



BIRMINGHAM CITY
University

CMP5329 Logbook

Lewis Higgins - Student ID 22133848

January - March, 2024

Contents

Introduction	2
1 OpenSSL	3
1.1 Version checking and ciphers	3
1.2 Symmetric encryption	3
1.2.1 DES symmetric encryption	4
1.2.2 AES256 symmetric encryption and decryption	4
1.3 Asymmetric encryption	5
1.3.1 Generating an RSA private key	5
1.3.2 Storing DES3 & passphrase encrypted RSA keys in a file	6
1.3.3 Getting a public key from the private key	6
1.3.4 Obtaining a message/file digest	8
1.3.5 Signing a digest	9
2 Usage of GPG	10
2.1 Creating test users	10
2.1.1 Elevating the terminal	10
2.1.2 Creating Bob and Alice	10
2.2 Exchanging encrypted files over an insecure channel	13
2.2.1 Generating public/private key-pairs	13
2.2.2 Exporting public keys	14
2.2.3 Importing and signing public keys	14
2.2.4 Encrypting and decrypting data	16
5 Discretionary Access Control	18
5.1 Creating test users and groups	18
5.1.1 Creating groups	18
5.1.2 Adding users to groups	18
5.2 Using chmod and chgrp to assign permissions	21
5.2.1 Restricting directory access	21
5.2.2 Chgrp and chown	24
6 Password Cracking	27
6.1 Linux password storage	27
6.2 crack.c	28
6.2.1 Importing and compilation	28
6.2.2 Creating a test user	29
6.2.3 Cracking the password	30
Reflective report on Cryptography and Access Control	32

Introduction

This logbook documents the work completed and knowledge gained across the CMP5329 labs, showcasing the use of a wide variety of security techniques and access control methods on a Linux OS. This logbook specifically covers the following labs:

- Lab 1, covering OpenSSL.
- Lab 2, covering simple usage of GPG.
- Lab 5, covering the use of Linux Discretionary Access Control commands.
- Lab 6, covering password cracking.

As per module specifications, screenshots taken in each lab include the date and time at which they were taken.

Example note

Additional notes, such as minor issues encountered or omitted screenshots due to work having already been done in earlier labs, are documented using these orange notes.

Example important note

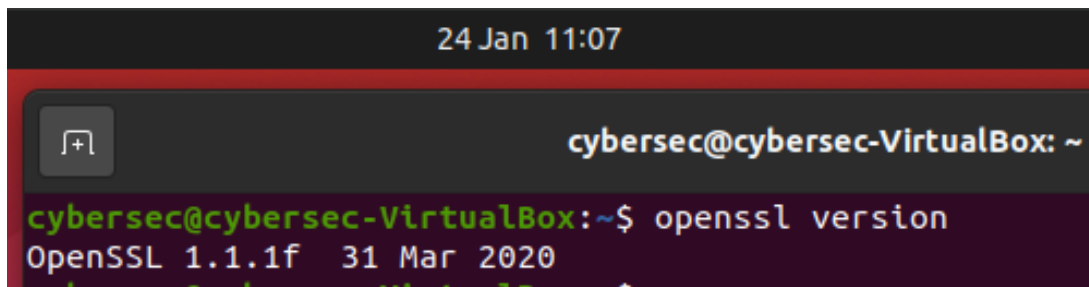
Critical issues that required special workarounds are documented using these red notes.

OpenSSL

This lab was an introduction to the usage of OpenSSL to encrypt and decrypt data using the DES and AES256 symmetric encryption algorithms, as well as RSA private keys used in asymmetric encryption and how to generate and gather public and private keys, alongside message digests.

1.1 Version checking and ciphers

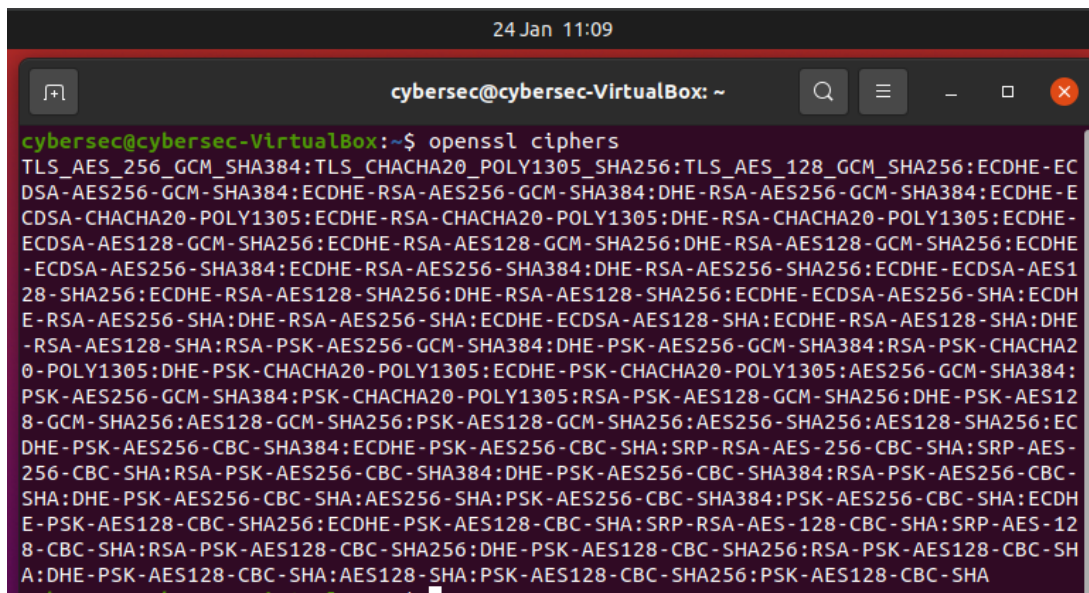
To check the installed version of OpenSSL, "openssl version" can be executed. The provided virtual machine from [the CMP5329 Moodle page](#) uses OpenSSL version 1.1.1f, dated 31st March 2020.



```
24 Jan 11:07
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ openssl version
OpenSSL 1.1.1f 31 Mar 2020
```

Figure 1.1: Getting the OpenSSL version

The list of OpenSSL ciphers can be viewed via "openssl ciphers".



```
24 Jan 11:09
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ openssl ciphers
TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:ECDHE-EC
DSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-E
CDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-CHACHA20-POLY1305:ECDHE-
ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:ECDHE-
ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES1
28-SHA256:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:EC DH
E-RSA-AES256-SHA:DHE-RSA-AES256-SHA:EC DH E-ECDSA-AES128-SHA:EC DH E-RSA-AES128-SHA:DHE
-RSA-AES128-SHA:RSA-PSK-AES256-GCM-SHA384:DHE-PSK-AES256-GCM-SHA384:RSA-PSK-CHACHA2
0-POLY1305:DHE-PSK-CHACHA20-POLY1305:EC DH E-PSK-CHACHA20-POLY1305:AES256-GCM-SHA384:
PSK-AES256-GCM-SHA384:PSK-CHACHA20-POLY1305:RSA-PSK-AES128-GCM-SHA256:DHE-PSK-AES12
8-GCM-SHA256:AES128-GCM-SHA256:PSK-AES128-GCM-SHA256:AES256-SHA256:AES128-SHA256:EC
DH E-PSK-AES256-CBC-SHA384:EC DH E-PSK-AES256-CBC-SHA:SRP-RSA-AES-256-CBC-SHA:SRP-AES-
256-CBC-SHA:RSA-PSK-AES256-CBC-SHA384:DHE-PSK-AES256-CBC-SHA384:RSA-PSK-AES256-CBC-
SHA:DHE-PSK-AES256-CBC-SHA:AES256-SHA:PSK-AES256-CBC-SHA384:PSK-AES256-CBC-SHA:EC DH
E-PSK-AES128-CBC-SHA256:EC DH E-PSK-AES128-CBC-SHA:SRP-RSA-AES-128-CBC-SHA:SRP-AES-12
8-CBC-SHA:RSA-PSK-AES128-CBC-SHA256:DHE-PSK-AES128-CBC-SHA256:RSA-PSK-AES128-CBC-SH
A:DHE-PSK-AES128-CBC-SHA:AES128-SHA:PSK-AES128-CBC-SHA256:PSK-AES128-CBC-SHA
```

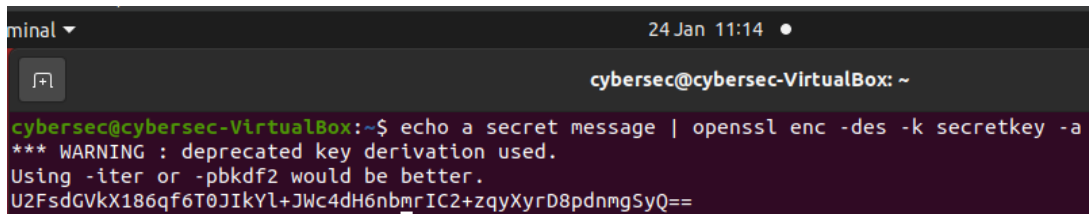
Figure 1.2: Getting the OpenSSL ciphers

1.2 Symmetric encryption

Symmetric cryptography refers to the process of transferring data that has been encrypted by a single key. Both the sender and receiver of this data use the same key to encrypt and decrypt the data.

1.2.1 DES symmetric encryption

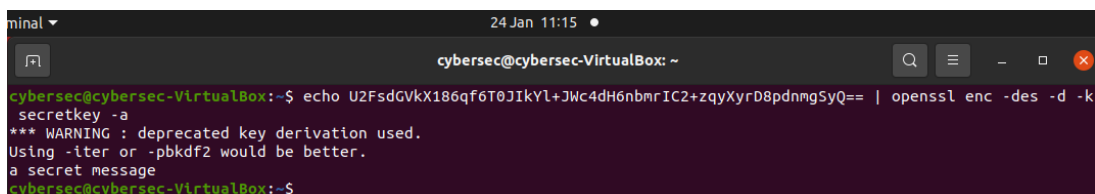
OpenSSL can be used to encrypt plaintext into ciphertext. Many algorithms exist to generate ciphertext, but the DES symmetric encryption algorithm will be used here.



```
minal 24 Jan 11:14
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ echo a secret message | openssl enc -des -k secretkey -a
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
U2FsdGVkX186qf6T0JIKYL+JWc4dH6nbmrIC2+zqyXyrD8pdnmgSyQ==
```

Figure 1.3: Converting "a secret message" to ciphertext using DES with key "secretkey".

This ciphertext can then be decoded if you know the key it was encoded with.



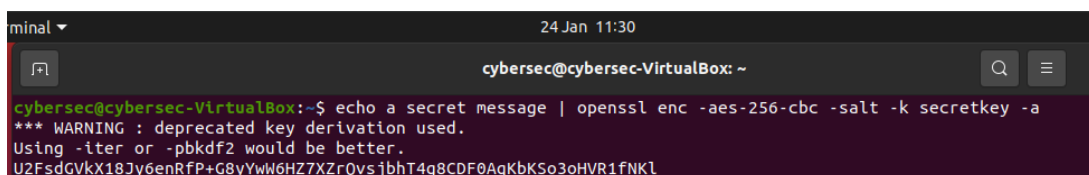
```
minal 24 Jan 11:15
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ echo U2FsdGVkX186qf6T0JIKYL+JWc4dH6nbmrIC2+zqyXyrD8pdnmgSyQ== | openssl enc -des -d -k secretkey -a
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
a secret message
cybersec@cybersec-VirtualBox:~$
```

Figure 1.4: Decoding the ciphertext back to its original form using the key "secretkey".

1.2.2 AES256 symmetric encryption and decryption

The DES algorithm is considered weak due to how simple it is to brute-force using today's processing power. Newer algorithms were therefore developed, with one of these being AES.

I researched how to use this algorithm in OpenSSL, finding [this help page](#) (Heinlein, 2016) which provided details on encrypting text using the AES-256-cbc cipher.



```
minal 24 Jan 11:30
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ echo a secret message | openssl enc -aes-256-cbc -salt -k secretkey -a
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
U2FsdGVkX18Jy6enRfP+G8yYwW6HZ7XZrQvsjbhT4g8CDF0AqKbKSo3oHVR1fNKL
```

Figure 1.5: Encoding the plaintext with AES-256-cbc using the key "secretkey".

In this command the AES-256-cbc cipher is used, and the optional -salt flag was added, which salts the text to provide different ciphertext.

