Лабораторная работа № 10
Сокрытие информации на HTML – страницах

1. Цель работы

Изучить принцип скрытой передачи информации на HTML-страницах, получить навыки в шифровании данных.

2. Общие сведения

Идея сокрытия информации состоит в следующем. Символы открытого текста заменяют двоичными числами в соответствии с какой-либо кодовой таблицей. Скрываемый текст размещают после закрывающего тега </html>, причём вместо единиц записывают пробелы, а вместо нулей — символы табуляции. Эти символы на странице не видны (электронный аналог симпатических чернил).

Предположим, что с помощью Интернет нужно скрытно передать слово «Щит». В соответствии с кодовой таблицей CP-1251 буквам этого слова соответствуют три десятичных числа: 217, 232 и 242. В двоичной системе счисления эти числа выглядят так: 11011001, 11101000, 11110010. Заменив единицы и нули соответственно на пробелы и символы табуляции, скрытый текст размещают на HTML-странице ниже последнего тега. На приёмной стороне увидеть (проявить) закодированный текст можно с помощью текстового редактора MS Word, включив режим "Непечатаемые знаки".

```
<html>¶
<head>¶
<title>·Пример·сокрытия·текста·на·Web-странице</title>¶
</head>¶
<body>¶
Простейшая·Web-страница¶
</body>¶
</html>¶
·· →  ·· →    →  ·¶
··· →  · →    →    →  ¶
···· →    →  · →  ¶
```

Последние три строки кода программы содержат скрытую информацию. Здесь пробелы отображаются точками, символы табуляции — стрелками. Символ ¶ является служебным и обозначает конец абзаца и перевод строки. Предварительное шифрование текста позволяет повысить криптостойкость передаваемого сообщения.

3. Задания на выполнение лабораторной работы

3.1. Задание 1. Сокрытие информации в HTML-контейнере

Используя блокнот Notepad, создать HTML-страницу. В соответствии с вариантом выполнить кодирование текста и поместить код в контейнер, в качестве которого используется HTML-страница. Скрываемый текст указан в таблице 3.1.1.

Таблица 3.1.1

Вар.	Афоризмы
1	Кто открывает школы, тот закрывает тюрьмы.
2	Лучше быть без ума от женщины, чем дураком от природы.
3	Время останавливается только перед встречей любимых.
4	Путь не меньшее счастье, чем цель.
5	Грех сладок, а человек падок.
6	Не ищи пятна на греющем тебя солнце.
7	Ученье - свет, а неучёных – тьма.
8	Возьмите методичку и перепишите всё наизусть!
9	Звёзды – это осколки моего сердца, разбитого тобой.
10	Ядерная бомба всегда попадает в эпицентр.
11	Бороться и искать, найти и перепрятать.
12	Опрос будет письменный, но устно.
13	Компьютер никогда не заменит человека. Людоед.
14	Мысль изречённая есть ложь!
15	Легче забыть десять поцелуев, чем один.
16	Идеи могут быть обезврежены только идеями.

3.2. Задание 2. Извлечение информации из контейнера

Извлечь скрытый текст из HTML-контейнера. Номер контейнера, из которого следует извлекать текст, соответствует номеру варианта. Путь к контейнерам указывается преподавателем.

3.3. Задание 3. Распределение скрываемой информации по четырём HTML-контейнерам

Создать четыре HTML-страницы, используя блокнот Notepad. В соответствии с вариантом преобразовать заданный текст в непечатаемые символы и распределить созданный код по четырём контейнерам согласно заданному ключу. Открытый текст, разбитый на четыре части, и ключ для распределения указаны в таблице 3.3.1.

Таблица 3.3.1

Вар	Афоризм	Ключ
1	Кто мешает тебе выдумать порох непромокаемый? *К. Прутков.*	1324
2	Если чувства опережают рассудок, значит последний в плохой спортивной форме. *Э. Восарот*	1432
3	Когда на твой вопрос отвечает философ, перестаёшь понимать вопрос. *А. Жид*	2341
4	Сошедшему с пьедестала трудно менять позу. *В. Хочинский.*	3142
5	Хороший врач спасает если не от болезни, то хотя бы от плохого врача. *Жан Поль*	4123
6	Женские глаза — всегда океан: то Тихий, то Северный Ледовитый. *М. Мамчич*	3421
7	Слова –самый сильный наркотик из всех, которое изобрело человечество. *Р. Киплинг*	1324
8	Руководить – это значит не мешать хорошим людям работать. *П. Капица*	3142
9	Если вы хотите узнать, что на самом деле думает женщина, смотрите на неё, но не слушайте. *Уайльд*	4132
10	То, что истинно при свете лампы, не обязательно истинно при свете солнца. *Жан Поль*	4321
11	Робкий боится заранее, трусливый — в момент опасности, а смелый — после. *Жан Поль*	4213
12	Жизнь — это небольшая прогулка перед вечным сном. *Фаина Раневская*	4123
13	Каждый человек настолько тщеславен, насколько ему не хватает ума. *Ф. Ницше*	1243
14	Какой бы сладкой ни была любовь, компота из неё не сваришь. *Пословица*	1432
15	Не делайте умное лицо, не забывайте, что Вы – будущий бакалавр. *Армейский юмор*	3241
16	У красивой женщины всегда красивое имя. *Ю. Булатович*	2341

3.4. Задание 4. Извлечение скрытой информации

Извлечь текст, скрытый в четырёх HTML-контейнерах, и восстановить его, расположив части текста в правильном порядке. Очерёдность следования фрагментов текста определена ключом,

указанным в таблице 3.4.1. Номер папки, содержащей контейнеры, соответствует номеру варианта.

Таблица 3.4.1

Вариант	Ключ	Вариант	Ключ
1	1234	9	4132
2	1432	10	4321
3	2341	11	4213
4	3142	12	4123
5	4123	13	1243
6	3421	14	1432
7	1324	15	3241
8	3142	16	2341

3.5. Задание 5. Сокрытие зашифрованной информации

Используя блокнот Notepad, создать четыре HTML-страницы. В соответствии с вариантом зашифровать открытый текст методом гаммирования и побайтно распределить криптограмму по четырём контейнерам согласно заданному ключу. Открытый текст, ключ для шифрования текста методом гаммирования и ключ для пространственного распределения букв приведены в таблице 3.5.1.

