Lab08 - Block Ciphers - Baby Rijndael and AES

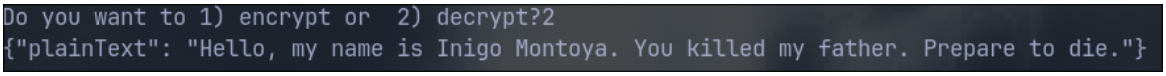
Part 01

1. **Encrypt the plaintext 372c using the key of 6b5d.**
    a. **You need to output the labels for each state and the final ciphertext block to earn full credit.**
    (10 points total)
    b. Please upload a **separate document (like my example)** to Canvas.
    (10 points total)
    c. **Correct encrypted value** plainly shown
    (10 points total)

2. **Functional code submitted to Canvas.**
    (10 points total)

Part 02

3. **Include a screenshot of the json dumps result when encrypting the part02_plainText.json in your lab report. Must be 4 fields**
    (10 points total)
    - {"nonce": "OsJ6453RzUJQlsRIDOZ34Q==", "tag": "txhR6naB0UE9UGN1ntWgdA==", "cipherText": "Et5AwogS1Xlv5Xs5De9Vd8odhyG04GmdzS0H95B+yMhznUJdgjqzljwcuh+LaSaB5MyFCpZVRuMp4rH//fZoebVe1+f0WQ==", "key": "dSIw6FZ2vAfkaNMwfAxtiA==}

4. **Include a screenshot of the json dumps result when decrypting the encrypted part02_plainText.json you just encrypted in your lab report.**
    (10 points total)
    - 

5. Attempt to decrypt the cipherText found in `part02_cipherText_a.json`. *This will result in an **intentional** error for this part of the lab.* **Explain what the error means and why it would occur.**
    (10 points total)
    - The message authentication code error in this situation means that there is something wrong with the expected authentication tag. If the expected tag during the decryption process doesn't match the one during decryption then this error can occur.

6. **Include a screenshot of the error in your lab report.**
    (10 points total)

-
```
[tech180@TechTop-G14L:~/Documents/College/fall2023/cpre331/lab08/part02]$ python3 part02_skel.py part02_cipherText_a.json
test.json
Do you want to 1) encrypt or  2) decrypt?2
Traceback (most recent call last):
  File "/home/tech180/Documents/College/fall2023/cpre331/lab08/part02/part02_skel.py", line 170, in <module>
    main()
  File "/home/tech180/Documents/College/fall2023/cpre331/lab08/part02/part02_skel.py", line 143, in main
    plainText = cipher.decrypt_and_verify(cipherText, tag)
                ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/nix/store/j2h053vxhml7slvwfpyf1jch7hla029a-python3-3.11.4-env/lib/python3.11/site-packages/Crypto/Cipher/_mode_gc
m.py", line 567, in decrypt_and_verify
    self.verify(received_mac_tag)
  File "/nix/store/j2h053vxhml7slvwfpyf1jch7hla029a-python3-3.11.4-env/lib/python3.11/site-packages/Crypto/Cipher/_mode_gc
m.py", line 508, in verify
    raise ValueError("MAC check failed")
ValueError: MAC check failed
```

7. **Include a screenshot of the json dumps result when decrypting part02_cipherText_b.json in your lab report.**
   (10 points total)
   -
```
Do you want to 1) encrypt or  2) decrypt?2
{"plainText": "I do not mean to pry, but you don't by any chance happen to have six fingers on your right hand?"}
```

8. **Upload python code for part 02**.
   (10 points)