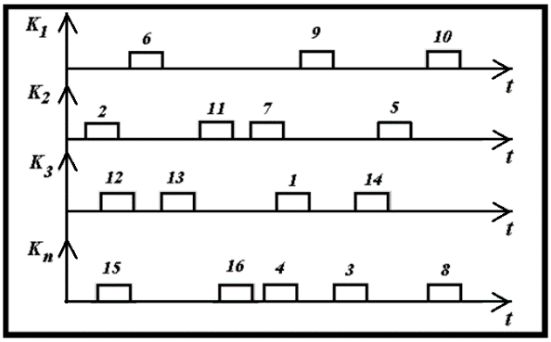
Принципиально новым подходом к защите информации может стать метод формирования нескольких уровней защиты сообщений (см. рисунок). На рисунке показано пять возможных барьеров защиты информации. Под сообщением будем понимать любую передаваемую (хранимую) информацию или данные.

Одним из дополнительных барьеров защиты (помимо криптографического и стеганографического) может стать пространственное распыление защищаемой информации.



Основная идея пространственного распыления информации состоит в том, что сообщение дробят на возможно мелкие составляющие (предложения, слова, символы, блоки символов, группы байт, байты, группы бит, биты) и передают частями, распределяя их по нескольким каналам связи $(K_1 ... K_n)$. Перехват нарушителем С (см. следующий рисунок) всех составляющих сообщения осложняется тем, что у корреспондентов А и В есть возможность использования нескольких доступных им телекоммуникационных каналов (радио, спутниковые, проводные, кабельные, радиорелейные).

Передача информации в глобальных сетях возможна с помощью множества существующих услуг (электронная почта, мессенджеры, чаты, форумы, блоги, распределённые базы данных WWW и т.п.). Использование сотовой связи позволяет распылить сообщение по нескольким MMS или SMS и передать их с помощью большого числа телефонных каналов.



Помимо трёх перечисленных уровней защиты передаваемой информации можно создать ещё один уровень (четвёртый), который технически и алгоритмически гармонично сочетается с ранее рассмотренными барьерами. Это - временное разделение сообщения (передача данных по заранее согласованному расписанию).

Пространственное и временное разделение сообщения удачно сочетаются между собой, дополняя друг друга. Эти два барьера можно представлять в виде единого барьера и назвать его пространственно-временным рас-

пылением сообщения. Идею пространственно-временного распыления сообщения иллюстрирует рисунок.

Информационные блоки 1…9, содержащие транслируемое сообщение, передаются в псевдослучайном порядке по каналам связи $(K_1 ... K_n)$. Моменты передачи блоков сообщения также является псевдослучайными. Передача информационных блоков перемежается посылкой маскирующих (дезинформирующих) блоков 10…16. Порядок трансляции блоков, номера каналов и временные окна устанавливают с помощью секретного ключа.

Заметим, что если для связи используется только один телекоммуникационный канал, то пространственно-временной барьер превращается во временной барьер.

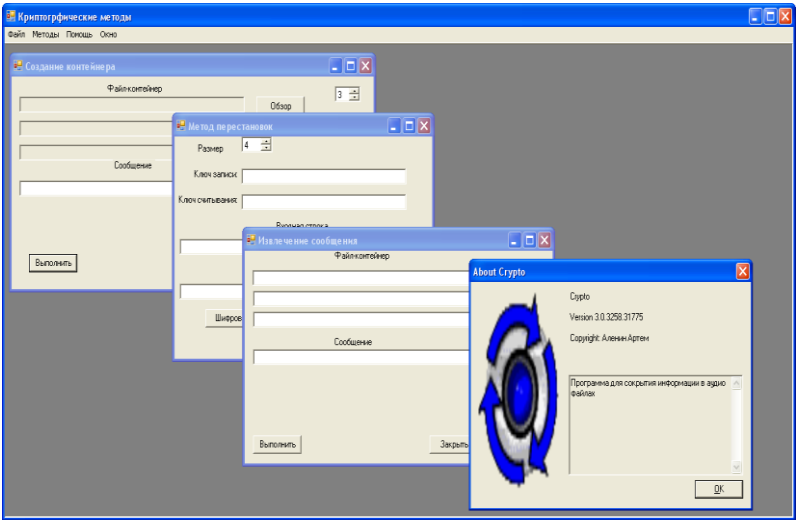
Пятый (алгоритмический) барьер базируется на таком способе обработки передаваемых блоков криптограммы, при котором отсутствие хотя бы одного перехваченного блока вызывает у криптоаналитика труднопреодолимые вычислительные сложности. Ближе всего по идеологии (по замыслу и использованию) к этому барьеру находятся режимы шифрования, которые описаны в отечественном стандарте ГОСТ 28147-89, американском стандарте DES и многих публикациях. Пятый барьер как бы является продолжением криптографического барьера, однако методологически его целесообразно выделить в отдельный уровень защиты.

