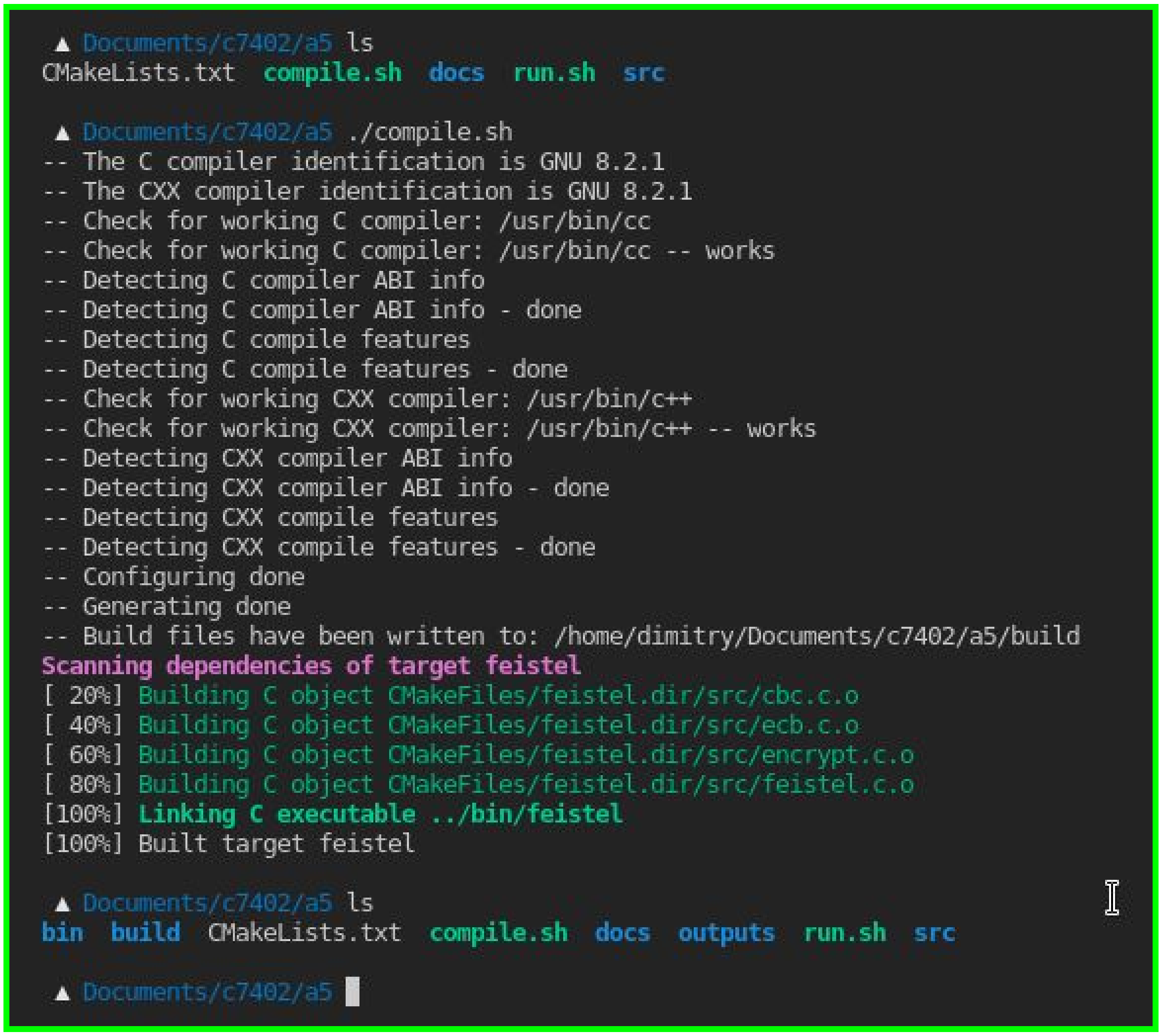
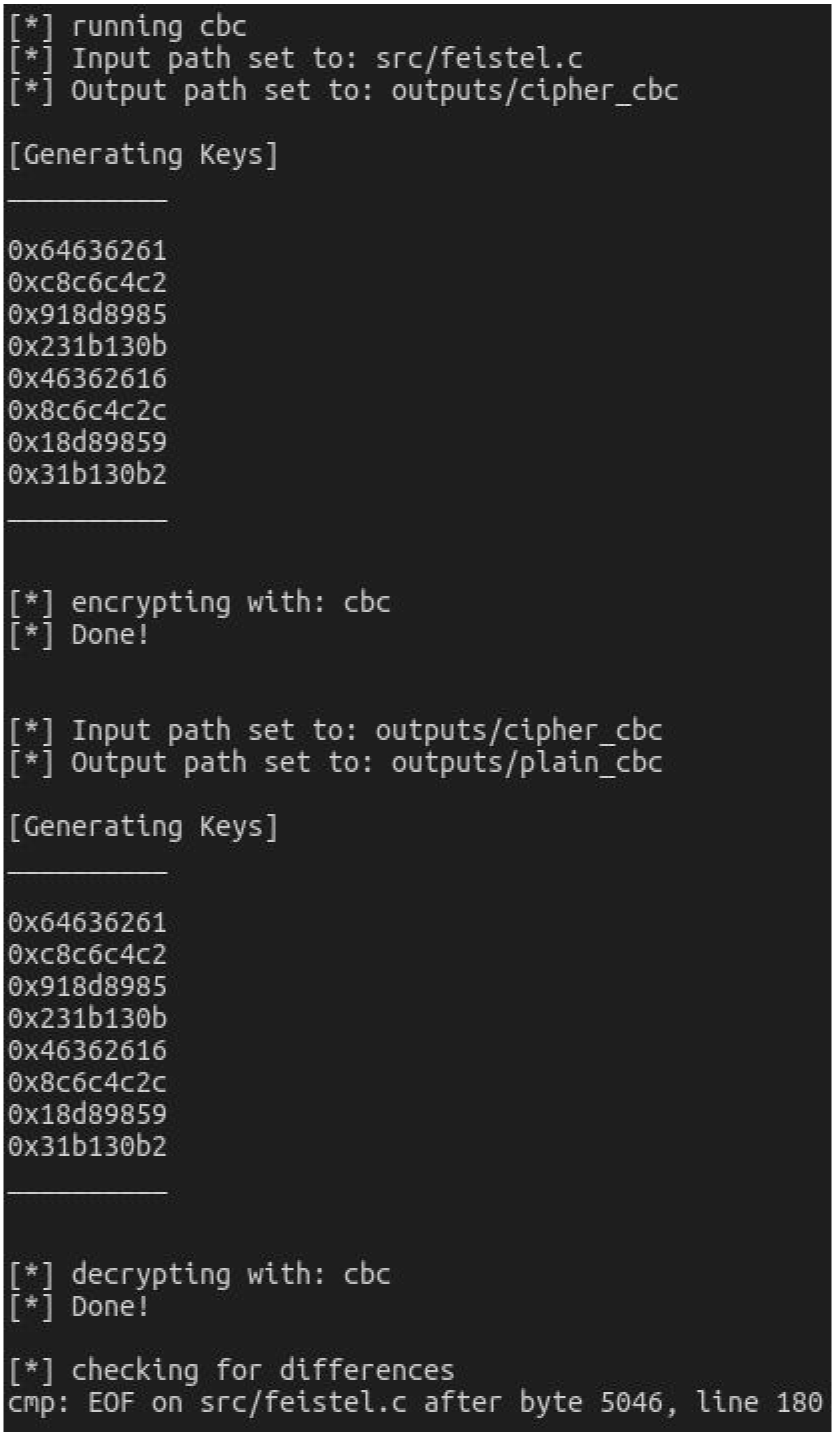
Testing

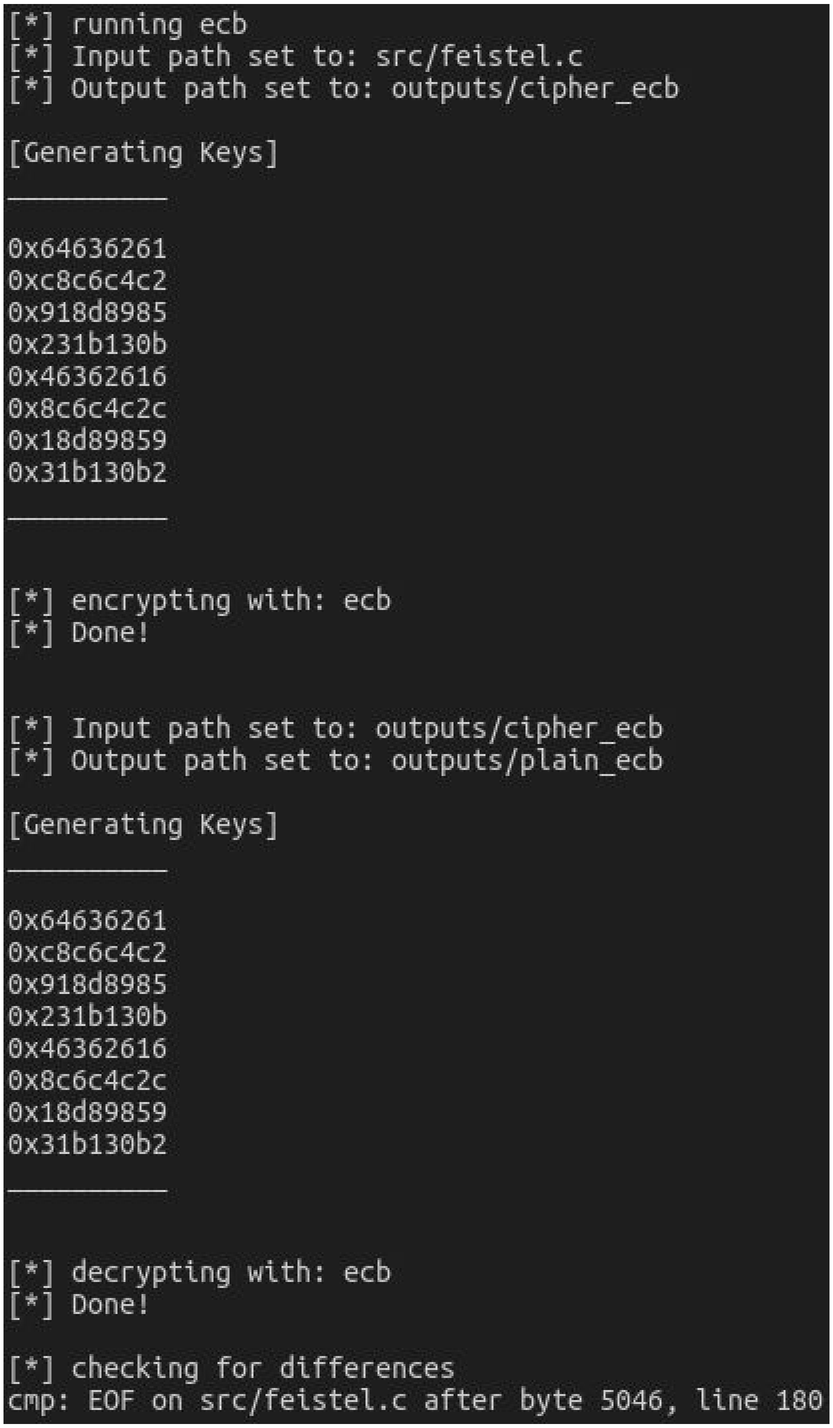
Test # 1 - Success	
Command	Expected output
./compile.sh	CMake output that signifies that the finary bin/fiestel has been built.
