Lab2-Report

Name: Guo Ziyun **No: t0930044** **Group: 7**

Writeup task 3.1

Q1: Experimental Procedures

For the .bmp file, the first 54 bytes contain the header information about the picture, we have to set it correctly, so the encrypted file can be treated as a legitimate .bmp file. We will replace the header of the encrypted picture with that of the original picture.

We run command as follow, which outputs the header information into .txt file:

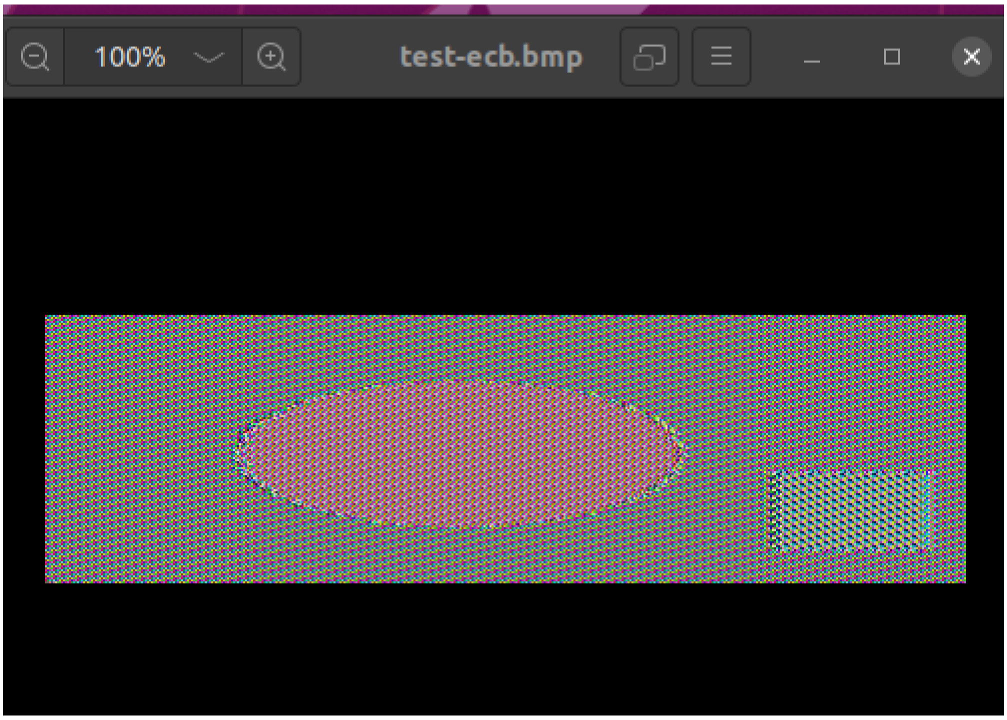
```
head -c 54 1.bmp > header.txt
```

Then we output binary code from the 55th byte into body file, using command as follow:

```
tail -c +55 1.bmp > body.bin
```

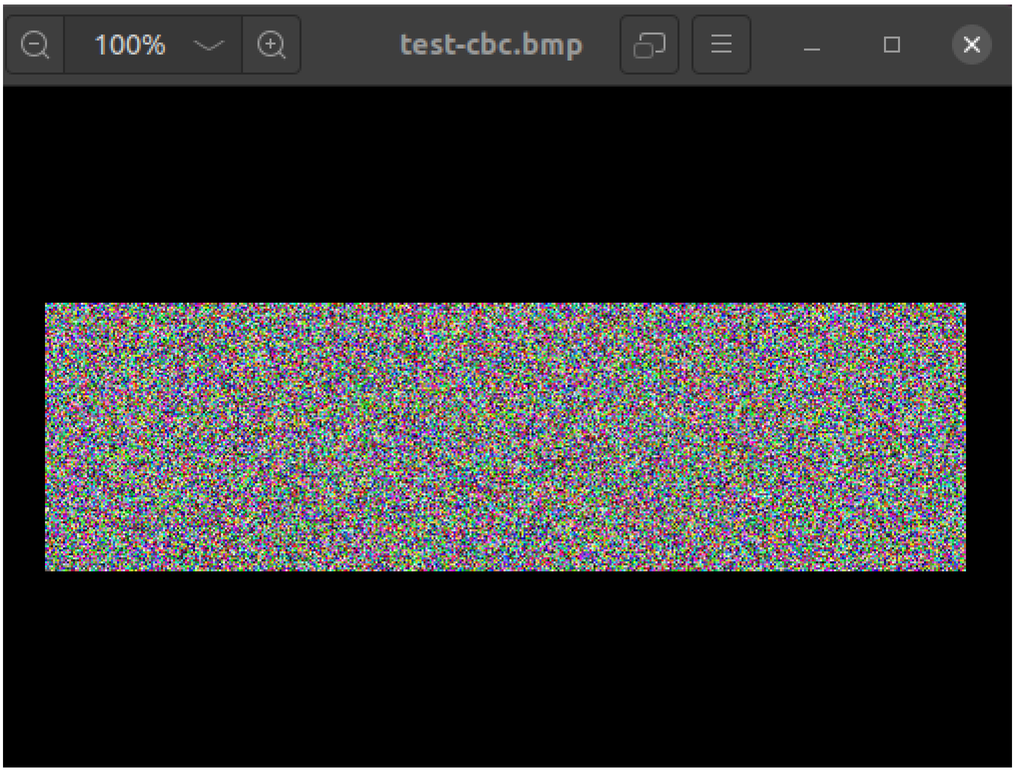
We use ecb mode to encrypt binary body data:

```
openssl enc -aes-128-ecb -e -in body.bin -out body.ecb.bin -k 123456 -iv
0102030405060708
```

