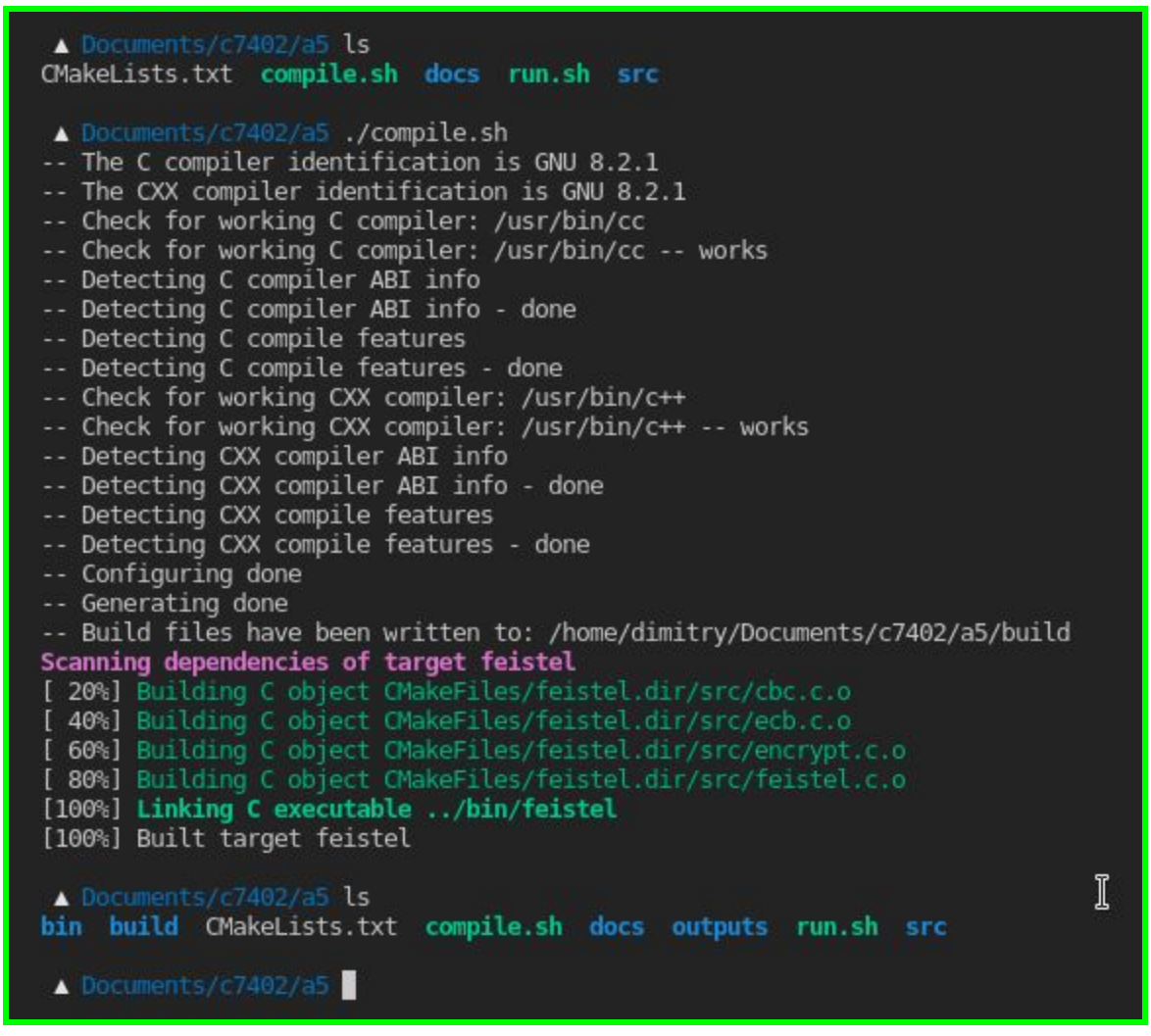
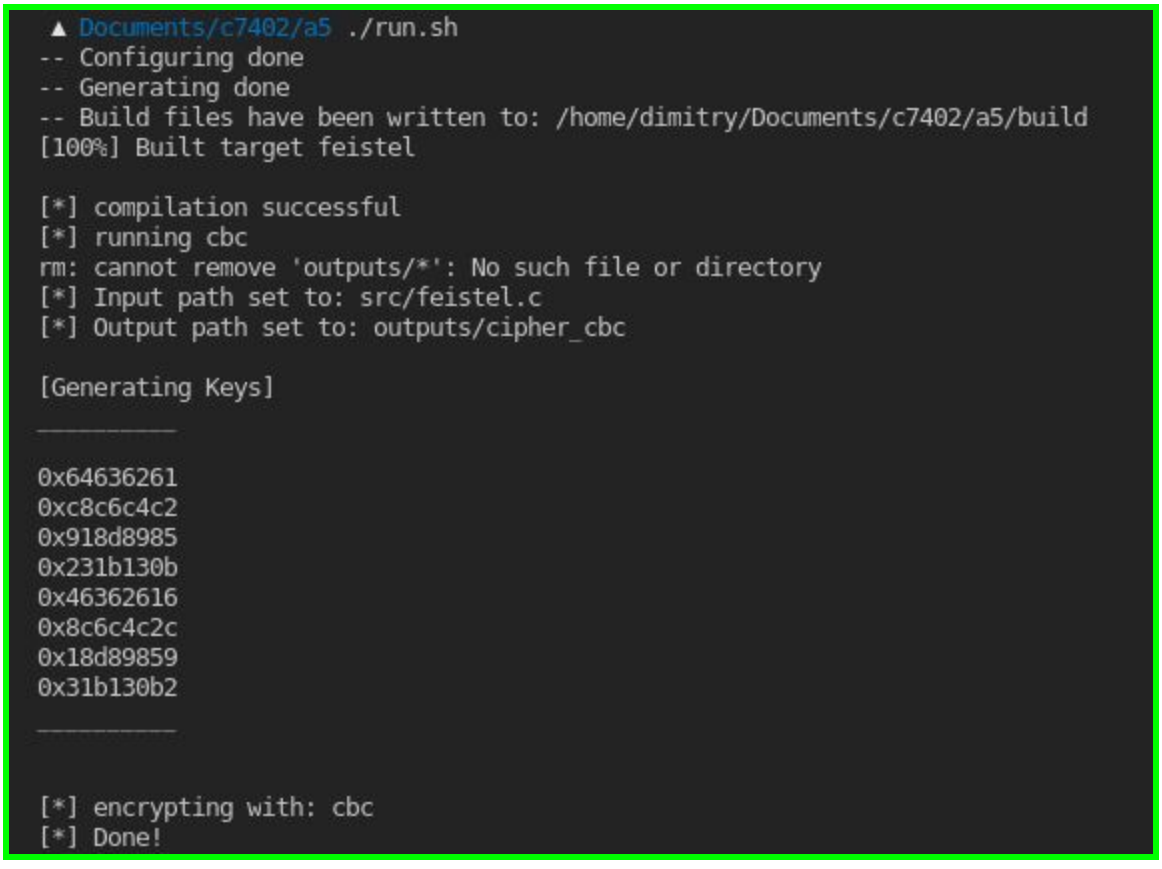
