CEG-4750 Information Security

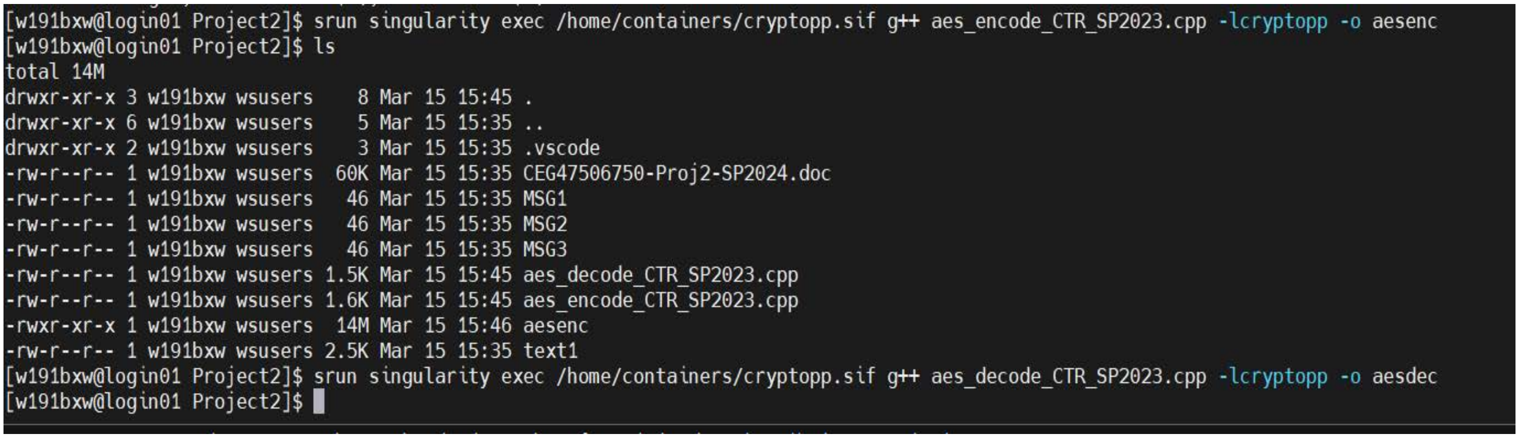
Brandon Walker

Meilin Liu

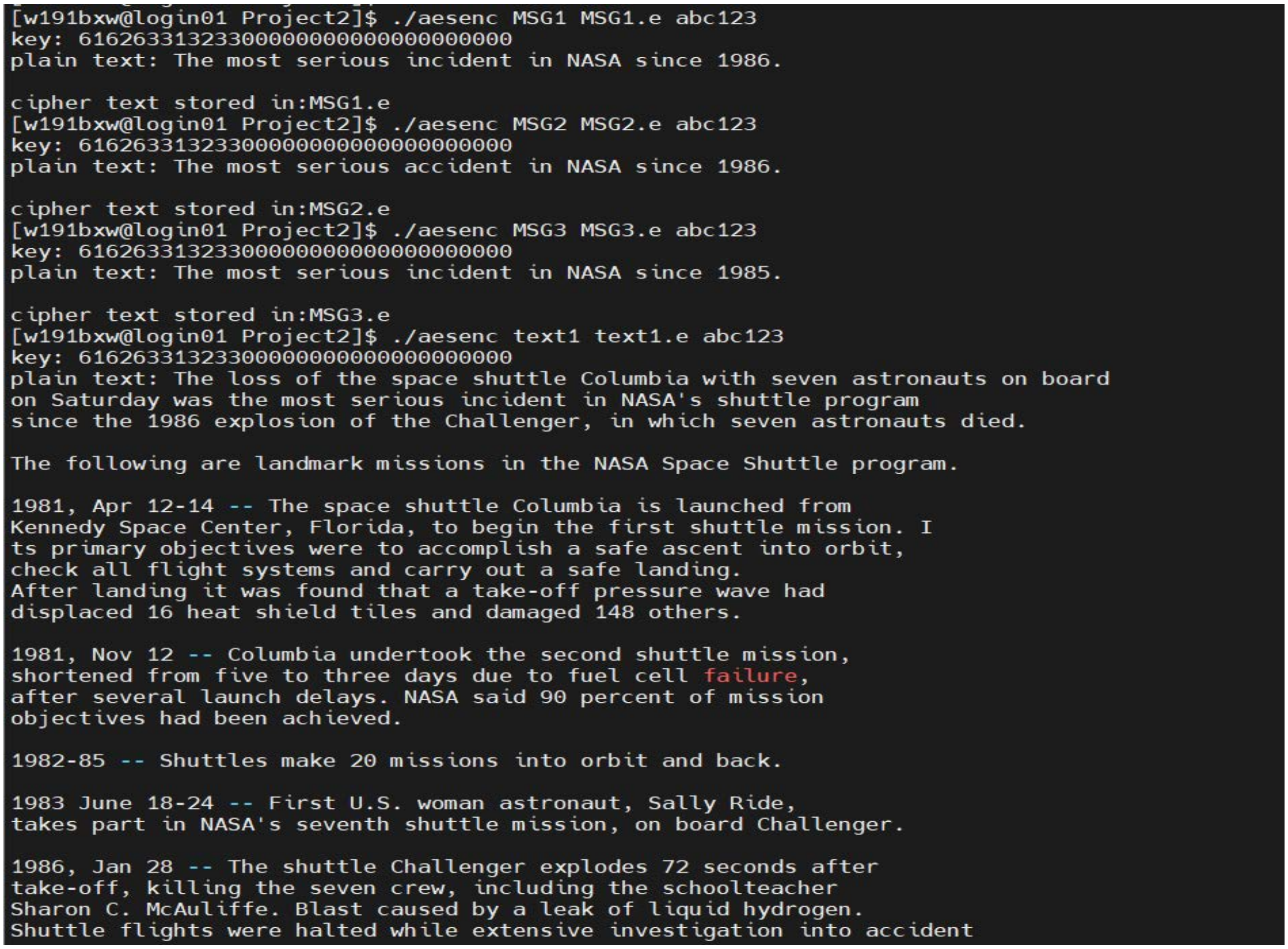
03/16/2024

Project 2

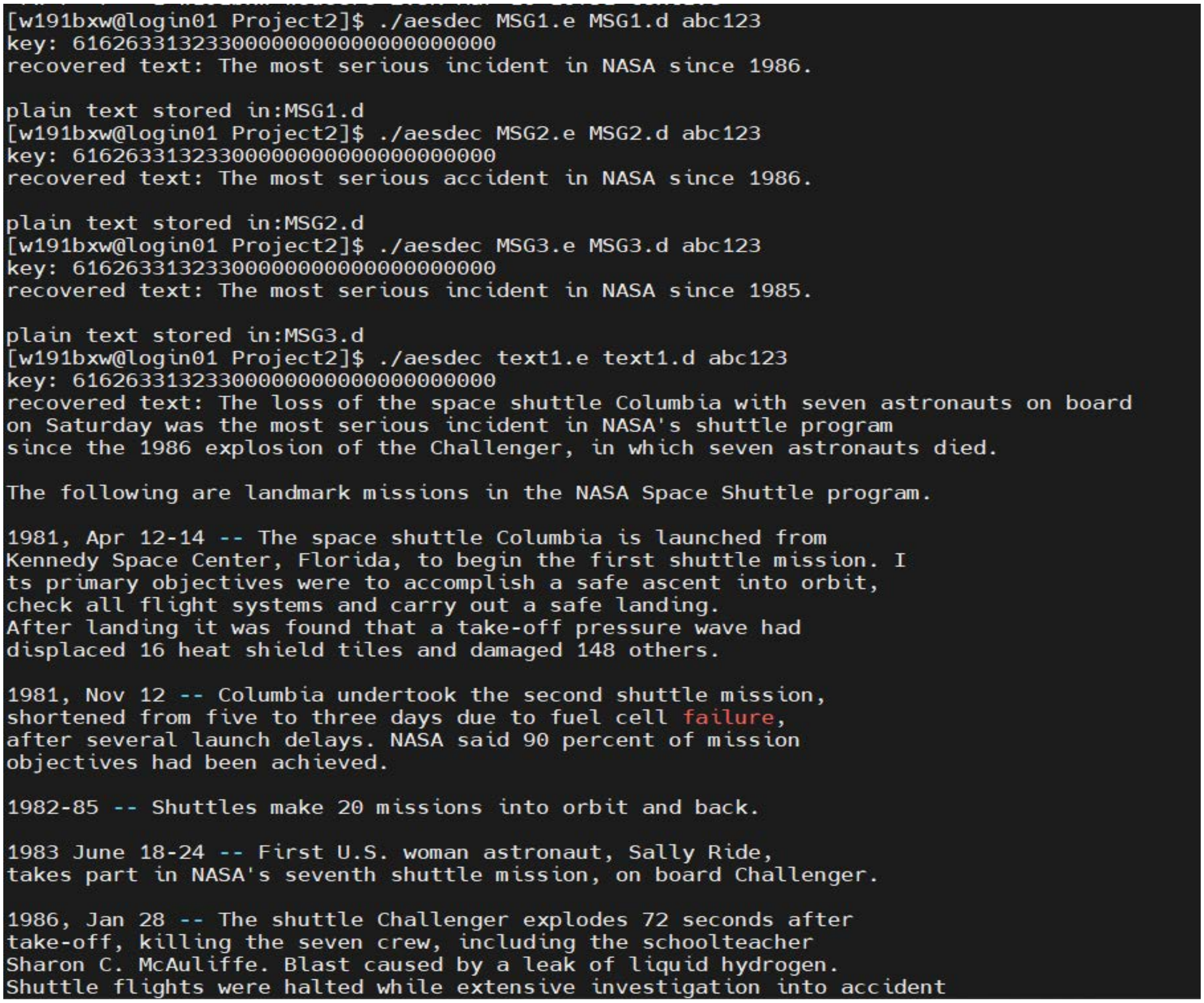
I opened up the encryption and decryption code in vscode and modified the files by changing ECB to CTR, setkey to setkeywithiv, added a byte iv[] field to the encryption/decryption method, and to the method call in main, added an iv field to main right after the key is declared and hardcoded it. I then connected to fry and compiled the