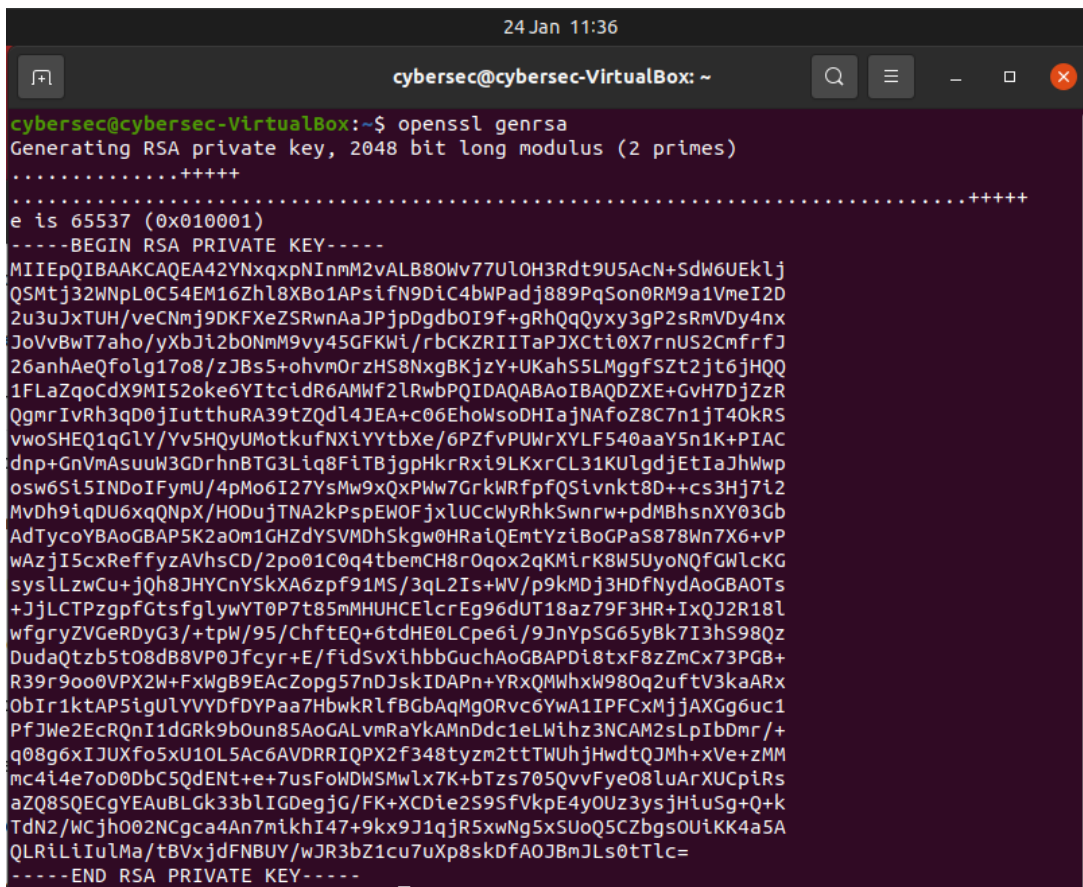
Salting is the process of adding random data to the text prior to encoding it, which will change the resulting ciphertext, making it harder to decrypt and increasing the strength of the encryption.

1.3 Asymmetric encryption

Asymmetric cryptography is the practice of using two keys when transmitting data: a public key used to encrypt data, and a private key used to decrypt it. This is unlike symmetric encryption which uses one key for both users, but can be much more secure. Data transferred this way has a digital signature attached, which allows for non-repudiation, as it cannot be denied that the data originated from the user with the private key associated with the signature.

1.3.1 Generating an RSA private key

OpenSSL can be used to generate these keys by using the "openssl genrsa" command.



```

24 Jan 11:36
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ openssl genrsa
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAA42YNxqpNInmM2vALB80Wv77U0H3Rdt9U5ACn+SdW6UEklj
QSMtj32WnPL0C54EM16Zhl8XBo1APsifN9DiC4bWPadj889PqSon0RM9a1VmeI2D
2u3uJxTUH/veCNmj9DKFXeZSRwnAaJPjpDgdb0I9f+gRhQqQyxy3gP2sRmVDy4nx
JoVvBwT7aho/yXbJi2b0NmM9vy45GFKWi/rbCKZRIITaPJXcti0X7rnUS2CmfrfJ
26anhAeQfolg17o8/zJBs5+ohvmOrzHS8NxbKjzY+UKahS5LMggfSZt2jt6jHQQ
1FLaZqCdX9MI52oke6YItcidR6AMwf2lRwbPQIDAQABAoIBAQDZXE+GvH7DjZZR
QgmrIvRh3qd0jIutthuRA39tZQdL4JEA+c06EhowsDHtaJNAfoZ8C7n1jt40kRS
vwoSHEQ1qGLY/Yv5HQyUMotkufNXiYYtbXe/6PZfvPUWrXYLF540aaY5n1K+PIAC
dnp+GnVmAsuuW3GDrhnBTG3LiQ8FiTBjgpHkrRxi9LKxrCL31KULgdjEtIaJhWwp
osw6Si5INDoIFymU/4pMo6I27YsMw9xQxPWw7GrkWRfpfQSiVnkt8D++cs3Hj7i2
MvDh9iqDU6xQNPX/HODujTNA2kPspEWOEfxlUCCWYRhKSwncrw+pdMBhsnXY03Gb
AdTycoYBAoGBAP5K2aOm1GHZdYSVMDhSkgw0HRaiQEmtYziBoGPas878Wn7X6+vP
wAzjI5cxReffyzAVhsCD/2po01C0q4tbemCH8rOqox2qKMirK8W5UyoNQfGWLcKG
sysLLZcw+jQh8JHYCnYSkXA6zpf91MS/3qL2Is+WV/p9kMDj3HdfNydAoGBAOTs
+JjLCTPzpgfGtsfglywYT0P7t85mMHUHCeLcrEg96dUT18az79F3HR+IxQJ2R18l
wfgryZVGeRdyG3/+tpW/95/ChftEQ+6tdHE0LCpe6i/9JnYpSG65yBk7I3hs98Qz
DudaQtzb5t08dB8VP0Jfcyr+E/fldSvXihbbGuchAoGBAPDi8txF8ZmCx73PGB+
R39r9oo0VPX2W+FxWgB9EAcZopp57nDJskIDAPn+YRxQMWhxw980q2uftV3kaARx
ObIr1ktAP5igULVYDFDYpaa7HbwkRlFBGbAqMgORvc6Ywa1IPFCxMjjAXGg6uc1
PfJWe2EcRQnI1dGRk9b0un85AoGALvmRaYkAMnDdc1eLWihz3NCAM2sLpIbDmr/+
q08g6xIJUXFo5xU10L5Ac6AVDRRIQPX2f348tyzm2ttTWUjhHwdtQJMH+xVe+zMM
mc4i4e7oD0DbC5QdENT+e+7usFoWDSMwLx7K+bTzs705QvvFye08luArXUCpiRs
aZQ8SQECgYEaUoBLGk33bLIGDegjG/FK+XCDie2S9SfVkpE4y0Uz3ysjHiusg+Q+k
TdN2/WCjh002NCgca4An7mikhI47+9kx9J1qjR5xwNg5XsUoQ5CZbgs0UiKK4a5A
QLRiLiIulMa/tBVxjdfNBuY/wJR3bZ1cu7uXp8skDfAOJBmJLs0tTlc=
-----END RSA PRIVATE KEY-----

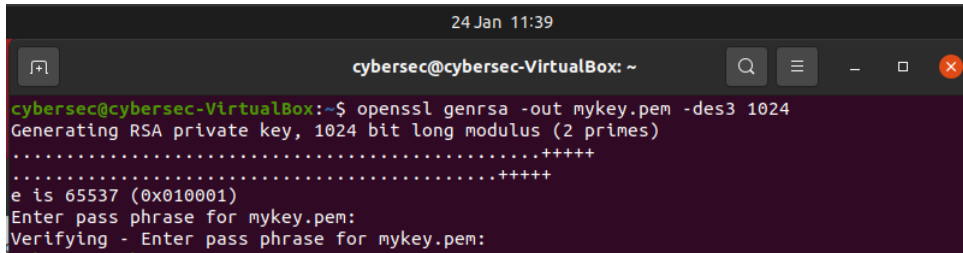
```

Figure 1.6: Generating a 2048-bit private key using genrsa.

1.3.2 Storing DES3 & passphrase encrypted RSA keys in a file

The key generated can then be encrypted using an encryption algorithm and a passphrase. It can then be stored into a Privacy Enhanced Mail (.pem) file, which is a file format 'to provide the creation and validation of digital signatures, and in addition the encryption and decryption of signed data, based on asymmetric and symmetric cryptography.' (Kolletzki, 1996, p. 1894)

In this example, a 1024-bit key is created using DES3 and the passphrase "secretkey".

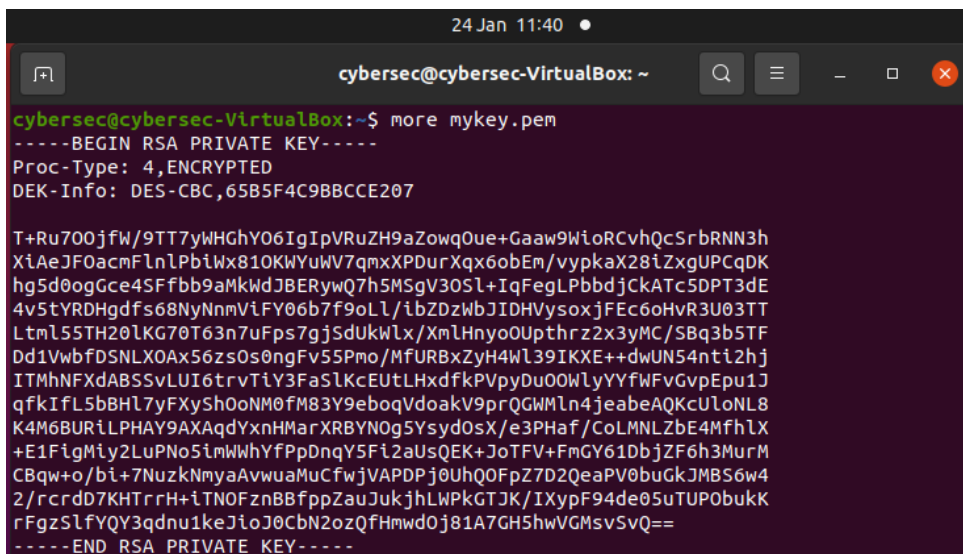


```

24 Jan 11:39
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ openssl genrsa -out mykey.pem -des3 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for mykey.pem:
Verifying - Enter pass phrase for mykey.pem:

```

Figure 1.7: Generating and storing a 1024-bit private key using genrsa, DES3 and the passphrase "secretkey".



```

24 Jan 11:40
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ more mykey.pem
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-CBC,65B5F4C9BBCCE207

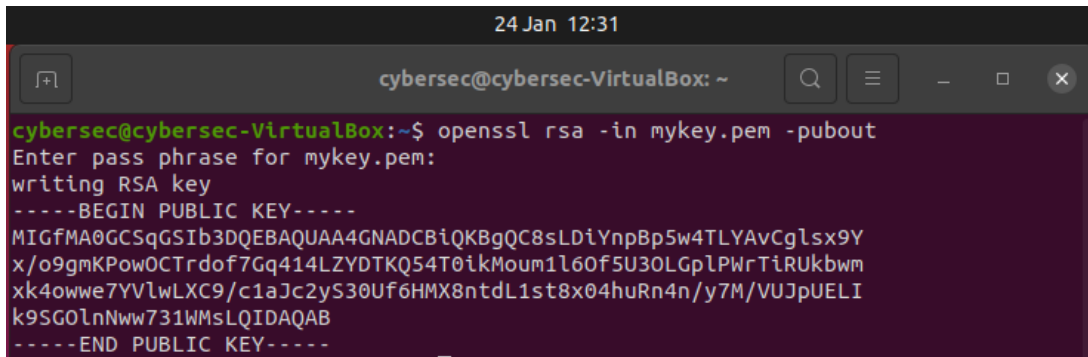
T+Ru700jfw/9TT7yWHGhY06IgIpVRuZH9aZowqOue+Gaaw9WioRCvhQcSrbRNN3h
XiAeJFOacmFlnPbiWx810KWYuWV7qmxXPDurXqx6obEm/vypkaX28iZxgUPCqDK
hg5d0ogGce4SFfb9aMkwDJBERYwQ7h5MSgV30Sl+IqFegLPbbdjCkATc5DPT3dE
4v5tYRDHgdFs68NyNmViFY06b7f9oLl/ibZDzWbJIDHvysoxjFEc6oHvR3U03TT
LtmL55TH20lKG70T63n7uFps7gjSdUkWlX/XmLHnyo0Upthrz2x3yMC/SBq3b5TF
Dd1VwbFDSNLX0Ax56zs0s0ngFv55Pmo/MfURBxZyH4wL39IKXE++dwUN54nti2hj
ITMhNFXdABSSvLUI6trvTiY3FaSlKcEutLHxdfkPVpyDu00WlyYYfWFvGvpEpu1J
qfkiFL5bBHl7yFXySh0oNM0fM83Y9eboqVdoakV9prQGWMLn4jeabeAQKcUloNL8
K4M6BURiLPHAY9AXAqdYxnHMarXRBYN0g5Ysyd0sX/e3PHaf/CoLMNLZbE4MfhLX
+E1FigMiy2LuPNo5iMWhYfPpDnqY5Fi2aUsQEK+JoTFV+FmGY61DbjZF6h3MurM
CBqw+o/bi+7NuzkNmyaAvwuaMuCfwjVAPDPj0UHQ0FpZ7D2QeaPV0buGkJMB56w4
2/rccrd07KHTrRH+iTNOfznBBfppZauJukjhLWPkGTJK/IXypF94de05uTUPObukK
rFgzSlfYQY3qdnu1keJioJ0CbN2ozQfHmwd0j81A7GH5hwVGMsvSvQ==
-----END RSA PRIVATE KEY-----

```

Figure 1.8: The key stored in mykey.pem.

