МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий
Кафедра «Инфокогнитивные технологии»

ЛАБОРАТОРНАЯ РАБОТА №3

на тему: *«Применение блочных шифров»*

Направление подготовки 09.03.03 «Прикладная информатика»
Профиль «Корпоративные информационные системы»
Дисциплина «Защита информации»

Выполнил:

студентка группы 201-361

Саблина Анна Викторовна

Проверил:

Харченко Елена Алексеевна

Москва 2023

Теоретическая часть

AES (Advanced Encryption Standard) – это симметричный алгоритм блочного шифрования, разработанный для защиты информации путем шифрования и расшифрования данных.

AES оперирует на блоках данных размером 128 бит и использует ключи различной длины: 128 бит, 192 бит и 256 бит. Он состоит из нескольких раундов шифрования, в каждом из которых выполняются определенные операции над данными.

Раунды AES:

1. SubBytes: каждый байт входного блока заменяется на другой байт из специальной таблицы замен (S-блок). Это помогает внести нелинейность в шифрование.
2. ShiftRows: каждая строка входного блока сдвигается влево. При этом первая строка остается на месте, вторая сдвигается на одну позицию влево, третья на две позиции влево, а четвертая на три позиции влево. Это делается для перестановки байтов внутри каждого блока.
3. MixColumns: каждый столбец входного блока перемешивается. Каждый байт в столбце умножается на определенные значения и складывается по модулю. Это помогает в перемешивании байтов между столбцами блока.
4. AddRoundKey: каждый байт входного блока комбинируется с байтом из раундового ключа с использованием побитовой операции XOR. Раундовой ключ генерируется из основного ключа с использованием специального расписания ключей.

После выполнения всех раундов, за исключением последнего, выполняется финальный раунд без операции MixColumns.

Режимы шифрования AES позволяют использовать AES для защиты данных большего размера или для выполнения различных задач шифрования:

1. *ECB (Electronic Codebook)* – электронная книга кодов. Каждый блок данных шифруется независимо от других блоков. Однако этот режим не обеспечивает конфиденциальность для одинаковых блоков данных.
2. *CBC (Cipher Block Chaining)* – режим связывания блоков шифрования. Каждый блок данных перед шифрованием комбинируется с предыдущим зашифрованным блоком данных путем побитовой операции XOR. Это обеспечивает конфиденциальность и стойкость к атакам с повторением блоков.
3. *CFB (Cipher Feedback)* – режим обратной связи по шифротексту. В этом режиме шифрования предыдущий зашифрованный блок данных обратно связывается с функцией обратной связи и используется для шифрования следующего блока данных. Он позволяет шифровать данные меньшего размера и обеспечивает конфиденциальность и целостность данных.
4. *OFB (Output Feedback)* – режим обратной связи по выходу. В этом режиме шифрования предыдущий блок шифротекста используется для генерации потока псевдослучайных битов, который затем комбинируется с открытым текстом путем побитовой операции XOR для получения шифротекста. Этот режим обеспечивает конфиденциальность и независимость от блоков данных.

- *Вектор обратной связи (Feedback Vector, IV)* – это случайно выбираемое начальное значение, которое используется в режимах блочного шифрования с обратной связью, таких как CBC, CFB и OFB.

Все эти режимы шифрования и раунды AES вместе образуют надежную систему шифрования, обеспечивая конфиденциальность, целостность и защиту данных от несанкционированного доступа и атак.

В задании работы предлагается использовать файл формата PNG.