	

```
 ▲ Documents/c7402/a5 ls
CMakeLists.txt  compile.sh  docs  run.sh  src

 ▲ Documents/c7402/a5 ./compile.sh
-- The C compiler identification is GNU 8.2.1
-- The CXX compiler identification is GNU 8.2.1
-- Check for working C compiler: /usr/bin/cc
-- Check for working C compiler: /usr/bin/cc -- works
-- Detecting C compiler ABI info
-- Detecting C compiler ABI info - done
-- Detecting C compile features
-- Detecting C compile features - done
-- Check for working CXX compiler: /usr/bin/c++
-- Check for working CXX compiler: /usr/bin/c++ -- works
-- Detecting CXX compiler ABI info
-- Detecting CXX compiler ABI info - done
-- Detecting CXX compile features
-- Detecting CXX compile features - done
-- Configuring done
-- Generating done
-- Build files have been written to: /home/dimitry/Documents/c7402/a5/build
Scanning dependencies of target feistel
[ 20%] Building C object CMakeFiles/feistel.dir/src/cbc.c.o
[ 40%] Building C object CMakeFiles/feistel.dir/src/ecb.c.o
[ 60%] Building C object CMakeFiles/feistel.dir/src/encrypt.c.o
[ 80%] Building C object CMakeFiles/feistel.dir/src/feistel.c.o
[100%] Linking C executable ../bin/feistel
[100%] Built target feistel

 ▲ Documents/c7402/a5 ls
bin  build  CMakeLists.txt  compile.sh  docs  outputs  run.sh  src

 ▲ Documents/c7402/a5
```

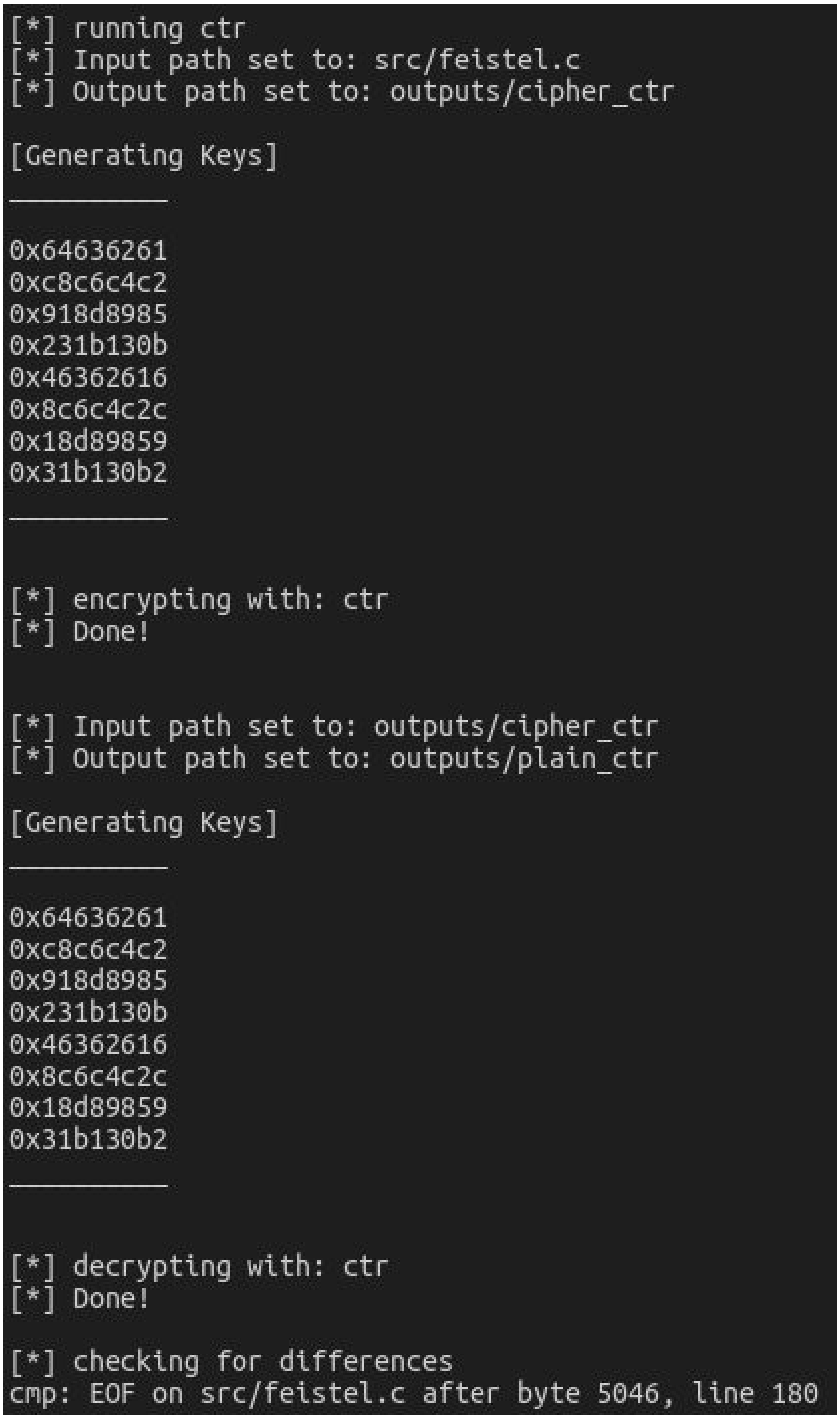
