Project 1: Implement CTR and CBC modes for AES-256

Chaoyun Li

September 2022

1 The cipher

The official spec and test vectors of AES-256 is available online[1]. For this project you should install the PyCryptodome library[2]. In your implementations, you are only allowed to use the ECB mode as a function doing an AES encryption or decryption on a 128-bit block.

```
from Crypto.Cipher import AES
key = get_random_bytes(32)
cipher = AES.new(key, AES.MODE_ECB)
```

For more details of the library, please refer to the documentation of the Crypto.Cipher package[3].

2 Your tasks

The main tasks:

1. Implement the CTR and CBC modes for AES-256. You should implement both encryption and decryption functions.

2. Use both of your implementations to encrypt a long message and then decrypt the ciphertext. You need to check if the decrypted message is identical to the original plaintext. If not matched, then clearly your implementation has some problems. Please download the file plaintext.txt from Moodle.

3. Redo the encryption and decryption by calling the Crypto.Cipher.AES.MODE_CBC and Crypto.Cipher.AES.MODE_CTR, respectively. Compare the time used by your implementations and by the library implementations.

[1] https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901427
[2] https://pycryptodome.readthedocs.io/en/latest/index.html
[3] https://pycryptodome.readthedocs.io/en/latest/src/cipher/cipher.html

To ease the grading, please submit the source codes and write detailed comments in your codes! Please also submit a README file to show how to run your programs to reproduce your result. Please also submit the encrypted message in a txt file.

Your experimental results should be summarized in a report. The report should contain the following details.

- In your implementation, how you set up the key and IV.
- How do you encode the message so that your implementations can be applied. (Hint: encoding methods including ASCII and base64 can be found at `https://en.wikipedia.org/wiki/Binary-to-text_encoding`)
- How long it takes to do the encryption and decryption with your implementations and the library implementations.