programs. I encrypted every file and saved to a '.e' file. I then decrypted all the files and saved them to a '.d' file. I ran diff on every files original and '.d' version, and finally ran od -b on every file to compare the bytes of the files. There were no differences between the originals and the decrypted versions. There were only 2 bytes of difference between MSG1.e and MSG2.e, and 1 byte of difference between MSG1.e and MSG3.e. I suspect this is why I saw info about not using the same IV repeatedly, as I used the same IV for every file, I am sure a different IV each time would give a bigger difference, and a new key every time would increase that difference. All images will be included in this folder with names describing what part of the process they document.



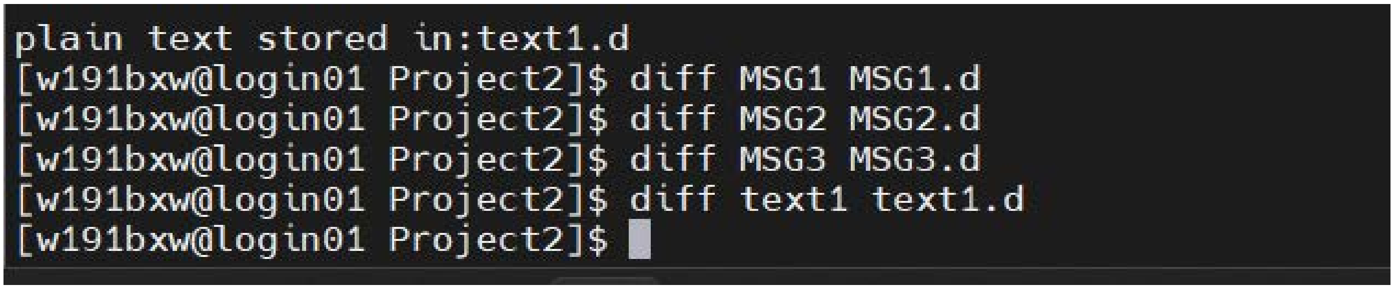
```
[w191bxw@login01 Project2]$ srun singularity exec /home/containers/cryptopp.sif g++ aes_encode_CTR_SP2023.cpp -lcryptopp -o aesenc
[w191bxw@login01 Project2]$ ls
total 14M
drwxr-xr-x 3 w191bxw wsusers    8 Mar 15 15:45 .
drwxr-xr-x 6 w191bxw wsusers    5 Mar 15 15:35 ..