Test # 2 - Partial Success	
Command	Expected output
./run.sh	Calls compile.sh and then proceeds to run the both of the encryption and decryption modes on the file src/fiestel.c After the execution is complete the program calculates differences between the original file and the decrypted version. The success is partial because in each of the files cmp finds a one byte difference. This is a bug with the encryption program fiestel.c.



```
[*] running cbc
[*] Input path set to: src/feistel.c
[*] Output path set to: outputs/cipher_cbc

[Generating Keys]
__________

0x64636261
0xc8c6c4c2
0x918d8985
0x231b130b
0x46362616
0x8c6c4c2c
0x18d89859
0x31b130b2
__________


[*] encrypting with: cbc
[*] Done!


[*] Input path set to: outputs/cipher_cbc
[*] Output path set to: outputs/plain_cbc

[Generating Keys]
__________

0x64636261
0xc8c6c4c2
0x918d8985
0x231b130b
0x46362616
0x8c6c4c2c
0x18d89859
0x31b130b2
__________


[*] decrypting with: cbc
[*] Done!

[*] checking for differences
cmp: EOF on src/feistel.c after byte 5046, line 180
```

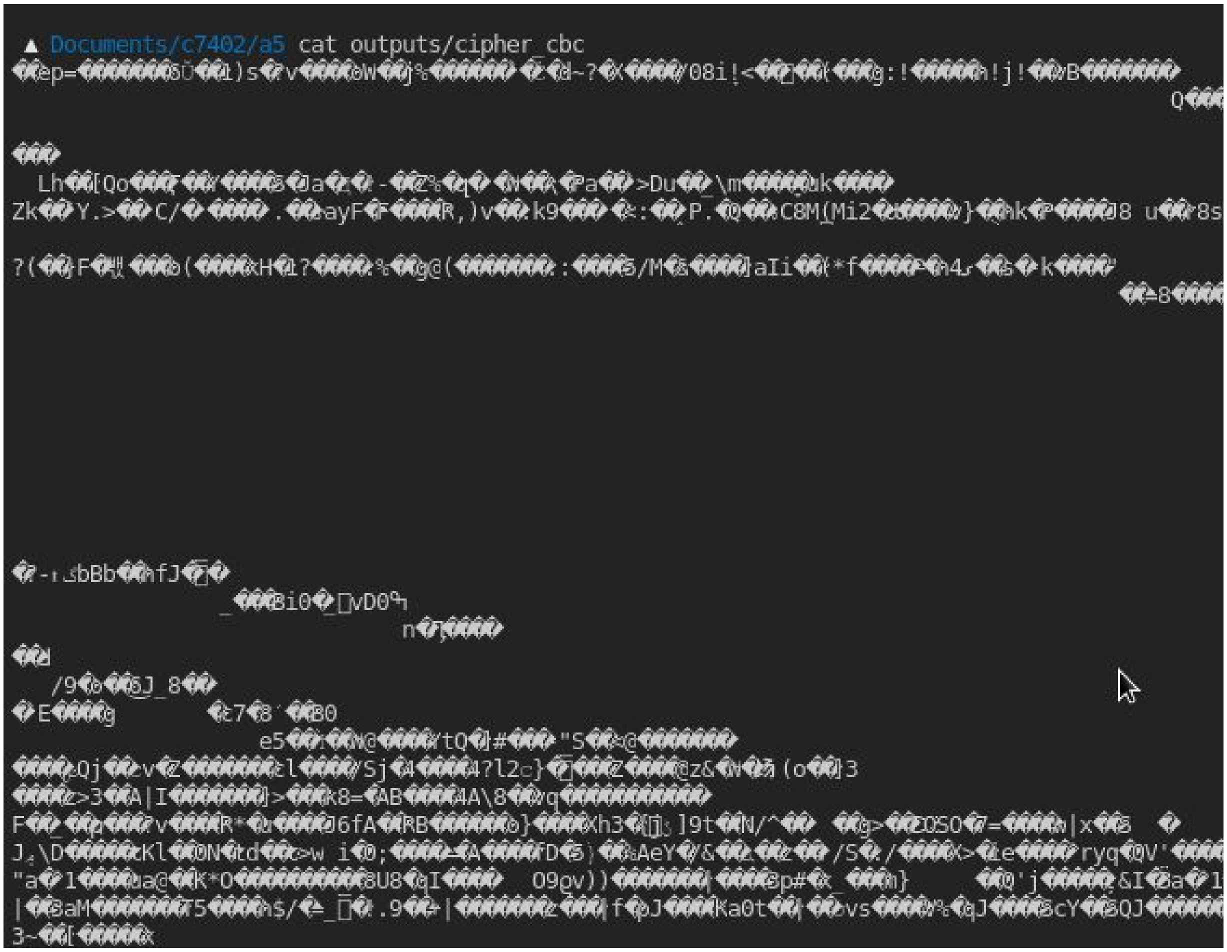


```
[*] running ecb
[*] Input path set to: src/feistel.c
[*] Output path set to: outputs/cipher_ecb

[Generating Keys]
__________

0x64636261
0xc8c6c4c2
0x918d8985
0x231b130b
0x46362616
0x8c6c4c2c
0x18d89859
0x31b130b2
__________


[*] encrypting with: ecb
[*] Done!