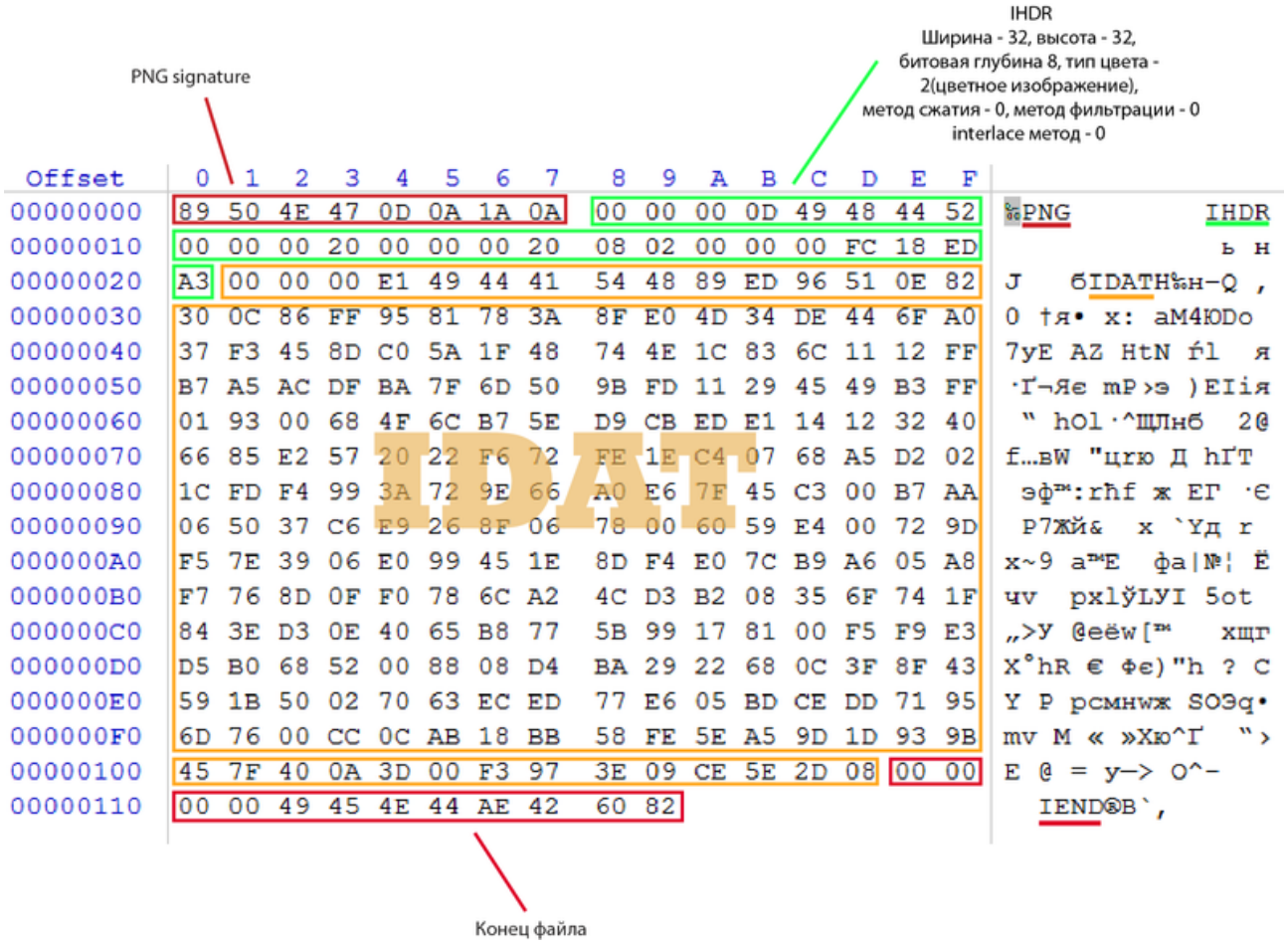

Рисунок 1 – Структура PNG-файла

Чанки – это основные блоки данных, из которых состоит файл PNG. Каждый чанк представляет собой независимую единицу информации, которая содержит определенные данные, такие как изображение, метаданные или палитра цветов.

