Лабораторная работа 2: «Применение стеганографических методов для сокрытия информации»[1] [до 28 апреля]

1. О деталях реализации и средствах разработки

- Структура 8-битного BMP-файла следующая. Первые 122 байта занимает служебная информация – «Bitmap File Header» (14 байтов), «DIB Header» (40 байтов) и «Color Table». Остальное – «Image Data» – является последовательным описанием цветов пикселей изображения. Байтами 3-6 описывается размер файла (в байтах), а байтами 19-22 и 23-26 – ширина и высота изображения (в пикселях) соответственно. Цвет каждого пикселя кодируется в модели RGB тремя байтами (по байту на красную, синюю и зеленую составляющие).

- Генерация случайного числа (здесь 20 байтов) с помощью утилиты `openssl.exe`:

```
openssl rand -hex 20
```

- Некоторые побитовые операции в Java:

```
int x = 123;
System.out.println(Integer.toBinaryString(x));

//Сдвиг вправо на один бит (деление на два):
System.out.println(Integer.toBinaryString(x>>1));

//Взятие последнего бита (побитовая конъюнкция):
System.out.println(Integer.toBinaryString(x&1));
```

2. Постановка задачи

Напишите программу для внедрения в файл `28.bmp` и извлечения из него хешкода файла `leasing.txt`, полученного с помощью алгоритма SHA-1. Метод реализации – LSB Replacement. Номера байтов-контейнеров должны содержаться в предварительно сгенерированном ключе. С помощью

[1] Например: 1) «водяные знаки» (англ. *watermark*) – одинаковы для всех копий документа; 2) «отпечатки пальцев» (англ. *fingerprint*) – различны в копиях документа.

сторонних приложений оцените объемы получившегося и исходного изображений после сжатия.

3. Задания для подготовки к экзамену

1. Напишите программу для внедрения в файл `28.bmp` и извлечения из него хешкода файла `leasing.txt`, полученного с помощью алгоритма SHA-1. Метод реализации – LSB Matching. Номера байтов-контейнеров должны содержаться в предварительно сгенерированном ключе. С помощью сторонних приложений оцените объемы получившегося и исходного изображений после сжатия.

2. xxx