[*] Input path set to: outputs/cipher_ecb
[*] Output path set to: outputs/plain_ecb

[Generating Keys]
__________

0x64636261
0xc8c6c4c2
0x918d8985
0x231b130b
0x46362616
0x8c6c4c2c
0x18d89859
0x31b130b2
__________


[*] decrypting with: ecb
[*] Done!

[*] checking for differences
cmp: EOF on src/feistel.c after byte 5046, line 180
```



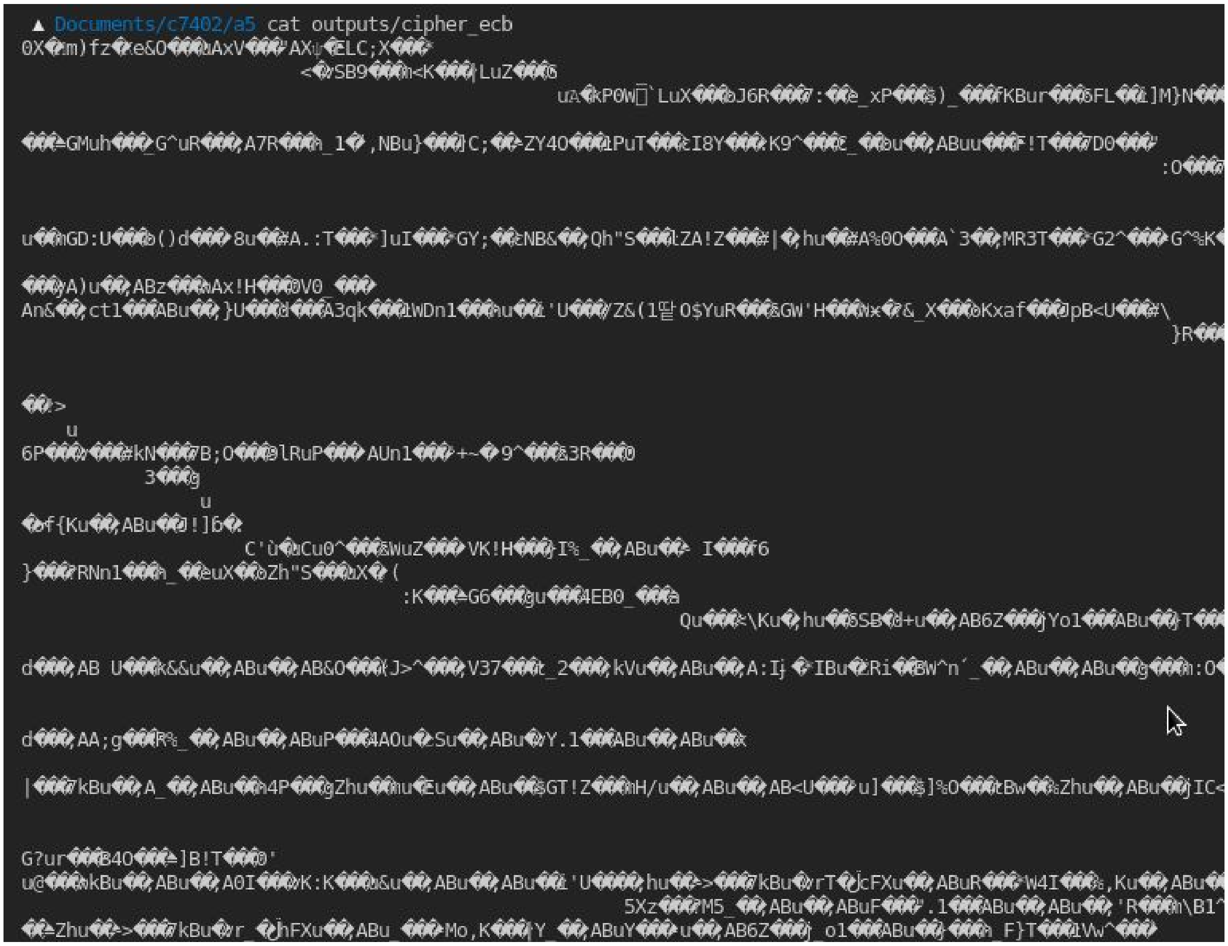
```
[*] running ctr
[*] Input path set to: src/feistel.c
[*] Output path set to: outputs/cipher_ctr

[Generating Keys]
__________

0x64636261
0xc8c6c4c2
0x918d8985
0x231b130b
0x46362616
0x8c6c4c2c
0x18d89859
0x31b130b2
__________


[*] encrypting with: ctr
[*] Done!