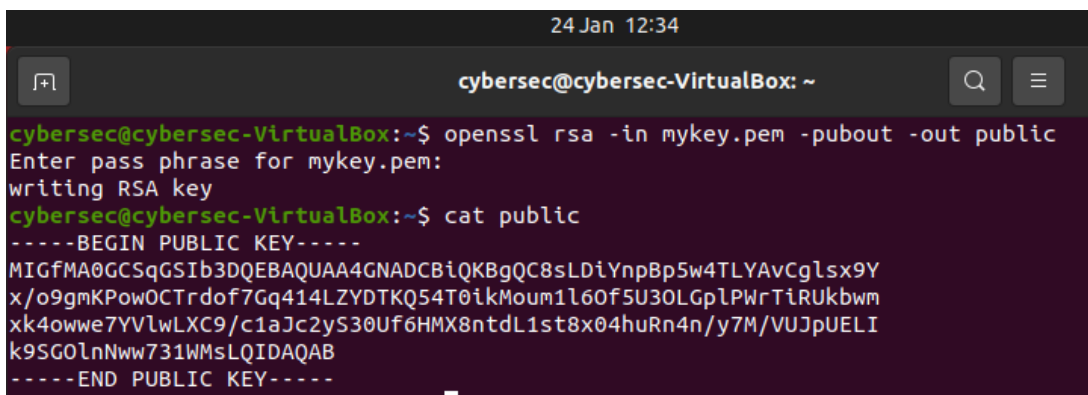
1.3.3 Getting a public key from the private key

The private key stored into "mykey.pem" by the previous command can be accessed again to generate a public key.



```
24 Jan 12:31
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ openssl rsa -in mykey.pem -pubout
Enter pass phrase for mykey.pem:
writing RSA key
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8sLDiYnpBp5w4TLyAvCglsx9Y
x/o9gmKPowOCTrdof7Gq414LZYDTKQ54T0ikMoum1l6Of5U30LGplPwrtiRukbwm
xk4owwe7YVlwLXC9/c1aJc2yS30Uf6HMX8ntdL1st8x04huRn4n/y7M/VUJpUELI
k9SG0lnNww731WmsLQIDAQAB
-----END PUBLIC KEY-----
```

Figure 1.9: The public key generated from mykey.pem.



```
24 Jan 12:34
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ openssl rsa -in mykey.pem -pubout -out public
Enter pass phrase for mykey.pem:
writing RSA key
cybersec@cybersec-VirtualBox:~$ cat public
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8sLDiYnpBp5w4TLyAvCglsx9Y
x/o9gmKPowOCTrdof7Gq414LZYDTKQ54T0ikMoum1l6Of5U30LGplPwrtiRukbwm
xk4owwe7YVlwLXC9/c1aJc2yS30Uf6HMX8ntdL1st8x04huRn4n/y7M/VUJpUELI
k9SG0lnNww731WmsLQIDAQAB
-----END PUBLIC KEY-----
```

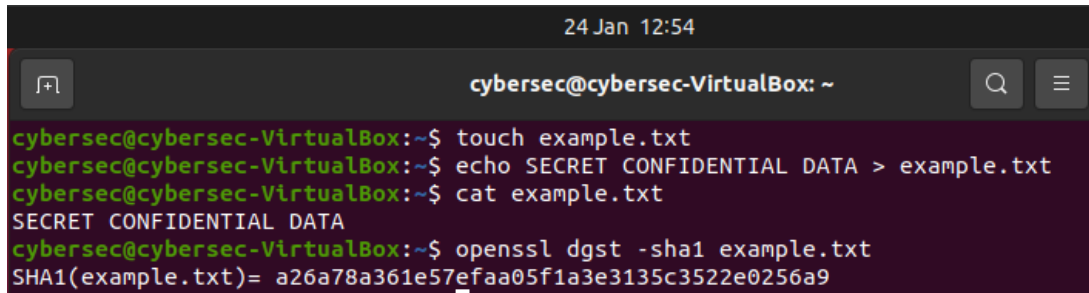
Figure 1.10: Storing the public key in a file.

"-out public" writes the key to a file called "public". This file can then be read using cat.

1.3.4 Obtaining a message/file digest

To mitigate the risks of data interception or corruption, files can have "digests", which are the result of hashing their contents. If the file is modified whatsoever, the digest would be different.

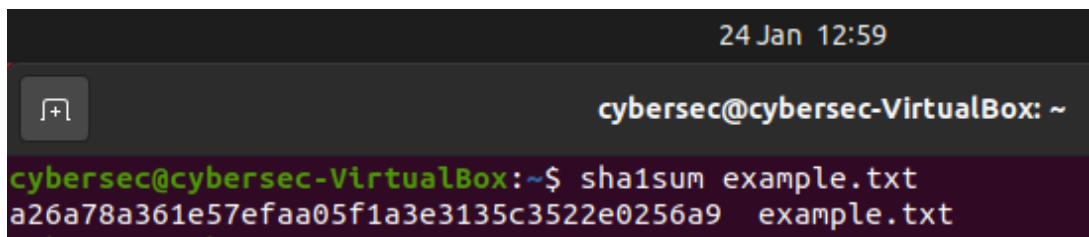
OpenSSL can generate digests using its "dgst" command.



```
24 Jan 12:54
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ touch example.txt
cybersec@cybersec-VirtualBox:~$ echo SECRET CONFIDENTIAL DATA > example.txt
cybersec@cybersec-VirtualBox:~$ cat example.txt
SECRET CONFIDENTIAL DATA
cybersec@cybersec-VirtualBox:~$ openssl dgst -sha1 example.txt
SHA1(example.txt)= a26a78a361e57efaa05f1a3e3135c3522e0256a9
```

Figure 1.11: Creating a file, then getting the SHA1 digest of it.

This can also be verified by using sha1sum, which returns the same digest.



```
24 Jan 12:59
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ sha1sum example.txt
a26a78a361e57efaa05f1a3e3135c3522e0256a9 example.txt
```

Figure 1.12: Verifying the digest.

1.3.5 Signing a digest

Signing a message digest using your private key definitively proves you sent it, meaning that it cannot be denied that the file was sent, nor who it was sent by.

The previously used "example.txt" can again be used here to generate a digest encrypted using the "mykey.pem" private key established earlier, which signs the digest.

[illegible]


Figure 1.13: Writing a signed digest to a file.

Note that when we try to read this file, it is completely illegible, as it is not in Base64/ASCII format. It can be converted to Base64 using OpenSSL's "enc" command.

```
24 Jan 13:09
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ openssl enc -base64 -in example.txt.sha1
iuFRtg0qh9iF//E69oS8IA90y2Fv5oJh2+uIbeaOMRq3tP8leaieIgYUMmrKNpHr
caIfC6pleKt6ADYt0n3Yw40BrOEqfb64EEo0iS2v9q+zd1lUenv7usC/KzBWYyAX
fVy9jEe9qTr9XCp7R/2IyggUiMqLu3Cy1yJFYwXGgk4=
```

Figure 1.14: Encoding the signed digest to Base64.

Now that we have the signed digest, it can be verified using the public key, which confirms the authenticity of the data in example.txt.



The screenshot shows a terminal window with a dark background. The title bar at the top indicates the date and time as "24 Jan 13:11". The terminal prompt is "cybersec@cybersec-VirtualBox: ~". The command entered is "openssl dgst -sha1 -verify public -signature example.txt.sha1 example.txt". The output of the command is "Verified OK".

Figure 1.15: Verifying the signature of example.txt.

This returns "Verified OK" as intended. If the file does get modified through either corruption or a threat agent's interference, the digest would not be the same, seen below:

```
cybersec@cybersec-VirtualBox: ~  
cybersec@cybersec-VirtualBox:~$ echo MODIFIED DATA > example.txt  
cybersec@cybersec-VirtualBox:~$ openssl dgst -sha1 -verify public -signature example.txt.sha1 example.txt  
Verification Failure
```

Figure 1.16: Failing to verify the signature of example.txt, as it has been modified.

Usage of GPG

Important note

In this lab, an incompatibility meant that instead of using the base GPG program, the alternative **GnuPG1** was used. Therefore, commands use the phrase "gpg1" instead of "gpg".

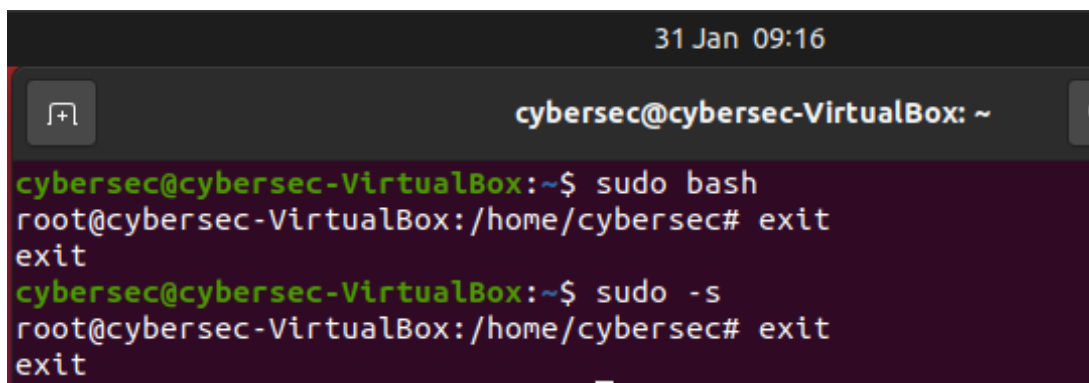
This lab expanded on the concepts of asymmetric encryption through the use of GPG/GnuPG (GNU Privacy Guard) to produce, sign and verify public and private keys.

2.1 Creating test users

For this lab, two test users were created and used to execute the necessary commands.

2.1.1 Elevating the terminal

To add users to the system, administrative privileges are required. To gain the necessary privileges, the command "sudo -s" or "sudo bash" can be entered which will change the terminal to be at root level.

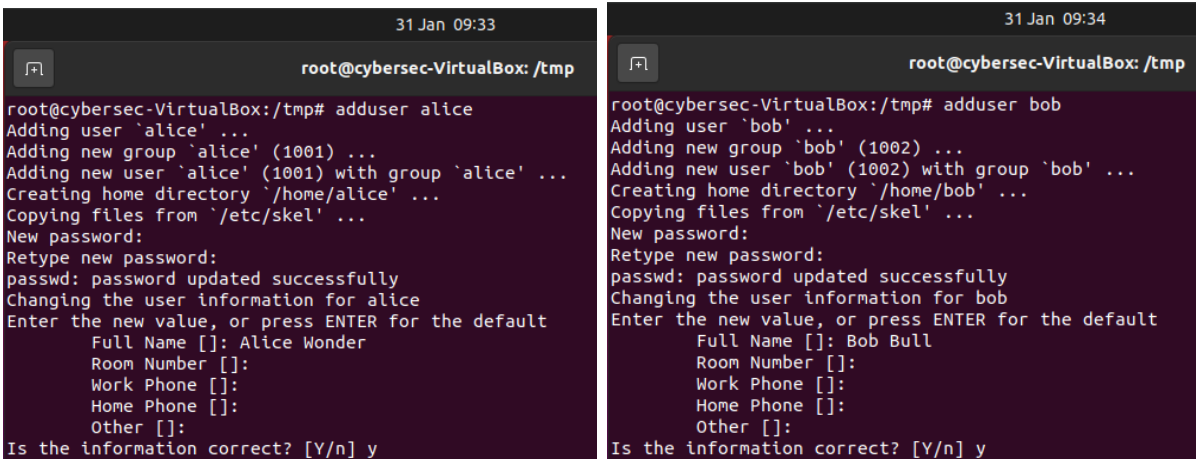


```
31 Jan 09:16
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ sudo bash
root@cybersec-VirtualBox:/home/cybersec# exit
exit
cybersec@cybersec-VirtualBox:~$ sudo -s
root@cybersec-VirtualBox:/home/cybersec# exit
exit
```

Figure 2.1: Elevating the terminal.

