University of Regina

Department of Computer Science

Winter 2019

CS 834 - Fundamentals of Computer System Security

Lab 2 - Symmetric Encryption

Submitted to Dr. Habib Louafi

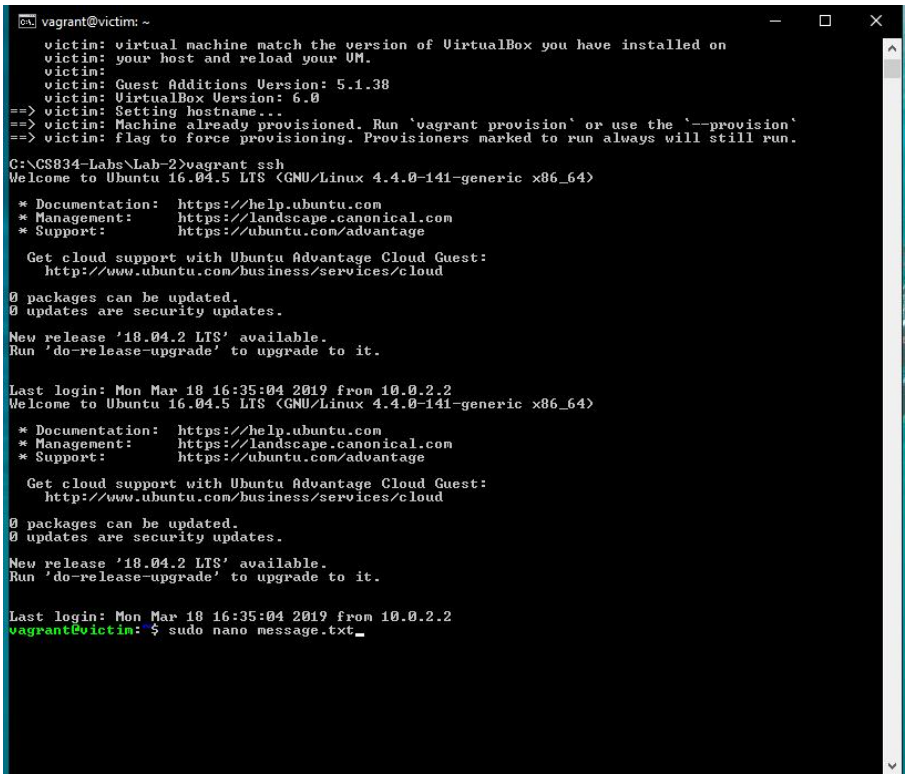
By

Chao Zhang
&
Betrand Nnamdi

Regina, March 18, 2019

I. Setup

Creating a text file and name it: **message.txt**



Adding the following content to the file and save it:

II. 3DES Encryption Algorithm

A. 3DES with operation mode CBC

a. Encrypt the message (the output is .enc):

The command used:

screenshot of encrypted message:

b. Decrypt the message (the output is .dec):

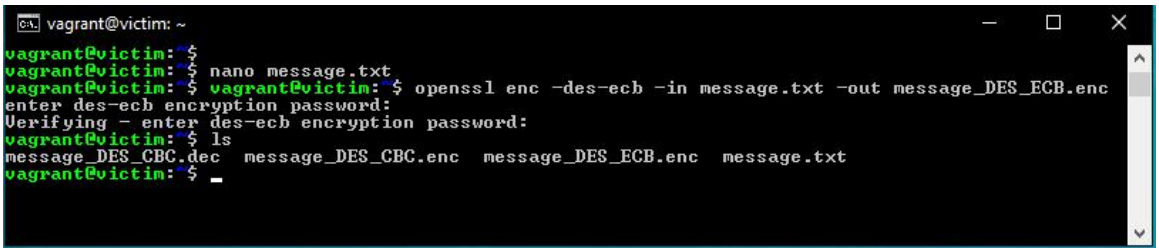
The command used:

screenshot of decrypted message:

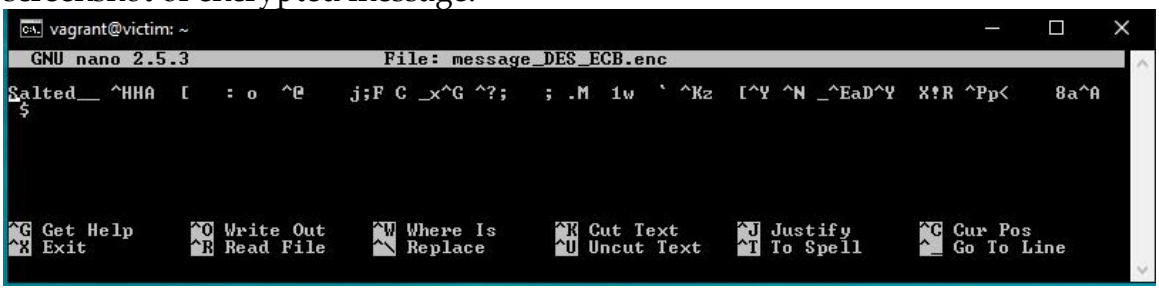
B. 3DES with operation mode ECB

a. Encrypt the message (the output is .enc):

The command used:



screenshot of encrypted message:



b. Decrypt the message (the output is .dec):

The command used:

screenshot of decrypted message:

C. 3DES with operation mode CFB

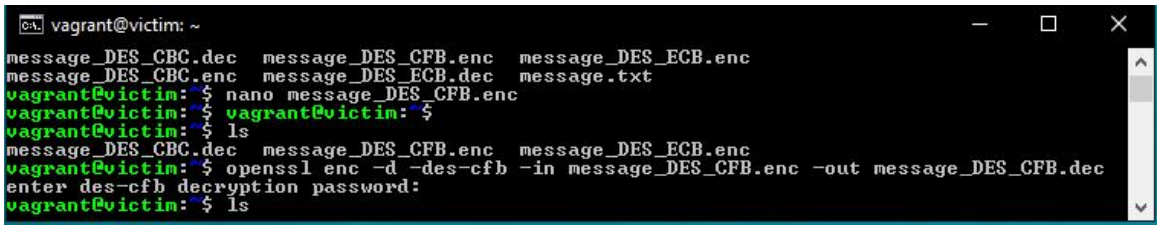
a. Encrypt the message (the output is .enc):

The command used:

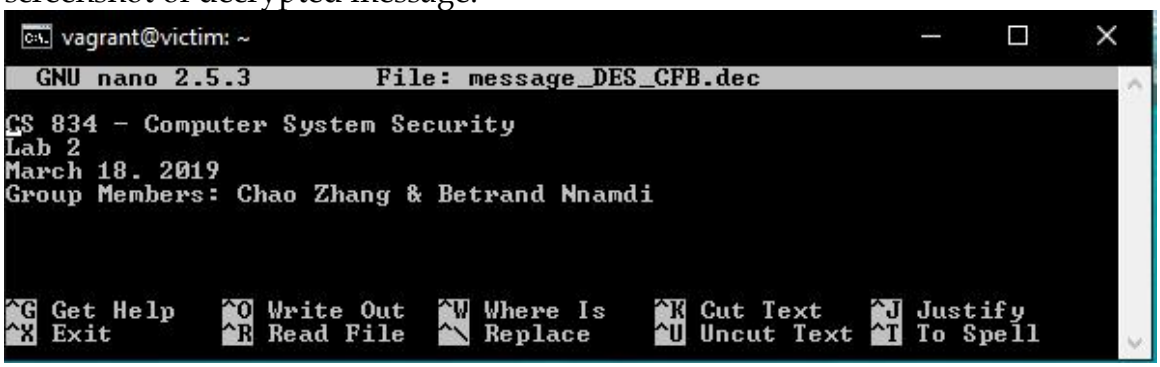
screenshot of encrypted message:

b. Decrypt the message (the output is .dec):