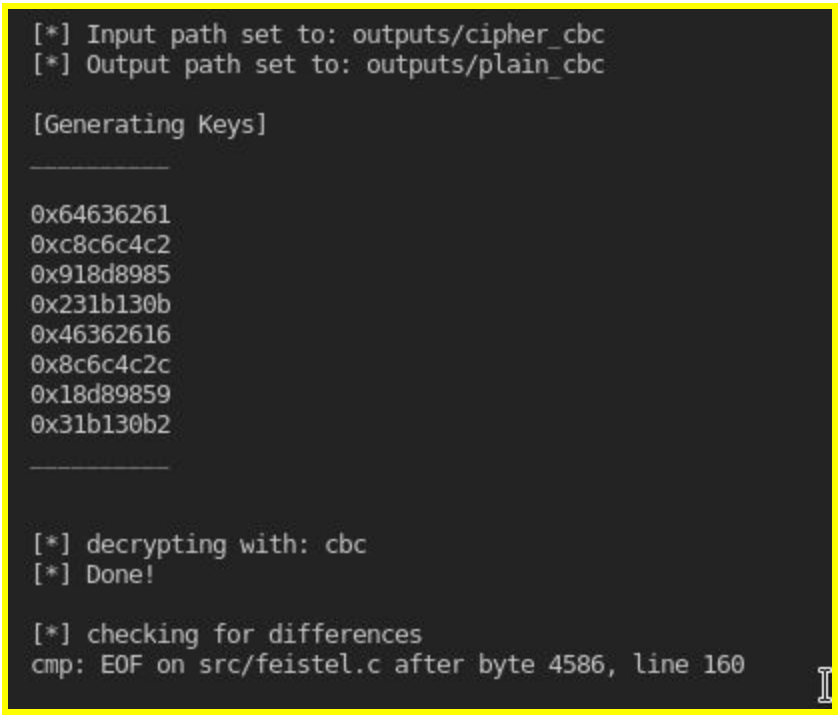
Testing