Таблица 3.5.1

Вар.	Открытый текст	Ключ для шифрования	Ключ для пространственного распределения букв
1	Агония	Курсив	1 4 3 2 4 3
2	Зодиак	Вектор	4 2 3 1 3 4
3	Доцент	Пленум	2 1 3 1 4 2
4	Витязь	Радиус	3 2 4 2 1 4
5	Сажень	Обшлаг	4 3 1 3 1 2
6	Наклон	Сделка	1 3 2 1 4 3
7	Умысел	Магнит	2 4 3 1 3 4
8	Ливень	Гранит	3 1 4 2 3 2
9	Жребий	Формат	1 3 2 4 3 1
10	Рябина	Нектар	2 1 4 1 3 4
11	Медаль	Банкет	4 3 1 4 2 1
12	Термин	Экипаж	1 3 4 1 2 4
13	Чеснок	Шинель	3 2 1 3 4 1
14	Ошибка	Воздух	2 1 3 4 2 3
15	Январь	Родник	3 4 1 2 1 3
16	Иволга	Хозяин	4 2 1 2 1 3

3.6. Задание 6. Извлечение зашифрованной информации

Извлечь зашифрованный текст из четырёх контейнеров, расшифровать его и расположить части текста в правильном порядке. Ключ для пространственного распыления букв и ключ для шифрования текста приведены в таблице 3.6.1. Номер папки, содержащей контейнеры, соответствует номеру варианта.

Таблица 3.6.1

Вар.	Ключ для расшифрования текста	Ключ для пространственного распыления букв
1	Газель	1 4 3 2 4 3
2	Дельта	4 2 3 1 3 4
3	Мишура	2 1 3 1 4 2
4	Реванш	3 2 4 2 1 4
5	Шкипер	4 3 1 3 1 2
6	Свитер	1 3 2 1 4 3
7	Ладонь	2 4 3 1 3 4
8	Вампир	3 1 4 2 3 2
9	Унисон	1 3 2 4 3 1
10	Блюдце	2 1 4 1 3 4
11	Жаргон	4 3 1 4 2 1
12	Тесьма	1 3 4 1 2 4
13	Зарево	3 2 1 3 4 1
14	Калибр	2 1 3 4 2 3
15	Импорт	3 4 1 2 1 3
16	Лакмус	4 2 1 2 1 3

3.7. Задание 7. Побайтное шифрование с помощью матриц

Создать четыре HTML-страницы, используя блокнот Notepad. Выполнить кодирование текста, состоящего из 32-х знаков, включая пробелы и знаки препинания, и поместить его в матрицу. Пробелы, которые нужно кодировать, выделены знаком подчёркивания «_». Другие пробелы кодировать не надо. Размер матрицы – 16x16.

Затем нужно побайтно считать по столбцам информацию из матрицы и распылить её по четырём HTML-контейнерам согласно ключу, указанному в таблице 3.7.1.

Таблица 3.7.1

№ варианта	Афоризм	Ключ распыления
1	Лень_делает_всякое_дело_трудным.	2 1 3 4
2	Умирать_от_любви - значит_жить_ею.	3 4 1 2
3	Сладчайшая_месть_-_это_прощение.	4 3 1 2
4	Легче_простить_врага,_чем_друга.	1 4 2 3
5	Дружба_-_это_любовь_без_крыльев.	4 2 1 3
6	Чтобы_дойти_до_цели_,_надо_идти.	2 4 3 1
7	Страх_не_должен_подавать_совета.	3 1 2 4
8	Кто_чего_хочет, тот_в_то_и_верит.	1 2 4 3
9	Свободен_тот, кто_может_не_лгать.	1 4 3 2
10	О_чем_не_знают_,_того_не_желают.	4 2 3 1
11	Путь_силы_-_это_неизменный_путь.	3 1 4 2
12	Обаяние - непринужденность_чувств.	2 4 1 3
13	Начало - более_чем_половина_всего.	1 3 2 4
14	Понимание -_это_начало_согласия.	3 2 4 1
15	Все,что_прекрасно,-_нравственно.	4 1 2 3
16	Истинное_мужество -_осторожность.	2 3 4 1

3.8. Задание 8. Побайтное расшифрование с помощью матриц

Извлечь зашифрованный текст из четырёх контейнеров, записать его в матрицу побайтно, согласно ключу, указанному в таблице 3.8.1. Затем считать информацию из матрицы и расшифровать её. Номер папки, содержащей контейнеры, соответствует номеру варианта.

Таблица 3.8.1.

Вариант	Ключ	Вариант	Ключ
1	1432	9	2134
2	4231	10	3412
3	3142	11	4312
4	2413	12	1423
5	1324	13	4213
6	3241	14	2431
7	4123	15	3124
8	2341	16	1243

3.9. Задание 9. Побитное шифрование с помощью матриц

Создать пять HTML-страниц. Выполнить кодирование текста и поместить код в матрицу 16x16, из которой считать её побитно и распылить по пяти контейнерам согласно ключу (табл. 3.9.1).

Таблица 3.9.1.

Вариант	Афоризм	Ключ
1	Сострадание_-_основа_всей_морали.	52134
2	Причина_ошибки - незнание_лучшего.	35412
3	Великая_судьба -_великое_рабство.	43512
4	Где_не_было_умысла, там_нет_вины.	51423
5	Исход_дела - наставник_неразумных.	42153
6	Бойся_думать_без_участия_сердца.	24315
7	Жизнь -_это_борьба_за_бессмертие.	35124
8	Правда -_это_общая_совесть_людей.	12453
9	Дело_художника -_рождать_радость.	14325
10	Будущее -это_зеркало_без_стекла.	42531
11	Если_сомневаешься - говори_правду.	35142
12	Словами_подобает_скрашивать_зло.	24153
13	Политика_-_искусство_возможного.	51324
14	В_одном_часе_любви -_целая_жизнь.	32541
15	Кто_ясно_мыслит_,_ясно_излагает.	45123
16	Взывать_к_чуду -_развращать_волю.	23451

3.10. Задание 10. Побитное расшифрование данных

Извлечь зашифрованный методом перестановок текст из пяти HTML-контейнеров, записать его в матрицу 16x16 побитно, согласно ключу, указанному в табл. 3.10.1. Затем считать информацию из матрицы и расшифровать её. Номер папки, содержащей контейнеры, соответствует номеру варианта.

Таблица 3.10.1

Вариант	Ключ	Вариант	Ключ
1	14325	9	52134
2	42531	10	35412
3	35142	11	43512
4	24153	12	51423
5	51324	13	42153
6	32541	14	24315
7	45123	15	35124
8	23451	16	12453

4. Порядок выполнения лабораторной работы

4.1. Методические указания к заданию 3.1.

Чтобы внедрить скрываемую информацию в HTML-контейнер, необходимо выполнить следующие действия.

1. Преобразовать символы скрываемого текста, включая пробелы и знаки препинания, в десятичные числа. Для этого следует использовать таблицу CP-1251.

2. Преобразовать полученные десятичные числа в двоичные числа. Ниже приведён пример, который следует использовать как образец при оформлении отчёта (см. таблицу 4.1.1).

