

Kush Patel

## Computer and Network Forensics

### Assignment 1

This assignment will be performed under the Kali Linux VM.

1. **Symmetric key encryption and decryption with AES.** Read <https://github.com/xinwenfu/GenCyber/tree/main/SymmetricKeyCrypto> and work on the hands-on labs

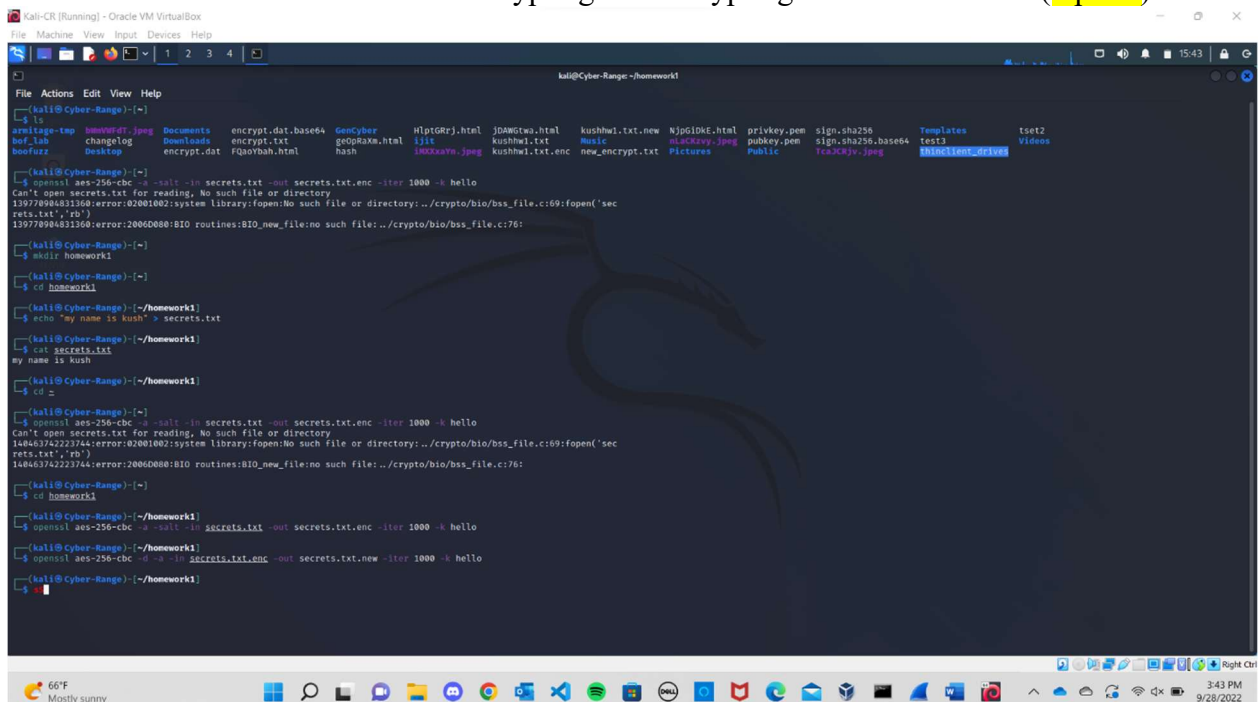
- a. *Hands-on 1: Decipher Caesar cipher encrypted text.* What is the plaintext message? (2 points)

It is a period of civil wars in the galaxy. A brave alliance of underground freedom fighters has challenged the tyranny and oppression of the awesome GALACTIC EMPIRE.

Striking from a fortress hidden among the billion stars of the galaxy, rebel spaceships have won their first victory in a battle with the powerful Imperial Starfleet. The EMPIRE fears that another defeat could bring a thousand more solar systems into the rebellion, and Imperial control over the galaxy would be lost forever.

To crush the rebellion once and for all, the EMPIRE is constructing a sinister new battle station. Powerful enough to destroy an entire planet, its completion spells certain doom for the champions of freedom.

