**Задания по стеганографии**

**Задача 1 (Метод 1).** Есть текст и в нем надо скрыть некоторую фразу, состоящую из букв. Буквы этой фразы представляются как байты. Эти байты надо разбить на биты.

Текст, в котором будет прятаться сообщение, должен иметь много строчек (как стихотворение). Мы должны разбить скрываемый текст на биты. И если очередной бит скрываемой информации равен единице, то в конец очередной строки текста-контейнера дописываем пробел. Если же бит равен нулю, то в конец строки не пишем пробел.

После шифрования, шифровку надо будет обратно раскодировать.

**Задача 2 (Метод 2).** Есть некий текст и в нем тоже надо спрятать другой текст. Аналогичным образом скрываемый текст разбиваем на биты. И если очередной бит секретного сообщения равен единице, то в тексте-контейнере удваиваем пробел. Если очередной бит скрываемого текста равен нулю, то пробел остается одним. Обычные буквы пропускаются в тексте-контейнере. То есть, для того, чтобы скрыть слово "мама" (4 буквы, 4 байта или 32 бита), нужен текст-контейнер как минимум, с 32-мя пробелами.

Таким же методом надо расшифровать сообщение обратно.

**Задача 3 (Метод 3).** Подготовка та же, что и в задаче 3. Только если бит секретного сообщения равен единице, то в тексте-контейнере меняем русскую букву на английский аналог. Если бит равен нулю, то очередную букву-аналог в тексте-контейнере оставляем без изменений. Буквы-аналоги - это буквы русского языка, имеющие аналогичное начертание в англ. языке.

Таким образом, нужно иметь вспомогательные массивы информации, в которых задано взаимно-однозначное соответствие русских и латинских букв сходного начертания.

Так же, надо расшифровать текст обратно.

**Задания по антивирусной защите**

**Задача 4.** Поиск по сигнатуре заданного файла в указанной директории.

Cначала берётся сигнатура у заданного файла, т.е. программа должна выбирать последовательность символом не менее 16 байт из участка файла, заведомо не могущего повторяться в отличных от него файлах. Это может быть отдельная программа, а может быть модуль единой программы.

Далее указывается директория для поиска и находятся все копии исходного файла по сигнатуре. Поиск осуществляется во всей директории, т.е. по всем файлам и каталогам, которые в ней хранятся. На выходе программы выводится список путей к найденным файлам.

**Задания по шифрованию**

**Задача 5.** Схема шифрования Вижинера**.**

Таблица Вижинера представляет собой квадратную матрицу с n2 элементами, где n — число символов используемого алфавита. Каждая строка получена циклическим сдвигом всего алфавита на символ.

Для шифрования выбирается буквенный ключ, в соответствии с которым формируется рабочая матрица шифрования.

Из полной таблицы выбирается первая строка и те строки, первые буквы которых соответствуют буквам ключа. Первой размешается первая строка, а под нею — строки, соответствующие буквам ключа в порядке следования этих букв в ключе.

1) под каждой буквой шифруемого текста записываются буквы ключа. Ключ при этом повторяется необходимое число раз;

2) каждая буква шифруемого текста заменяется по подматрице Вижинера буквами, находящимися на пересечении линий, соединяющих буквы шифруемого текста в первой строке подматрицы и находящихся под ними букв ключа;

Расшифровка текста производится в следующей последовательности:

1) над буквами зашифрованного текста последовательно надписываются буквы ключа, причем ключ повторяется необходимое количество раз.

2) в строке подматрицы Вижинера, соответствующей букве ключа, отыскивается буква, соответствующая знаку зашифрованного текста. Находящаяся под ней буква первой строки подматрицы и будет буквой исходного текста.

***! Задание состоит в написании программы для шифрования текста по схеме Вижинера. Текст для шифрования и ключ должны быть в русской кодировке и вводиться в диалоговом режиме.***

***Можно применять и свой алгоритм, например, генерация таблицы сдвигом или вычисление замены по формуле.***

**Задача 6.** Шифрование каталога.

Написать программу шифрования каталога, действующую по следующему алгоритму:

1. шифрование:
   1. программе указывается каталог для шифрования
   2. программе указывается ключ
   3. программа сворачивает каталог в зашифрованный файл
   4. программа удаляет каталог (можно обычным образом, без затирания тела)
2. расшифровывание:
   1. программе указывается каталог для расшифровывания
   2. программе указывается ключ
   3. программа разворачивает зашифрованный файл в каталог
   4. программа удаляет файл

***Используется любой алгоритм шифрования с ключом.***