Таблица 4.1.1

Открытый текст	Десятичное число	Двоичное число
Ж	198	11000110
и	232	11101000
з	231	11100111
н	237	11101101
ь	252	11111100
пробел	32	00100000
п	239	11101111
р	240	11110000
е	229	11100101
к	234	11101010
р	240	11110000
а	224	11100000
с	241	11110001
н	237	11101101
а	224	11100000
!	33	00100001

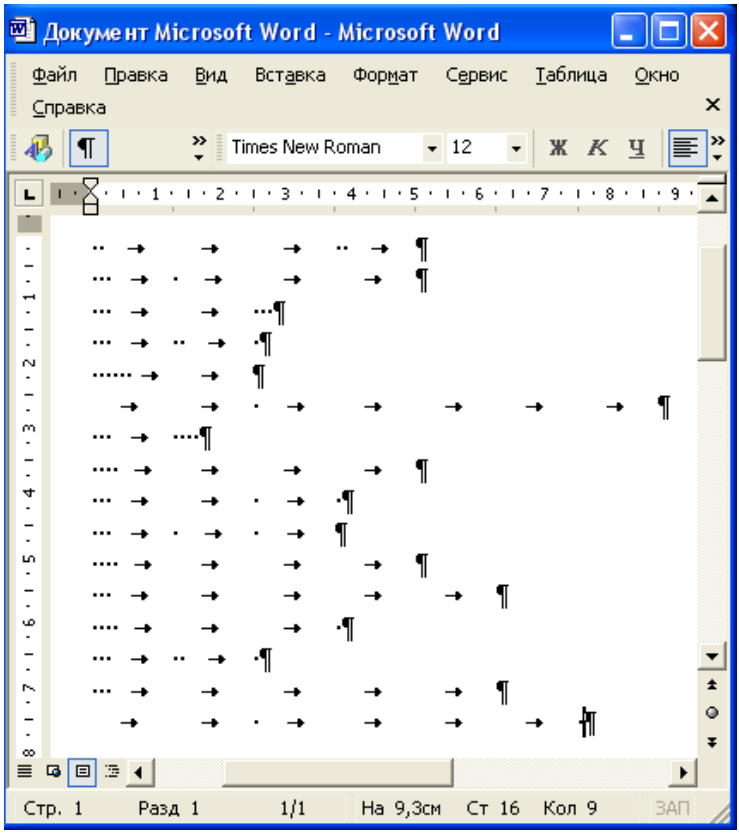
3. С помощью блокнота Notepad создать HTML-страницу. Код страницы приведён в **Общих сведениях** данной лабораторной работы, а также он показан на рисунке данного раздела.

4. Вставить в созданную HTML-страницу сформированный код (табл. 4.1.1). Скрываемый текст размещают после закрывающего тега </html>, причём вместо единиц записывают пробелы, а вместо нулей – символы табуляции.

Каждый скрываемый символ (букву, байт) располагают на отдельной строке. Удобнее сначала ввести данные в документ MS Word, где можно увидеть вводимые символы, используя режим

“Непечатаемые знаки” (кнопка **Непечатаемые знаки** находится на вкладке **Абзац**.). После этого скопировать полученную последовательность символов в Блокнот.

Пример записи двоичных чисел с помощью непечатаемых символов показан на следующем рисунке.

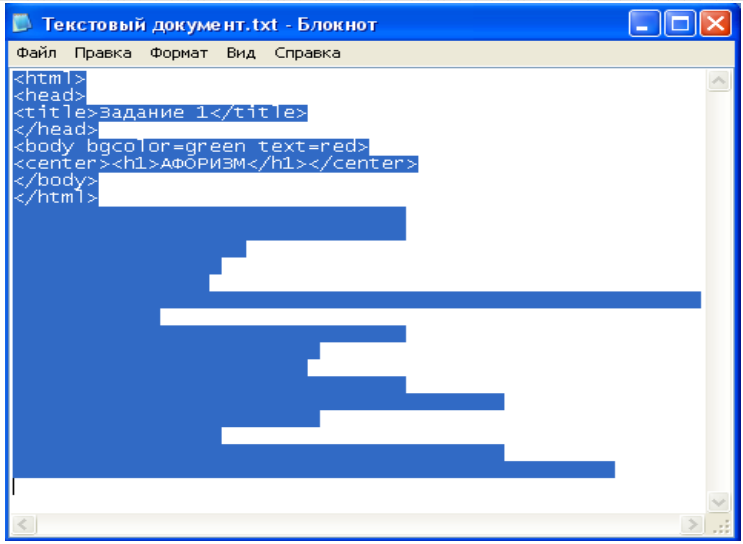


На следующем рисунке показан код HTML-страницы, которая содержит скрытно передаваемый текст.

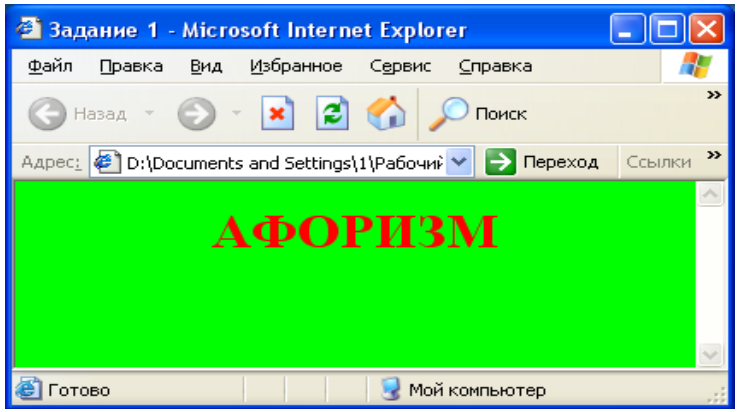
Код может быть использован как образец (пример) для создания собственного HTML-контейнера. Целесообразно в заголовке HTML-страницы указать фамилию студента, номер задания и номер варианта.

Например,

<title>Иванов_Задание_1_Вариант_7</title>.



Внешний вид HTML-страницы, на которой скрыта информация показан на следующем рисунке



Как видно из рисунка, скрытую информацию визуально обнаружить невозможно. Именно так будет выглядеть страница для любого пользователя Internet.

4.2. Методические указания к заданию 3.2.

Чтобы извлечь скрытую информацию из HTML-контейнера, необходимо выполнить следующие действия.

1. Открыть HTML-страницу, содержащую вложение.
2. Создать документ MS Word, и скопировать в него содержимое HTML-страницы, включая область ниже тега </html>.
3. Войти в режим “Непечатаемые знаки” (кнопка **Непечатаемые знаки** находится на вкладке **Абзац**.). Полученные комбинации пробелов и символов табуляции представляют собой двоичные числа, где пробел эквивалентен единице, а символ табуляции – нулю.
4. Преобразовать двоичные числа в десятичные (таблица 4.2.1).
5. Определить по таблице CP-1251 символы, соответствующие этим десятичным числам.