Таким образом, путём создания множества барьеров разного вида можно осуществить принцип комплексной, многоуровневой защиты информации. В каждом конкретном случае стороны обоснованно выбирают достаточную степень защищённости сообщения (число используемых барьеров, вид шифра, длину ключа, виды стеганографических контейнеров, способы стеганографического внедрения информации в контейнеры, вид и число используемых каналов связи или носителей хранения информации, количество временных окон для передачи информации).

Ясно, что реализация предлагаемых мер повышения криптостойкости сопровождается увеличением времени передачи сообщения, числа ошибок при передаче сообщения, усложняет процедуру передачи, снижает удобство хранения информации. Регулировать степень защиты сообщения (значит, и варьировать время передачи сообщения, изменять сервисные свойства) можно путём выборочного использования не всех барьеров, а только достаточной их части. Оперативная передача информации (когда ценность информации исчисляется часами и даже минутами) может происходить при минимальном числе используемых барьеров.

Программа Crypto ЗА-001 (см. рисунок) предназначена для скрытой передачи (или хранения) сообщений в файл-контейнерах, с использованием принципов стеганографии. В частности, в данной программе применяется метод замены наименьшего значащего бита (LSB). Этот метод может быть использован для внедрения информации в звуковые файлы, так как самый

последний бит не воспринимается органами слуха человека.



В программе в качестве файла-контейнера используется несжатый файл формата WAV. Для повышения степени защиты скрываемой информации сообщение делится 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 шифруется с использованием различных алгоритмов: шифр Цезаря, шифр атбаш, квадрат Полибия, прямоугольник Плейфейра, метод перестановок, метод гаммирования, аффинные криптосистемы, таблица Виженера. Все перечисленные методы реализованы в данной программе.

3. Задания на выполнение лабораторной работы

3.1. Задание 1. Сокрытие информации в звуковом файле

В соответствии с номером своего варианта необходимо скрыть текстовую информацию в файлах формата WAV (табл. 3.1.1). Контейнеры находятся в папке **Задание 1**, местоположение которой указывает преподаватель.

Таблица 3.1.1

	Файл	Текст
1.	Вариант 1.1.wav,Вариант 1.2.wav.,Вариант 1.3wav	Казаки шпорами звенят, а студенты шпорами шуршат. *АПА*
2.	Вариант 2.1.wav Вариант 2.2.wav Вариант 2.3.wav	Доценты учат студентов уму-маразму. *АПА*
3.	Вариант 3.1.wav Вариант 3.2.wav Вариант 3.3.wav	Век шесть степеней свободы не видать! *АПА*
4.	Вариант 4.1.wav Вариант 4.2.wav Вариант 4.3.wav	Готов к экзамену на все 100. Но требуют 1000. *АПА*
5.	Вариант 5.1.wav Вариант 5.2.wav Вариант 5.3.wav	Если ненормальных много, то именно они считаются нормальными. *АПА*
6.	Вариант 6.1.wav Вариант 6.2.wav Вариант 6.3.wav	На судаков рыбачим, о рыбалке судачим. *АПА*
7.	Вариант 7.1.wav Вариант 7.2.wav Вариант 7.3.wav	Флюгеры указывают куда должен дуть ветер. *АПА*
8.	Вариант 8.1.wav Вариант 8.2.wav Вариант 8.3.wav	1, 2, 3, 4, 5, 6, 7 и так далее до восьми. *АПА*
9.	Вариант 9.1.wav Вариант 9.2.wav Вариант 9.3.wav	Любимые конфеты программистов «Мишка на сервере» *АПА*
10.	Вариант 10.1.wav Вариант 10.2.wav Вариант 10.3.wav	Программисты празднуют следующие юбилеи: 16, 32, 64 и 128 лет. *АПА*
11.	Вариант 11.1.wav Вариант 11.2.wav Вариант 11.3.wav	Заочник – единственная птица, которую ощипывают многократно. *АПА*
12.	Вариант 12.1.wav Вариант 12.2.wav Вариант 12.3.wav	Математик – это человек, который преобразует водку в теоремы. *АПА*
13.	Вариант 13.1.wav Вариант 13.2.wav Вариант 13.3.wav	Мы с тобой одно уравнение с двумя неизвестными. *АПА*
14.	Вариант 14.1.wav Вариант 14.2.wav Вариант 14.3.wav	Отдых хающий отдыхающий. *АПА*
15.	Вариант 15.1.wav Вариант 15.2.wav Вариант 15.3.wav	Чтобы открыть душу, нужно развязать язык. *АПА*
16.	Вариант 16.1.wav Вариант 16.2.wav Вариант 16.3.wav	Между женским «да» и «нет» - небольшой просвет. *АПА*

Задание 3.2. Извлечение информации, скрытой в файл-контейнере

В соответствии со своим номером варианта необходимо извлечь текстовую информацию, которая скрыта в трёх файлах формата WAV (табл. 3.2.1). Контейнеры находятся в папке Задание 2. Для шифрования использовать любой алгоритм.

