

# 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

<b>User Guide</b>	<b>3</b>
<b>Testing</b>	<b>4</b>
<b>Analysis</b>	<b>7</b>
Figures Used	7
Diffusion	8
Confusion	8

# 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	<pre>19:44:25masterisaac@HMS-Brixford:7402-ass4 ↳ ./feistel.py usage: ./feistel.py {e, d} /path/to/input /path/to/output 19:44:27masterisaac@HMS-Brixford:7402-ass4</pre>
Argument Validation	Run ./feistel.py not_valid_arguments in out	<pre>19:48:12masterisaac@HMS-Brixford:7402-ass4 ↳ ./feistel.py not_valid_arguments in out unknown directive not_valid_arguments 19:48:19masterisaac@HMS-Brixford:7402-ass4</pre>

<p>Sample Encryption</p>	<p>./feistel.py e LICENSE out</p>	<pre> 19:48:19masterisaac@HMS-Brixford:7402-ass4 &gt; ./feistel.py e LICENSE output 19:49:15masterisaac@HMS-Brixford:7402-ass4 &gt; cat 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. 19:49:22masterisaac@HMS-Brixford:7402-ass4 &gt; cat output MIT Lice#:#F# yright ([IUXJohn Aga:  VmG(saac Mor*G?rmissionRS  y grant G of charG JAny persoYDing a com0is softEWassociatS  LSoftwares restricTdeal* imitatiMTghts toIA  Permit pe whom thEW; T re is fu J IUto do soXOS t to theTF TAcThe abov1HOht noti This permI ydmnEXPRESS F ANtial porSP the Soft E)eIthe SOFT estPROVIDEDppi  ED, INCLennT NOT LIi THE WARrriOF MERct y, FITN *nA PARTIClrPOSE ANDp INGEMENTgn m teVENT SH nhBAUTHORS t  rIGHT HOL  1LIABLE FLAIM, DA OTHER Li rCT, TORTcRWISE, A kROM, OUTr  EuN CONNECi n H THE SOt esR THE USeo  R DEALI sd IHE SOFTW 0}EEWT 19:49:25masterisaac@HMS-Brixford:7402-ass4 </pre>
		<p>While the encryption is poor, its due to the poor choice of f</p>

Simple Decryption	Run the test case above ./feistel.py d output decrypt	<pre> 19:49:25masterisaac@HMS-Brixford:7402-ass4 &gt; ./feistel.py d output decrypt 19:53:29masterisaac@HMS-Brixford:7402-ass4 &gt; cat decrypt 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. 19:53:32masterisaac@HMS-Brixford:7402-ass4 &gt; </pre> <p>As can be seen decrypting reverses the cipher as expected</p>
Broken data	Run the simple encryption test case Run head -n 10 output > broken_output Run ./feistel.py d output decrypt	<pre> 19:55:07masterisaac@HMS-Brixford:7402-ass4 &gt; head -n 10 output &gt; broken_output 19:55:26masterisaac@HMS-Brixford:7402-ass4 &gt; ./feistel.py d broken_output decrypt Traceback (most recent call last):   File "./feistel.py", line 66, in &lt;module&gt;     raise ValueError('Ciphertext is not a valid length, it must be corrupted') ValueError: Ciphertext is not a valid length, it must be corrupted 19:55:34masterisaac@HMS-Brixford:7402-ass4 &gt; </pre> <p>The program detects when padding removed and the data was corrupted</p>



# 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

```
20:40:37masterisaac@HMS-Brixford:7402-ass4
> cat 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.
```

