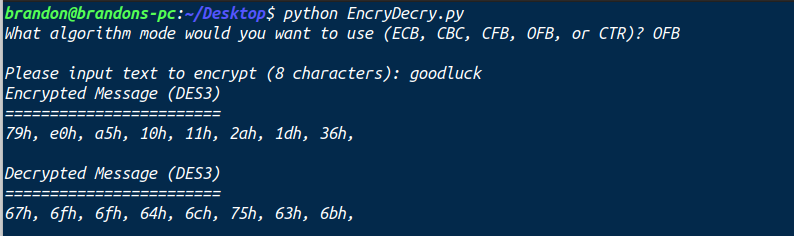
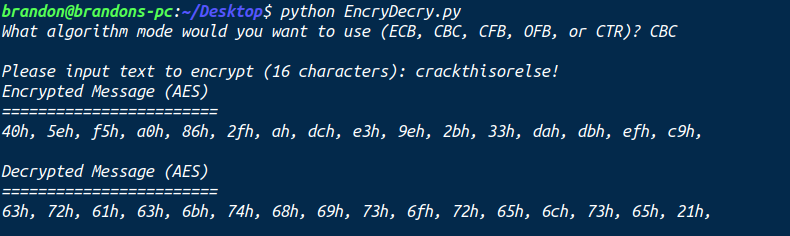
**Task 1 Implement DES and AES ciphers. (50 points)**  
  
I used OFB (output feedback) for encrypting and decrypting with DES3 (Data Encryption Standard) as shown below:



I used CBC (cipher block chaining) for encrypting and decrypting with AES (Advanced Encryption Standard) as shown below:



**Task 2 Investigate Properties of Modes in DES and AES (50 points)**

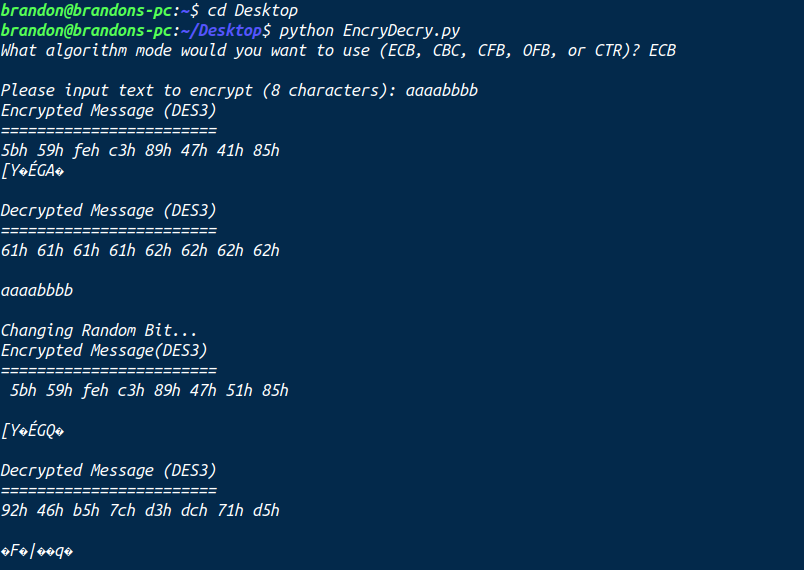
I used DES3 with the five modes (ECB, CBC, CFB, OFB, and CTR). The mode that the script will run depends on the mode that is given by the user input. The script will ask the user to select a mode, then the text they want to encrypt (must be in blocks of 8 characters).

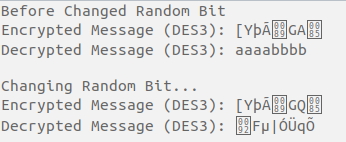
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | ECB | CBC | CFB | OFB | CTR |
| Pattern preservation |  |  |  |  |  |
| Error propagation |  |  |  |  |  |

I was unable to use the CTR mode with DES3, so I did it with AES instead. From my testing, the pattern was not persevered for any of the modes of encryption.

