CSCE 548

Project 1

Group 9

Member: Andrew Cox, Joy Ray, Sebastian Martin, Xiyuan Zheng

Readme file

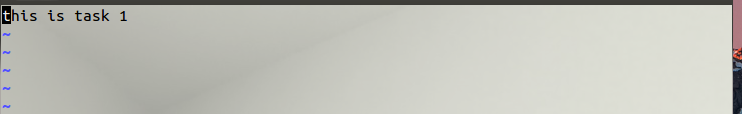
Task 1: Encryption using OpenSSL commands with different cipher and mode options

----------------------------------------------------------------------------------------------------------------

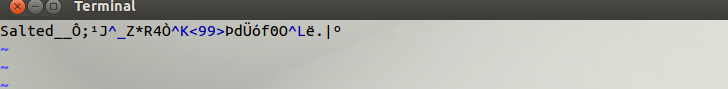
1. Mode 1 using CBC
2. Encryption

* openssl enc -des-ede-cbc -e -in plain.txt -out cipherbin.bin -k password

this command encrypts a text file with CBC mode and with a password

this is the plain text file: using command vim plain.txt

this is what the encrypted file looks like: using command vim cipherbin.bin

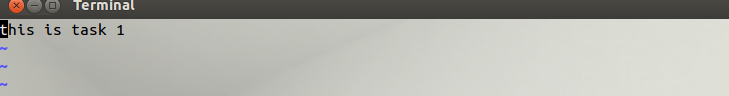


1. Decryption

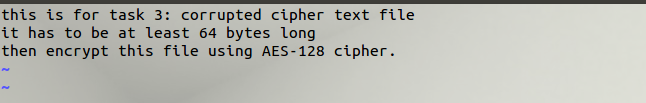
* openssl enc -des-ede-cbc -d -in cipherbin.bin -out cipherout.txt -k password

this command decrypts bin file with CBC mode and passed in the password

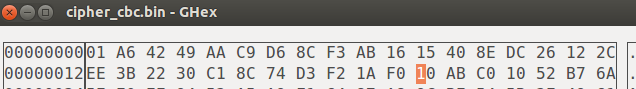
this is what decrypted file looks like: using command vim cipherout.txt



This is the original file.



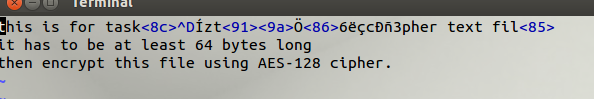
The 30th byte was 10



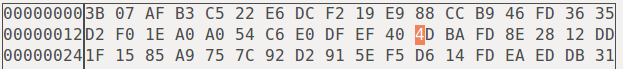
Then change it into F0



Then decrypted, to show the contents of the corrupted file



ECB mode, original file, its 30th byte was 4D.



Then change it into AD



Decrypted to get the content of corrupted file