Таблица 4.2.1

Двоичное число	Десятичное число	Текст
11000110	198	Ж
11101000	232	и
11100111	231	з
11101101	237	н
11111100	252	ь
00100000	32	пробел
11101111	239	п
11110000	240	р
11100101	229	е
11101010	234	к
11110000	240	р
11100000	224	а
11110001	241	с
11101101	237	н
11100000	224	а
00100001	33	!

Из полученных символов составить фразу. В данном случае принято сообщение: «Жизнь прекрасна!».

4.3. Методические указания к заданию 3.3.

Чтобы распределить скрываемую информацию по четырём HTML-контейнерам, необходимо выполнить следующие действия.

1. Разбить текст, который нужно скрыть, на четыре примерно одинаковые части. Разделять слова недопустимо. Ниже приведён пример разделения текста на части.

Честность /– лучшая/ политика./ М.Сервантес

2. Преобразовать символы открытого текста, включая пробелы и знаки препинания, в десятичные числа, используя таблицу CP-1251.

3. Преобразовать полученные десятичные числа в двоичные числа (таблица 4.3.1).

4. Распределить фрагменты текста по четырём HTML-страницам в соответствии с заданным ключом, например, 4123 (см. следующий рисунок). Скрываемый текст размещают после закрывающего тега </html>, причём вместо единиц записывают пробелы, а вместо нулей – символы табуляции. Каждый символ (байт) располагают на отдельной строке. Удобнее сначала ввести данные в документ MS Word, где можно увидеть вводимые символы, используя режим “Непечатаемые знаки” (кнопка **Непечатаемые знаки** находится на вкладке **Абзац**.). Затем нужно скопировать полученную последовательность символов в Notepad.

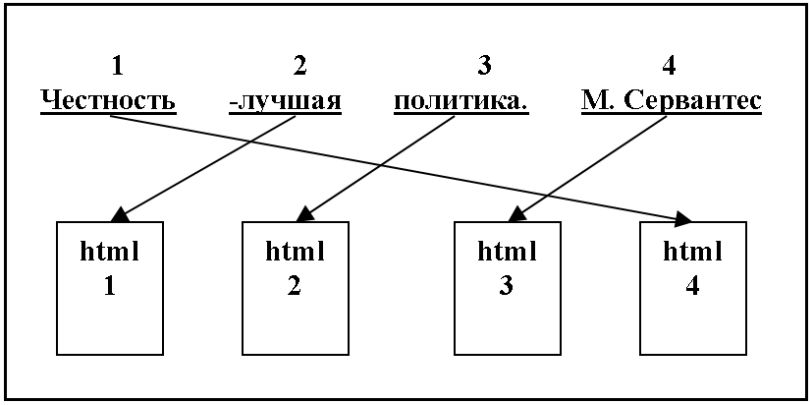


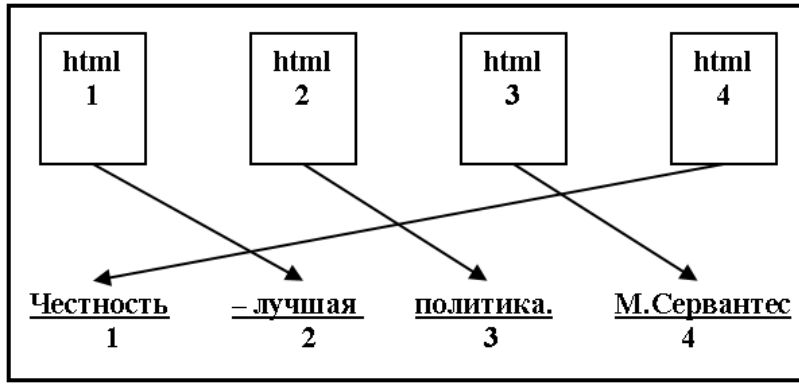
Таблица 4.3.1

Текст	Десятичное число	Двоичное число
Ч	215	11010111
е	229	11100101
с	241	11110001
т	242	11110010
н	237	11101101
о	238	11101110
с	241	11110001
т	242	11110010
ь	252	11111100
пробел	32	00100000
-	45	00101101
пробел	32	00100000
л	235	11101011
у	243	11110011
ч	247	11110111
ш	248	11111000
а	224	11100000
я	255	11111111
пробел	32	00100000
п	239	11101111
о	238	11101110
л	235	11101011
и	232	11101000
т	242	11110010
и	232	11101000
к	234	11101010
а	224	11100000
.	46	00101110
М	204	11001100
.	46	00101110
С	209	11010001
е	229	11100101
р	240	11110000
в	226	11100010
а	224	11100000
н	237	11101101
т	242	11110010
е	229	11100101
с	241	11110001

4.4. Методические указания к заданию 3.4.

Чтобы извлечь скрытую информацию, распределённую по четырём HTML-контейнерам, необходимо выполнить следующие действия.

1. Открыть HTML-страницу, содержащую первую часть текста (в соответствии с заданным ключом). В рассматриваемом примере это четвертая HTML-страница, так как задан ключ 4123 (см. п.4.3.).
2. Создать документ MS Word и скопировать в него содержимое HTML-страницы.
3. Войти в режим “Непечатаемые знаки” (кнопка **Непечатаемые знаки** находится на вкладке **Абзац**.). Полученные комбинации пробелов и символов табуляции представляют собой двоичные числа, где пробел соответствует единице, а символ табуляции – нулю.
4. Преобразовать двоичные числа в десятичные.
5. Определить по таблице CP-1251 символы, соответствующие этим десятичным числам.



Аналогичную процедуру проделать с другими HTML-страницами в соответствии с заданным ключом. Из полученных фрагментов текста следует составить фразу.

В этом задании скрываемый текст распределяется (распыляется) по контейнерам большими фрагментами текста. При обнаружении противником одного из нескольких контейнеров криптоаналитик сможет прочитать существенный фрагмент сообщения.

4.5. Методические указания к заданию 3.5.

Чтобы побайтно распределить зашифрованную методом гаммирования информацию по четырём контейнерам, необходимо выполнить следующие действия.

1. Преобразовать каждую букву открытого текста и ключа для его шифрования в десятичные числа, используя таблицу CP-1251.

2. Преобразовать полученные десятичные числа в двоичные (таблица 4.5.1).

