7402 Asn 4 Testing and User Guide

“How to flip the bits today? i dare say! a pinch of left with a dash of right will hide our message in the night”

Isaac Morneau; A00958405
John Agapeyev; A00928238

User Guide

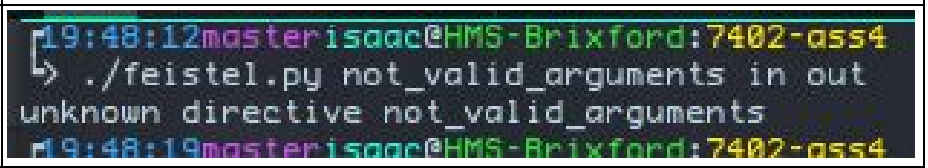
The program is very straightforward as follows:

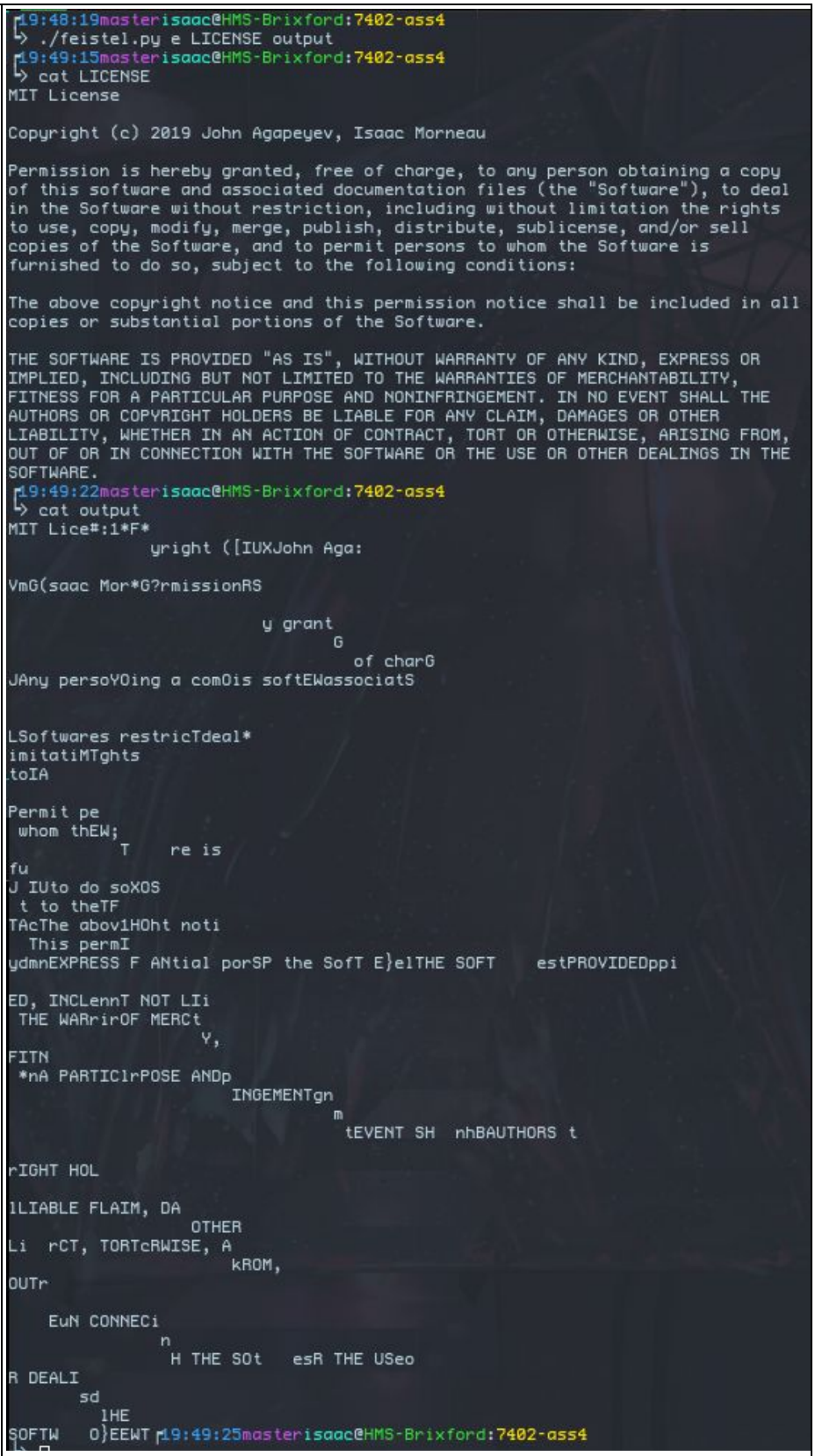
```
./feistel.py
usage: ./feistel.py {e, d} /path/to/input /path/to/output
```

