Лабораторная работа 3: «Применение блочных шифров» [до 5 мая]

1. О деталях реализации и средствах разработки

- Генерация случайного числа для использования в качестве ключа (длина ключа – 128 бит):

```
openssl rand -hex 16 > key.bin
```

- Шифрование файла с помощью шифра AES (длина блока – 256 бит, режим шифрования – CBC):

```
openssl enc -aes-256-cbc -in message.in -out message.enc -pass
↪  file:key.bin
```

  По умолчанию утилита `openssl` извлекает инициализационный вектор из предоставленного пароля. Чтобы указать отдельно ключ и инициализационный вектор, нужно вместо `-pass` использовать `-K` и `-iv` соотвественно.

- Расшифрование файла, зашифрованного с помощью шифра AES:

```
openssl enc -d -aes-256-cbc -in message.enc -out message.dec -pass
↪  file:key.bin
```

2. Постановка задачи

Напишите программу, шифрующую изображение `tux.png` (формат не принципиален) с помощью шифра AES. Режимы шифрования: ECB, CBC, CFB и OFB (нужно получить четыре варианта зашифрованного изображения). В учебных целях заголовочную часть файла зашифровывать не нужно. Сравните скорости выполнения алгоритмов и результаты шифрования.

3. Задания для подготовки к экзамену

1. Распишите (на примере) процедуру применения шифра Simplified DES для шифрования и расшифрования одного блока сообщения. Входные данные: открытое сообщение – 01011101, ключ – 1000000010.

2. Распишите (на примере) процедуру применения шифра Simplified AES для шифрования и расшифрования одного блока сообщения. Входные данные: открытое сообщение – 0010100011010111, ключ – 1011010100001010.