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

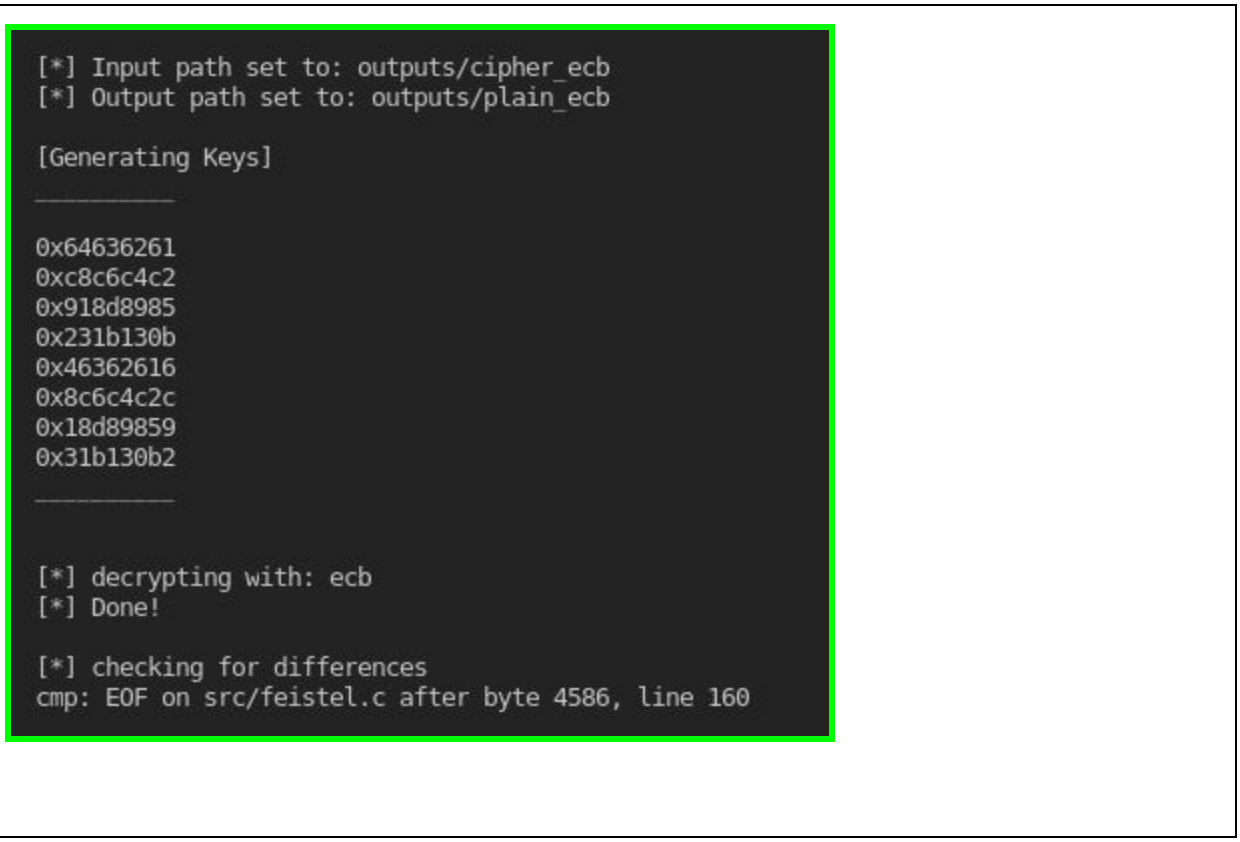


Test # 2 - Partial Success	
Command	Expected output
./run.sh	Calls compile.sh and then proceeds to run the both of the encryption and decryption modes on the file src/fiestel.c After the execution is complete the program calculates differences between the original file and the decrypted version. The 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.




[*] 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 # 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.

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.