Figure 1 plane text

```
20:50:56masterisaac@HMS-Brixford:7402-ass4
> xxd -c 40 -g 0 output_key_7
00000000: 233a312a452a0c156e73650a0a436f701a5b49555845190863292032303139203a0a110b566d4728
00000028: 70657965762c20491d0400162a473f176e561750a0a506552041a531b0c1d0b2069732068657265
00000050: 071d0c4714130b1165642c2066726565470a0a08170741136752c20746f206100594f1211131a01
00000078: 6e206f627461696e19176d4f0700170770790a5f66207468080145530e08105761726520616e6420
000000a0: 0417530b0c0a1419656420646f63756d45081d0d11a4f462066690c65732028001f04524771464a
000000c8: 747761726522292c2a1d0100d044c0a636e207468652873180f001f0e071120776974686f7574
000000f0: 541b0a1d585200d74696f6e2c20696e1405010c061b1308776974686f7574203074d1d1c04541b
00000118: 6f6e20746865287249121b115f2a170207573652c20636f1600000000a100e66792c206d657267
00000140: 10440c50110b1f1d73082c2064697374011c00191d06494e7375626c6963656e1c170c5304020825
00000168: 6f722073656c6c0a054f040100537300662074686520536f071a1341060a0c50616e6420746f2070
00000190: 170102070700040a72736f6e7320746f45573b000b5403096520536f66747761000b491a1b6f0255
000001b8: 726e697308656420584f53110d4a160c2c207375626a656354461b034c1b1f0c20666f6c6c6f7769
000001e0: 1a0e4f0d1c546e6374696f6e7330a0a03148064f111b1d1f6520636f70797269040d5441000b541d
00000208: 636520616e642074011a00491f0b5203697373696f6e206e0e18054307455301616c6c2062652069
00000230: 070d4c1408096e43696e20616c6c0a054f031c0700540e1c207375627374616e00000e0253500014
00000258: 74696f6e73206f6e54030917457d656c747761726520a0a03091765730615745741524520495320
00000280: 70700e5690d1666202241532049532278000008061a0e1b542057415252414e0d796b06080646d6e
000002a8: 59204b494e442c200a0a5a1b08031f094f520a494d504c491000050e0e0e01195544494e47204255
000002d0: 19691a0a100018064d4954454420544f721506116912127252414e54494553200e08740c071b0f01
000002f8: 414e544142494c49110a7f2a0006066e45535320464f5220146c111372041c11554c415220505552
00000320: 70011c0b690f0816204e4f4e494e4652676e0e0b6d0b01742e20494e204e4f20041a096e00681642
00000348: 414c4c205448450a0e07740b00020a724f5220434f5059520d021a07000a0a6c4445525320424520
00000370: 031b6103021c00054f5220414e59204301000e087f000b134d41474553204f52690e1601091b5e15
00000398: 494142494c4954597e001e06651506655220494e20414e2007631706011a720e4620434f4e545241
000003c0: 631b7e001b1b1a11204f52204f544845001e1a1a0b6b0007524953494e47204672000b0c451d751d
000003e8: 204f46204f5220491a090c016e190c1754494f4e205749540e74030917657300465457415245204f
00000410: 17081b1a656f011b45204f52204f54480b1573640c0f6c1d4e475320494e205409174f74d45455754
00000438: 4152452e0a030303
20:52:16masterisaac@HMS-Brixford:7402-ass4
k
```

Figure 2 secret key: 7

```

r20:49:53masterisaac@HMS-Brixford:7402-oss4
↳ xxd -c 40 -g 0 output_key_6
00000000: 6e73650a0a436f704d4954204c69636563292032030313920797269676874202870657965762c2049
00000028: 4a6f686e204167616e6561750a0a506573616163204d6f722069732068657265726d697373696f6e
00000050: 65642c20667265656279206772616e7467652c20746f72061206f6620636861726e206f627461696e
00000078: 6e7920706572736f7079a6f66207468696e67206120636f61726520616e6420697320736f667477
000000a0: 656420646f63756d6173736f636961742066696c65732028656e746174096f6e747761726522292c
000000c8: 7468652022536f660a696e207468652020746f7206465616c20776974686f7574536f667477617265
000000f0: 74696f6e2c20696e2072657374726963776974686f757420636c7564696e67206f6e207468652072
00000118: 6c696d6974617469207573652c20636f69676874730a746f66792c206d65726770792c206d6f6469
00000140: 73682c20646973746952c207075626c697375626c6963656e7269627574652c206f722073656c6c0a
00000168: 73652c20616e642f652074686520536f636f70696573206f616e6420746f72066674776172652c20
00000190: 72736f6e7320746f65726d69742070656520536f6674776172077686f6d207468726e697368656420
000001b8: 72652069730a66752c207375626a6563746f720646f20736f720666f6c6c6f77697420746f720746865
000001e0: 74696f6e7330a0a6e6720636f6e64696520636f707972695468652061626f76636520616e642074
00000208: 676874206a6f7469697373696f6e206e686973207065726d616c6c20626520696f74696365207368
00000230: 696e20616c6c0a636e636c7564656420207375627374616e6f70696573206f7274696f6e73206f66
00000258: 7469616c20706f7274776172652e0a0a2074686520536f66574152452049532054484520534f4654
00000280: 202241532049532250524f56494444544542057415252414e2c20574954484f5559204b494e442c20
000002a8: 5459204f4620414e4f520a494d504c4945585052455353205544494e4720425545442c20494e434c
000002d0: 4d4944454420544f54204c4952414e54494553202054484520574152414e544142494c49
000002f8: 4f46204d4552434845535320464f522054992c0a4649544e554c4152205055524120504152544943
00000320: 204e4f4e494e4652504f534520414e442e20494e204e4f720494e47454d454e54414c4c205448450a
00000348: 4550454e542053484f5220434f505952415554484f52532044455253204245204947485420484f4c
00000370: 4f5220414e5920434c4941424c4520464d41474553204f524c41494d2c204441494142494c495459
00000398: 204f54484520a4c5220494e20414e202c205748455448454620434f4e545241414354494f4e204f
000003c0: 204f52204f54484543542c20544f5254524953494e47204652574953452c2041204f46204f522049
000003e8: 524fd2c0a4f555454494f4e205749544e20434f4e4e4543465457415245204f482054484520534f
00000410: 45204f52204f544852205448452055534e475320494e20544552204445414c494152452e0a030303
00000438: 48450a534f465457
r20:52:03masterisaac@HMS-Brixford:7402-oss4
↳

```

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.