Lab 07 - Block Ciphers Baby Fiestel (DES)

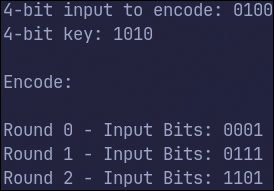
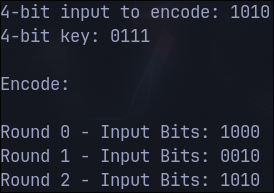
**Part 01**

* 1. **Upload python code for babyFeistel cipher**

(10 points)

* 1. **Final 4-bit ciphertext**

(10 points)

* 
* 
  1. **Screenshot of encrypting**

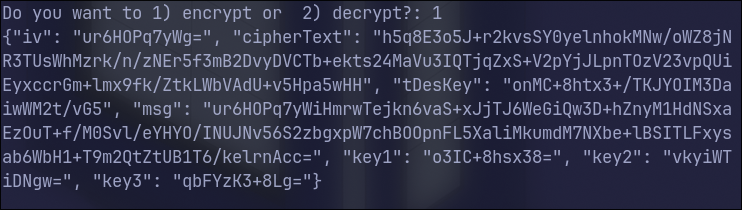
(10 points)

* 

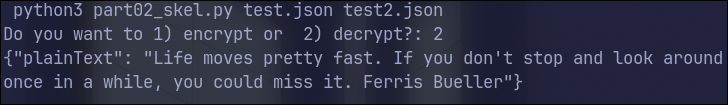
**Part 02**

* 1. **Include a screenshot of the json dumps result when encrypting the part02\_plainText.json in your lab report. Must be 7 fields**

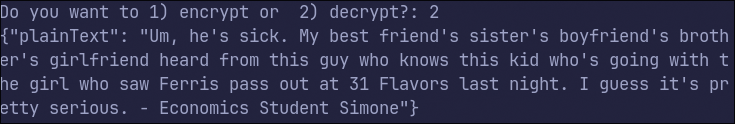
(10 points total)

* 
  1. **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)

* 
  1. **Include a screenshot of the json dumps result when decrypting part02\_cipherText.json in your lab report.**

(10 points total)

* 
  1. Upload python code for part 02.

(10 points)

* 1. What block cipher mode are you using in this implementation of Triple DES?

(10 points)

* It tells you within this line   
  cipher = DES3.new(tDesKey, DES3.MODE\_CFB)  
  Which is Cipher Feedback Mode.
  1. Explain why, even though you create 24 bytes of key, the effective key size is 112 bits. (10 points)
* The keying process is done by using 56-bit keys. The three keys 1,2,3 are different by the middle key being the same as the first key and the third key being the same as the middle key. This reduces the choices because there are only 2^56 possible keys. Since the middle stage acts as an decryption, it reduces the key to 112 because the first and third stages must use the same key.
  1. Historically, there has been a way to use a single key in Triple DES where you set key1=key2=key3. Why would you want to do that? What is the effective key size when key1=key2=key3?

(10 points)

* When key1=key2=key3 it reduces 3DES to DES. This is because the middle stage is decryption, and pretty much undoes the encryption performed by the first step and doesn’t provide additional security and the effective key size is still only 56 bits. So you might as well just use DES than go through a slower process with the same result.