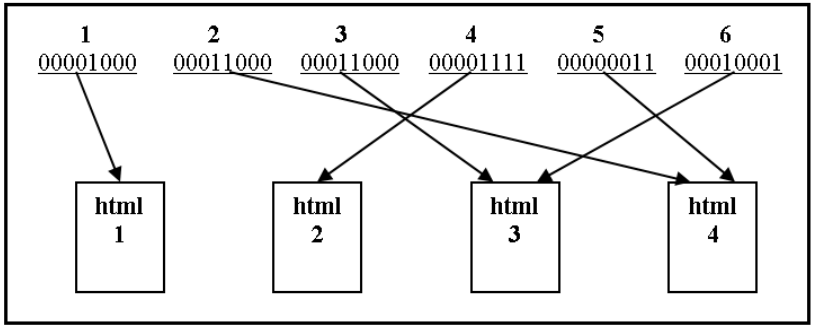
Таблица 4.5.1

Текст	Десятичное число	Двоичное число
Д	196	11000100
р	240	11110000
а	224	11100000
к	234	11101010
о	238	11101110
н	237	11101101
Ключ для шифрования	Десятичное число	Двоичное число
М	204	11001100
и	232	11101000
ш	248	11111000
е	229	11100101
н	237	11101101
ь	252	11111100

3. Выполнить в двоичном коде сложение каждой буквы открытого текста с буквами ключевого слова с помощью операции Исключающее ИЛИ.

Д ⊕ М	р ⊕ и	а ⊕ ш	к ⊕ е	о ⊕ н	н ⊕ ь
11000100	11110000	11100000	11101010	11101110	11101101
11001100	11101000	11111000	11100101	11101101	11111100
00001000	00011000	00011000	00001111	00000011	00010001

4. Разместить криптограмму побайтно (по восемь бит) на четырёх HTML-страницах в соответствии с заданным ключом, например, 143243 (см. рисунок). Байты располагают после закрывающего тега </html>, причём стандартно вместо единиц записывают пробелы, а вместо нулей – символы табуляции.



В отличии от предыдущего задания здесь распыление скрываемой информации происходит побайтно (каждая буква в псевдослучайном порядке попадает на отдельную HTML-страницу).

4.6. Методические указания к заданию 3.6.

Чтобы извлечь зашифрованную методом гаммирования информацию, распределённую по четырём контейнерам, необходимо выполнить следующие действия.

1. Открыть HTML-страницу, содержащую первую часть текста согласно ключу для пространственного распределения букв.

2. Создать документ MS Word и скопировать в него содержимое HTML-страницы.

3. Считать непечатаемые знаки. Преобразовать в двоичные числа.

4. Преобразовать каждую букву ключа шифрования в десятичное число, используя таблицу CP-1251.

5. Преобразовать полученные десятичные числа в двоичные (таблица 4.6.1).

6. Выполнить логическую операцию Исключающее ИЛИ над двоичным числом, извлечённым из HTML-страницы, и двоичным числом, соответствующим первой букве ключа.

$$\begin{array}{r} \oplus\ 00001000 \\ \underline{11001100} \\ 11000100 \end{array}$$

Таблица 4.6.1

Ключ для шифрования	Десятичное число	Двоичное число
М	204	11001100
и	232	11101000
ш	248	11111000
е	229	11100101
н	237	11101101
ь	252	11111100

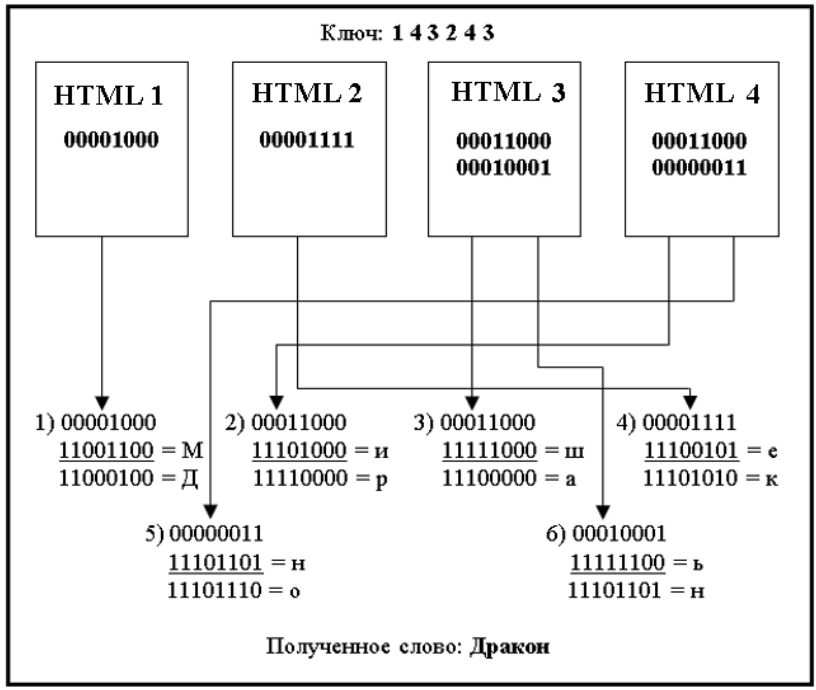
7. Преобразовать полученное в результате выполнения логической операции двоичное число в десятичное.

$$1 + 1 + 0 + 0 + 0 + 1 + 0 + 0 = 2^7 + 2^6 + 2^2 = 196$$

8. Определить по таблице CP-1251 символ, который соответствует этому двоичному числу: 196 →Д.

Аналогичную процедуру (пункты 6-8) следует повторить для остальных символов в соответствии с ключом для пространственного

распределения букв. Из полученных букв нужно составить слово (см. рисунок).



4.7. Методические указания к заданию 3.7.

Чтобы зашифровать информацию побайтно с помощью матрицы и распределить её по четырём HTML-контейнерам, необходимо выполнить следующие действия.

1. Создать четыре HTML-страницы (в заголовке указать номер страницы, например, <titlte>Страница_3</title>).

2. Преобразовать каждый символ открытого текста в десятичные числа, используя таблицу СР-1251.

3. Преобразовать полученные десятичные числа в двоичные числа.

4. Сформировать матрицу размером 16x16 ячеек.

5. Записать построчно (слева направо, сверху вниз) в матрицу байты информации, соответствующие символам открытого текста.

6. Считать из матрицы байты и распределить их по четырём HTML-страницам в соответствии с заданным ключом, например, 3241 (см. рисунок).