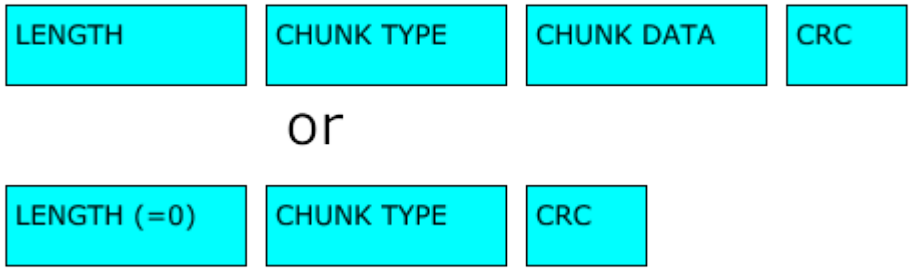

Рисунок 2 – Структура чанков

Представленные выше рисунки демонстрируют структуру файла. Это означает, что для успешного обработки файла необходимо не только отсечь

заголовок, но также обрезать окончание файла, а также учитывать структуру чанков, из которых состоит формат PNG. В каждом чанке, помимо прочего, присутствует контрольная сумма, которая обеспечивает целостность файла. При шифровании файлов контрольная сумма изменяется, что может привести к неправильному отображению изображения или невозможности его открытия. Поэтому в данном случае был выбран аналогичный файл формата BMP, который не имеет чанков и контрольных сумм.

Хедер файла BMP состоит из нескольких параметров, содержащих переменные значения заголовка. В данном конкретном случае, заголовок составляет 110 байт.

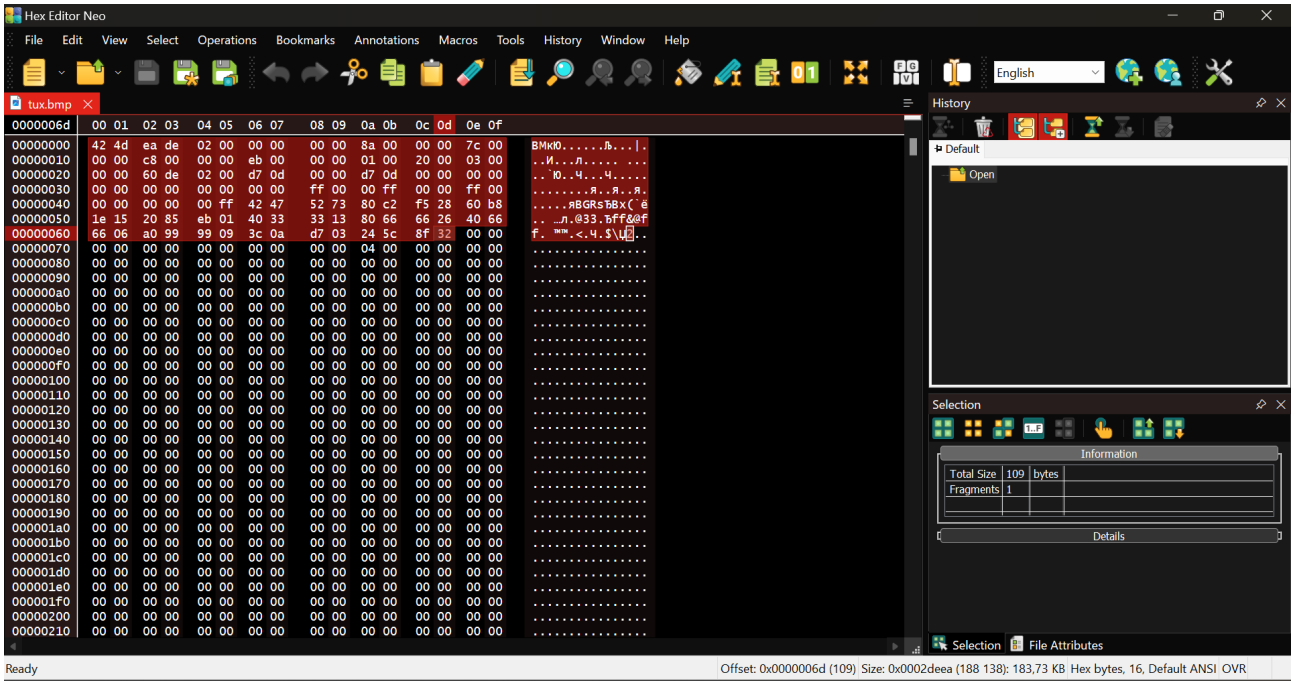

Рисунок 3 –Структура tux.bmp с выделенным заголовком

Таким образом, было принято решение использовать файлы данного формата для обработки, чтобы избежать проблем с контрольными суммами и структурой чанков, присущих формату PNG.

Практическая часть

Для реализации программы, способной зашифровать файл tux.bmp с помощью шифра AES в режимах шифрования ECB, CBC, CFB, OFB, был выбран пакет `javax.crypto` стандартной библиотеки JavaX. Пакет `javax.crypto` является частью *Java Cryptography Architecture (JCA)* и предоставляет набор классов и интерфейсов для поддержки криптографических операций в Java.

Был создан проект на языке Java.

В данной программе для шифрования данных изображения использовался класс `Cipher` из пакета `javax.crypto`. Класс `Cipher` предоставляет функциональность для шифрования и дешифрования данных с использованием различных алгоритмов шифрования.

Для генерации ключа в программе использовался класс `KeyGenerator` также из пакета `javax.crypto`. Класс `KeyGenerator` предоставляет методы для генерации секретных ключей, в том числе для алгоритма шифрования AES.

Общий принцип работы программы:

1. Файл `tux.bmp` считывается в байтовый массив `imageData`.
2. Заголовок изображения копируется в отдельный массив `header`.
3. Остаток байтов из массива `imageData`, исключая заголовок, копируется в отдельный массив `imageDataWithoutHeader`.
4. Данные изображения шифруются с использованием различных режимов шифрования AES, таких как ECB, CBC, CFB и OFB.
5. Генерируется ключ AES с длиной 128 бит с помощью `KeyGenerator`.
6. Создается экземпляр `Cipher`, который инициализируется с использованием ключа AES и указанного режима шифрования.
7. Данные изображения шифруются с помощью `Cipher` в режиме шифрования.

8. Заголовок и зашифрованные данные объединяются в единый байтовый массив `encryptedImage`.
9. Зашифрованное изображение сохраняется в отдельный файл. В файл записывается содержимое массива `encryptedImage`.
10. Процесс шифрования и сохранения повторяется для каждого режима шифрования.

```
public static void main(String[] args) {
    String inputFileName = "tux.bmp";
    byte[] imageData;
    byte[] header;
    int headerLength = 110;

    try {
        // Чтение входного файла изображения
        imageData = Files.readAllBytes(new File(inputFileName).toPath());
        header = new byte[headerLength];
        System.arraycopy(imageData, 0, header, 0, headerLength);

        // Разделение данных заголовка и изображения
        byte[] imageDataWithoutHeader = new byte[imageData.length - headerLength];
        System.arraycopy(imageData, headerLength, imageDataWithoutHeader, 0,
                         imageData.length - headerLength);

        // Сохранение изображения без заголовка в новый файл
        FileOutputStream outputStream = new FileOutputStream("tux_without_header.bmp");
        outputStream.write(imageDataWithoutHeader);
        outputStream.close();

        // Шифрование и сохранение данных изображения
        // с помощью различных режимов шифрования AES
        encryptAndSaveData(imageDataWithoutHeader, header, "ECB");
        encryptAndSaveData(imageDataWithoutHeader, header, "CBC");
        encryptAndSaveData(imageDataWithoutHeader, header, "CFB");
        encryptAndSaveData(imageDataWithoutHeader, header, "OFB");

    } catch (IOException e) {
        e.printStackTrace();
    }
}
```