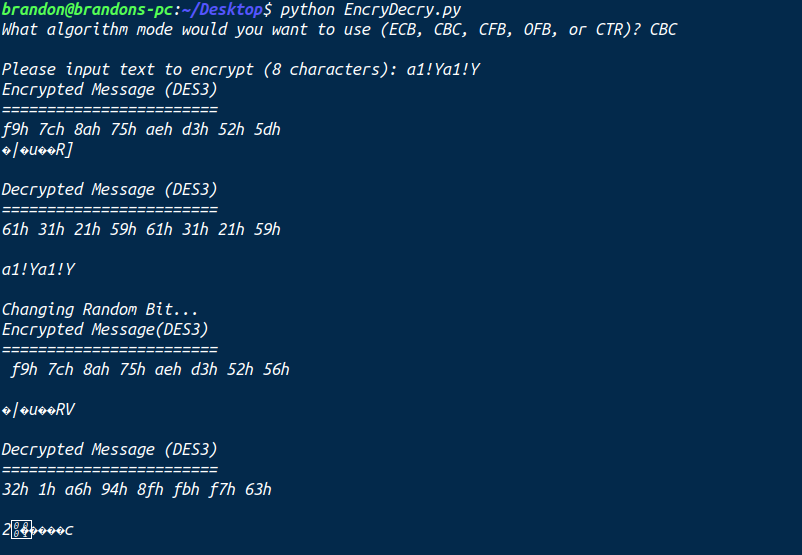
**Test Cases:**

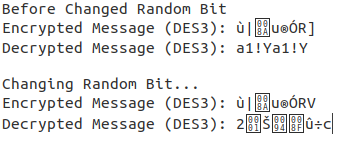
**Case 1 (DES3 & ECB):**

Output To File:

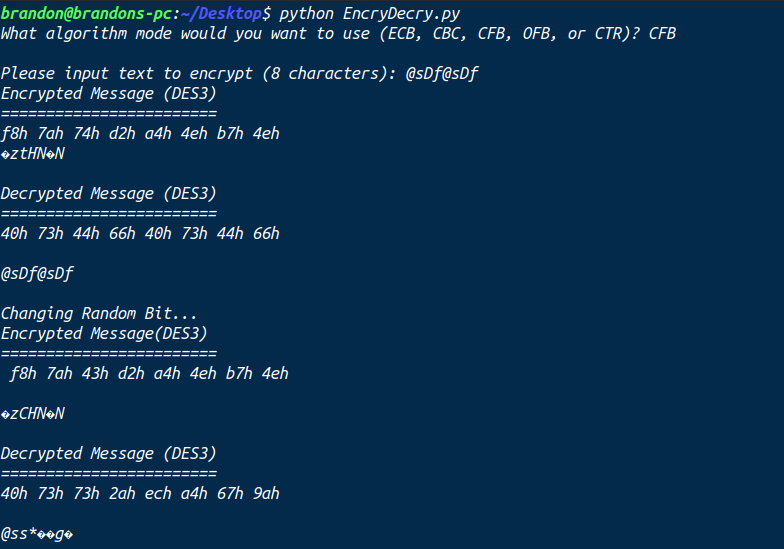


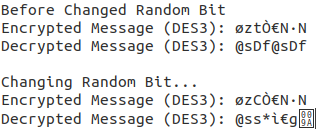
**Case 2 (DES3 & CBC):**

Output To File:

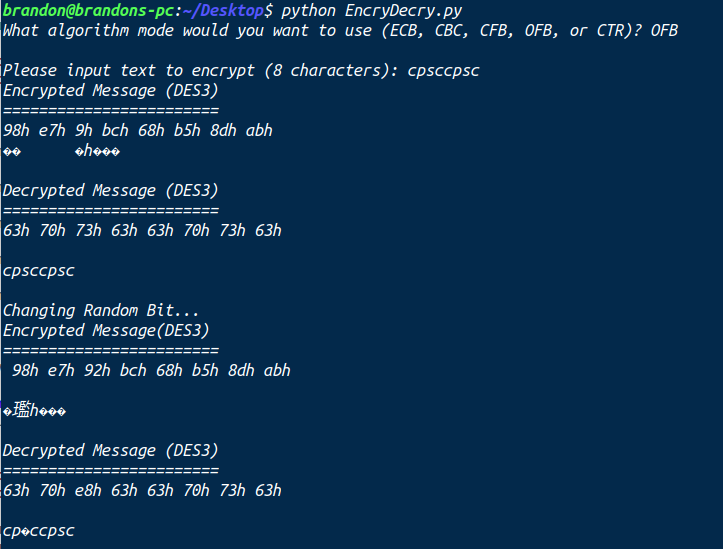


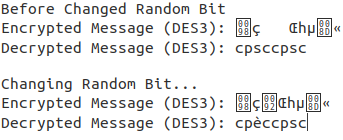
**Case 3 (DES3 & CFB):**

Output To File:

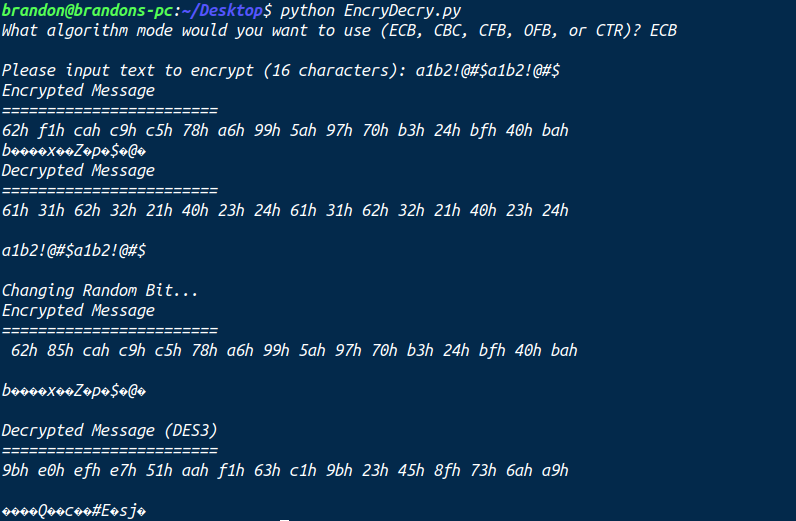


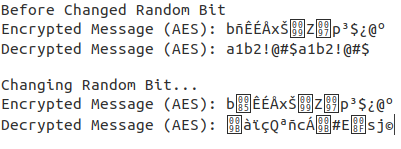
**Case 4 (DES3 & OFB):**

Output To File:

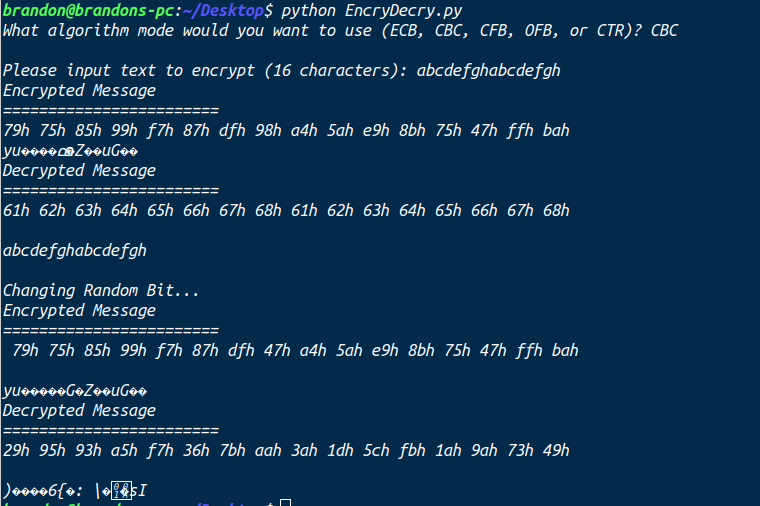


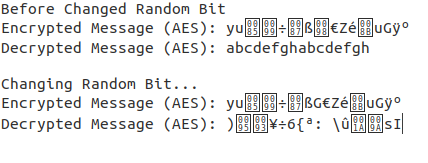
**Case 5 (AES & ECB):**

Output To File:

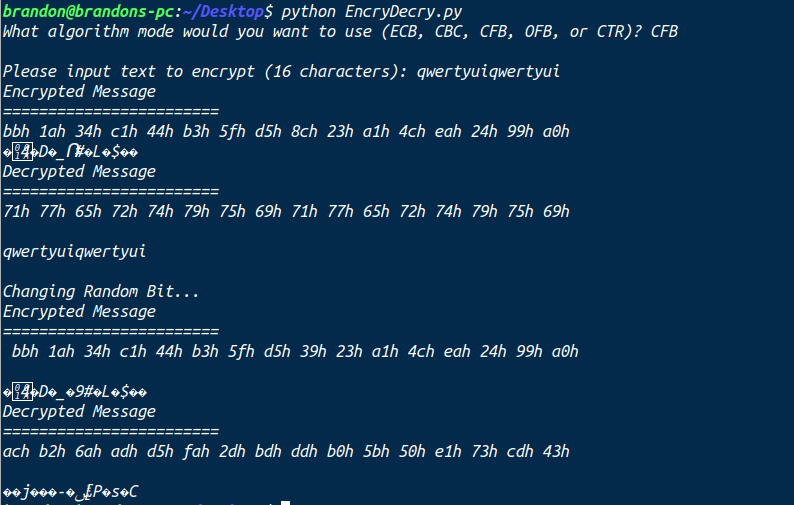


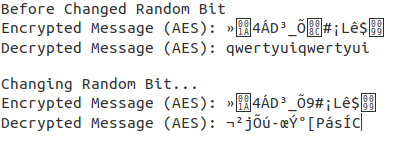
**Case 6 (AES & CBC):**

Output To File:



**Case 7 (AES & CFB):**

Output To File:



**Case 8 (AES & OFB):**

**Case 9 (AES & CTR):**

As for error propagation,

Conclusion ...