	3	4	3	4	3	4	3	4	3	4	3	4	3	4	3	4	
Д	1	1	0	0	0	1	0	0	1	1	1	1	0	0	0	0	р
у	1	1	1	1	0	0	1	1	1	1	1	0	0	1	1	0	ж
б	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	0	а
-	0	0	1	0	1	1	0	1	1	1	1	1	1	1	0	1	з
т	1	1	1	1	0	0	1	0	1	1	1	0	1	1	1	0	о
_	0	0	1	0	0	0	0	0	1	1	1	1	0	0	1	1	у
м	1	1	1	0	1	1	0	0	1	1	1	0	0	1	0	1	е
н	1	1	1	0	1	1	0	1	1	1	1	0	1	0	0	0	и
е	1	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	_
м	1	1	1	0	1	1	0	0	1	1	1	0	1	1	1	0	о
л	1	1	1	0	1	0	1	1	1	1	1	1	0	1	1	1	ч
а	1	1	1	0	0	0	0	0	1	1	1	1	0	0	1	0	т
ь	1	1	1	1	1	1	0	0	0	0	1	0	0	0	0	0	_
в	1	1	1	0	0	0	1	0	1	1	1	0	0	1	0	0	д
в	1	1	1	0	0	0	1	0	1	1	1	0	1	1	1	0	о
е	1	1	1	0	0	1	0	1	1	1	1	0	1	1	0	0	м
	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	

Считывание данных из матрицы производят по столбцам. Каждый столбец матрицы 16x16 содержит два байта информации. Из каждого столбца поочерёдно берут лишь восемь бит (один байт). Каждый байт отправляют на одну из четырёх HTML-страниц. Ключ распыления байтов повторяют циклически. Скрываемый текст размещают после закрывающего тега </html>, причём вместо единиц записывают пробелы, а вместо нулей – символы табуляции.

На предыдущем рисунке показан пример использования матрицы 16x16. В матрицу построчно записан афоризм Василия Аксенова «Дружба – это умение молчать вдвоём».

На горизонтальных сторонах матрицы циклически записан повторяющийся ключ 3241 (см. верхнюю и нижнюю стороны матрицы). На вертикальных сторонах матрицы с двух сторон записаны символы афоризма. Внутри матрицы каждый символ представлен двоичным числом. В соответствии с матрицей на каждую из четырёх HTML-страниц будет отправлено по 8 байт (символов).

На HTML-страницу 3 нужно поместить следующие 64 бита информации (они записаны в две строки).

11101011011111110001001101001000
11111111111111110001100101001100

На страницу 2 следует отправить следующую последовательность битов:

11111111111111110110100000100110
01110111111111110100001101110010

На страницу 4 отправляют такую последовательность битов.

11101011010010001001001101110001
11111111100101000101101000010110

На странице 1 размещают биты:

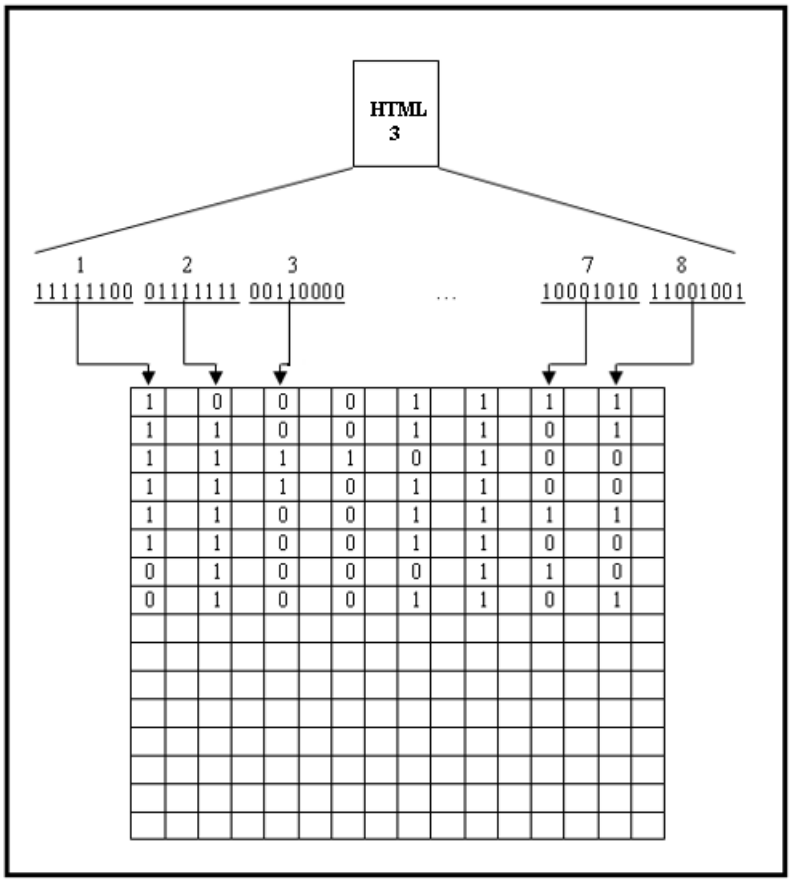
11111111000010001100100110100001
01110111001100000110011100100000

4.8. Методические указания к заданию 3.8.

Чтобы извлечь информацию, зашифрованную побайтно с помощью матрицы, необходимо выполнить следующие действия.

1. В соответствии с заданным ключом открыть первую HTML-страницу, содержащую часть криптограммы. В рассматриваемом примере первой нужно открыть HTML-страницу номер 3, так как ключ распыления информации 3241 начинается с цифры 3. Напомним, что ключ определяет порядок извлечения информации из контейнеров.
2. Создать документ MS Word, и скопировать в него содержимое третьей HTML-страницы.
3. Войти в режим “Непечатаемые знаки”.
4. Разбить последовательность символов на байты (группы по восемь бит). Заменить пробелы и символы табуляции соответственно на единицы и нули. Замену удобно проводить с помощью кнопки **Заменить**, которая находится на вкладке **Главная** (MS Word). Символу табуляции соответствует комбинация клавиш ^t.
5. Повторить операции, описанные в пунктах 1- 4, для страниц, содержащих вторую, третью и четвертую части криптограммы.
6. Подготовить матрицу размером 16x16.
7. Записать байты информации в матрицу 16x16. Запись производят столбцами, слева направо; по ключу, который повторяется циклически. Таким образом, в первом столбце матрицы будут записаны первые байты с HTML-страниц 3 (вверху) и 2 (внизу). Во втором столбце разместятся первые байты с HTML-страниц 4 и 1. В третьем столбце следует поместить вторые байты с HTML-страниц 3 и 2. В четвёртом столбце разместятся вторые байты с HTML-страниц 4 и 1 и т.д.

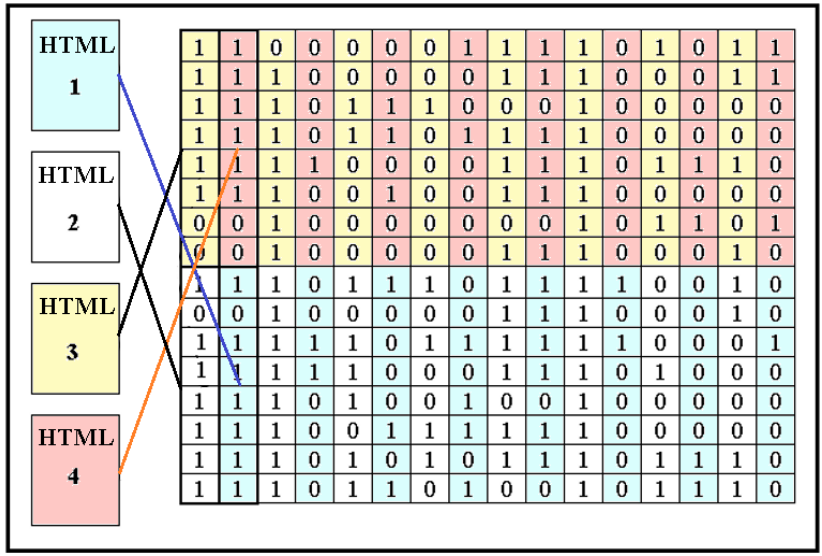
На рисунке показан порядок записи байтов в матрицу из HTML-страницы номер 3.



8. После занесения в матрицу 32-х байтов нужно считать информацию. Считывание производится построчно слева направо, сверху вниз. Каждый байт представляет собой один символ текста (букву, пробел, знак препинания).

1	2	3	4	...	32
11000001	11101011	11100000	11100011	...	00101110

На следующем рисунке показана матрица, заполненная байтами в соответствии с заданным ключом.



1	1	0	0	0	0	0	1	1	1	1	0	1	0	1	1
1	1	1	0	0	0	0	0	1	1	1	0	0	0	1	1
1	1	1	0	1	1	1	0	0	0	1	0	0	0	0	0
1	1	1	0	1	1	0	1	1	1	1	0	0	0	0	0
1	1	1	1	0	0	0	0	1	1	1	0	1	1	1	0
1	1	1	0	0	1	0	0	1	1	1	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0	1	0	1	1	0	1
0	0	1	0	0	0	0	0	1	1	1	0	0	0	1	0
1	1	1	0	1	1	1	0	1	1	1	1	0	0	1	0
0	0	1	0	0	0	0	0	1	1	1	0	0	0	1	0
1	1	1	1	1	0	1	1	1	1	1	1	0	0	0	1
1	1	1	1	1	0	0	0	1	1	1	0	1	0	0	0
1	1	1	0	1	0	0	1	0	0	1	0	0	0	0	0
1	1	1	0	0	1	1	1	1	1	1	0	0	0	0	0
1	1	1	0	1	0	1	0	1	1	1	0	1	1	1	0
1	1	1	0	1	1	0	1	0	0	1	0	1	1	1	0

9. Преобразовать считанные двоичные числа в десятичные числа.

10. Определить по таблице CP-1251 символы, соответствующие этим десятичным числам (таблица 4.8.1).

11. Из полученных символов составить принятую фразу. В данном случае:

«Благо народа – вот высший закон».

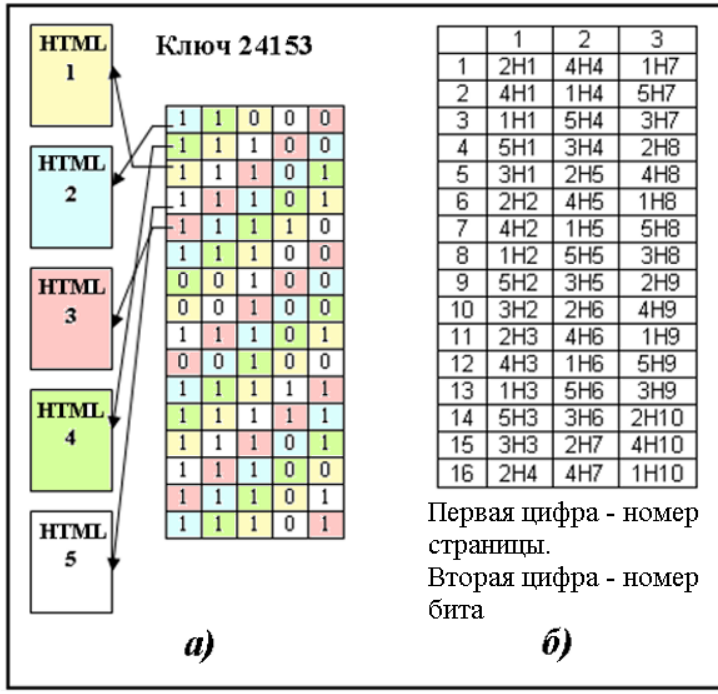
Таблица 4.8.1

Байт	Двоичное число	Десятичное число	Открытый текст
1	11000001	193	Б
2	11101011	235	л
3	11100000	224	а
4	11100011	227	г
5	11101110	238	о
6	00100000	32	пробел
7	11101101	237	н
8	11100000	224	а
9	11110000	240	р
10	11101110	238	о
11	11100100	228	д
12	11100000	224	а
13	00100000	32	пробел
14	00101101	45	-
15	00100000	32	пробел
16	11100010	226	в
17	11101110	238	о
18	11110010	242	т
19	00100000	32	пробел
20	11100010	226	в
21	11111011	251	ы
22	11110001	241	с
23	11111000	248	ш
24	11101000	232	и
25	11101001	233	й
26	00100000	32	пробел
27	11100111	231	з
28	11100000	224	а
29	11101010	234	к
30	11101110	238	о
31	11101101	237	н
32	00101110	46	.

4.9. Методические указания к заданию 3.9.

Чтобы зашифровать информацию побитно с помощью матрицы 16x16 и распределить криптограмму по пяти контейнерам, необходимо выполнить следующие действия.

1. Используя таблицу СР-1251, преобразовать каждый символ открытого текста, состоящего из 32-х символов, в десятичное число.
2. Преобразовать десятичные числа в двоичные числа.



	1	2	3
1	2H1	4H4	1H7
2	4H1	1H4	5H7
3	1H1	5H4	3H7
4	5H1	3H4	2H8
5	3H1	2H5	4H8
6	2H2	4H5	1H8
7	4H2	1H5	5H8
8	1H2	5H5	3H8
9	5H2	3H5	2H9
10	3H2	2H6	4H9
11	2H3	4H6	1H9
12	4H3	1H6	5H9
13	1H3	5H6	3H9
14	5H3	3H6	2H10
15	3H3	2H7	4H10
16	2H4	4H7	1H10

3. Подготовить матрицу размером 16x16 ячеек.
4. Записать построчно в матрицу байты информации, соответствующие символам открытого текста (см. рис. *а*). На рис. *а* показано только пять столбцов матрицы, а на рис. *б* – только три.
5. Считать из матрицы информацию. Считывание производится побитно по столбцам сверху вниз. Биты информации в соответствии с заданным ключом (например, 24153) размещаются на пяти HTML-страницах (рис. *а*). На этом рисунке показан перенос из матрицы в контейнеры только первых битов.