2.1.2 Creating Bob and Alice

Sudo allows us to add users to the system using "adduser" followed by the given username. A password for the user will then be necessary, followed by optional information such as phone numbers, which are left blank.



The image contains two side-by-side terminal window screenshots. The left window, titled 'root@cybersec-VirtualBox: /tmp' with a timestamp of '31 Jan 09:33', shows the command 'adduser alice' being executed. It prompts for a password, confirms the user 'alice' (ID 1001) is added to the 'alice' group, and asks for personal details like full name, room number, and phone numbers. The right window, titled 'root@cybersec-VirtualBox: /tmp' with a timestamp of '31 Jan 09:34', shows the command 'adduser bob' being executed. It follows a similar process for adding user 'bob' (ID 1002) to the 'bob' group, also asking for personal details.

Figure 2.2: Creating users 'bob' and 'alice'.

For ease of access, multiple terminal tabs can be open at a time, so I elected to use one for the superuser root, and one each for Bob and Alice.

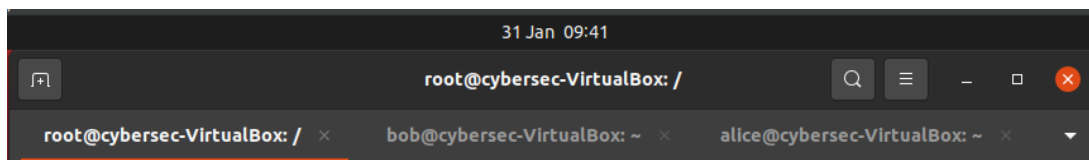


Figure 2.3: Multiple terminal tabs.

I also added these new users to the "sudo" group, allowing them to also use the sudo command to execute commands with elevated permissions.

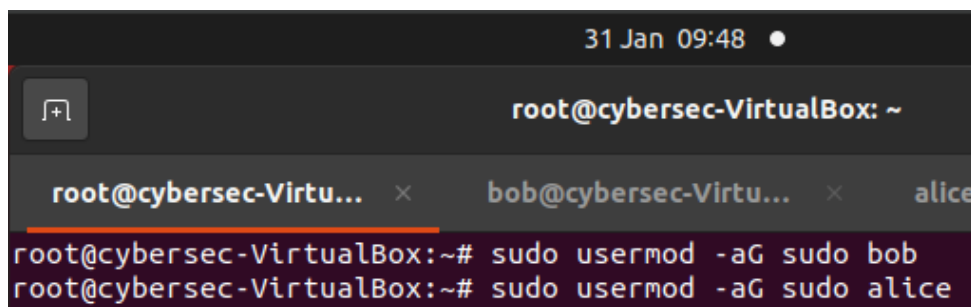
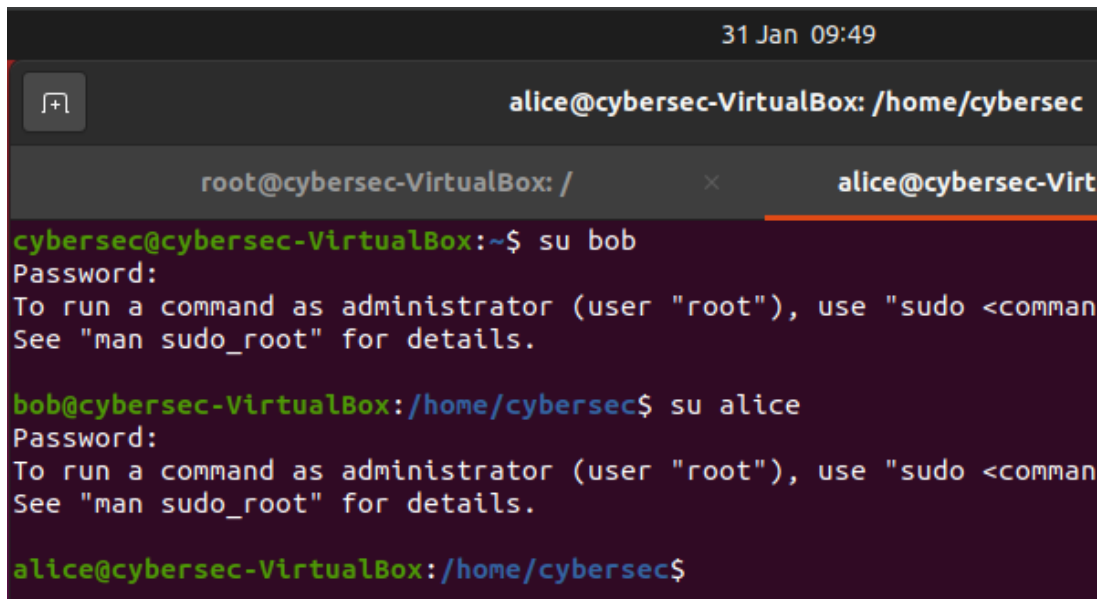


Figure 2.4: Adding bob and alice to sudo.

It is possible to switch the active terminal user using the command "su" followed by the account to switch to, and then the password of the given account.



The screenshot shows a terminal window titled "31 Jan 09:49". The active tab is "alice@cybersec-VirtualBox: /home/cybersec". Below the tab bar, there is a sub-tab bar with "root@cybersec-VirtualBox: /" and "alice@cybersec-Virt". The terminal content shows the following sequence of commands and output:

```
alice@cybersec-VirtualBox: /home/cybersec
cybersec@cybersec-VirtualBox:~$ su bob
Password:
To run a command as administrator (user "root"), use "sudo <command>"
See "man sudo_root" for details.

bob@cybersec-VirtualBox:/home/cybersec$ su alice
Password:
To run a command as administrator (user "root"), use "sudo <command>"
See "man sudo_root" for details.

alice@cybersec-VirtualBox:/home/cybersec$
```

Figure 2.5: Switching the active terminal user.

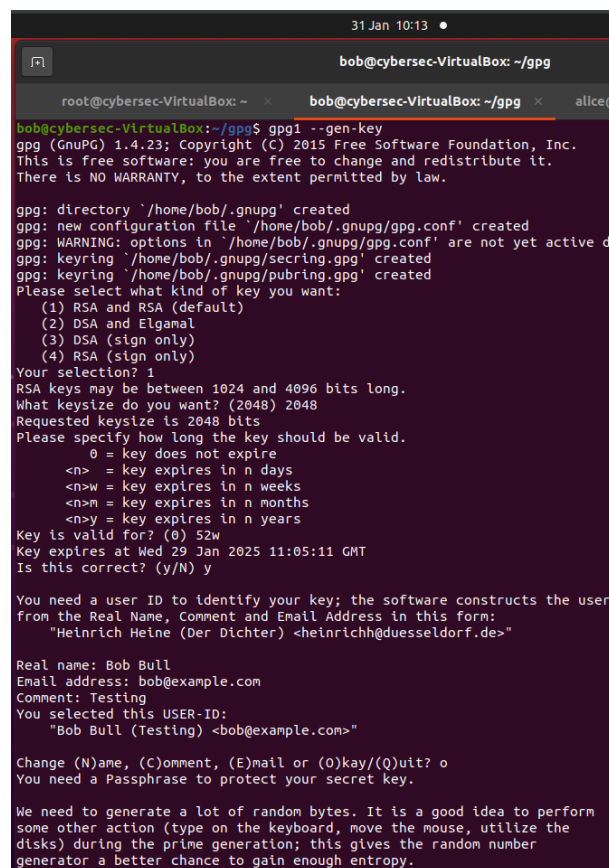
2.2 Exchanging encrypted files over an insecure channel

For this section, assume that all commands have been executed on **both** the Bob and Alice user accounts unless stated otherwise.

On standard Linux distributions, the `/tmp` directory is a public directory where all users can read files placed there.¹ To transfer files across insecure channels such as `/tmp/`, they should first be encrypted so that they can only be read and/or used by their intended recipient. Therefore, GPG can be used to generate and store public and private asymmetric keys.

2.2.1 Generating public/private key-pairs

"`gpg1 --gen-key`" generates a private key.



```

31 Jan 10:13 •
bob@cybersec-VirtualBox: ~/gpg
root@cybersec-VirtualBox: ~
bob@cybersec-VirtualBox: ~/gpg
alice@
bob@cybersec-VirtualBox:~/gpg$ gpg1 --gen-key
gpg (GnuPG) 1.4.23; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory '/home/bob/.gnupg' created
gpg: new configuration file '/home/bob/.gnupg/gpg.conf' created
gpg: WARNING: options in '/home/bob/.gnupg/gpg.conf' are not yet active du
gpg: keyring '/home/bob/.gnupg/secring.gpg' created
gpg: keyring '/home/bob/.gnupg/pubring.gpg' created
Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 2048
Requested keysize is 2048 bits
Please specify how long the key should be valid.
    0 = key does not expire
    <n> = key expires in n days
    <n>w = key expires in n weeks
    <n>m = key expires in n months
    <n>y = key expires in n years
Key is valid for? (0) 52w
Key expires at Wed 29 Jan 2025 11:05:11 GMT
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user
from the Real Name, Comment and Email Address in this form:
"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Bob Bull
Email address: bob@example.com
Comment: Testing
You selected this USER-ID:
"Bob Bull (Testing) <bob@example.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
  
```

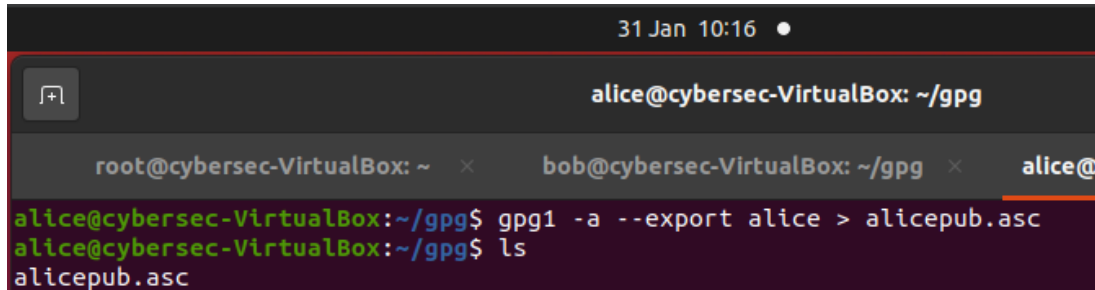
Figure 2.6: Generating a private key.

This will open a submenu where the user can select the kind of key they wish to generate, and its size and expiry date. After this, they must create a user ID if one doesn't exist, with their full name, email address and an optional comment. While the key generates, the user is prompted to perform random inputs to enhance its entropy. A key was also generated for Alice.

¹However, they cannot update/change them without `sudo` permissions.

2.2.2 Exporting public keys

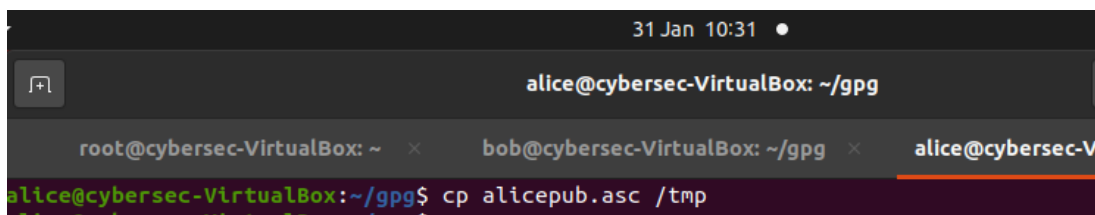
It is possible to export the public keys from the generated key-pairs using GPG's export command.



```
31 Jan 10:16 ●
alice@cybersec-VirtualBox: ~/gpg
root@cybersec-VirtualBox: ~ x bob@cybersec-VirtualBox: ~/gpg x alice@
alice@cybersec-VirtualBox:~/gpg$ gpg1 -a --export alice > alicepub.asc
alice@cybersec-VirtualBox:~/gpg$ ls
alicepub.asc
```

Figure 2.7: Exporting Alice's public key.

This exports the public key in ASCII format (due to the use of the `-a` flag) to the file "alicepub.asc".² Because this is Alice's **public** key, we are comfortable sharing this to the public `/tmp/` directory where all users can see it.