drwxr-xr-x 2 w191bxw wsusers    3 Mar 15 15:35 .vscode
-rw-r--r-- 1 w191bxw wsusers  60K Mar 15 15:35 CEG47506750-Proj2-SP2024.doc
-rw-r--r-- 1 w191bxw wsusers   46 Mar 15 15:35 MSG1
-rw-r--r-- 1 w191bxw wsusers   46 Mar 15 15:35 MSG2
-rw-r--r-- 1 w191bxw wsusers   46 Mar 15 15:35 MSG3
-rw-r--r-- 1 w191bxw wsusers 1.5K Mar 15 15:45 aes_decode_CTR_SP2023.cpp
-rw-r--r-- 1 w191bxw wsusers 1.6K Mar 15 15:45 aes_encode_CTR_SP2023.cpp
-rwxr-xr-x 1 w191bxw wsusers  14M Mar 15 15:46 aesenc
-rw-r--r-- 1 w191bxw wsusers 2.5K Mar 15 15:35 text1
[w191bxw@login01 Project2]$ srun singularity exec /home/containers/cryptopp.sif g++ aes_decode_CTR_SP2023.cpp -lcryptopp -o aesdec
[w191bxw@login01 Project2]$ 
```



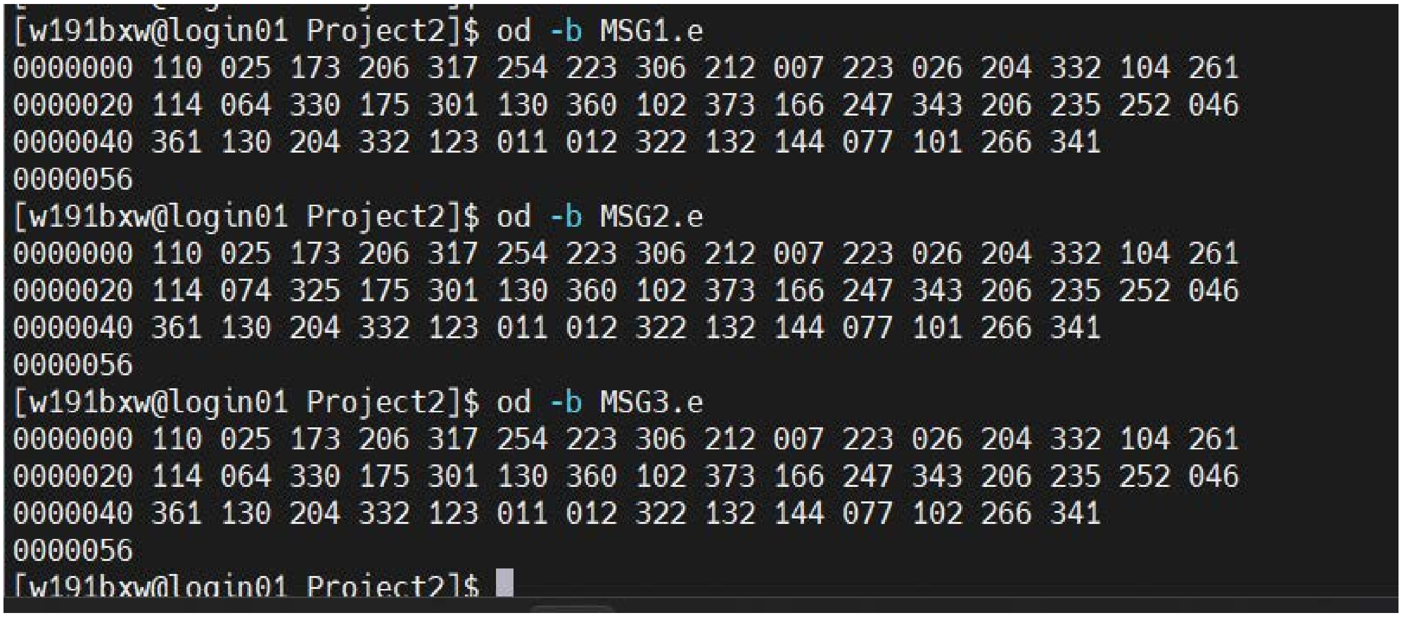
```
[w191bxw@login01 Project2]$ ./aesenc MSG1 MSG1.e abc123
key: 61626331323300000000000000000000
plain text: The most serious incident in NASA since 1986.

cipher text stored in:MSG1.e
[w191bxw@login01 Project2]$ ./aesenc MSG2 MSG2.e abc123
key: 61626331323300000000000000000000
plain text: The most serious accident in NASA since 1986.

cipher text stored in:MSG2.e
[w191bxw@login01 Project2]$ ./aesenc MSG3 MSG3.e abc123
key: 61626331323300000000000000000000
plain text: The most serious incident in NASA since 1985.

cipher text stored in:MSG3.e
[w191bxw@login01 Project2]$ ./aesenc text1 text1.e abc123
key: 61626331323300000000000000000000
plain text: The loss of the space shuttle Columbia with seven astronauts on board
on Saturday was the most serious incident in NASA's shuttle program
since the 1986 explosion of the Challenger, in which seven astronauts died.

The following are landmark missions in the NASA Space Shuttle program.

