Evan Krug

CS3840

Lab1

I created a plaintext file containing the phrase: “There once was a man from Peru who dreamed he was eating his shoe” as seen in Figure 1.

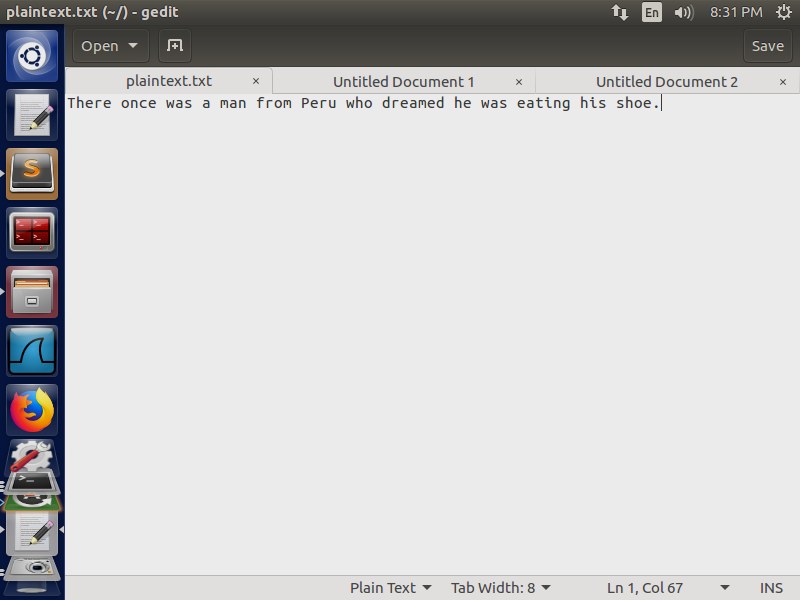


Figure 1 The Plaintext used in this lab

To produce the first ciphertext, as seen in Figure 2, I used the aes-128-cbc cipher type with key:123456789987654321212345678987654 and IV: 9951249858587474. The input file was called plaintext.txt and the output file was called cipher.bin.

The command I used was: **openssl enc -aes-128-cbc -e -in plaintext.txt -out cipher.bin**. I then decrypted the ciphertext and outputted the result into a different text file to verify my work.

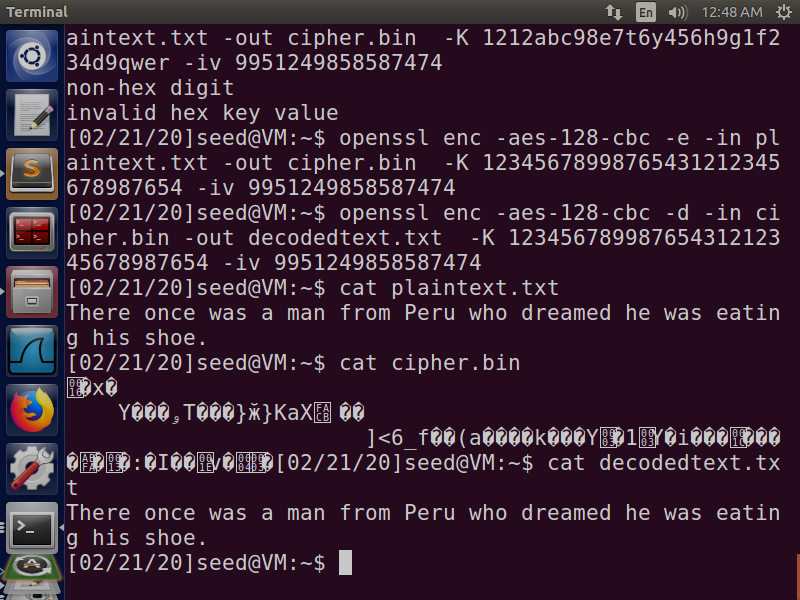


Figure 2:Commands to produce the first ciphertext

To produce the second ciphertext, as seen in Figure 3, I used the aes-128-cfb cipher type with key:123456789987654321212345678987654 and IV: 9951249858587474. The input file was called plaintext.txt and the output file was called cipher.bin.

