

Testing

Test # 1 - Success	
Command	Expected output
./compile.sh	CMake output that signifies that the binary bin/feistel 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	<p>Calls compile.sh and then proceeds to run the both of the encryption and decryption modes on the file src/feistel.c</p> <p>After the execution is complete the program calculates differences between the original file and the decrypted version.</p> <p>The success is partial because in each of the files cmp finds a one byte difference. This is a bug with the encryption program feistel.c.</p>
 <pre> ▲ Documents/c7402/a5 ./run.sh -- Configuring done -- Generating done -- Build files have been written to: /home/dimitry/Documents/c7402/a5/build [100%] Built target feistel [*] compilation successful [*] running cbc rm: cannot remove 'outputs/*': No such file or directory [*] 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! </pre>	

```
[*] 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 4586, line 160
```

```
[*] 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 4586, line 160
```


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) fzreS0uAxV AXuELC;X
<wSB9i<K LuZ
uA kP0W LuXJ6R: e_xP) fKBurFL M}N
G Muh_ G^uR, A7R_1 , NBu} C; ZY40LPuT I8Y K9^ _ bu, ABuu! T D0
: 0

uGD: U() d 8u#A. : T ] uI GY; eNB& Qh" S LZA! Z # | hu#A%0 A` 3 MR3T G2^ G^K
(A) u ABz Ax! H V0
An& ct1 ABu, } U A3qk W Dn1 hu ' U Z& (1 딸 O$ YuR Gw' H x & _ X Kxaf pB< U # \
} R

>
u
6P kN B; 0 lRuP AUn +~ 9^ & 3R
3 g
u
f{ Ku, ABu ! } 6
C' ù Cu0^ WuZ VK! H I% , ABu I f6
} RNn1 _ euX Zh" S X (
: K G6 gu EB0_ a
Qu & \ Ku, hu SB d+u, AB6Z j Yo1 ABu, T
d AB U k& & u, ABu, AB&0 { J>^ V37 t_ 2 kVu, ABu, A: Ij IBu Ri Bw^n' _ ABu, ABu g m: 0
d AA; g R% _ ABu, ABu P A0u Su, ABu Y. 1 ABu, ABu x
| kBu, A_ , ABu 4P g Zhu mu Cu, ABu SGT! Z mH/u, ABu, AB<U u ] %0 k Bw % Zhu, ABu IC<
G7ur B40 B! T
u@ kBu, ABu, A0I K: K Su, ABu, ABu ' U hu > kBu rT j cFXu, ABuR w4I , Ku, ABu
5Xz M5_ , ABu, ABuF . 1 ABu, ABu ' R \ B1^
Zhu > kBu r j hFXu, ABu Mo, K Y , ABuY u, AB6Z j o1 ABu, F} T Vw^

```

