Jon Franck

4/26/2021

CSC 4413

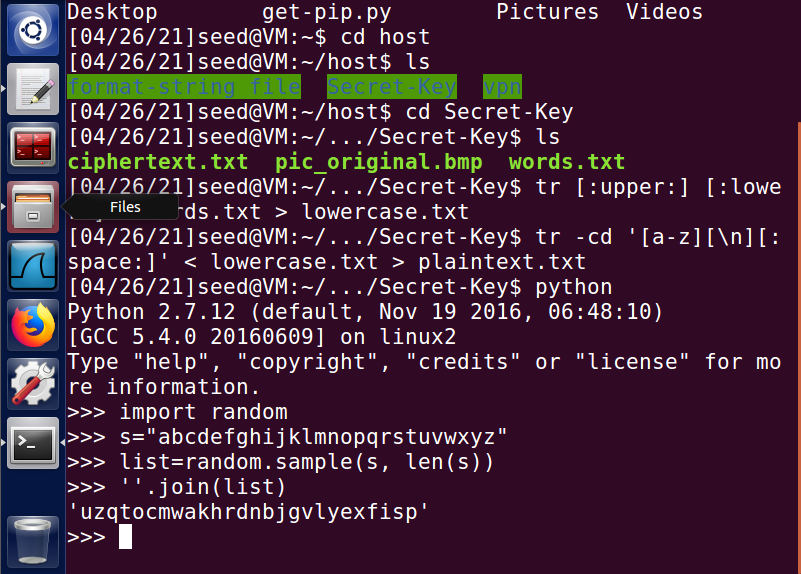
# Secret Key Encryption Lab

**Objective** The learning objective of this lab is for students to get familiar with the concepts in the secret-key encryption. After finishing the lab, students should be able to gain a first-hand experience on encryption algorithms, encryption modes, paddings, and initial vector (IV). Moreover, students will be able to use tools and write programs to encrypt/decrypt messages. This lab covers the following topics:

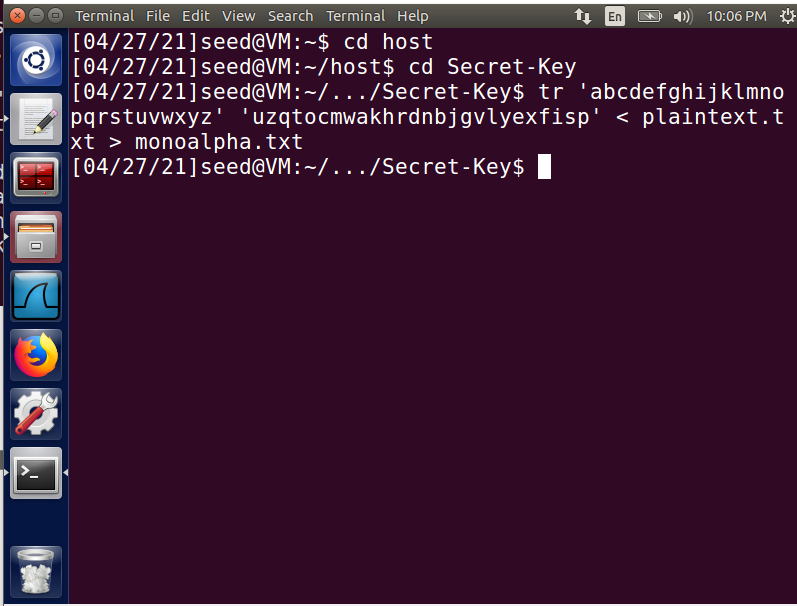
• Secret-key encryption  
• Substitution cipher and frequency analysis  
• Encryption modes and paddings  
• Programming using the crypto library

## Task 1: Frequency Analysis Against Monoalphabetic Substitution Cipher

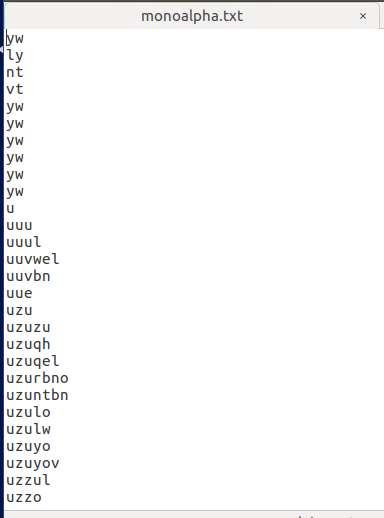
Create a monoalphabetic substation cipher:



First, we change all uppercase letters to lowercase and delete any characters other than alphabetic characters. Then we use a python function to randomly shuffle the alphabet.



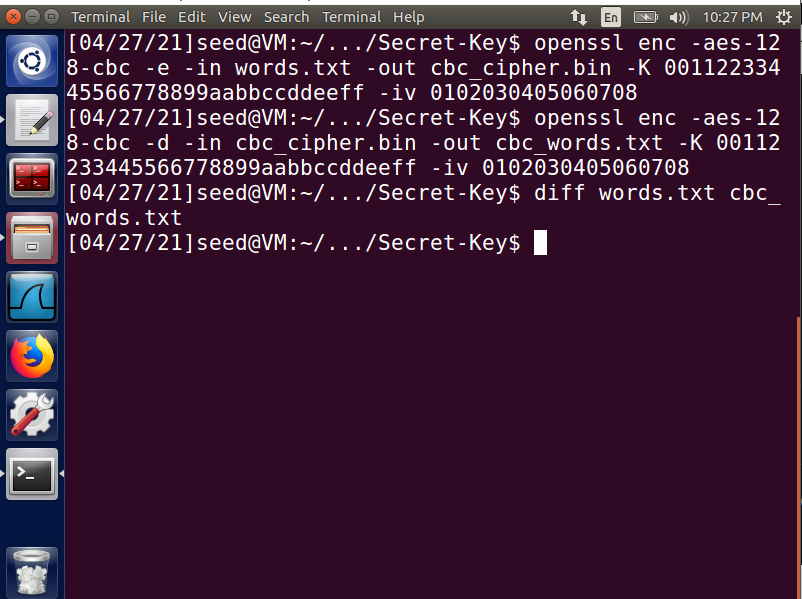
Next, we substitute the alphabet with the randomized key to make the document unreadable:

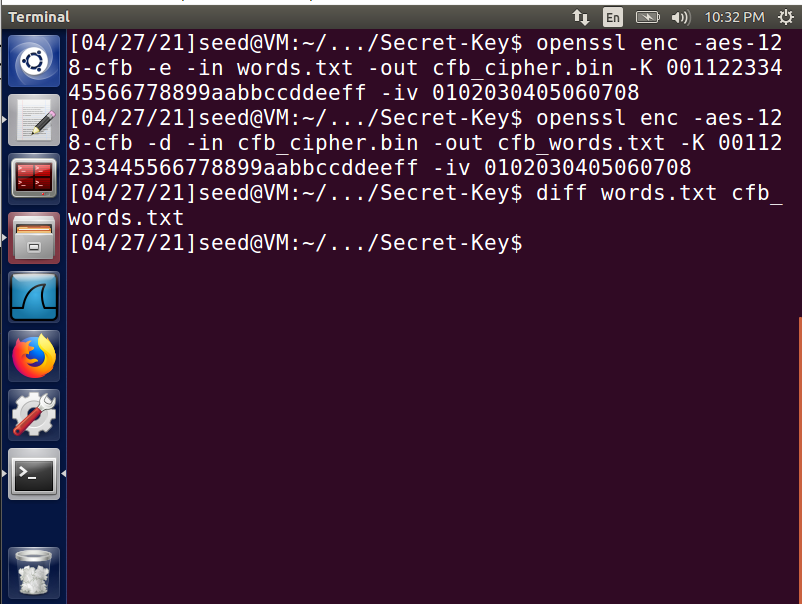
## Task 2: Encryption using Different Ciphers and Modes

Try using the openssl enc function on three different ciphers

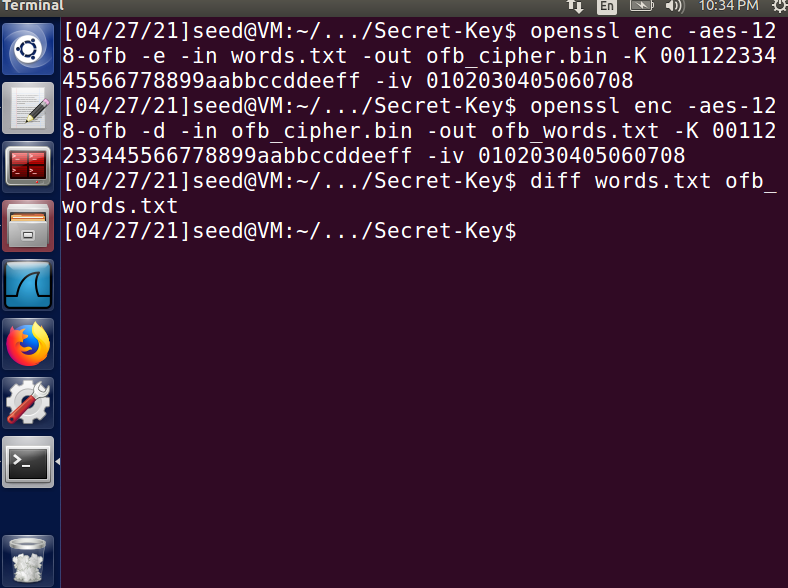
Cipher Block Chaining:



Cipher Feedback:



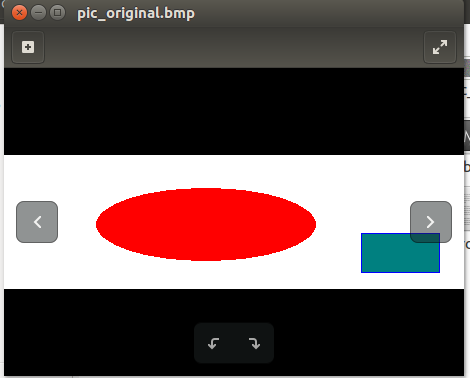
Output Feedback:



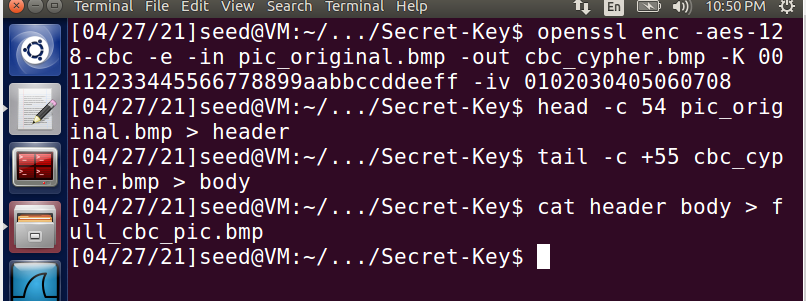
**Note: if the files did not decrypt into the exact same as the original file, the diff function would give an error message.**

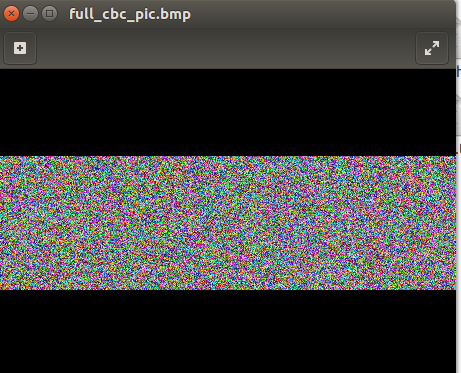
## Task 3: Encryption Mode – ECB vs. CBC

Encrypt the following picture with both ECB and CBC and change the header so the files can be opened by a media program:

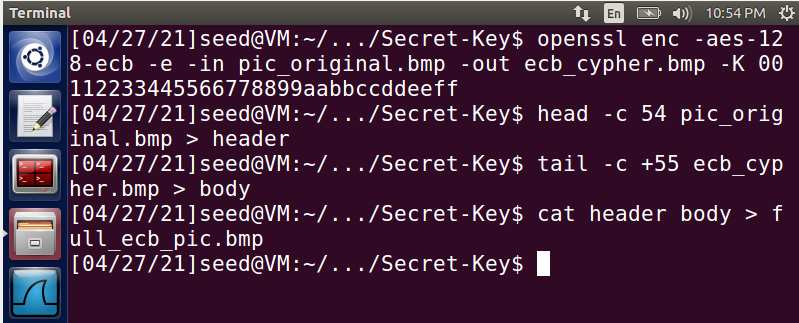


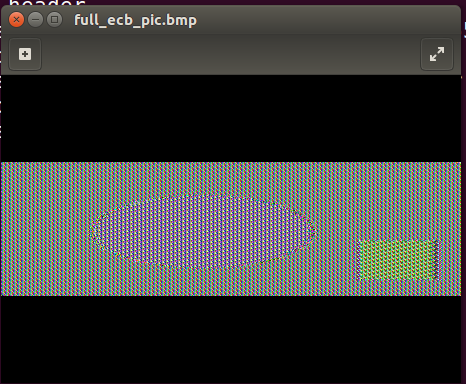
CBC:





ECB:





**Observation:** As the picture encrypted with ECB is still somewhat recognizable, CBC is clearly the better encryption method. This is likely due to the fact that ECB does not have a parameter for the IV.