1981, Apr 12-14 -- The space shuttle Columbia is launched from
Kennedy Space Center, Florida, to begin the first shuttle mission. I
ts primary objectives were to accomplish a safe ascent into orbit,
check all flight systems and carry out a safe landing.
After landing it was found that a take-off pressure wave had
displaced 16 heat shield tiles and damaged 148 others.

1981, Nov 12 -- Columbia undertook the second shuttle mission,
shortened from five to three days due to fuel cell failure,
after several launch delays. NASA said 90 percent of mission
objectives had been achieved.

1982-85 -- Shuttles make 20 missions into orbit and back.

1983 June 18-24 -- First U.S. woman astronaut, Sally Ride,
takes part in NASA's seventh shuttle mission, on board Challenger.

1986, Jan 28 -- The shuttle Challenger explodes 72 seconds after
take-off, killing the seven crew, including the schoolteacher
Sharon C. McAuliffe. Blast caused by a leak of liquid hydrogen.
Shuttle flights were halted while extensive investigation into accident
```



```
[w191bxw@login01 Project2]$ ./aesdec MSG1.e MSG1.d abc123
key: 61626331323300000000000000000000
recovered text: The most serious incident in NASA since 1986.

plain text stored in:MSG1.d
[w191bxw@login01 Project2]$ ./aesdec MSG2.e MSG2.d abc123
key: 61626331323300000000000000000000
recovered text: The most serious accident in NASA since 1986.

plain text stored in:MSG2.d
[w191bxw@login01 Project2]$ ./aesdec MSG3.e MSG3.d abc123
key: 61626331323300000000000000000000
recovered text: The most serious incident in NASA since 1985.

plain text stored in:MSG3.d
[w191bxw@login01 Project2]$ ./aesdec text1.e text1.d abc123
key: 61626331323300000000000000000000
recovered text: The loss of the space shuttle Columbia with seven astronauts on board
on Saturday was the most serious incident in NASA's shuttle program
since the 1986 explosion of the Challenger, in which seven astronauts died.

The following are landmark missions in the NASA Space Shuttle program.

1981, Apr 12-14 -- The space shuttle Columbia is launched from
Kennedy Space Center, Florida, to begin the first shuttle mission. I
ts primary objectives were to accomplish a safe ascent into orbit,
check all flight systems and carry out a safe landing.
After landing it was found that a take-off pressure wave had
displaced 16 heat shield tiles and damaged 148 others.

1981, Nov 12 -- Columbia undertook the second shuttle mission,
shortened from five to three days due to fuel cell failure,
after several launch delays. NASA said 90 percent of mission
objectives had been achieved.

1982-85 -- Shuttles make 20 missions into orbit and back.

1983 June 18-24 -- First U.S. woman astronaut, Sally Ride,
takes part in NASA's seventh shuttle mission, on board Challenger.

1986, Jan 28 -- The shuttle Challenger explodes 72 seconds after
take-off, killing the seven crew, including the schoolteacher
Sharon C. McAuliffe. Blast caused by a leak of liquid hydrogen.
Shuttle flights were halted while extensive investigation into accident
```



```
plain text stored in:text1.d
[w191bxw@login01 Project2]$ diff MSG1 MSG1.d
[w191bxw@login01 Project2]$ diff MSG2 MSG2.d
[w191bxw@login01 Project2]$ diff MSG3 MSG3.d
[w191bxw@login01 Project2]$ diff text1 text1.d
[w191bxw@login01 Project2]$
```



```
[w191bxw@login01 Project2]$ od -b MSG1.e
0000000 110 025 173 206 317 254 223 306 212 007 223 026 204 332 104 261
0000020 114 064 330 175 301 130 360 102 373 166 247 343 206 235 252 046
0000040 361 130 204 332 123 011 012 322 132 144 077 101 266 341
0000056
[w191bxw@login01 Project2]$ od -b MSG2.e
0000000 110 025 173 206 317 254 223 306 212 007 223 026 204 332 104 261
0000020 114 074 325 175 301 130 360 102 373 166 247 343 206 235 252 046
0000040 361 130 204 332 123 011 012 322 132 144 077 101 266 341
0000056
[w191bxw@login01 Project2]$ od -b MSG3.e
0000000 110 025 173 206 317 254 223 306 212 007 223 026 204 332 104 261
0000020 114 064 330 175 301 130 360 102 373 166 247 343 206 235 252 046
0000040 361 130 204 332 123 011 012 322 132 144 077 102 266 341
0000056
[w191bxw@login01 Project2]$
```