The command used:



screenshot of decrypted message:

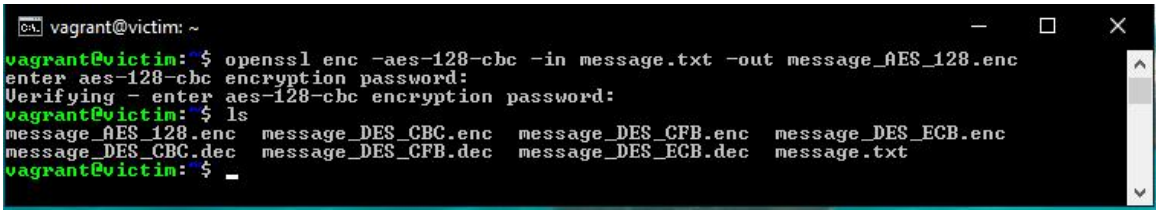


III. AES Encryption Algorithm

A. AES with operation mode CBC and key size 128

a. Encrypt the message (the output is .enc):

The command used:

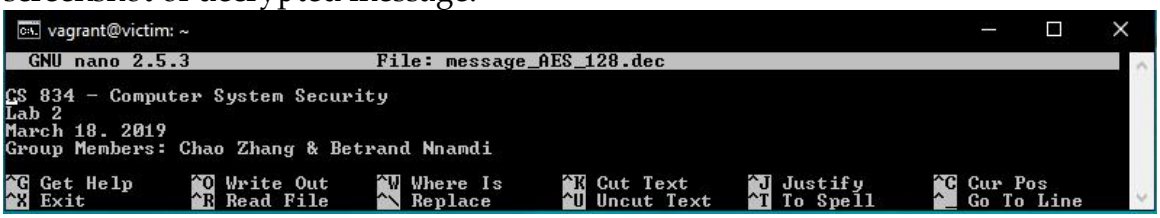


screenshot of encrypted message:

b. Decrypt the message (the output is .dec):

The command used:

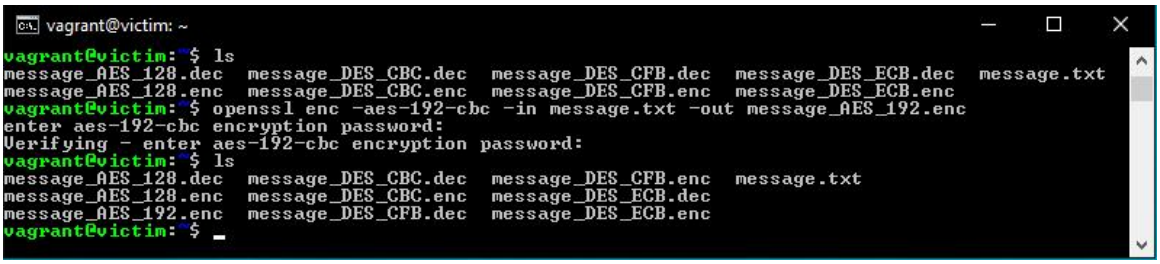
screenshot of decrypted message:



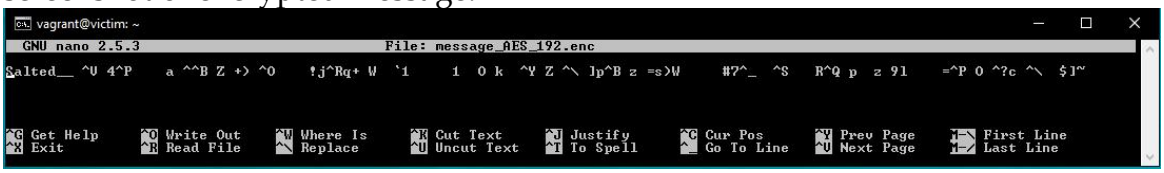
B. AES with operation mode CBC and key size 192

a. Encrypt the message (the output is .enc):