[*] Input path set to: outputs/cipher_ctr
[*] Output path set to: outputs/plain_ctr

[Generating Keys]
__________

0x64636261
0xc8c6c4c2
0x918d8985
0x231b130b
0x46362616
0x8c6c4c2c
0x18d89859
0x31b130b2
__________


[*] decrypting with: ctr
[*] Done!

[*] checking for differences
cmp: EOF on src/feistel.c after byte 5046, line 180
```

Test # 3 - Success	
Command	Expected output
Reading the CBC output to check that it is in fact random. cat outputs/cipher_cbc	The data is random but english characters are still present. This is to be expected because ascii characters 65 - 122 fit within the cipher space. There appears to be less readable characters in the CBC output than in the ECB output. None of the original data is present in the same place.

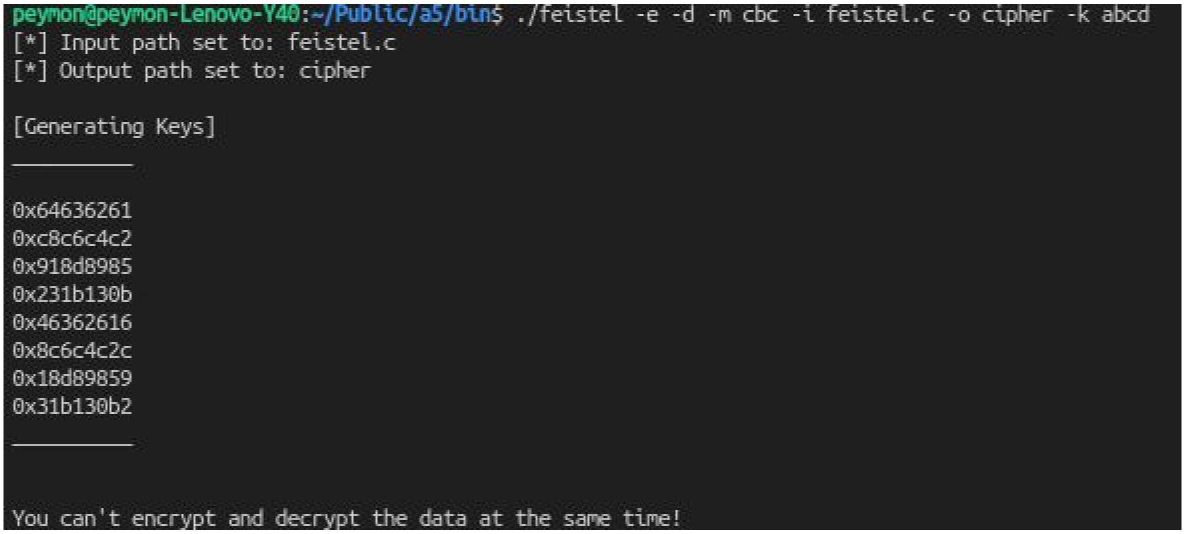


```
 ▲ Documents/c7402/a5 cat outputs/cipher_cbc
��ep=��������5Ü���1)s��v�����oW���j%�������� ��Z��d~?���X�����/08i!<���7���(����g:!������h!j!���/B��������
                                                                                                                                        Q���

���
  Lh���[Qo����F����/�����3��Ja���Z�� -���Z%���q�� ��N����\��Pa���>Du���_\m������uk�����
Zk���Y.>���C/�������� .���ayF��F�����R,)v���k9����� ���:���P.��Q���C8M(Mi2��������}���nk��P�����J8 u���r8s

?(����F��빥 ����b(������H��1?������%���g@(���������:�����5/M��&�����]aIi���(*f�������h4,���s��k�����
                                                                                                                               ���≙8�����








��-ı¿bBb����nfJ����
                _����Bi0��_▯vD0ㅎ
                              n���ㅋ�����
���
  /9���b���6J_8���
��E�����g       ���7��8´���B0
                   e5������N@�����/tQ���]#���� "S����@��������
�����Qj����v��Z��������l�����/Sj��4�����4?l2c}��7�����Z�����@z&���N���(o���]3
�����>3���A|I��������]>����k8=��AB�����4A\8���q��������������
F���_����p����v�����R*���u�����J6fA���RB��������o}�����Xh3��[▯]9t���N/^��� ���g>���ZOSO��7=�������|x���8  ��
J、\D��������Kl���0N���td����>w i��0;����������A������fD���5 ����AeY��/&�������� /S���/������X>���e�����ryq���QV'�����
"a��1������a@���K*O��������������8U8���qI�����  O9gv))���������|�����3p#���x_����m}    ����Q'j�������&I���a��1
|���3aM����������T5������n$/��≙_▯���.9���|���������Z�����|f��pJ������Ka0t����|����vs�������%���qJ�����3cY���8QJ�������
3~����[������x
```

Test # 4 - Success	
Command	Expected output
Reading the ECB output to test that the data is in fact encrypted. cat outputs/cipher_ecb	While this file is still quite random, in comparison to the CBC file there seems to be more readable characters. None of the data from the original file is present though.