- b. *Hands-on 4: Encrypting and Decrypting File with AES.* Include a screenshot below on the commands used on encrypting and decrypting the file with AES. (1 point)



```
kali@Cyber-Range: ~$ cat secrets.txt
my name is kush

kali@Cyber-Range: ~$ openssl aes-256-cbc -s -salt -in secrets.txt -out secrets.txt.enc -iter 1000 -k hello
Can't open secrets.txt for reading, No such file or directory
159770984831360:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:169:fopen('sec
rets.txt','rb')
159770984831360:error:20060080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:

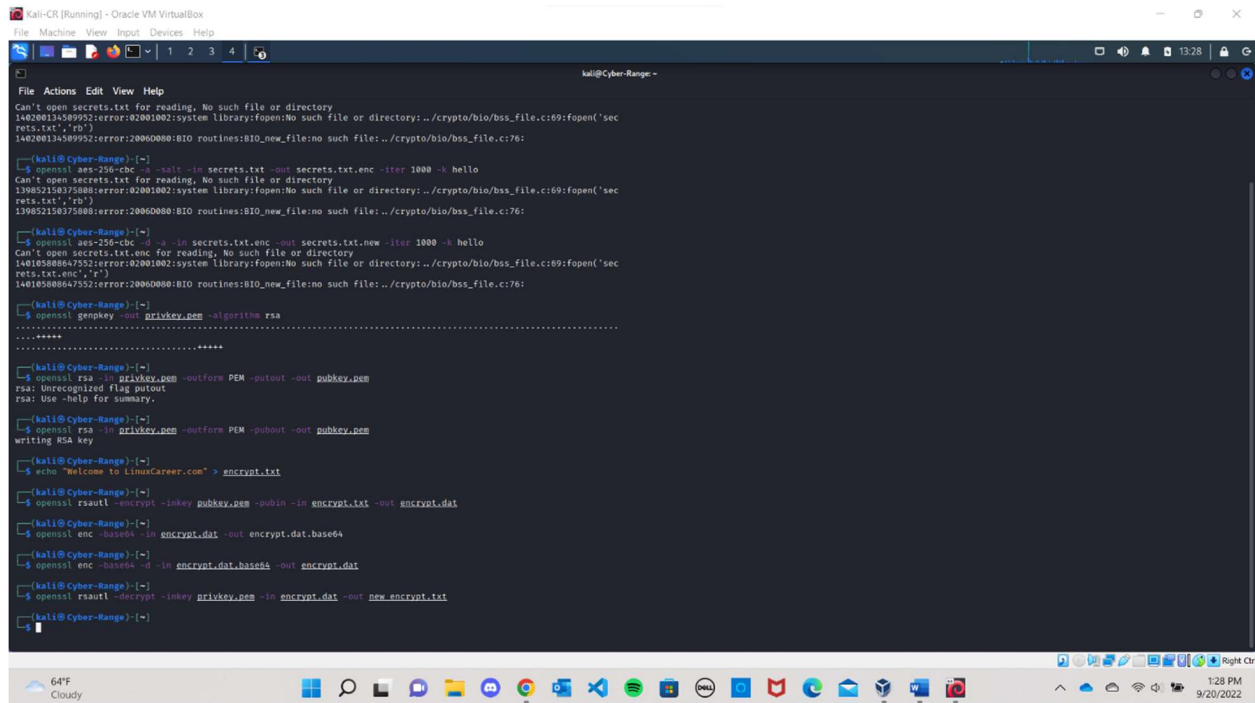
kali@Cyber-Range: ~$ cd ~/homework1
kali@Cyber-Range: ~/homework1$ echo "my name is kush" > secrets.txt
kali@Cyber-Range: ~/homework1$ cat secrets.txt
my name is kush
kali@Cyber-Range: ~/homework1$ cd ~
kali@Cyber-Range: ~$ openssl aes-256-cbc -s -salt -in secrets.txt -out secrets.txt.enc -iter 1000 -k hello
Can't open secrets.txt for reading, No such file or directory
140463742223744:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:169:fopen('sec
rets.txt','rb')
140463742223744:error:20060080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:

kali@Cyber-Range: ~$ cd ~/homework1
kali@Cyber-Range: ~/homework1$ openssl aes-256-cbc -d -s -salt -in secrets.txt.enc -out secrets.txt.new -iter 1000 -k hello
kali@Cyber-Range: ~/homework1$ cat secrets.txt.new
my name is kush
```

## 2. Public key encryption and decryption. Read

<https://github.com/xinwenfu/GenCyber/tree/main/AsymmetricKeyCrypto> and work on the hands-on labs.