The command used:



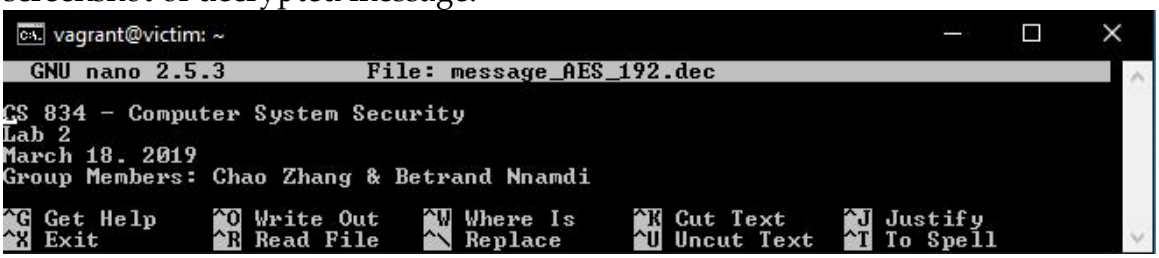
screenshot of encrypted message:



b. Decrypt the message (the output is .dec):

The command used:

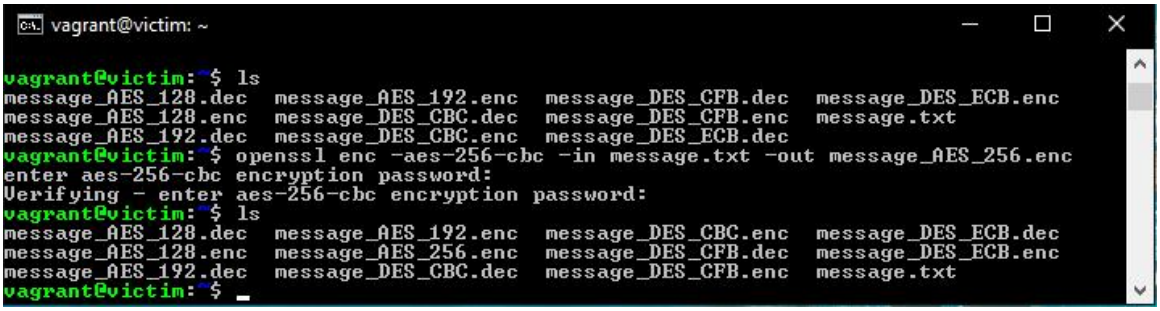
screenshot of decrypted message:



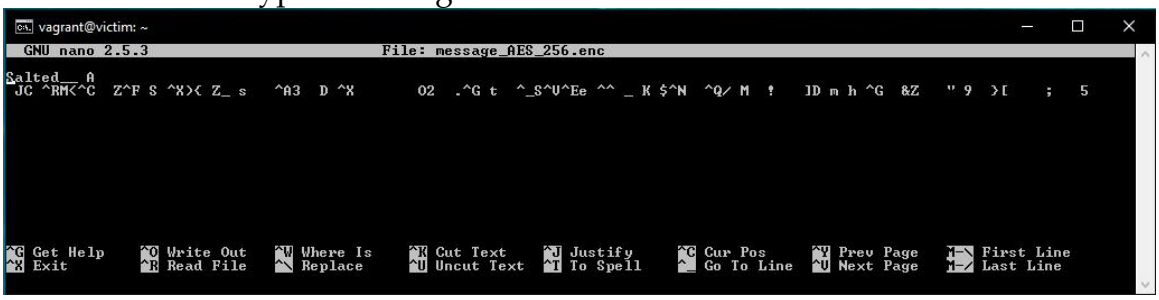
C. AES with operation mode CBC and key size 256

a. Encrypt the message (the output is .enc):

The command used:



screenshot of encrypted message:



b. Decrypt the message (the output is .dec):

The command used:

screenshot of decrypted message: