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

I. Setup

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

```
victin: virtual machine match the version of VirtualBox you have installed on victin: your host and reload your VM.

^ victin: Cuest Additions Version: 5.1.38

victin: Cuest Additions Version: 6.0

- victin: Setting hostname...
-- victin: Setting hostname...
-- victin: Hack for force provisioning. Provisioners marked to run always will still run.

C:C:CSS34-Labs_Lab-2/vagrant ssh

Velcone to Ubuntu 16.04.5 LTS (CNU/Linux 4.4.0-141-generic x86_64)

* Documentation: https://blp.ubuntu.com
* Hamagement: https://blp.ubuntu.com
* Support: https://blp.ubuntu.com/addontage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/businses/services/cloud

Ø packages can be updated.
Ø updates are security updates.

New release '18.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Mar 18 16:35:04 2019 from 10.0.2.2

Velcone to Ubuntu 16.04.5 LTS (CNU/Linux 4.4.0-141-generic x86_64)

* Documentation: https://blp.ubuntu.com
* Hamagement: https://blp.ubuntu.com
* Support: https://blmtu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/businses/services/cloud

Ø packages can be updated.
Ø updates are security updates.

New release '18.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Mar 18 16:35:04 2019 from 10.0.2.2

vagrant@victim: $ sudo nano 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:

```
vagrant@victim: $
ls
message_DES_CBC.enc
message_txt
vagrant@victim: $
nano message_DES_CBC.enc
```

screenshot of encrypted message:



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

The command used:

```
opens11: command not found
vagrant@victim: $ openss1 enc -d -des-cbc -in message_DES_CBC.enc -out message_DES_CBC.dec
enter des-cbc decryption password:
vagrant@victim: $ 1s
message_DES_CBC.dec message_DES_CBC.enc message_txt
vagrant@victim: $ nano message_DES_CBC.dec
```



B. 3DES with operation mode ECB

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

The command used:

```
vagrant@victim: $
vagrant@victim: $
vagrant@victim: $ nano message.txt
vagrant@victim: $ vagrant@victim: $ openssl enc -des-ecb -in message.txt -out message_DES_ECB.enc
enter des-ecb encryption password:
Uerifying - enter des-ecb encryption password:
vagrant@victim: $ ls
message_DES_CBC.dec message_DES_CBC.enc message_DES_ECB.enc message.txt
vagrant@victim: $ ______
```

screenshot of encrypted message:



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

The command used:

```
wagrant@victim: $ 1s
message_DES_CBC.dec message_DES_CBC.enc message_DES_ECB.enc message.txt
vagrant@victim: $ nano message_DES_ECB.enc
vagrant@victim: $ vagrant@victim: $ 1s
message_DES_CBC.dec message_DES_CBC.enc message_DES_ECB.enc
vagrant@victim: $ openss1 enc -d -des-ecb -in message_DES_ECB.enc -out message_DES_ECB.dec
enter des-ecb decryption password:
```



C. 3DES with operation mode CFB

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

The command used:

```
vagrant@victim: $ 1s
message_DES_CBC.dec message_DES_CBC.enc message_DES_ECB.dec message_DES_ECB.enc message.txt
vagrant@victim: $
vagrant
```

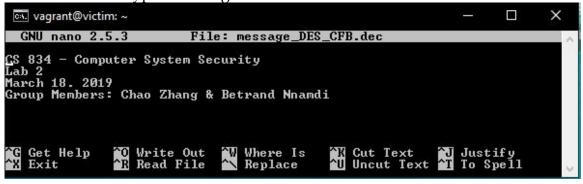
screenshot of encrypted message:



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

The command used:

```
message_DES_CBC.dec message_DES_CFB.enc message_DES_ECB.enc
message_DES_CBC.enc message_DES_ECB.dec message_txt
vagrant@victim: $ nano message_DES_CFB.enc
vagrant@victim: $ vagrant@victim: $ vagrant@victim: $ vagrant@victim: $ vagrant@victim: $ 1s
message_DES_CBC.dec message_DES_CFB.enc
vagrant@victim: $ 0penss1 enc -d -des-cfb -in message_DES_CFB.enc -out message_DES_CFB.dec
enter des-cfb decryption password:
vagrant@victim: $ 1s
```



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:



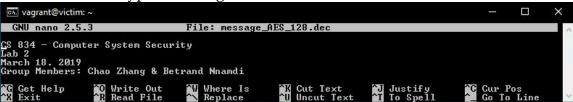
b. Decrypt the message (the output is .dec):

The command used:

```
wagrant@victim: ~ — — X

message_AES_128.enc message_DES_CBC.enc message_DES_CBB.dec message_DES_CBB.dec message_DES_CBB.dec message_DES_EB.dec message_AES_128.enc out message_AES_128.dec
message_AES_128.dec message_DES_CBC.dec message_DES_CFB.dec message_AES_128.enc out message_AES_128.dec
message_AES_128.dec message_DES_CBC.dec message_DES_CFB.dec message_DES_CFB.dec message_DES_CFB.enc
message_AES_128.enc message_DES_CBC.enc message_DES_CFB.enc

wagrant@victim: $
```



B. AES with operation mode CBC and key size 192

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

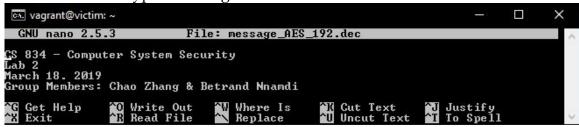
The command used:

screenshot of encrypted message:



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

The command used:



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:

```
vagrant@victim: $ 1s
message_RES_128.dec message_RES_192.dec message_RES_256.enc
message_RES_128.enc message_RES_192.enc message_RES_CBC.dec message_RES_CBC.dec message_RES_256.enc
message_RES_128.enc message_RES_128.enc message_RES_256.enc
message_RES_128.enc message_RES_128.dec message_RES_256.enc
message_RES_128.dec message_RES_128.dec message_RES_256.enc
message_RES_128.dec message_RES_128.dec message_RES_256.dec message_RES_128.dec messa
```