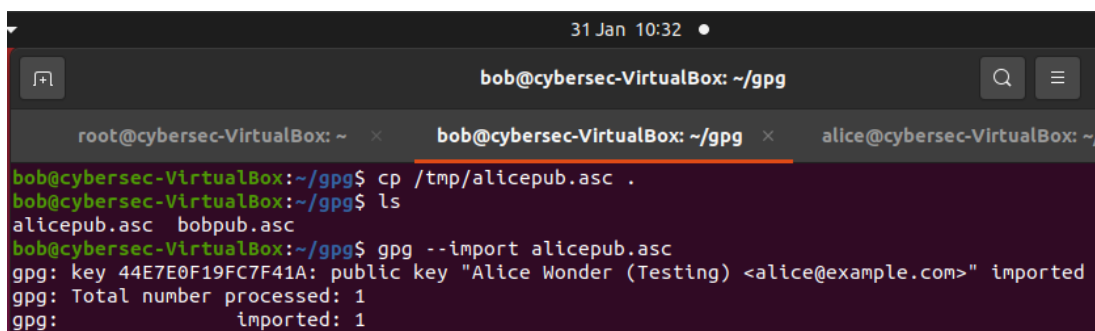


```
31 Jan 10:31 ●
alice@cybersec-VirtualBox: ~/gpg
root@cybersec-VirtualBox: ~ x bob@cybersec-VirtualBox: ~/gpg x alice@cybersec-V
alice@cybersec-VirtualBox:~/gpg$ cp alicepub.asc /tmp
```

Figure 2.8: Copying Alice's public key to `/tmp`.

2.2.3 Importing and signing public keys

Bob can copy and import Alice's public key from `/tmp`.

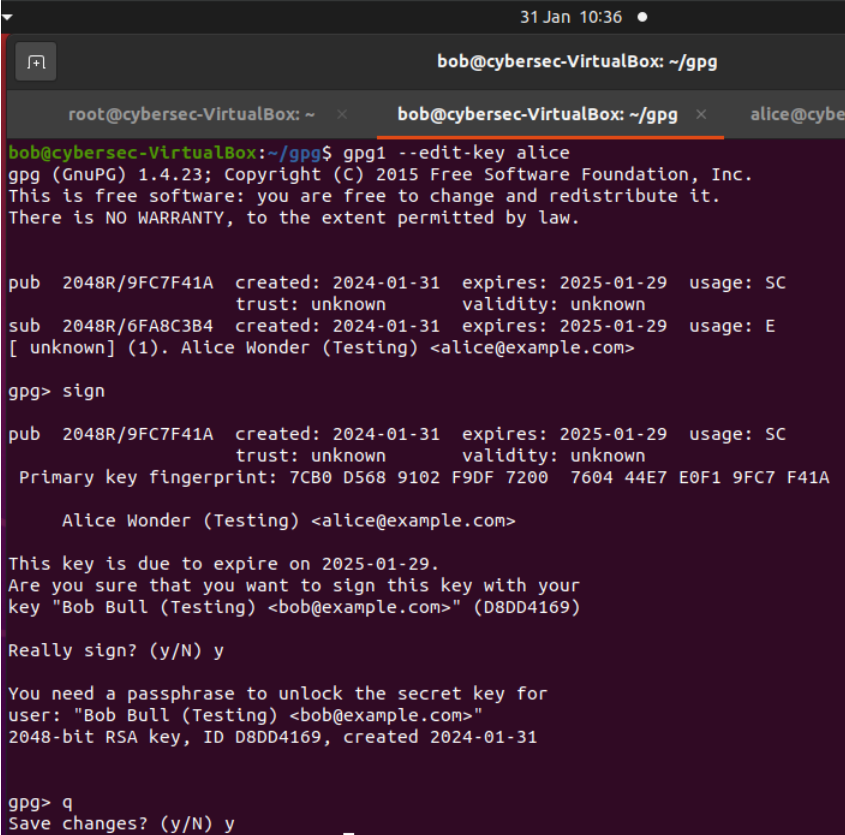


```
31 Jan 10:32 ●
bob@cybersec-VirtualBox: ~/gpg
root@cybersec-VirtualBox: ~ x bob@cybersec-VirtualBox: ~/gpg x alice@cybersec-VirtualBox: ~
bob@cybersec-VirtualBox:~/gpg$ cp /tmp/alicepub.asc .
bob@cybersec-VirtualBox:~/gpg$ ls
alicepub.asc  bobpub.asc
bob@cybersec-VirtualBox:~/gpg$ gpg --import alicepub.asc
gpg: key 44E7E0F19FC7F41A: public key "Alice Wonder (Testing) <alice@example.com>" imported
gpg: Total number processed: 1
gpg: imported: 1
```

Figure 2.9: Importing Alice's public key as Bob.

²The file can be read using "cat alicepub.asc", but it is a 2048-bit key, so it would completely fill the terminal window.

Bob can then **sign** this key, verifying that he trusts that this key does belong to Alice. This is done by editing Alice's key as Bob and signing it.



```
31 Jan 10:36
bob@cybersec-VirtualBox: ~/gpg
root@cybersec-VirtualBox: ~ x bob@cybersec-VirtualBox: ~/gpg x alice@cybe
bob@cybersec-VirtualBox:~/gpg$ gpg1 --edit-key alice
gpg (GnuPG) 1.4.23; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

pub 2048R/9FC7F41A created: 2024-01-31 expires: 2025-01-29 usage: SC
trust: unknown validity: unknown
sub 2048R/6FA8C3B4 created: 2024-01-31 expires: 2025-01-29 usage: E
[ unknown] (1). Alice Wonder (Testing) <alice@example.com>

gpg> sign

pub 2048R/9FC7F41A created: 2024-01-31 expires: 2025-01-29 usage: SC
trust: unknown validity: unknown
Primary key fingerprint: 7CB0 D568 9102 F9DF 7200 7604 44E7 E0F1 9FC7 F41A

Alice Wonder (Testing) <alice@example.com>

This key is due to expire on 2025-01-29.
Are you sure that you want to sign this key with your
key "Bob Bull (Testing) <bob@example.com>" (D8DD4169)

Really sign? (y/N) y

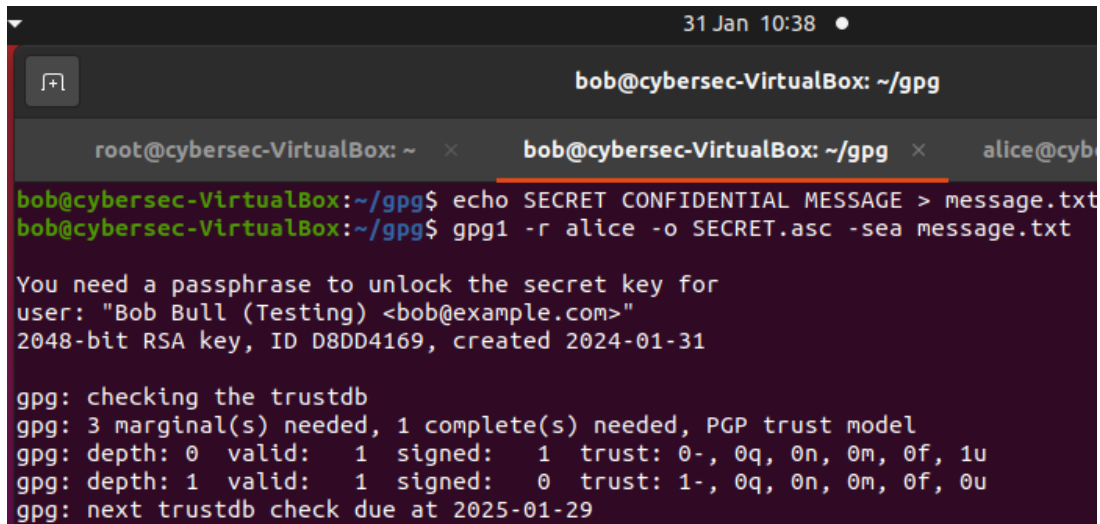
You need a passphrase to unlock the secret key for
user: "Bob Bull (Testing) <bob@example.com>"
2048-bit RSA key, ID D8DD4169, created 2024-01-31

gpg> q
Save changes? (y/N) y
```

Figure 2.10: Bob signing Alice's public key.

2.2.4 Encrypting and decrypting data

Now that Alice and Bob have their key-pairs generated, they can transfer asymmetrically encrypted data to each other. This was tested by making a file, encrypting it using Alice's public key, and copying it to the /tmp directory.



```
31 Jan 10:38
bob@cybersec-VirtualBox: ~/gpg
root@cybersec-VirtualBox: ~ x bob@cybersec-VirtualBox: ~/gpg x alice@cybersec-VirtualBox: ~/gpg
bob@cybersec-VirtualBox:~/gpg$ echo SECRET CONFIDENTIAL MESSAGE > message.txt
bob@cybersec-VirtualBox:~/gpg$ gpg1 -r alice -o SECRET.asc -sea message.txt

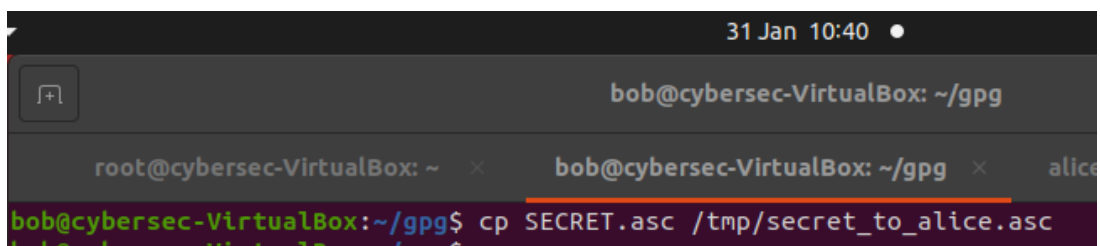
You need a passphrase to unlock the secret key for
user: "Bob Bull (Testing) <bob@example.com>"
2048-bit RSA key, ID D8DD4169, created 2024-01-31

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid: 1  signed: 1  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: depth: 1  valid: 1  signed: 0  trust: 1-, 0q, 0n, 0m, 0f, 0u
gpg: next trustdb check due at 2025-01-29
```

Figure 2.11: Making a file and encrypting it using Alice's public key.

This command can be broken down to its components:

- `-r alice` - Uses Alice's public key for encryption.
- `-o SECRET.asc` - Outputs the encrypted data to SECRET.asc.
- `-sea message.txt` - Sign and encrypt the contents of message.txt in ASCII format.



```
31 Jan 10:40
bob@cybersec-VirtualBox: ~/gpg
root@cybersec-VirtualBox: ~ x bob@cybersec-VirtualBox: ~/gpg x alice@cybersec-VirtualBox: ~/gpg
bob@cybersec-VirtualBox:~/gpg$ cp SECRET.asc /tmp/secret_to_alice.asc
```

Figure 2.12: Copying the encrypted file to /tmp with the name "secret_to_alice.asc".

Alice can decrypt the file to "message.txt", where it can be read in human-legible form.

```
31 Jan 10:45 ●
alice@cybersec-VirtualBox: ~/gpg
root@cybersec-VirtualBox: ~ x bob@cybersec-VirtualBox: ~/gpg x alice@cybersec-Vi
alice@cybersec-VirtualBox:~/gpg$ gpg1 -o message.txt -d /tmp/secret_to_alice.asc
You need a passphrase to unlock the secret key for
user: "Alice Wonder (Testing) <alice@example.com>"
2048-bit RSA key, ID 6FA8C3B4, created 2024-01-31 (main key ID 9FC7F41A)

gpg: encrypted with 2048-bit RSA key, ID 6FA8C3B4, created 2024-01-31
      "Alice Wonder (Testing) <alice@example.com>"
gpg: Signature made Wed 31 Jan 2024 10:38:43 GMT using RSA key ID D8DD4169
gpg: Good signature from "Bob Bull (Testing) <bob@example.com>"
alice@cybersec-VirtualBox:~/gpg$ ls
alicepub.asc bobpub.asc message.txt
alice@cybersec-VirtualBox:~/gpg$ cat message.txt
SECRET CONFIDENTIAL MESSAGE
```

Figure 2.13: Decrypting the encrypted message and reading it.

Discretionary Access Control

This lab explored the use of Discretionary Access Control methods on a Linux system, which allows the owner of an object to assign the level of access that other entities will have to said object.

5.1 Creating test users and groups

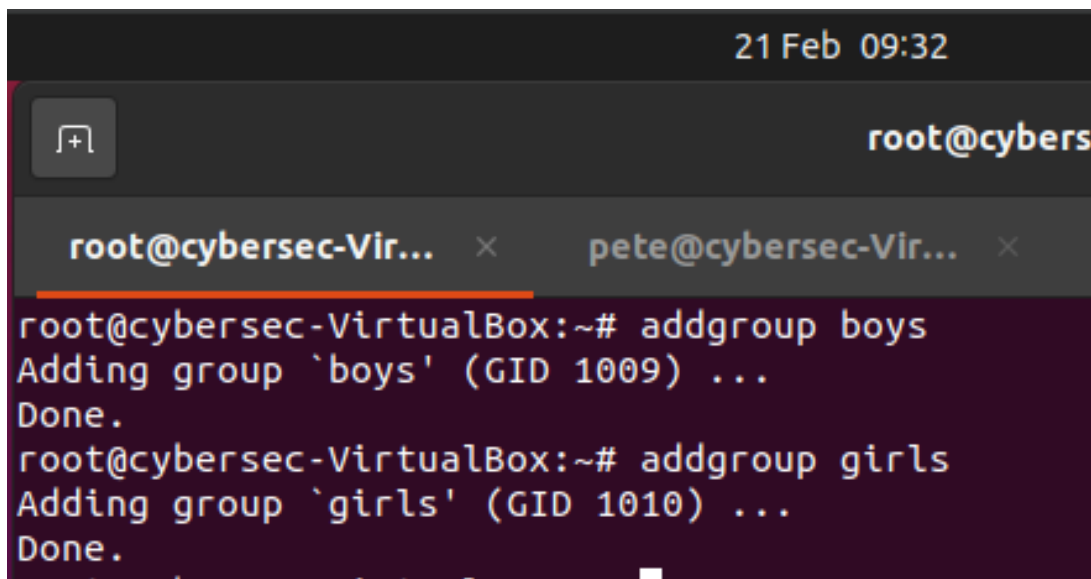
Note

Creating users was already showcased and explained in further detail in Lab 2, specifically in figures 2.1, 2.2 and 2.4 of section 2.1.

For this lab, three test users "Pete", "Ali" and "Mary" were added to the system. Pete and Ali were assigned to the "Boys" group, whereas Mary was assigned to the "Girls" group.

5.1.1 Creating groups

With sudo privileges, additional groups can be added to the system.

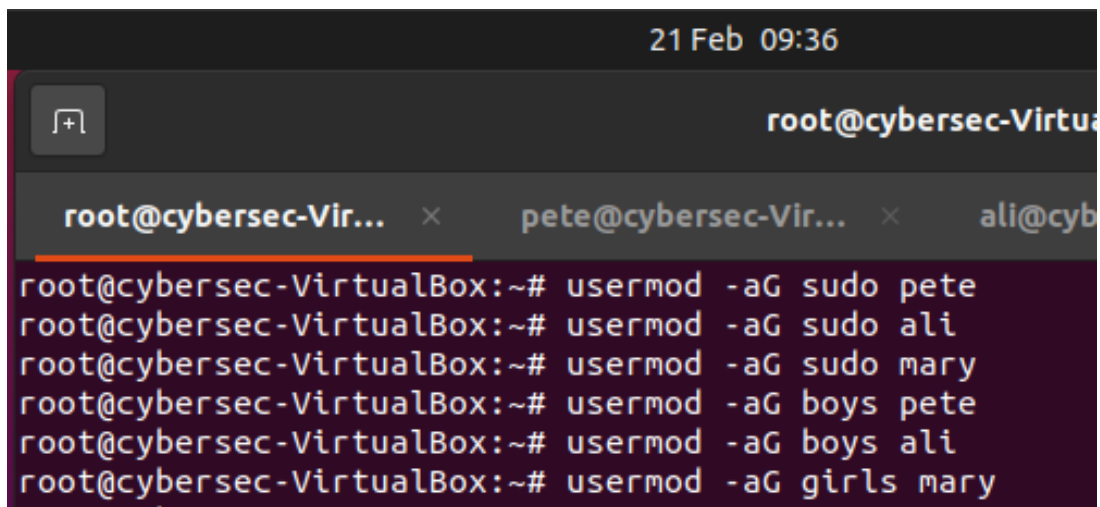
A screenshot of a terminal window with a dark background. At the top right, the date and time '21 Feb 09:32' are displayed. Below the title bar, there are two tabs: 'root@cybersec-Vir...' and 'pete@cybersec-Vir...'. The main terminal area shows the following commands and output:

```
root@cybersec-VirtualBox:~# addgroup boys
Adding group `boys' (GID 1009) ...
Done.
root@cybersec-VirtualBox:~# addgroup girls
Adding group `girls' (GID 1010) ...
Done.
```

Figure 5.1: Making the "boys" and "girls" groups.

5.1.2 Adding users to groups

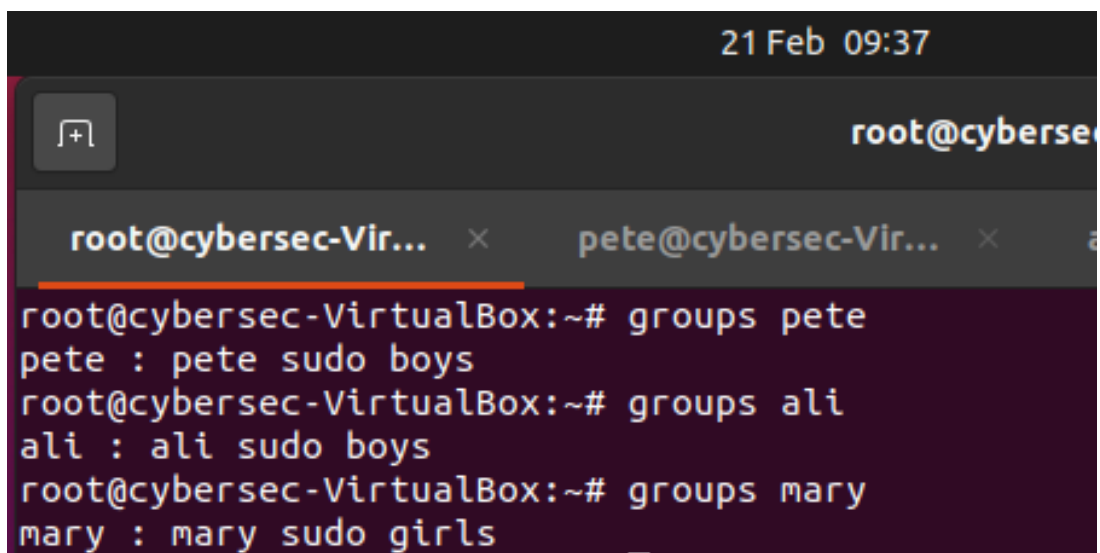
The new users were added to the groups mentioned above as well as the sudo group.



```
21 Feb 09:36
root@cybersec-Virtua
root@cybersec-Vir... x pete@cybersec-Vir... x ali@cyb
root@cybersec-VirtualBox:~# usermod -aG sudo pete
root@cybersec-VirtualBox:~# usermod -aG sudo ali
root@cybersec-VirtualBox:~# usermod -aG sudo mary
root@cybersec-VirtualBox:~# usermod -aG boys pete
root@cybersec-VirtualBox:~# usermod -aG boys ali
root@cybersec-VirtualBox:~# usermod -aG girls mary
```

Figure 5.2: Adding the users to sudo and their respective groups.

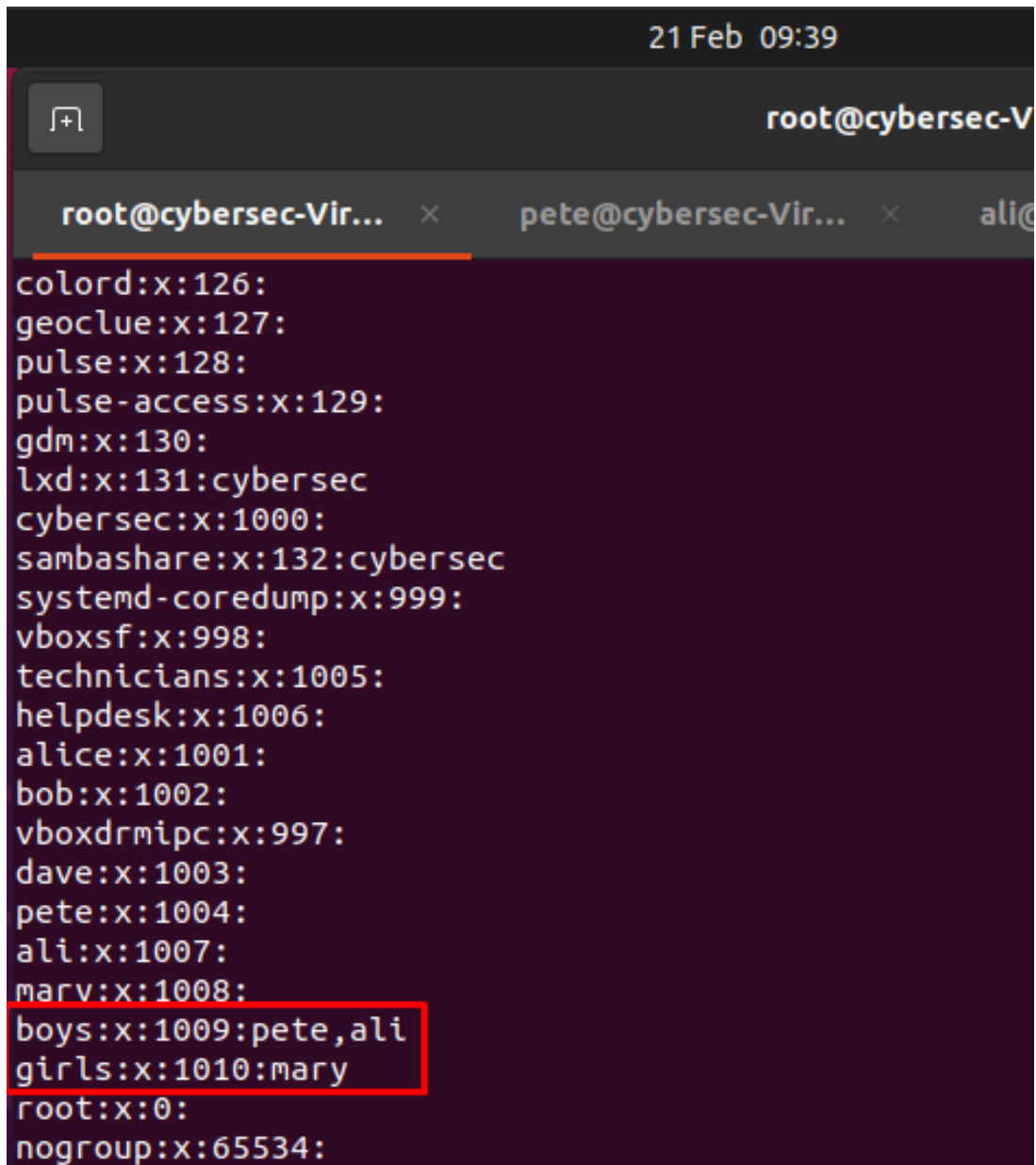
We can verify which groups a given user is in by using the "groups" command.



```
21 Feb 09:37
root@cybersec
root@cybersec-Vir... x pete@cybersec-Vir... x a
root@cybersec-VirtualBox:~# groups pete
pete : pete sudo boys
root@cybersec-VirtualBox:~# groups ali
ali : ali sudo boys
root@cybersec-VirtualBox:~# groups mary
mary : mary sudo girls
```

Figure 5.3: Verifying that the users were added to the groups.

This can also be checked by viewing all groups on the system via "getent groups".



```
21 Feb 09:39
root@cybersec-V...
root@cybersec-Vir... x pete@cybersec-Vir... x ali@
colord:x:126:
geoclue:x:127:
pulse:x:128:
pulse-access:x:129:
gdm:x:130:
lxd:x:131:cybersec
cybersec:x:1000:
sambashare:x:132:cybersec
systemd-coredump:x:999:
vboxsf:x:998:
technicians:x:1005:
helpdesk:x:1006:
alice:x:1001:
bob:x:1002:
vboxdrmipc:x:997:
dave:x:1003:
pete:x:1004:
ali:x:1007:
marv:x:1008:
boys:x:1009:pete,ali
girls:x:1010:mary
root:x:0:
nogroup:x:65534:
```

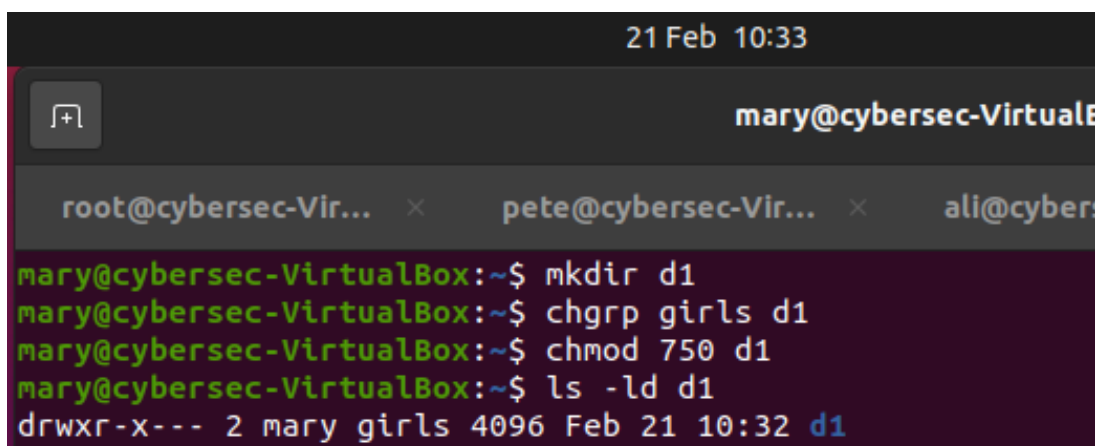
Figure 5.4: Seeing all groups (Boys and Girls are highlighted).