- a. *Hands-on 1: Use RSA to Encrypt and Decrypt a Message.* Include a screenshot below on the commands used to encrypting and decrypting a message. (3 points)



```
Kali-CR [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@Cyber-Range: ~
File Actions Edit View Help
Can't open secrets.txt for reading, No such file or directory
140200134589932:error:20001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69:fopen('secrets.txt','rb')
140200134589932:error:20000000:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:

kali@Cyber-Range:~$ openssl aes-256-cbc -k 1 -in secrets.txt -out secrets.txt.enc -iter 1000 -h hello
Can't open secrets.txt for reading, No such file or directory
139852158375888:error:20001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69:fopen('secrets.txt','rb')
139852158375888:error:20000000:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:

kali@Cyber-Range:~$ openssl aes-256-cbc -k 1 -in secrets.txt -out secrets.txt.new -iter 1000 -h hello
Can't open secrets.txt for reading, No such file or directory
140185888647552:error:20001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69:fopen('secrets.txt','rb')
140185888647552:error:20000000:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:

kali@Cyber-Range:~$ openssl genpkey -out prikey.pem -algorithm rsa
.....+++++
.....+++++

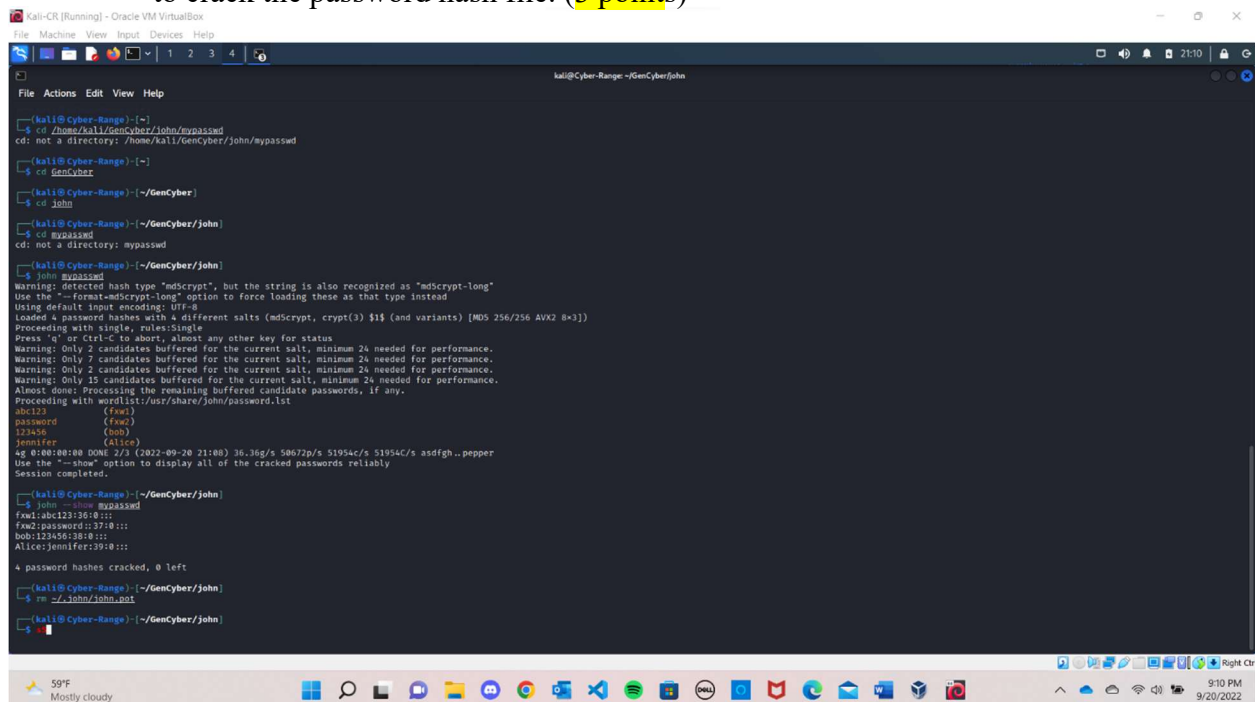
kali@Cyber-Range:~$ openssl rsa -in prikey.pem -outform PEM -pubout -out pubkey.pem
rsa: Unrecognized flag pubout
rsa: Use -help for summary.

kali@Cyber-Range:~$ openssl rsa -in prikey.pem -outform PEM -pubout -out pubkey.pem
writing RSA key

kali@Cyber-Range:~$ echo "Welcome to LinuxCareer.com" > encrypt.txt
kali@Cyber-Range:~$ openssl rsautl -encrypt -inkey pubkey.pem -pubin -in encrypt.txt -out encrypt.dat
kali@Cyber-Range:~$ openssl enc -base64 -in encrypt.dat -out encrypt.dat.base64
kali@Cyber-Range:~$ openssl enc -base64 -d -in encrypt.dat.base64 -out encrypt.dat
kali@Cyber-Range:~$ openssl rsautl -decrypt -inkey prikey.pem -in encrypt.dat -out new_encrypt.txt
kali@Cyber-Range:~$
```

## 3. Hash. Please read <https://github.com/xinwenfu/GenCyber/tree/main/Hash> and work on the hands-on labs.

- a. *Hands-on 3: Password Cracking.* Include a screenshot below on the commands used to crack the password hash file. (3 points)



```
Kali-CR [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@Cyber-Range: ~/GenCyber/john
File Actions Edit View Help

kali@Cyber-Range:~$ cd /home/kali/GenCyber/john/mypasswd
cd: not a directory: /home/kali/GenCyber/john/mypasswd

kali@Cyber-Range:~$ cd GenCyber
kali@Cyber-Range:~/GenCyber$ cd john
kali@Cyber-Range:~/GenCyber/john$ cd mypasswd
cd: not a directory: mypasswd

kali@Cyber-Range:~/GenCyber/john$ john mypasswd
Warning: detected hash type "mdcrypt", but the string is also recognized as "mdcrypt-long"
Use the "--format=mdcrypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (mdcrypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 15 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
abc123 (fox)
password (fox2)
123456 (bob)
jennifer (alice)
4g 0:00:00:00 DONE 2/3 (2022-09-20 21:00) 36.3kg/s 50672p/s 51954c/s 51954c/s asdfgh..pepper
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

kali@Cyber-Range:~/GenCyber/john$ john --show MD5PASSWD
fwi:abc123:36:0:::
fw2:password:1237:0:::
bob:123456:18:0:::
Alice:jennifer:39:0:::

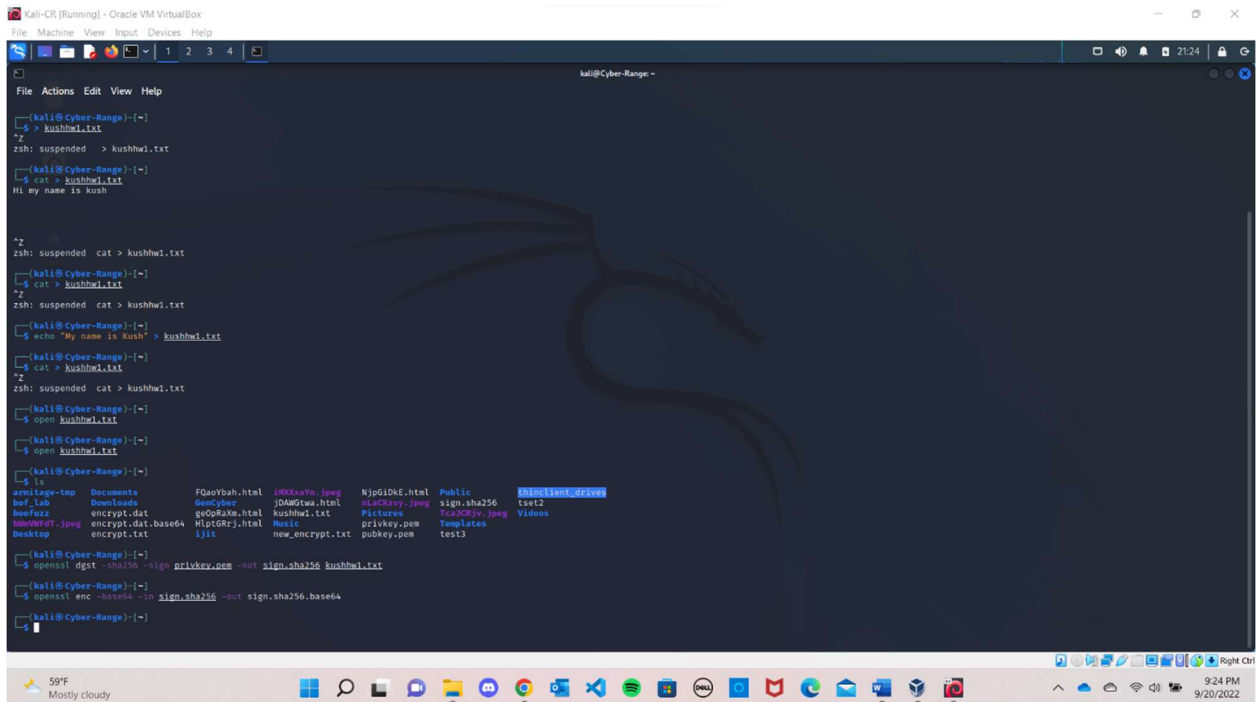
4 password hashes cracked, 0 left

kali@Cyber-Range:~/GenCyber/john$ rm -r john/john.txt
kali@Cyber-Range:~/GenCyber/john$
```

4. **Digital signature.** Please read

<https://github.com/xinwenfu/GenCyber/tree/main/DigitalSignature> and work on the hands-on labs. The instructions in the hands-on were for two students working together. In this assignment, a student works alone on the hands-on. Please create two folders, one for “sender” and the other for “receiver” to hold related files, and pretend to be the sender and receiver at the same time.

- a. *Hands-on 3: One student as Sender: Sign a file.* Include a screenshot below on the commands used to sign the file. (1 point)

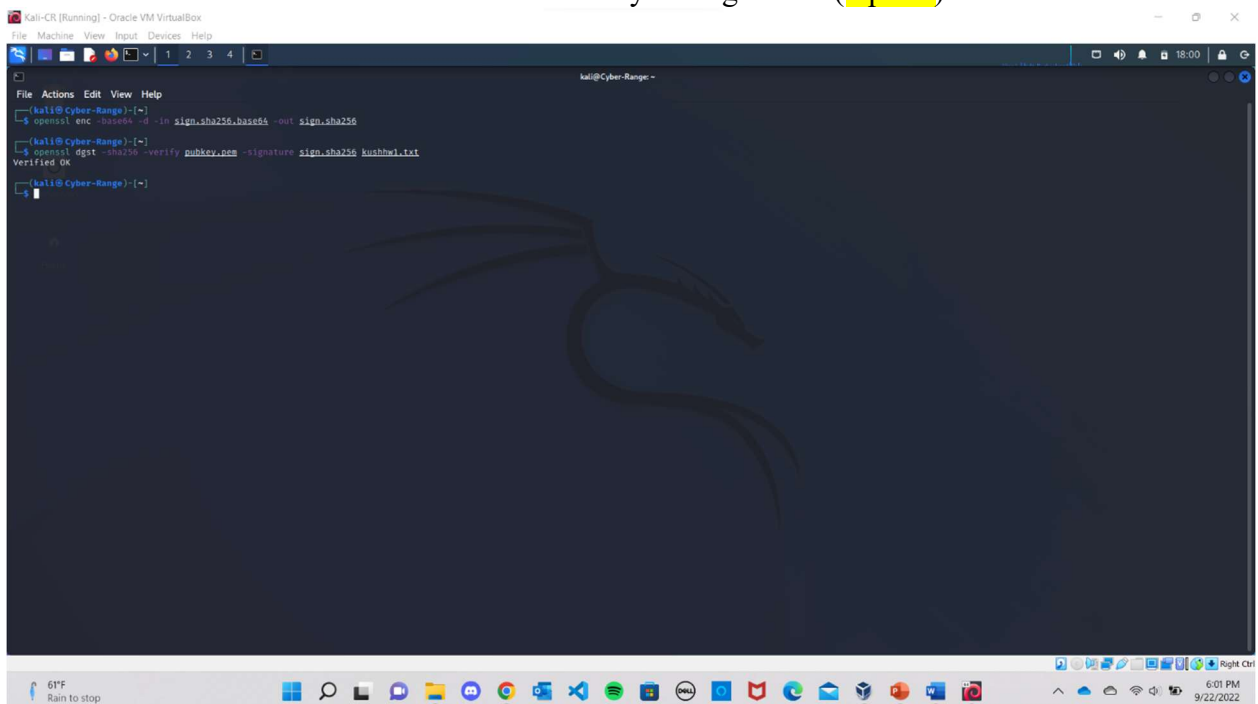


```
kali@Cyber-Range:~$ touch kushhw1.txt
kali@Cyber-Range:~$ cat kushhw1.txt
Hi my name is kush

kali@Cyber-Range:~$ echo "My name is kush" > kushhw1.txt
kali@Cyber-Range:~$ cat kushhw1.txt
My name is kush

kali@Cyber-Range:~$ openssl dgst -sha256 -sign privkey.pem -out sign.sha256 kushhw1.txt
kali@Cyber-Range:~$ openssl enc -base64 -in sign.sha256 -out sign.sha256.base64
```

- b. *Hands-on 4: Another Student as Receiver: Verify the Signature.* Include a screenshot below on the commands used to verify the signature. (1 point)



```
kali@Cyber-Range:~$ openssl dgst -sha256 -verify pubkey.pem -signature sign.sha256 kushhw1.txt
Verified OK
```