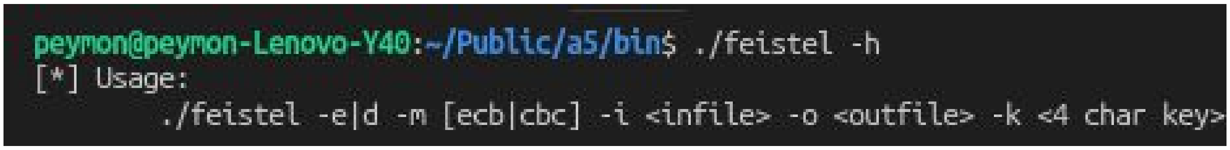


```
 ▲ Documents/c7402/a5 cat outputs/cipher_ecb
0X�m)fz�e&O���AxV���AX�ELC;X���
                         <�SB9���<K���LuZ���
                                                uA�kP0W`LuX���J6R���:��e_xP���)_���fKBur���FL���]M}N���

���GMuh���G^uR���,A7R���_1� ,NBu}���C;��-ZY40���PuT���I8Y���K9^���_��u��,ABuu���F!T���D0���
                                                                                                    :O���

u���GD:U���()d��� 8u���A.:T��� ]uI��� GY;���NB&��,Qh"S���ZA!Z���#|�,hu���A%0O���A`3��,MR3T���G2^���G^%K�

���A)u��,ABz���Ax!H���V0_���
An&��,ct1���ABu��,}U������A3qk���WDn1���u���'U���Z&(1딸O$YuR���GW'H���×�&_X���Kxaf���pB<U���#\
                                                                                                     }R���


��>
    u
6P������#kN���7B;O���lRuP��� AUn1���+~�9^���3R���
          3���
                u
��f{Ku��,ABu���!]6�
                   C'ù��Cu0^���WuZ��� VK!H���I%_��,ABu��- I���f6
}���RNn1���_���uX���Zh"S���X�(
                                   :K���G6���u���4EB0_���
                                                          Qu����\Ku�,hu���SB�d+u��,AB6Z���Yo1���ABu���T���

d���,AB U���k&&u��,ABu��,AB&O���J>^���,V37���_2���,kVu��,ABu��,A:I� �IBu�Ri���W^n´_��,ABu��,ABu������:O�


d���,AA;g���R%_��,ABu��,ABuP���4A0u�Su��,ABu��Y.1���ABu��,ABu��

|���kBu��,A_��,ABu���4P���Zhu���u�u��,ABu���GT!Z���H/u��,ABu��,AB<U��� u]���]%O���Bw���Zhu��,ABu���IC<


G?ur���B40���]B!T���'
u@����kBu��,ABu��,A0I���K:K�����u��,ABu��,ABu���'U����,hu��->���kBu��rT��cFXu��,ABuR���W4I���,Ku��,ABu��
                                                                 5Xz���M5_��,ABu��,ABuF���.1���ABu��,ABu��,'R����\B1^
���Zhu��->���kBu��r_��hFXu��,ABu_���Mo,K���Y_��,ABuY���u��,AB6Z���_o1���ABu�����_F}T���Vw^���
```

Test # 5 - Success	
Command	Expected output
Attempt to encrypt and decrypt on the same command ./feistel -e -d -m cbc -i feistel.c -o cipher -k abcd	File outputs error and exits
	

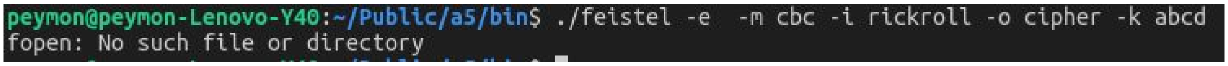
```
peymon@peymon-Lenovo-Y40:~/Public/a5/bin$ ./feistel -e -d -m cbc -i feistel.c -o cipher -k abcd
[*] Input path set to: feistel.c
[*] Output path set to: cipher

[Generating Keys]
__________

0x64636261
0xc8c6c4c2
0x918d8985
0x231b130b
0x46362616
0x8c6c4c2c
0x18d89859
0x31b130b2
__________


You can't encrypt and decrypt the data at the same time!