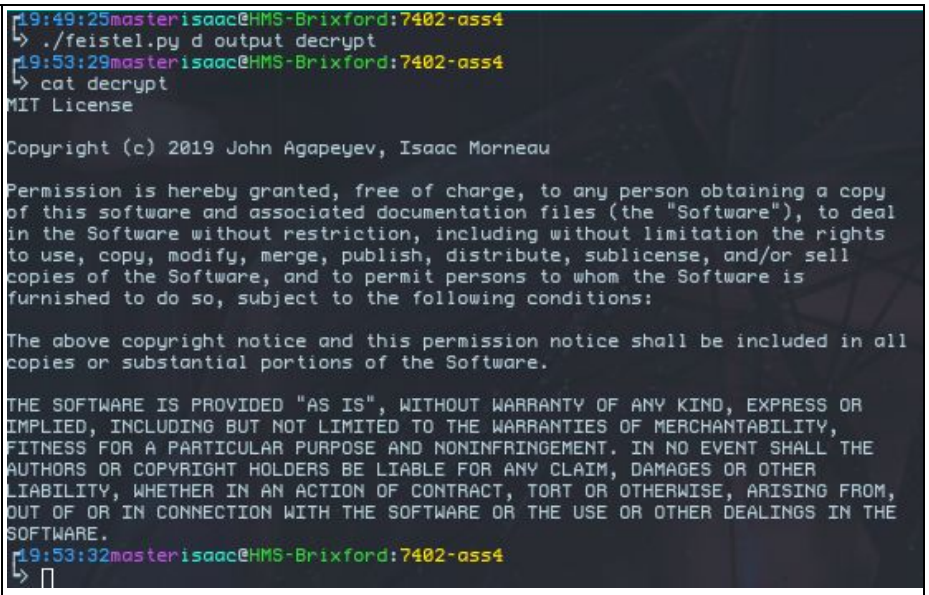
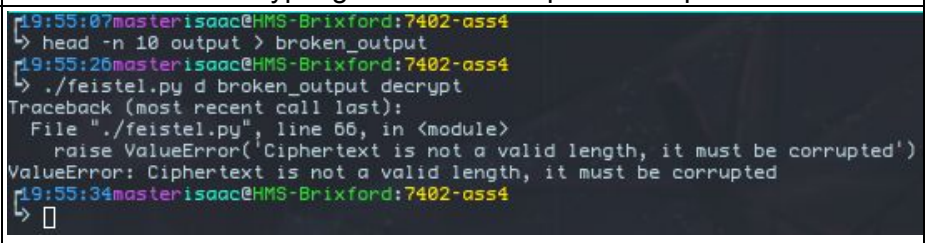
E is for encrypt

D is for decrypt

Testing

Test	Steps	Result
Get usage info	Run ./feistel.py alone	
Argument Validation	Run ./feistel.py not_valid_arguments in out	

Sample Encryption	./feistel.py e LICENCE out	 While the encryption is poor, its due to the poor choice of f

Simple Decryption	Run the test case above ./feistel.py d output decrypt	 As can be seen decrypting reverses the cipher as expected
Broken data	Run the simple encryption test case Run head -n 10 output > broken_output Run ./feistel.py d output decrypt	 The program detects when padding removed and the data was corrupted

Analysis

Figures Used

Function
Times each element in x by the round number then left shift it by key bits
F i(x) -> for E in x:
    E *= i
    E <<= k

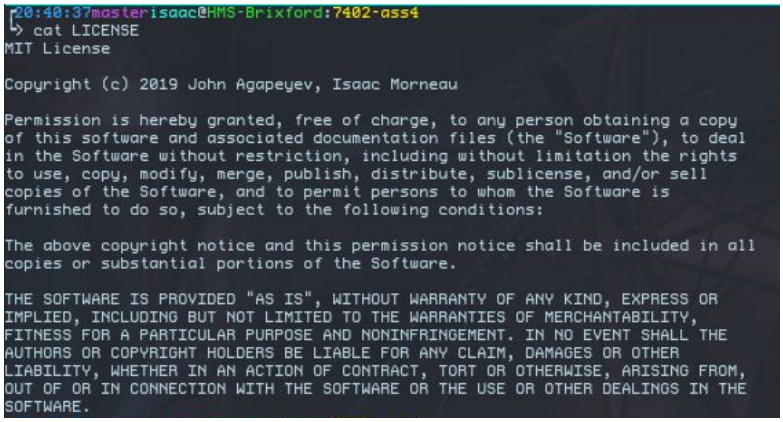


Figure 1 plane text

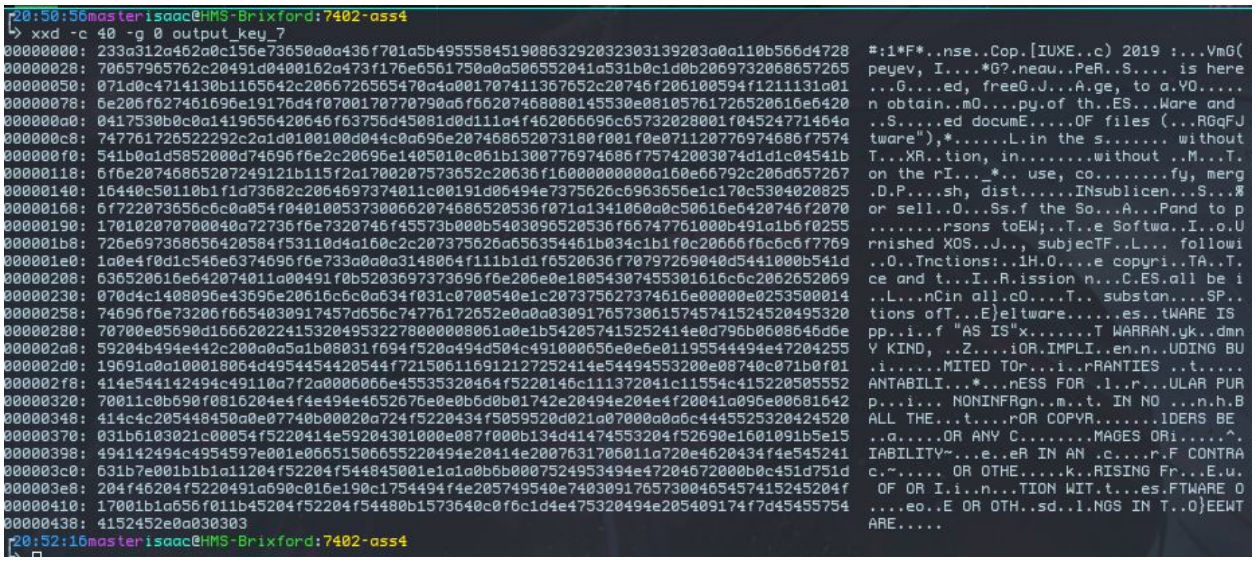


Figure 2 secret key: 7

Figure 3 secret key: 6

Diffusion

Comparing Figure 1 and Figure 2 you can see that not only was the change minor but in fact it made the encryption even worse than it was before. The function specified has horrible diffusion.

Confusion

Comparing figure 1 to figure 2 then comparing figure 1 to figure 3 it’s clear that much of the plaintext is clearly visible and has not been changed at all. This represents terrible confusion as well.