Федеральное агентство связи

Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ

ЭЛЕКТРОННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА

Самара

ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ
Кафедра Информатики и вычислительной техники

Методические указания на проведение лабораторных работ

"Внедрение информации в звуковой файл формата MP3"

по дисциплине «Информатика»,
специальности: 210400, 210401, 210402, 210403, 210404, 210405, 210406, 210302, 090106

Авторы-составители: доц., к.т.н. **Алексеев А.П.,**
ассист**. Макаров М.И.**
Под общей редакцией Алексеева А.П.

Самара, 2010

Введение

Постоянное увеличение объема конфиденциальной информации требует от специалистов телекоммуникаций знания современных методов криптографии и стеганографии.

Данные методические указания позволяют освоить основные приемы шифрования и сокрытия информации в звуковых файлах.

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.
5. Алексеев А. П., Орлов В.В. Стеганографические и криптографические методы защиты информации; учебное пособие. Самара: ИУНЛ ПГУТИ – 2010. - 330 с.

Лабораторная работа
«Внедрение информации в звуковой файл формата MP3»

1. Подготовка к работе

По указанной литературе и методическим указаниям изучить основные понятия стеганографии и криптографии, уяснить принцип сокрытия информации в mp3-тэгах. Ответить на контрольные вопросы.

2. Контрольные вопросы

2.1. В чем состоит принципиальное различие между криптографией и стеганографией?
2.2. Криптография и стеганография конкурируют между собой или дополняют друг друга?
2.3. Как можно увидеть (проявить) скрытый текст?
2.4. С какой целью для сокрытия информации используют несколько контейнеров (mp3-файлов)?
2.5. В чем состоит основная идея распыления информации в пространстве (по нескольким контейнерам)?
2.6. В каком случае криптостойкость будет выше: при распылении в пространстве предложений, слов, символов или отдельных битов?
2.7. Приведите примеры контейнеров, которые могут быть использованы в стеганографии.
2.8. Как преобразовать символ открытого текста в двоичное число?
2.9. Как преобразовать десятичное число в двоичное?
2.10. Как преобразовать двоичное число в десятичное?
2.11. Что такое “Шифр Цезаря”?

Задание 3.1. Сокрытие информации в контейнере и ее извлечение

3.1.1. Скрыть свои фамилию, имя, отчество в тегах звуковых файлов формата mp3. Контейнеры для размещения скрываемой информации находятся в папке «Задание 1».

3.1.2. Извлечь информацию из контейнера, по ключу в соответствии с вариантом. Контейнеры находятся в папке «Задание 2».

Таблица 1.

Вариант	Ключ
1	5
2	-2
3	3
4	4
5	-4
6	-5
7	-4
8	6
9	-1
10	2
11	3
12	1
13	-5
14	-4
15	-3
16	-1

Методические указания

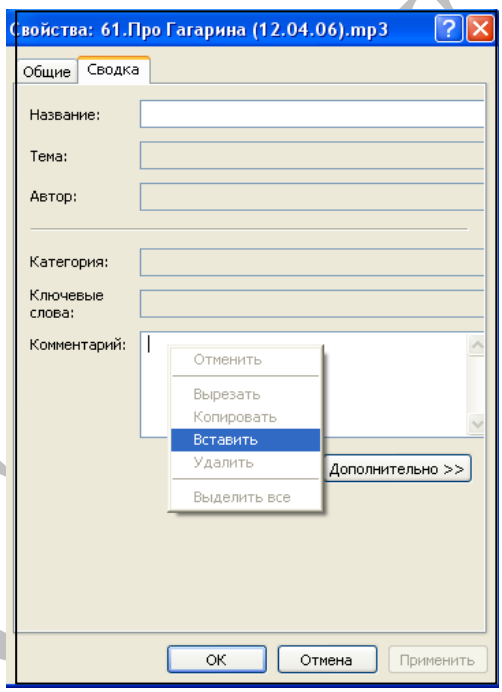
Методические указания к пункту 3.1.1.

Чтобы сокрыть информацию в mp3-тэги необходимо выполнить следующие действия.

1. Все символы сообщения перевести в десятичные значения по таблице CP-1251 (см. Приложение 1), а десятичные числа перевести в двоичные восьмиразрядные числа.

2. В текстовом редакторе заменить единицы символом “пробел”, а нули – “табуляция”.

3. Скрываемые данные следует поместить в MP3 файл, номер которого соответствует номеру варианта. Для этого в ОС Windows вызывается через контекстное меню пункт “Свойства”, в нём выбирается закладка “Сводка” и в поле «Комментарий» вводится скрываемая информация.



Методические указания к пункту 3.1.2.

Скрываемый текст обработан шифром Цезаря. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций.

Чтобы извлечь информацию из mp3-тэгов необходимо выполнить следующие действия.

1. Скопировать непечатаемые символы из тега “Комментарий”.
2. Пробелы заменить единицами, а знаки табуляции нулями.
3. Числа по 8 бит перевести из двоичной системы в десятичную систему счисления.
4. К каждому десятичному числу прибавить значение ключа (см. табл.1) и с помощью таблицы кодов CP-1251 определить значение открытого текста.

Приложение 1

Таблица CP-1251

пробел	32	**!**	33	**"**	34	**#**	35	**$**	36
%	37	**&**	38	**'**	39	**(**	40	**)**	41
*****	42	**+**	43	**,**	44	**-**	45	**.**	46
/	47	**0**	48	**1**	49	**2**	50	**3**	51
4	52	**5**	53	**6**	54	**7**	55	**8**	56
9	57	**:**	58	**;**	59	**<**	60	**=**	61
>	62	**?**	63	**@**	64	**A**	65	**B**	66
C	67	**D**	68	**E**	69	**F**	70	**G**	71
H	72	**I**	73	**J**	74	**K**	75	**L**	76
M	77	**N**	78	**O**	79	**P**	80	**Q**	81
R	82	**S**	83	**T**	84	**U**	85	**V**	86
W	87	**X**	88	**Y**	89	**Z**	90	**[**	91
****	92	**]**	93	**^**	94	**_**	95	**`**	96
a	97	**b**	98	**c**	99	**d**	100	**e**	101
f	102	**g**	103	**h**	104	**i**	105	**j**	106
k	107	**l**	108	**m**	109	**n**	110	**o**	111
p	112	**q**	113	**r**	114	**s**	115	**t**	116
u	117	**v**	118	**w**	119	**x**	120	**y**	121
z	122	**А**	192	**Б**	193	**В**	194	**Г**	195
Д	196	**Е**	197	**Ж**	198	**З**	199	**И**	200
Й	201	**К**	202	**Л**	203	**М**	204	**Н**	205
О	206	**П**	207	**Р**	208	**С**	209	**Т**	210
У	211	**Ф**	212	**Х**	213	**Ц**	214	**Ч**	215
Ш	216	**Щ**	217	**Ъ**	218	**Ы**	219	**Ь**	220
Э	221	**Ю**	222	**Я**	223	**а**	224	**б**	225
в	226	**г**	227	**д**	228	**е**	229	**ж**	230
з	231	**и**	232	**й**	233	**к**	234	**л**	235
м	236	**н**	237	**о**	238	**п**	239	**р**	240
с	241	**т**	242	**у**	243	**ф**	244	**х**	245
ц	246	**ч**	247	**ш**	248	**щ**	249	**ъ**	250
ы	251	**ь**	252	**э**	253	**ю**	254	**я**	255