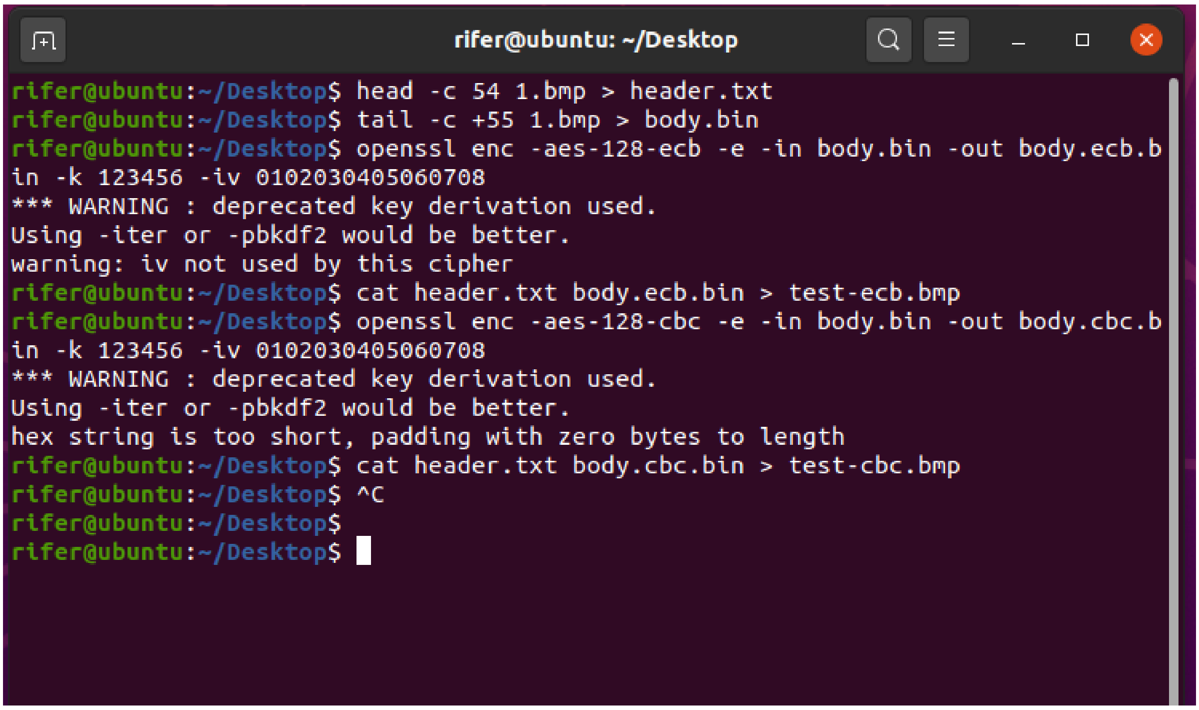


We use cbc mode to encrypt binary body data:

```
openssl enc -aes-128-cbc -e -in body.bin -out body.cbc.bin -k 123456 -iv
0102030405060708
```