Листинг 1 – Метод main

Метод `encryptAndSaveData(byte[] imageData, byte[] header, String encryptionMode)` шифрует и сохраняет данные изображения с использованием указанного режима шифрования.

```
public static void encryptAndSaveData(byte[] imageData, byte[] header,
                                       String encryptionMode) {
    try {
        // Генерация AES ключа
        KeyGenerator keyGenerator = KeyGenerator.getInstance("AES");
        keyGenerator.init(128);
        SecretKey secretKey = keyGenerator.generateKey();

        // Инициализация шифра с ключом AES и режимом шифрования
```

```
        Cipher cipher = Cipher.getInstance("AES/" + encryptionMode + "/PKCS5Padding");
        cipher.init(Cipher.ENCRYPT_MODE, secretKey);

        // Шифрование данных изображения
        byte[] encryptedData = cipher.doFinal(imageData);

        // Объединение заголовка и зашифрованных данных изображения
        byte[] encryptedImage = new byte[header.length + encryptedData.length];
        System.arraycopy(header, 0, encryptedImage, 0, header.length);
        System.arraycopy(encryptedData, 0, encryptedImage, header.length,
                         encryptedData.length);

        // Сохранение зашифрованного изображения в новый файл
        String outputFileName = "tux" + encryptionMode + "_encrypted.bmp";
        FileOutputStream outputStream = new FileOutputStream(outputFileName);
        outputStream.write(encryptedImage);
        outputStream.close();

        System.out.println("Image encrypted and saved: " + outputFileName);

    } catch (NoSuchAlgorithmException | NoSuchPaddingException | InvalidKeyException |
                 IllegalBlockSizeException | BadPaddingException | IOException e) {
        e.printStackTrace();
    }
}
```

Листинг 2 – Метод encryptAndSaveData(byte[] imageData, byte[] header, String encryptionMode)

Получившиеся в итоге зашифрованные изображения в формате .bmp:

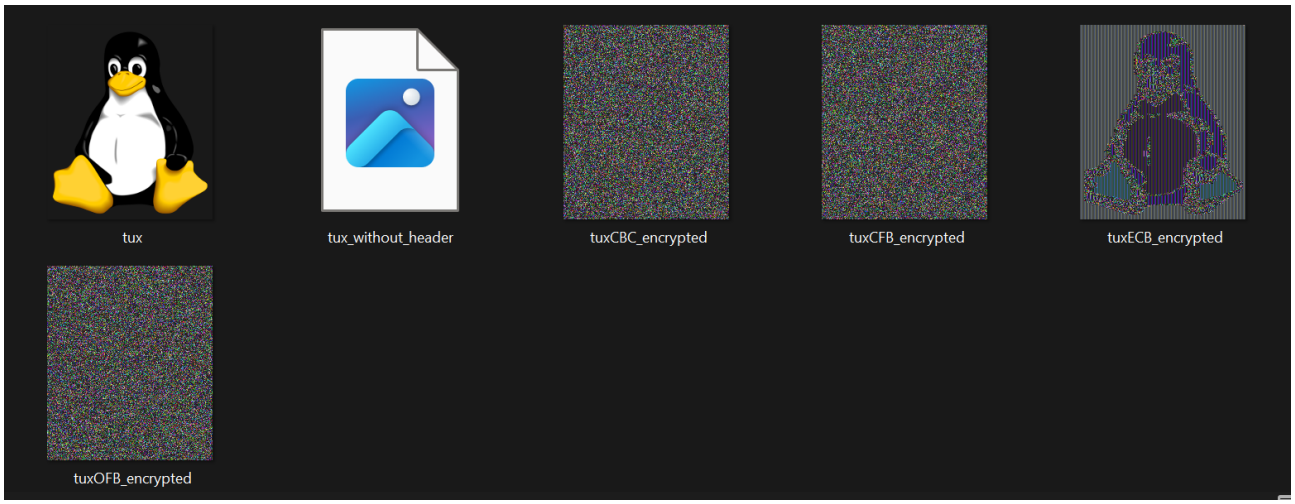

Рисунок 4 – Зашифрованные изображения

Ссылка на проект в репозитории GitHub:

– https://github.com/LazyShAman/dp/tree/main/3.