Таблица 3.2.1

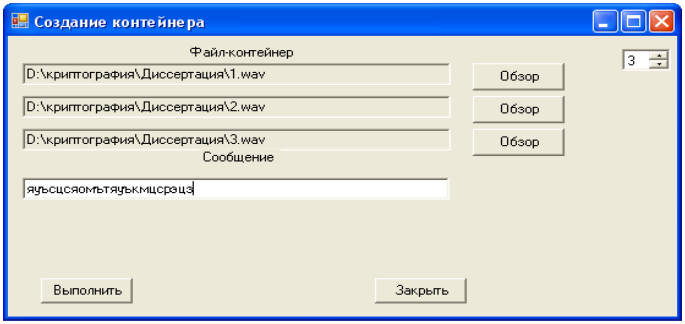
Вариант	Имя фалов	Ключ
1.	Вариант 1.1.wav Вариант 1.2.wav Вариант 1.3.wav	1-2-3
2.	Вариант 2.1.wav Вариант 2.2.wav Вариант 2.3.wav	3-2-1
3.	Вариант 3.1.wav Вариант 3.2.wav Вариант 3.3.wav	2-3-1
4.	Вариант 4.1.wav Вариант 4.2.wav Вариант 4.3.wav	1-3-2
5.	Вариант 5.1.wav Вариант 5.2.wav Вариант 5.3.wav	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 12.3.wav	3-2-1
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

4. Порядок выполнения лабораторной работы

4.1. Методические указания к заданию 3.1.

Для сокрытия сообщения необходимо выполнить следующие действия. В окне создания контейнера программы Crypto 3A-001 (см. рисунок) выбрать необходимое количество файл-контейнеров. Появятся соответствующие поля для ввода пути и имени файлов, в которых будет скрываться сообщение. Сокрытие информации в контейнере осуществляется методом LSB.

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.



Скрываемое сообщение можно предварительно зашифровать. Для этого необходимо нажать на кнопку **Методы**, находящуюся в Главном меню.

В результате появится список доступных методов шифрования, в котором нужно выбрать заданный метод шифрования. В открывшемся окне нужно в поле **Входная строка** ввести 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.

При нажатии 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.

4.2. Методические указания к заданию 3.2.

Для извлечения сообщения из трёх файлов необходимо выполнить следующие действия.

В окне извлечения сообщения выбрать требуемое количество 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 необходимо вводить в поля в той последовательности, в которой они вводились при сокрытии сообщения (последовательность указана с помощью ключа).

По умолчанию используется три контейнера. При нажатии кнопки **Выполнить**, происходит извлечение сообщения из файлов. Извлечённое 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 **Методы** Главного меню. В результате появится список доступных методов шифрования и дешифрования. В списке нужно выбрать нужный метод дешифрования. В открывшемся окне ввести в поле **Входная строка** извлечённое сообщение и ключ, если он необходим для выбранного метода, и нажать на кнопку **Дешифровать**. В поле **Выходная строка** появится дешифрованное сообщение.

5. Требования к отчёту

Отчёт подготавливается в электронном виде. Он должен содержать извлечённый и дешифрированный текст. В отчёте необходимо описать порядок сокрытия текстов в контейнерах с помощью программы Crypto 3A-001, привести скриншоты пользовательского интерфейса.

6. Контрольные вопросы

6.1. Какие основные цели и задачи стеганографии?

6.2. Какие основные цели и задачи криптографии?

6.3. Какое принципиальное отличие стеганографии от криптографии.

6.4. Какие типы файлов больше всего подходят для использования в стеганографии?

6.5. Перечислите наиболее распространённые методы сокрытия информации в файл-контейнерах.

6.6. Перечислите основные идеи (алгоритмы) сокрытия информации в электронных контейнерах.

6.7. Каким методом можно повысить стойкость скрытого сообщения к взлому?

6.8. Перечислите сферы применения стеганографии.

6.9. Можно ли совместно использовать криптографию и стеганографию?

6.10. Для чего предназначена программа Crypto 3A-001?

6.11. Какой метод сокрытия информации используется в программе Crypto 3A-001?

6.12. Каким образом задаётся ключ в программе Crypto 3A-001?

7. Список литературы

1.Алексеев А.П., Аленин А.А. Сокрытие информации в звуковых WAV-файлах. Методические указания на проведение лабораторных работ. – Самара: ПГУТИ, 2010. – 10 с.

2.Алексеев А.П., Аленин А.А. Исследование методов обнаружения вложений в звуковых файлах формата WAV//Безопасность информационных технологий, 2011, том 9, №1. С 51-56.

3.Алексеев А.П., Аленин А.А., Михайлов В.И. Выявление стеганографических вложений в WAV-файлах с помощью спектрального анализа// Инфокоммуникационные технологии, том 10, № 2, 2011. Стр.53-57.

4.Аленин А.А., Алексеев А.П. Программа для внедрения информации в аудиофайлы Crypto 3A-001. Свидетельство о регистрации электронного ресурса № 16896. ИНИМ РАО. Дата выдачи 1.04.2011 г.