The command I used was: **openssl enc -aes-128-cfb -e -in plaintext.txt -out cipher.bin**. I then decrypted the ciphertext and outputted the result into a different text file to verify my work.

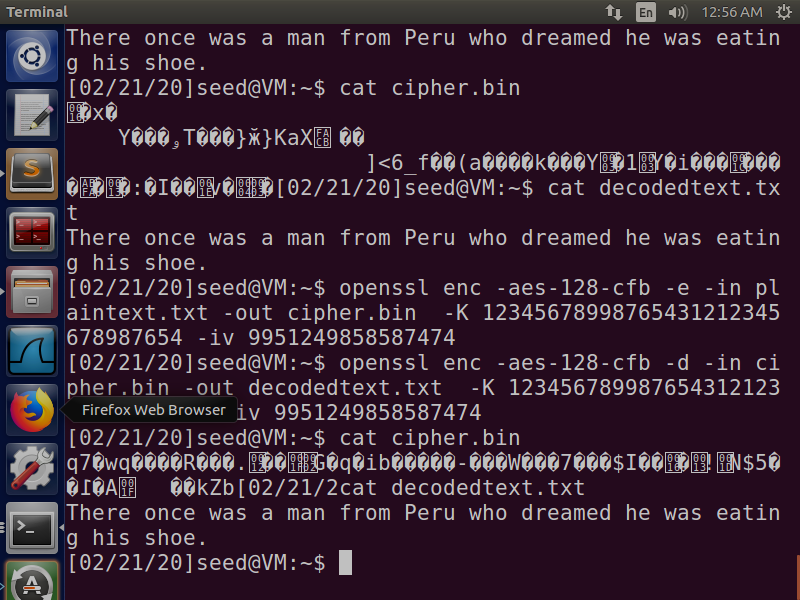


Figure :Commands to produce the second ciphertext

To produce the third ciphertext, as seen in Figure 4, I used the des-cbc cipher type with key:1234567899876544 and IV: 9951249858587474. The input file was called plaintext.txt and the output file was called cipher3.bin.

The command I used was: **openssl enc -des-cbc -e -in plaintext.txt -out cipher.bin**. I then decrypted the ciphertext and outputted the result into a different text file to verify my work.

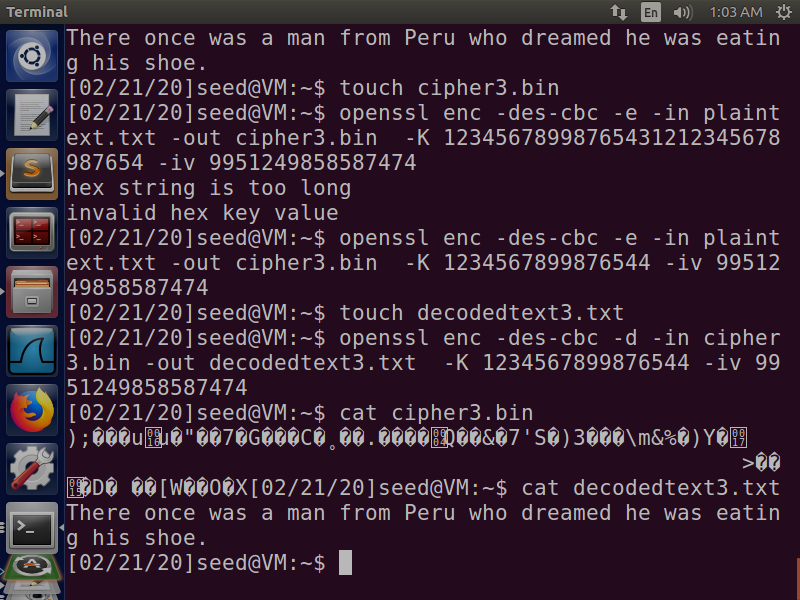


Figure : Commands to produce the third ciphertext