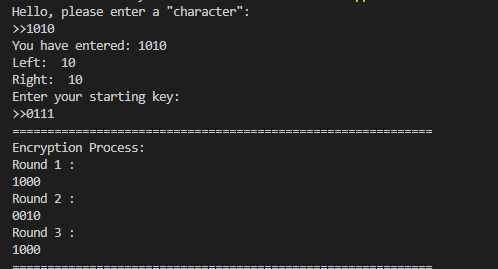
**Part 1:**

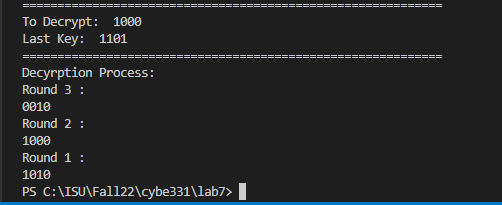
1. Upload python code for baby Feistel cipher.
   1. Attached.
2. 4-bit ciphertext.



1. Screenshot of encrypting and decrypting.
   1. Encryption:

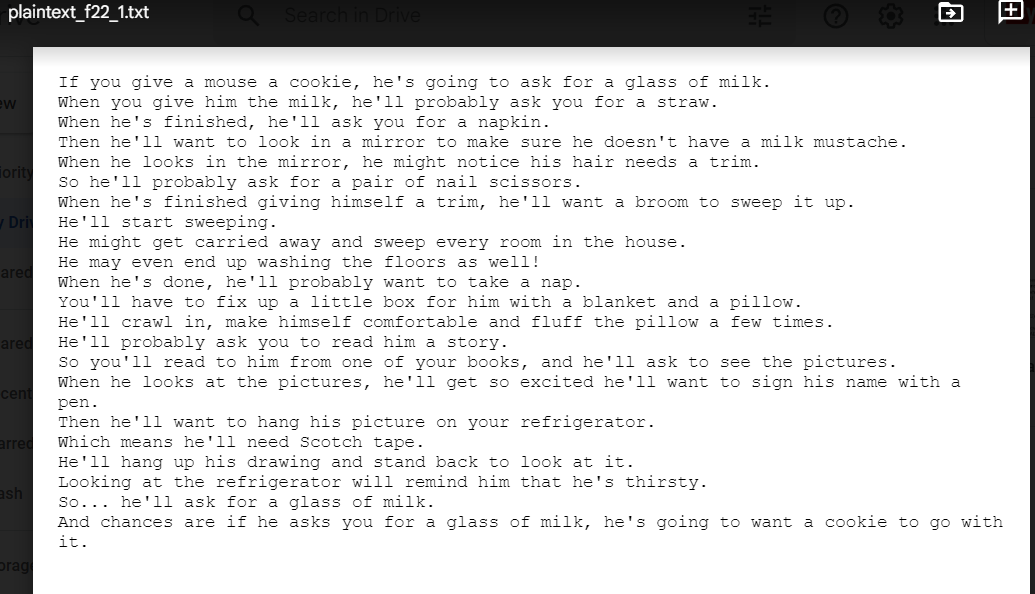


* 1. Decryption:



**Part 2:**

1. Decrypt cipher and record the title, author, and plaintext.
   1. Title: If You Give A Mouse A Cookie.
   2. Author: Laura Numeroff
   3. Plaintext:



1. Encrypt the plaintext provided and upload to Canvas.
   1. Attached

**Part 3:**

1. How many iterations for each cipher in 3 seconds using 8192-byte size blocks?
   1. GCM: 1203872 iterations
      1. 
   2. CBC: 300716 iterations
      1. 
2. How many megabytes can each cipher encrypt per second using 8192-byte size blocks?
   1. GCM: 3287.37 MB
   2. CBC: 821.16 MB
3. Which one is faster? Why?
   1. Each block in GCM gets encrypted independently, as it isn’t technically chained - thus allowing it to take advantage of multi-core processing whereas CBC is a chained block algorithm - thus requiring the previous block to be generated before carrying on - thus a slower throughput.

**Part 4:**

1. Submit the name of my favorite OS.
   1. FreeBSD
2. Answer the questions about my favorite OS.
   1. What mistake did I make?
      1. Used ECB block mode using a 128 bit key.
   2. What problem with this particular type of cipher block mode does this picture demonstrate?
      1. This picture demonstrates that ECB leaks information about the plaintext
   3. How do you get rid of this problem?
      1. It seems that even with an exceptionally long key, ECB will still leak information about the plaintext - therefore it is better to use another block key method.
3. Submit an encrypted bmp of your favorite OS’s mascot.
   1. Attached.