5.2 Using chmod and chgrp to assign permissions

Chmod changes the permissions for a given file or directory. It can change permissions for reading, writing and executing files for the owner of the file, a group of users and other users¹. I used [this help page](#) (*Unix File Permissions* n.d.) to assist in my learning of these commands as well as access control on UNIX systems.

5.2.1 Restricting directory access

For the purposes of testing, a directory called D1 was added to Mary's home. This directory was associated with the girls group via chgrp, and modified with a chmod command so that other users cannot access the directory whatsoever, but Mary and users of the girls group can read and execute from it.



```
21 Feb 10:33
mary@cybersec-Virtua...
root@cybersec-Vir... x pete@cybersec-Vir... x ali@cyber...
mary@cybersec-VirtualBox:~$ mkdir d1
mary@cybersec-VirtualBox:~$ chgrp girls d1
mary@cybersec-VirtualBox:~$ chmod 750 d1
mary@cybersec-VirtualBox:~$ ls -ld d1
drwxr-x--- 2 mary girls 4096 Feb 21 10:32 d1
```

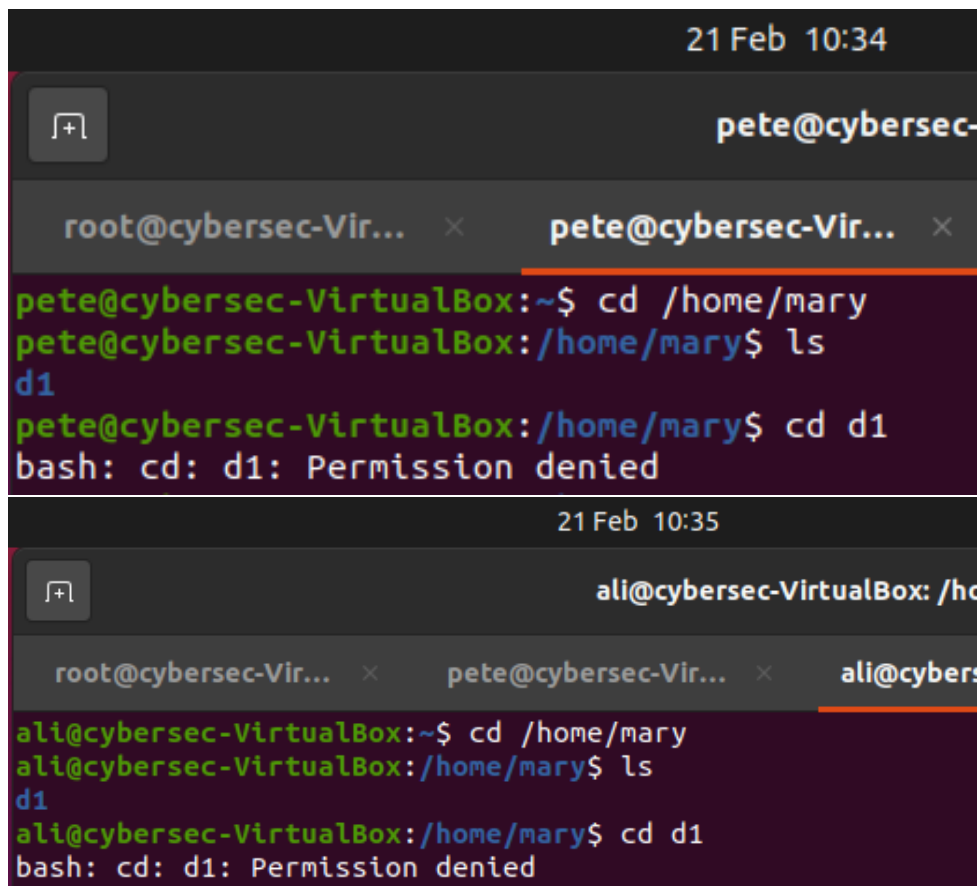
Figure 5.5: Creating D1 and modifying its permissions.

By using the command "ls -ld", the permissions of the directory are outputted. The returned message reveals that:

- The directory owner (Mary) has **R**ead, **W**rite and **eX**ecute permissions.
- Group members can **R**ead and **eX**ecute.
- Others can only **eX**ecute.

This can be tested using Ali and Pete's accounts, which are not members of the girls group, meaning they are "others".

¹Defined as users that aren't the owner or in an associated group with permissions.



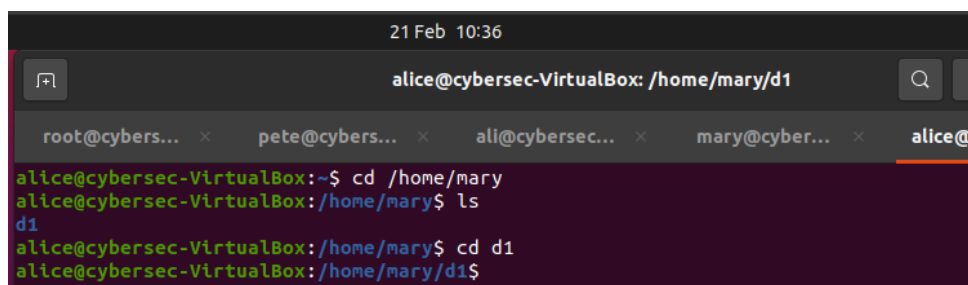
The figure consists of two terminal window screenshots. The top screenshot, timestamped 21 Feb 10:34, shows a terminal for user 'pete@cybersec-VirtualBox'. The user navigates to /home/mary and lists the contents, seeing 'd1'. When they attempt to 'cd d1', they receive the error 'bash: cd: d1: Permission denied'. The bottom screenshot, timestamped 21 Feb 10:35, shows a terminal for user 'ali@cybersec-VirtualBox'. Ali performs the same steps: navigating to /home/mary, listing contents to see 'd1', and attempting 'cd d1', which also results in 'bash: cd: d1: Permission denied'.

Figure 5.6: Attempting to access D1 as Pete and Ali.

Note

An issue arose here that I didn't have another user in the girls group to test access with. To fix this, I went back and added the existing Alice account from Lab 2 to the girls group with *sudo usermod -aG girls alice*.

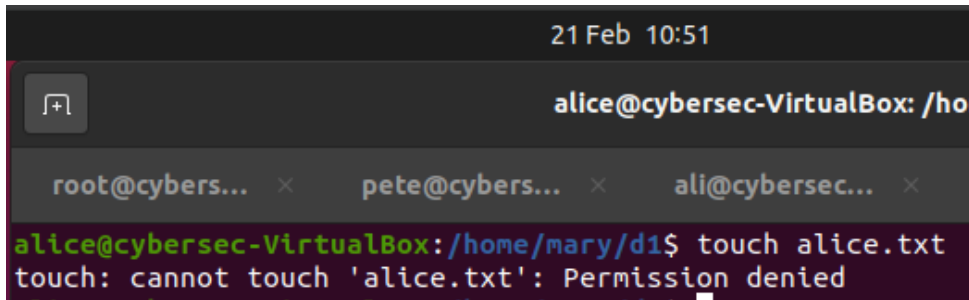
Using another account in the girls group, we can test if other girls can access the directory, which succeeds.



The screenshot shows a terminal window for user 'alice@cybersec-VirtualBox' at 21 Feb 10:36. The terminal title bar shows the current path as '/home/mary/d1'. The user navigates to /home/mary, lists contents to see 'd1', and then successfully executes 'cd d1', with the prompt changing to 'alice@cybersec-VirtualBox:/home/mary/d1\$'.

Figure 5.7: Successfully accessing D1 as Alice.

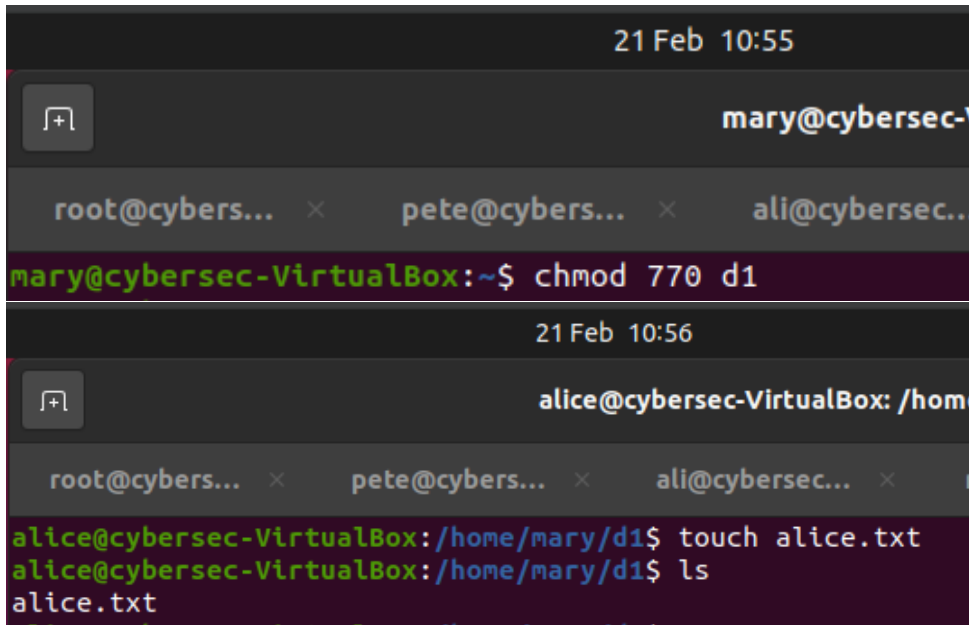
Alice is permitted to read the d1 directory and execute files within it, but she cannot write to it, as intended.



```
21 Feb 10:51
alice@cybersec-VirtualBox: /home/mary/d1$ touch alice.txt
touch: cannot touch 'alice.txt': Permission denied
```

Figure 5.8: Failing to write to D1 as Alice.

To test this further, the permissions can then be modified² again to allow girls to write files, which will then allow Alice to make the file.



```
21 Feb 10:55
mary@cybersec-VirtualBox: ~$ chmod 770 d1

21 Feb 10:56
alice@cybersec-VirtualBox: /home/mary/d1$ touch alice.txt
alice@cybersec-VirtualBox: /home/mary/d1$ ls
alice.txt
```

Figure 5.9: Modifying the permissions of D1, allowing Alice to write the file.

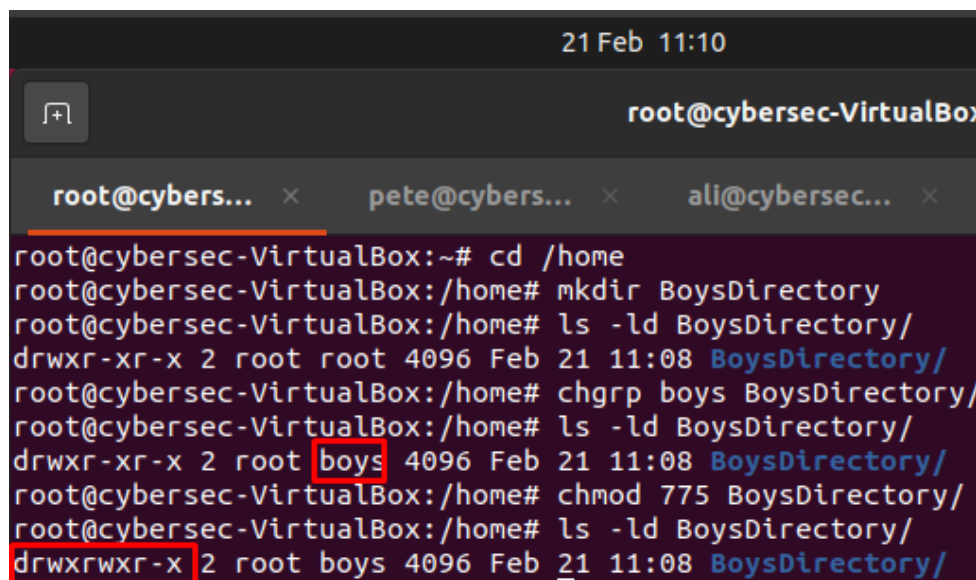
²770 is "rwxrwx—", which correlates to the file owner and members of the group having read, write and execute permissions, but other users have none.

