Sopheap Sok

so683950

CIS 3360 0R02, Spring 2018

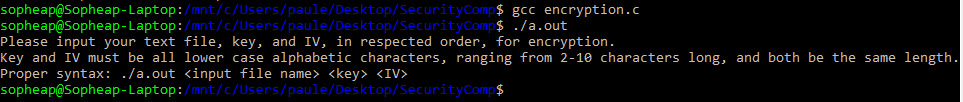
2/11/2018

Programming Assignment 1: Encryption and Decryption using Vigenere with Cipher Block Chaining (CBC)

I have taken Dr. Chu example text and added space, punctuations, caps, etc... and save as input1.txt to use. Any text file 4 kilobytes or less can be use as input.

How to compile and run encryption file:

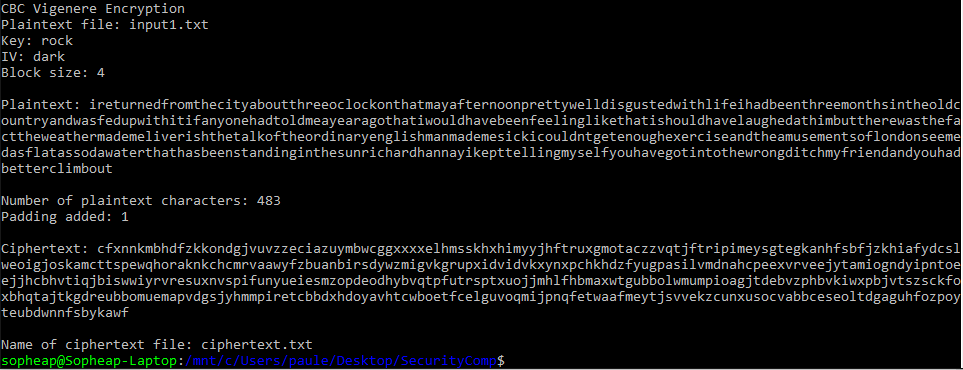
1. Type gcc encryption.c to compile.
2. Type ./a.out input1.txt (whatever key) (whatever IV). (Input file can be anything but must be in the same directory.)
3. If the above syntax is not given, the message below will appear to prompt for the correct syntax.



1. If the correct syntax is given, but the length of the key and IV does not match, the below message will appear, and you must re-enter your key and IV.

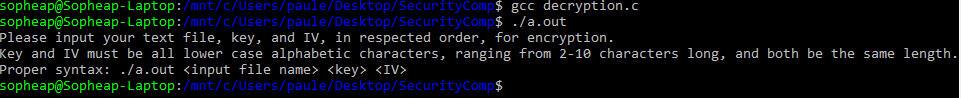


1. After entering an appropriate key and IV, the encryption should appear like the image below.



How to compile and run decryption file:

1. Type gcc decryption.c to compile.
2. Type ./a.out ciphertext.txt (same key used in encryption) (same IV used in encryption).
3. If the above syntax is not given, the message below will appear to prompt for the correct syntax.



1. If the correct syntax is given, but the length of the key and IV does not match, the below message will appear, and you must re-enter your key and IV.



1. After entering an appropriate key and IV, the decryption should appear like the image below.