```

Test # 6 - Success	
Command	Expected output
Show usage ./feistel -h or ./feistel	Print usage into terminal

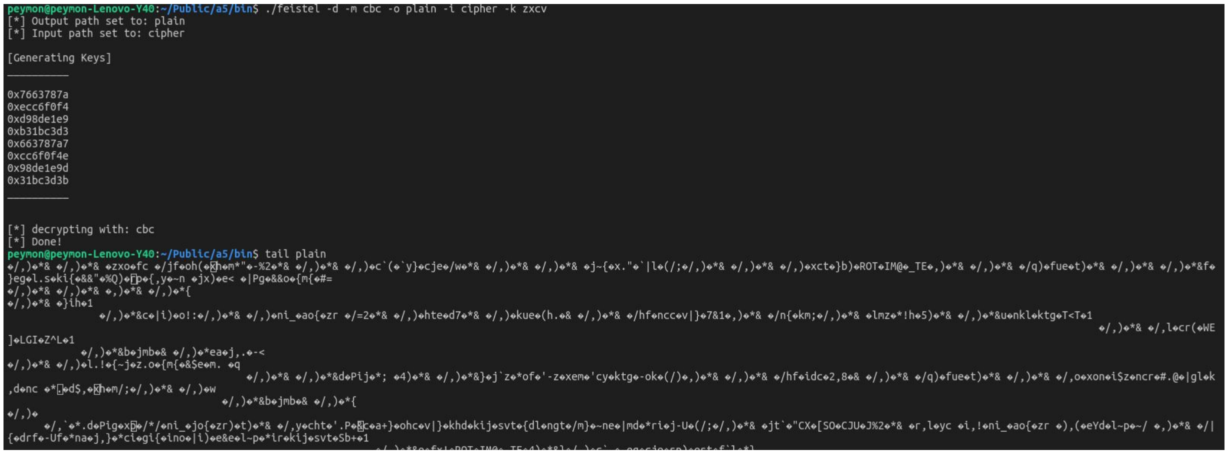


```
peymon@peymon-Lenovo-Y40:~/Public/a5/bin$ ./feistel -h
[*] Usage:
        ./feistel -e|d -m [ecb|cbc] -i <infile> -o <outfile> -k <4 char key>
```

Test # 7 - Success	
Command	Expected output
Invalid file input ./feistel	File outputs error and exits



```
peymon@peymon-Lenovo-Y40:~/Public/a5/bin$ ./feistel -e  -m cbc -i rickroll -o cipher -k abcd
fopen: No such file or directory
```

Test # 8 - Success	
Command	Expected output
Incorrect key for decrypting. Correct key: abcd ./feistel -d -m cbc -o plain -i cipher -k zxcv	Incoherent output file
	

```
peymon@peymon-Lenovo-Y40:~/Public/a5/bin$ ./feistel -d -m cbc -o plain -i cipher -k zxcv
[*] Output path set to: plain
[*] Input path set to: cipher

[Generating Keys]
__________

0x7663787a
0xecc6f0f4
0xd98de1e9
0xb31bc3d3
0x663787a7
0xcc6f0f4e
0x98de1e9d
0x31bc3d3b
__________


[*] decrypting with: cbc
[*] Done!
peymon@peymon-Lenovo-Y40:~/Public/a5/bin$ tail plain
�/,)�*& �/,)�*& �zxo�fc �/jf�oh(�□h�m*"�-%2�*& �/,)�*& �/,)�c`(�`y}�cje�/w�*& �/,)�*& �/,)�*& �j~{�x."�`|l�(/;�/,)�*& �/,)�*& �/,)�xct�}b)�ROT�IM@�_TE�,)�*& �/,)�*& �/q)�fue�t)�*& �/,)�*& �/,)�*&f�
}eg�l.s�ki{�&&"�%Q)�□p�{,y�~n �jx)�e< �|Pg�&&o�{m{�#=
�/,)�*& �/,)�*& �,)�*& �/,)�*{
�/,)�*& �}ih�1
               �/,)�*&c�|i)�o!:�/,)�*& �/,)�ni_�ao{�zr �/=2�*& �/,)�hte�d7�*& �/,)�kue�(h.�& �/,)�*& �/hf�ncc�v|}�7&1�,)�*& �/n{�km;�/,)�*& �lmz�*!h�5)�*& �/,)�*&u�nkl�ktg�T<T�1
                                                                                                                                                                                   �/,)�*& �/,l�cr(�WE
]�LGI�Z^L�1
            �/,)�*&b�jmb�& �/,)�*ea�j,.�-<
�/,)�*& �/,)�l.!�{~j�z.o�{m{�&$e�m. �q
                                       �/,)�*& �/,)�*&d�Pij�*; �4)�*& �/,)�*&}�j`z�*of�'-z�xem�'cy�ktg�-ok�(/)�,)�*& �/,)�*& �/hf�idc�2,8�& �/,)�*& �/q)�fue�t)�*& �/,)�*& �/,o�xon�i$z�ncr�#.@�|gl�k
,d�nc �*□�d$,�□h�m/;�/,)�*& �/,)�w
                                   �/,)�*&b�jmb�& �/,)�*{
�/,)�
      �/,`�*.d�Pig�x□�/*/�ni_�jo{�zr)�t)�*& �/,y�cht�'.P�□c�a+}�ohc�v|}�khd�kij�svt�{dl�ngt�/m}�~ne�|md�*ri�j-U�(/;�/,)�*& �jt`�"CX�[SO�CJU�J%2�*& �r,l�yc �i,!�ni_�ao{�zr �),(�eYd�l~p�~/ �,)�*& �/|
{�drf�-Uf�*na�j,}�*ci�gi{�ino�|i)�e&e�l~p�*ir�kij�svt�Sb+�1
                                                            �/,)�*&o�fx|�ROT�IM@�_TE�4)�*&]�/,)�c`�,�og�cjo�sp)�ost�f`l�*]
```