4.10. Методические указания к заданию 3.10.

Чтобы извлечь информацию, зашифрованную побитно с помощью матрицы, необходимо выполнить следующие действия.

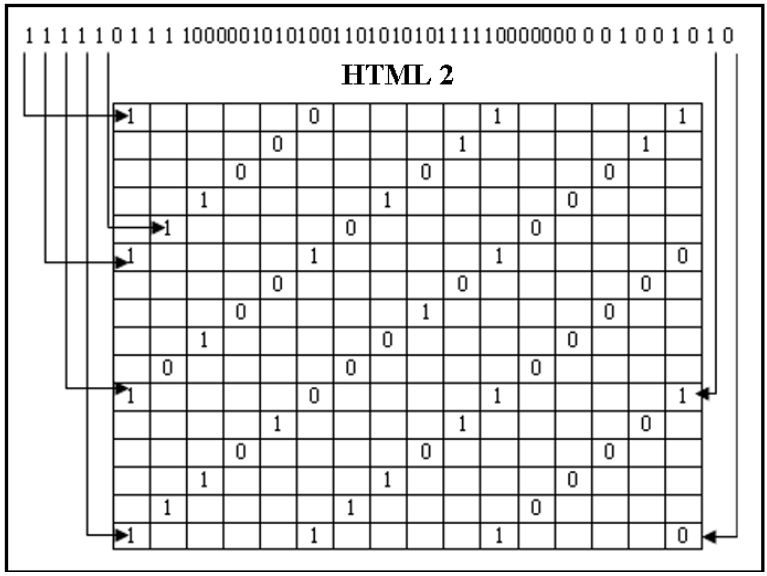
1. Открыть HTML-страницу, содержащую первую часть криптограммы (с учётом ключа). В рассматриваемом примере это вторая HTML-страница, так как ключ 24153.

2. Создать документ MS Word, и скопировать в него содержимое HTML-страницы.

3. Войти в режим “Непечатаемые знаки”. Проявить скрытый код и преобразовать его в двоичные числа.

4. Подготовить матрицу размером 16x16 ячеек.

5. Записать информацию в матрицу. Биты располагают в матрице по столбцам, причём они должны записываться в каждую пятую ячейку. Порядок записи информации в матрицу из страницы HTML 2 иллюстрирует следующий рисунок.



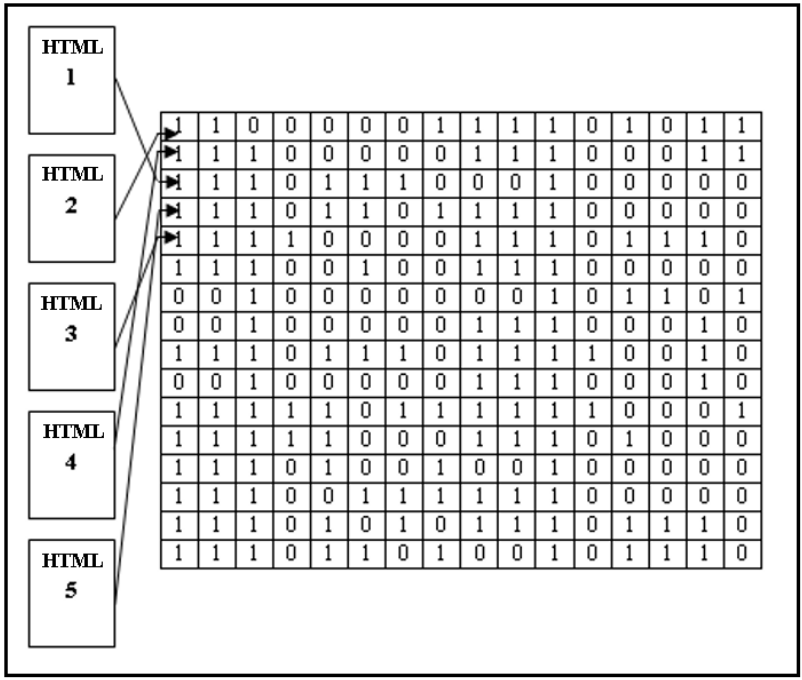
Аналогичную процедуру записи битов нужно проделать с другими HTML-страницами в соответствии с заданным ключом. Для страницы HTML 4 запись битов в матрицу следует производить во вторую, седьмую, двенадцатую, … ячейки первого столбца. Для HTML 1 биты заносят в третью, восьмую, тринадцатую ячейки и т.д.

6. Считать информацию из полученной матрицы. Считывание производится построчно, слева направо, сверху вниз. Каждый байт представляет собой один символ текста (буква, пробел, знак препинания, цифра).

1	2	3	4	5		32
11000001	11101011	11100000	11100011	11101110	…	00101110

7. Преобразовать двоичные числа в десятичные.

8. Определить по таблице CP-1251 символы, соответствующие этим десятичным числам.



Из полученных символов составить фразу. В данном примере получится:

Благо народа – вот высший закон.

5. Требования к отчёту

Отчёт подготавливается в электронном виде. Он должен содержать постановки задач, таблицы с преобразованием символов в двоичный код (и обратно), коды с проявленными невидимыми символами, скриншоты, которые иллюстрируют выполненные задания. Созданные HTML-контейнеры в заголовках должны содержать информацию о номере задания, номере варианта и фамилии студента.

6. Контрольные вопросы

6.1. Какие символы целесообразно использовать для скрытой передачи информации с помощью HTML- страницы?

6.2. В каком месте HTML-страницы удобно размещать скрываемый текст?

6.3. Как можно увидеть (проявить) скрытый на HTML-странице текст?

6.4. С какой целью для сокрытия информации используют несколько контейнеров (HTML-страниц)?

6.5. В чём состоит основная идея распыления информации в пространстве (по нескольким контейнерам)?

6.6. В каком случае криптостойкость будет выше: при распылении в пространстве предложений, слов, символов или отдельных битов?

6.7. В чём заключается основная идея шифрования текста с помощью матриц?

6.8. Приведите примеры контейнеров, которые могут быть использованы в стеганографии.

6.9. Опишите структуру HTML-страницы.

6.10. Перечислите методы скрытой передачи информации.

6.11. В чём состоит идея шифрования методом гаммирования?

6.12. Какие из трёх методов шифрования использованы в этой лабораторной работе: аддитивный, перестановок, замены?

7. Список литературы

1. Алексеев А.П. Введение в Web-дизайн. Учебное пособие с грифом УМО. - М.: СОЛОН – ПРЕСС, 2008. – 192 с.

2. Алексеев А.П., Вадикова Е.М. Сокрытие информации на HTML-страницах. Мет. указания на проведение лабораторных работ. Самара: ПГУТИ, 2008. - 46 с.