**Computer Security Lab**

**Lab 4**

**Third Semester 2023**

## Grade

**Name, Family Name: Omer Khan\_**

**ID: 391007603 Section: Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Objective**:

Implement hashing and cryptography algorithms using PowerShell

**Submission:**

Please submit the softcopy by end of the lab session.

**Instructions:**

* Apply Cryptography (encrypt and decrypt some text). Use Triple DES with CBC mode. And AES 256 with CBC mode using PowerShell.
* Take screenshots of the input and the output then include your screenshots at the end of this file.
* Download the program from this link:

<https://www.gpg4win.org/get-gpg4win.html>

**Tasks:**

1. Encrypt the following plaintext using (AES CBC mode):

“Computer Security Lab 2”

1 – open powershell

There is two options to encypt

{1}

1- Create .txt file then type Computer Security Lab 2 in it

* New-Item test.txt # create new file (test.txt)
* Set-Content test.txt 'Computer Security Lab 2’ # write ‘String’ to (test.txt)

2- use gpg to encrypt

* gpg -o encryptTest.txt --symmetric --cipher-algo AES256 .\test.txt

! the it will ask to enter phrase

# use gpg to encrypt contain of (test.txt) using AES alg and store it in (encryptTest.txt)

[For more explain](https://explainshell.com/explain?cmd=+gpg+-o+encryptTest.txt+--symmetric+--cipher-algo+AES256+./test.txt)

3- to check decrypt using gpg

* gpg --decrypt .\encryptTest.txt > decryptTest.txt

# use gpg to decrypt contain of (encryptTest.txt ) and output it to ( decryptTest.txt )

* cat .\decryptTest.txt # read contain of decryptTest.txt

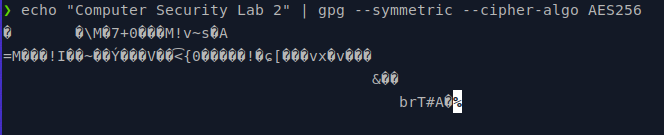
! it should show Computer Security Lab 2

{2}

* echo "Computer Security Lab 2" | gpg --symmetric --cipher-algo AES256

# display "Computer Security Lab 2" the encrypt it using gpg

! it should display encrypted text



1. Encrypt the following plaintext using (Triple DES CBC mode):

“Computer Security Lab 2”

1 – open powershell

There is two options to encypt

{1}

1- Create .txt file then type Computer Security Lab 2 in it

* New-Item test.txt # create new file (test.txt)
* Set-Content test.txt 'Computer Security Lab 2’ # write ‘String’ to (test.txt)

2- use gpg to encrypt

* gpg -o encryptTest.txt --symmetric --allow-old-cipher-algos --cipher-algo 3DES .\test.txt

! the it will ask to enter phrase

# use gpg to encrypt contain of (test.txt) using 3DES alg and store it in (encryptTest.txt)

3- to check decrypt using gpg

* gpg --decrypt .\encryptTest.txt > decryptTest.txt

# use gpg to decrypt contain of (encryptTest.txt ) and output it to ( decryptTest.txt )

* cat .\decryptTest.txt # read contain of decryptTest.txt

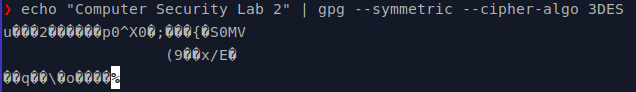
! it should show Computer Security Lab 2

{2}

* echo "Computer Security Lab 2" | gpg --symmetric --allow-old-cipher-algos --cipher-algo 3DES

# display "Computer Security Lab 2" the encrypt it using gpg

! it should display encrypted text

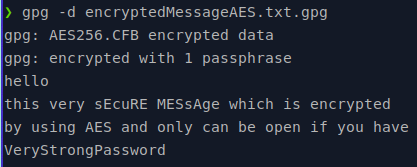


1. Decrypt the following ciphertext using (AES CBC mode):

Find the cihpertext in BlackBoard

The key: VeryStrongPassword

* gpg -d encryptedMessageAES.txt.gpg
  + enter the password
  + then you should see decrypted text



1. Decrypt the following ciphertext using (Triple DES CBC mode):

Find the cihpertext in BlackBoard

The key: VeryStrongPassword

* gpg -d encryptedMessage3DES.txt.gpg
  + enter the password
  + then you should see decrypted text

