7402 Asn 5 Testing and User Guide

“Slightly more secure than a 5 dollar wrench”

Isaac Morneau; A00958405
John Agapeyev; A00928238

User Guide 3

Testing 4

User Guide

Usage is all command line and is as follows.

```
usage:
    ./feistel.py [function] [mode] [quality] [input filename] [output filename]
            function is 'e' for encrypt, 'd' for decrypt
            mode is 'ecb' for ecb, 'cbc' for cbc, and 'ctr' for ctr
            quality is 'e' for easy, 'm' for medium, 'h' for hard

    ./feistel.py t [input filename]
            runs automated tests to compare the different modes using a given file
```

For example to encrypt:

```
./feistel.py e cbc h input.txt output.txt
```

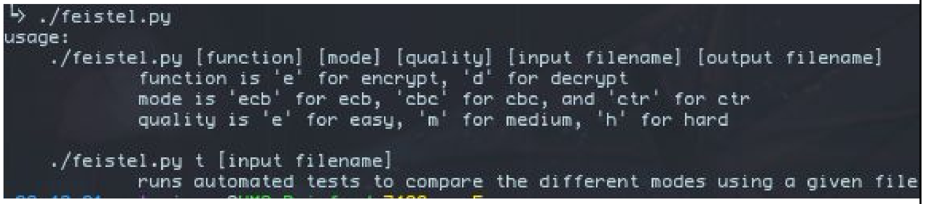
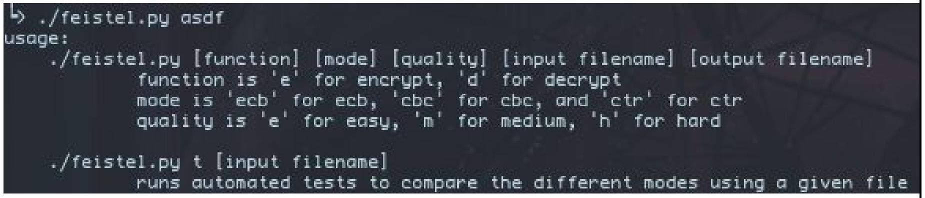
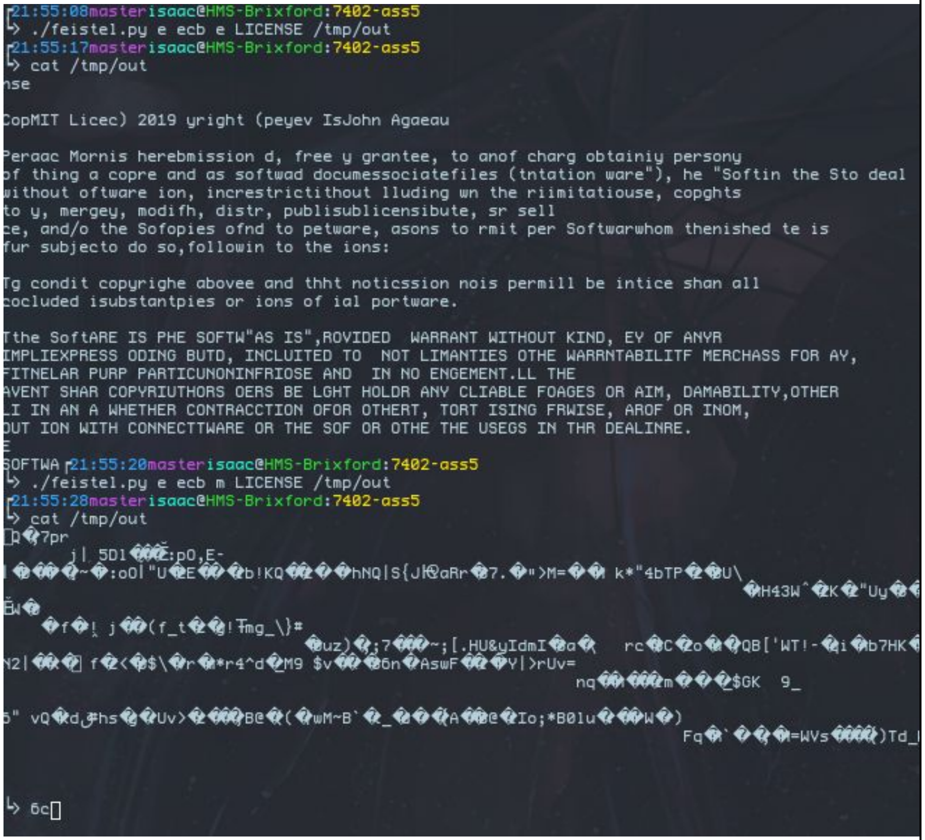
Would encrypt the file input.txt with AES in CBC mode

Likewise

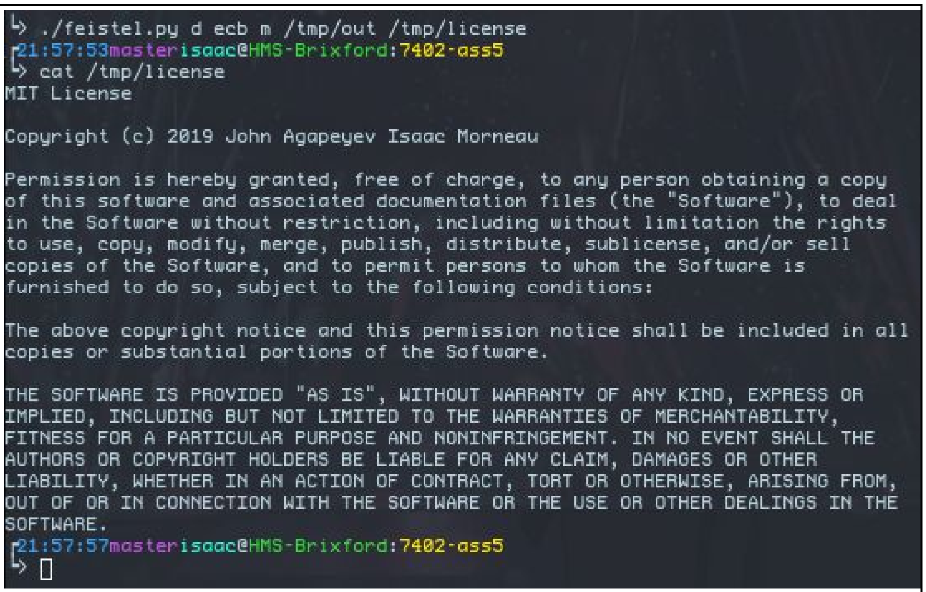
```
./feistel.py t input.txt
```

Would use the input.txt file as the plaintext for running the tests

Testing

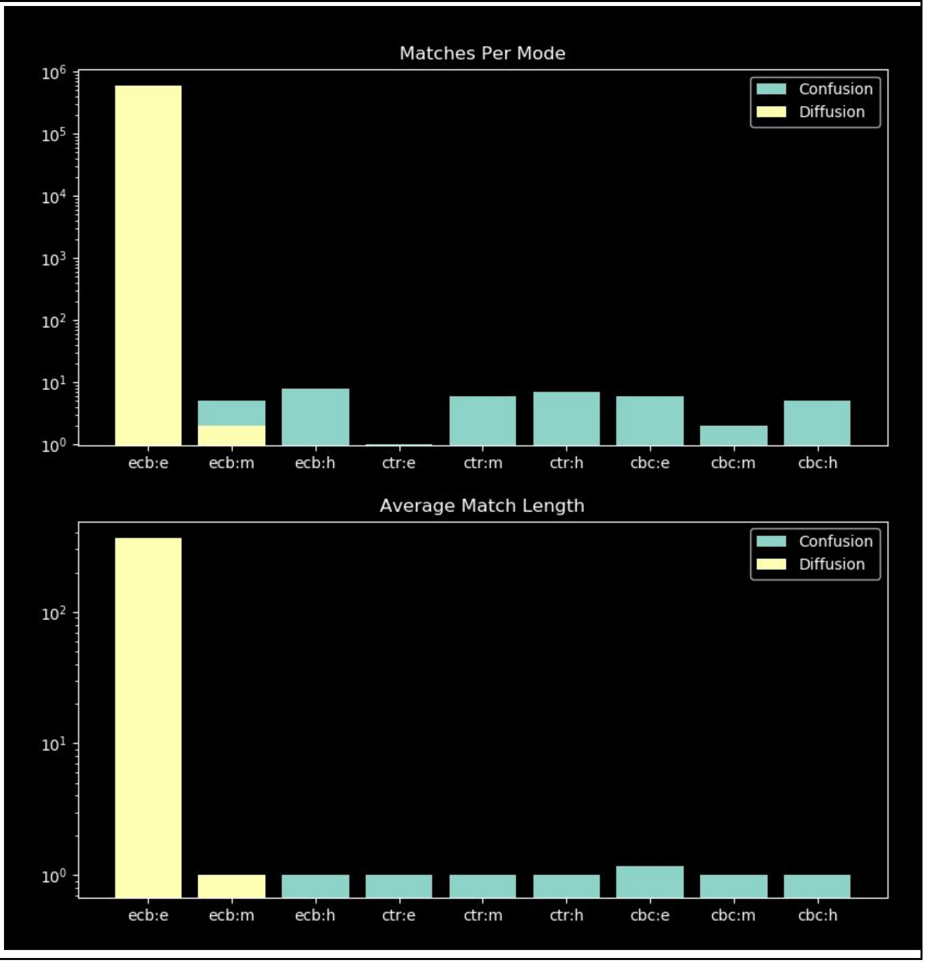
Test	Steps	Result
Get usage info	Run ./feistel.py alone	 ↳ ./feistel.py usage: ./feistel.py [function] [mode] [quality] [input filename] [output filename] function is 'e' for encrypt, 'd' for decrypt mode is 'ecb' for ecb, 'cbc' for cbc, and 'ctr' for ctr quality is 'e' for easy, 'm' for medium, 'h' for hard ./feistel.py t [input filename] runs automated tests to compare the different modes using a given file
Argument Validation	Run ./feistel.py asdf	 ↳ ./feistel.py asdf usage: ./feistel.py [function] [mode] [quality] [input filename] [output filename] function is 'e' for encrypt, 'd' for decrypt mode is 'ecb' for ecb, 'cbc' for cbc, and 'ctr' for ctr quality is 'e' for easy, 'm' for medium, 'h' for hard ./feistel.py t [input filename] runs automated tests to compare the different modes using a given file
Sample Encryption	Run ./feistel.py e ecb e LICENSE /tmp/out Run ./feistel.py e ecb m LICENSE /tmp/out	 ┌21:55:08masterisaac@HMS-Brixford:7402-ass5 ↳ ./feistel.py e ecb e LICENSE /tmp/out ┌21:55:17masterisaac@HMS-Brixford:7402-ass5 ↳ cat /tmp/out nse CopMIT Licec) 2019 yright (peyev IsJohn Agaeau Peraac Mornis herebmission d, free y grantee, to anof charg obtainiy persony of thing a copre and as softwad documessociatefiles (tntation ware"), he "Softin the Sto deal without oftware ion, increstrictithout llluding wn the riimitatiouse, copghts to y, mergey, modifh, distr, publisublicensibute, sr sell ce, and/o the Sofopies ofnd to petware, asons to rmit per Softwarwhom thenished te is fur subjecto do so,followin to the ions: Tg condit copyrighe abovee and thht noticssion nois permill be intice shan all cocluded isubstantpies or ions of ial portware. Tthe SoftARE IS PHE SOFTW"AS IS",ROVIDED WARRANT WITHOUT KIND, EY OF ANYR IMPLIEXPRESS ODING BUTD, INCLUITED TO NOT LIMANTIES OTHE WARRNTABILITF MERCHASS FOR AY, FITNELAR PURP PARTICUNONINFRIOSE AND IN NO ENGEMENT.LL THE AVENT SHAR COPYRIUTHORS OERS BE LGHT HOLDR ANY CLIABLE FOAGES OR AIM, DAMABILITY,OTHER LI IN AN A WHETHER CONTRACCTION OFOR OTHERT, TORT ISING FRWISE, AROF OR INOM, OUT ION WITH CONNECTTWARE OR THE SOF OR OTHE THE USEGS IN THR DEALINRE. E SOFTWA ┌21:55:20masterisaac@HMS-Brixford:7402-ass5 ↳ ./feistel.py e ecb m LICENSE /tmp/out ┌21:55:28masterisaac@HMS-Brixford:7402-ass5 ↳ cat /tmp/out □Q�7pr j| 5D1���:p0,E- |����~�:oOl"U�E����b!KQ����hNQ|S{J�aRr�7.�">M=�� k*"4bTP��U\ �H43W^�K�"Uy�� ĔW� �f�! j��(f_t��!Ŧmg_\}# �uz)�;7���~;[.HU&yIdmI�a� rc�C�o��QB['WT!-�i�b7HK� N2|���] f�<�$\�r�*r4^d�M9 $v��6n�AswF���Y\|>rUv= nq�����m���$GK 9_ 5" vQ�d,#hs��Uv>����BE�(�wM~B`�_���A��e�Io;*B0lu���W�) Fq�`���=WVs����)Td_ ↳ 6c□ While the easy encryption is quite poor once the encryption is medium or higher the data is no longer trivially recoverable.

<table>
<tr>
<td>Simple Decryption</td>
<td>Run ./feistel.py d ecb m /tmp/out /tmp/license</td>
<td>



```
↳ ./feistel.py d ecb m /tmp/out /tmp/license
┌21:57:53masterisaac@HMS-Brixford:7402-ass5
↳ cat /tmp/license
MIT License

Copyright (c) 2019 John Agapeyev Isaac Morneau

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
┌21:57:57masterisaac@HMS-Brixford:7402-ass5
↳
```

</td>
</tr>
<tr>
<td>Testing Graphs</td>
<td>Run ./feistel.py t LICENSE</td>
<td>



</td>
</tr>
</table>