Linux command:



```
rifer@ubuntu:~/Desktop$ head -c 54 1.bmp > header.txt
rifer@ubuntu:~/Desktop$ tail -c +55 1.bmp > body.bin
rifer@ubuntu:~/Desktop$ openssl enc -aes-128-ecb -e -in body.bin -out body.ecb.b
in -k 123456 -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
warning: iv not used by this cipher
rifer@ubuntu:~/Desktop$ cat header.txt body.ecb.bin > test-ecb.bmp
rifer@ubuntu:~/Desktop$ openssl enc -aes-128-cbc -e -in body.bin -out body.cbc.b
in -k 123456 -iv 0102030405060708
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
hex string is too short, padding with zero bytes to length
rifer@ubuntu:~/Desktop$ cat header.txt body.cbc.bin > test-cbc.bmp
rifer@ubuntu:~/Desktop$ ^C
rifer@ubuntu:~/Desktop$
rifer@ubuntu:~/Desktop$ 
```

Q2:Analysis

The encryption of each block in ECB is independent and separate, and the same part of the encryption results in the same result, which is more obvious in the image.

The quality of image encryption is determined by the degree of confusion, also known as entropy.

One-dimensional entropy:

$$H = -\sum_{i=0}^{255} p_i \mathrm{log} p_i$$

Writeup task 3.2

Q1: Information Can be Recovered

Answer

- In ECB mode, we can recover all the information except for the corrupted data block.
- In CBC mode,we can recover all the information except for the corrupted data block and the next data block.
- In CFB mode, to achieve greater flexibility, CFB mode introduces an integer parameter s. Plaintext is divided into blocks of size s. Furthermore, the length of the plaintext must be a multiple of s.In an s-bit CFB mode, the input to the encryption function is a shift register of size b. A single bit error in a ciphertext block can affect the decryption of at most

$$\lceil \frac{b}{s} \rceil$$

subsequent blocks.

- In OFB mode, if a single bit in the ciphertext is corrupted, **it will only affect the corresponding bit in the decrypted plaintext**. It will not impact the decryption of other ciphertext blocks.

Q2: Explaination

Answer

- **In ECB mode**, the encryption and decryption of each data block are independent of each other. Therefore, if a single bit in a data block is corrupted, only the decryption result of that specific block will be affected, while the other blocks can still be decrypted correctly. As a result, you can recover all the information except for the corrupted data block.
- **In CBC mode**, the encryption algorithm takes as input the current plaintext block Mi and the XOR of the previous ciphertext block Ci-1, and outputs the ciphertext block Ci. Due to the introduction of feedback, when there is a transmission error in the ciphertext caused by channel noise or other interference, a single bit error in the ciphertext will affect the decryption of the current block and the next block, but it will not impact other blocks.
- **In CFB mode**, to achieve greater flexibility, CFB mode introduces an integer parameter s. Plaintext is divided into blocks of size s. Furthermore, the length of the plaintext must be a multiple of s.This allows CFB mode to directly encrypt data with a length smaller than b by choosing an appropriate value for s. In an s-bit CFB mode, the input to the encryption function is a shift register of size b, which is initialized with an initialization vector (IV). The encryption function XORs the most significant (leftmost) s bits of the processed result with the first plaintext block M1 to generate the ciphertext block C1. Simultaneously, the value of the shift register is left-shifted by s bits, and the lowest (rightmost) s bits of the register are replaced with C1. This process is repeated until the encryption is complete.
  Due to the use of ciphertext feedback, in CFB mode, if a ciphertext block experiences one or

more bit errors during transmission, it will result in decryption errors not only in the current block but also in subsequent partial blocks. This is because decryption can only recover correctly once the erroneous ciphertext bits have been shifted out of the shift register. So a single bit error in a ciphertext block can affect the decryption of at most

$$\lceil \frac{b}{s} \rceil$$

subsequent blocks.

- **In OFB mode**, if a single bit in the ciphertext is corrupted, it will only affect the corresponding bit in the decrypted plaintext. It will not impact the decryption of other ciphertext blocks.Therefore, only the directly mapped plaintext bit of the corrupted bit will be affected, and the decryption of other ciphertext blocks will remain unaffected. This is because in OFB mode, the encryption keystream is not dependent on the plaintext or ciphertext but is solely based on the initialization vector (IV) and key generation. Hence, errors will not propagate to other ciphertext blocks in the subsequent decryption process.

Q3: Implication of Differences

The implications of these differences lie in the scope of the affected data and the amount of recoverable information. The advantage of ECB mode is that even if part of the data is corrupted, it can still correctly decrypt other data blocks. However, its drawback is the inability to hide patterns in the plaintext. In contrast, CBC, CFB, and OFB modes provide better error propagation and data hiding capabilities. However, in the case of partial data corruption, they cannot recover information beyond the damaged data block. Therefore, when choosing an encryption mode, it is important to consider the impact of these differences based on specific security requirements and data integrity considerations.