5.2.2 Chgrp and chown

Note

I used different directory names (*BoysDirectory* instead of *Photos*), but I have still demonstrated all exercises from this lab.

Chown assigns a file or directory's ownership to a specific user. For this example, we will create a directory in the shared /home folder and assign group ownership to Boys via chgrp, and using chmod to allow all Boys all permissions, and all other users read & execute permissions.

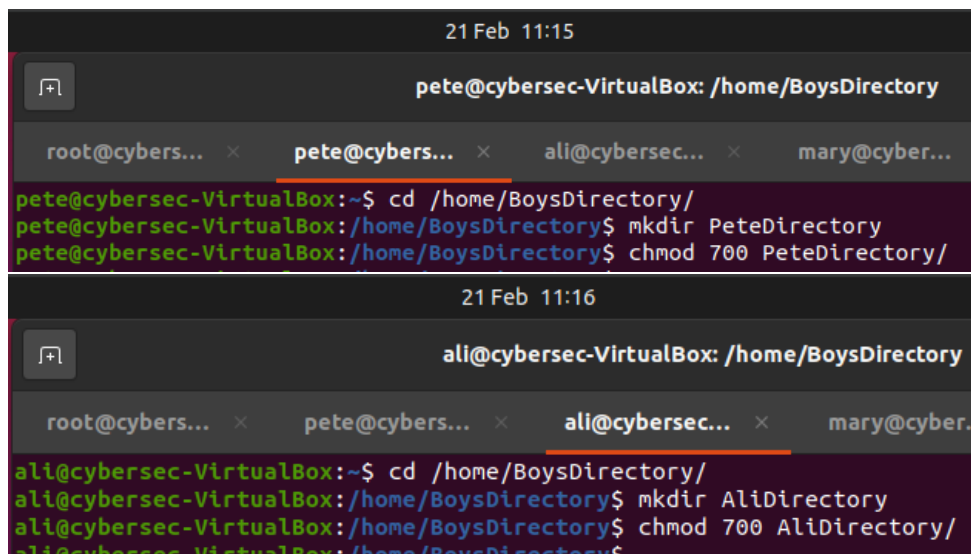


```
21 Feb 11:10
root@cybersec-VirtualBox
root@cybers... x  pete@cybers... x  ali@cybersec... x
root@cybersec-VirtualBox:~# cd /home
root@cybersec-VirtualBox:/home# mkdir BoysDirectory
root@cybersec-VirtualBox:/home# ls -ld BoysDirectory/
drwxr-xr-x 2 root root 4096 Feb 21 11:08 BoysDirectory/
root@cybersec-VirtualBox:/home# chgrp boys BoysDirectory/
root@cybersec-VirtualBox:/home# ls -ld BoysDirectory/
drwxr-xr-x 2 root boys 4096 Feb 21 11:08 BoysDirectory/
root@cybersec-VirtualBox:/home# chmod 775 BoysDirectory/
root@cybersec-VirtualBox:/home# ls -ld BoysDirectory/
drwxrwxr-x 2 root boys 4096 Feb 21 11:08 BoysDirectory/
```

Figure 5.10: Making BoysDirectory and giving group ownership to Boys.

This new directory can be accessed by all users, but only written to by boys. We can now test chown by making two subdirectories within BoysDirectory, where one will be owned by Pete, and one by Ali. Both users also modify the permissions of their own directories to only be accessible by them.³

³700 is "rwx—", which means only the owner may read, write and execute.



21 Feb 11:15

```
pete@cybersec-VirtualBox: /home/BoysDirectory
```

root@cybers... x pete@cybers... x ali@cybersec... x mary@cyber...

```
pete@cybersec-VirtualBox:~$ cd /home/BoysDirectory/
pete@cybersec-VirtualBox:/home/BoysDirectory$ mkdir PeteDirectory
pete@cybersec-VirtualBox:/home/BoysDirectory$ chmod 700 PeteDirectory/
```

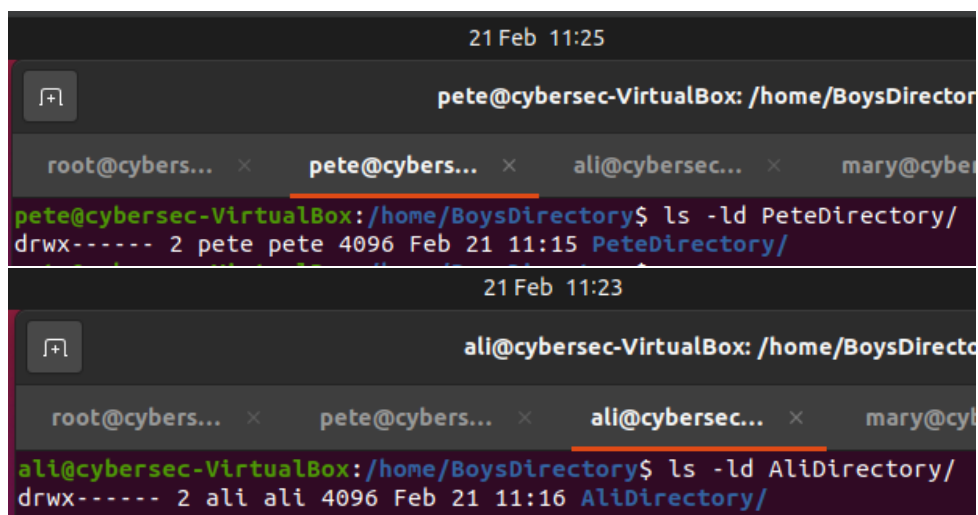
21 Feb 11:16

```
ali@cybersec-VirtualBox: /home/BoysDirectory
```

root@cybers... x pete@cybers... x ali@cybersec... x mary@cyber..

```
ali@cybersec-VirtualBox:~$ cd /home/BoysDirectory/
ali@cybersec-VirtualBox:/home/BoysDirectory$ mkdir AliDirectory
ali@cybersec-VirtualBox:/home/BoysDirectory$ chmod 700 AliDirectory/
```

Figure 5.11: Creating and modifying each user's directories and access permissions.



21 Feb 11:25

```
pete@cybersec-VirtualBox: /home/BoysDirector
```

root@cybers... x pete@cybers... x ali@cybersec... x mary@cyber

```
pete@cybersec-VirtualBox:/home/BoysDirectory$ ls -ld PeteDirectory/
drwx----- 2 pete pete 4096 Feb 21 11:15 PeteDirectory/
```

21 Feb 11:23

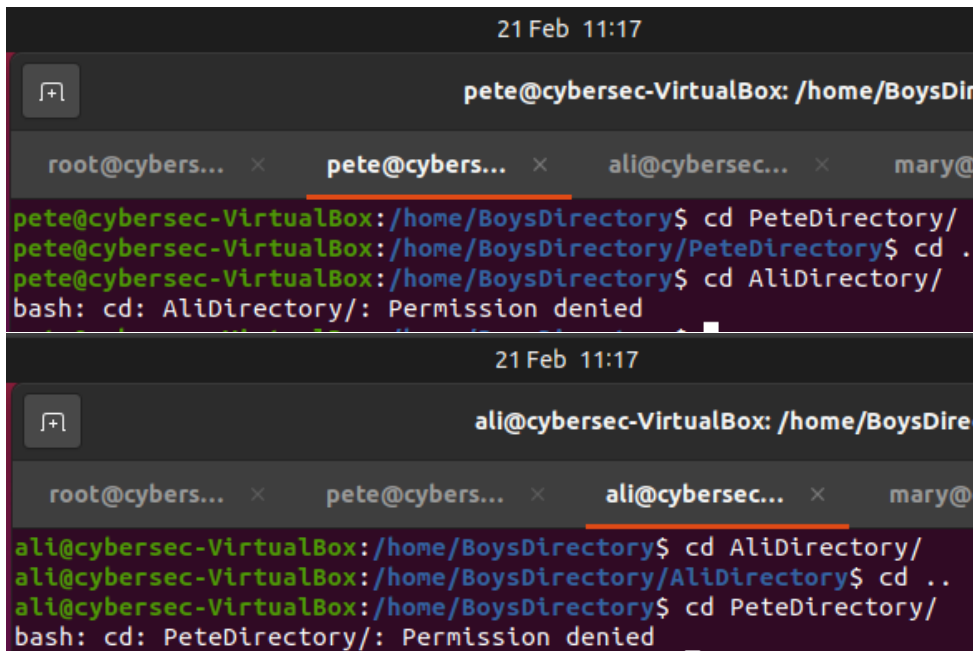
```
ali@cybersec-VirtualBox: /home/BoysDirecto
```

root@cybers... x pete@cybers... x ali@cybersec... x mary@cyl

```
ali@cybersec-VirtualBox:/home/BoysDirectory$ ls -ld AliDirectory/
drwx----- 2 ali ali 4096 Feb 21 11:16 AliDirectory/
```

Figure 5.12: Viewing the permissions of Pete and Ali's directories.

We can then prove that only the owners of the directories may access them by first accessing their own directory, but then attempting to access the other user's directory:



```
21 Feb 11:17
pete@cybersec-VirtualBox: /home/BoysDir...

root@cybers... x pete@cybers... x ali@cybersec... x mary@...

pete@cybersec-VirtualBox:/home/BoysDirectory$ cd PeteDirectory/
pete@cybersec-VirtualBox:/home/BoysDirectory/PeteDirectory$ cd .
pete@cybersec-VirtualBox:/home/BoysDirectory$ cd AliDirectory/
bash: cd: AliDirectory/: Permission denied

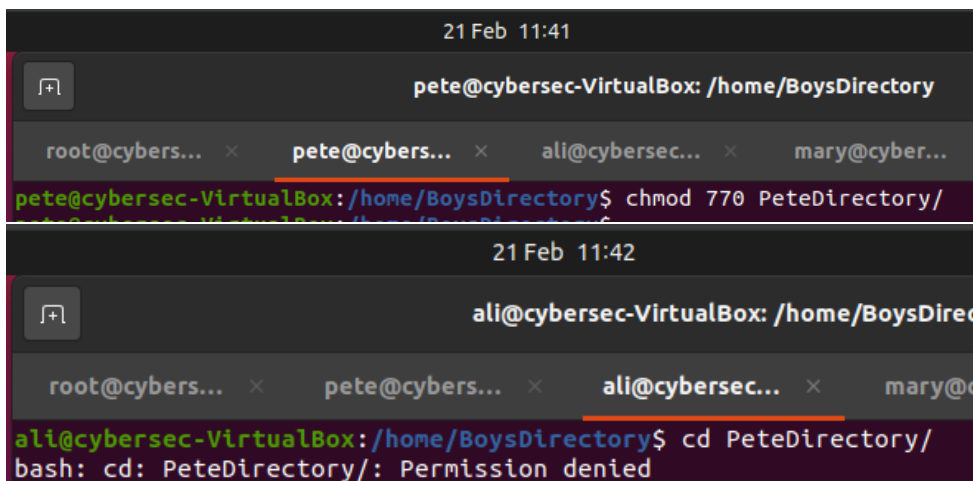
21 Feb 11:17
ali@cybersec-VirtualBox: /home/BoysDire...

root@cybers... x pete@cybers... x ali@cybersec... x mary@...

ali@cybersec-VirtualBox:/home/BoysDirectory$ cd AliDirectory/
ali@cybersec-VirtualBox:/home/BoysDirectory/AliDirectory$ cd ..
ali@cybersec-VirtualBox:/home/BoysDirectory$ cd PeteDirectory/
bash: cd: PeteDirectory/: Permission denied
```

Figure 5.13: Successfully accessing their own directory, but failing to access the other because the user isn't the owner.

An important distinction to be made here is that these subdirectories are owned by Pete and Ali respectively. They do **not** inherit the boys group ownership by default, meaning that commands to change group permissions will be ineffective for other boys, as everyone who is not the owner is considered "other" unless `chgrp` is used, as seen in Figure 5.13.



```
21 Feb 11:41
pete@cybersec-VirtualBox: /home/BoysDirectory

root@cybers... x pete@cybers... x ali@cybersec... x mary@cyber...

pete@cybersec-VirtualBox:/home/BoysDirectory$ chmod 770 PeteDirectory/

21 Feb 11:42
ali@cybersec-VirtualBox: /home/BoysDirec...

root@cybers... x pete@cybers... x ali@cybersec... x mary@c...

ali@cybersec-VirtualBox:/home/BoysDirectory$ cd PeteDirectory/
bash: cd: PeteDirectory/: Permission denied
```

Figure 5.14: Giving group RWX access to PeteDirectory

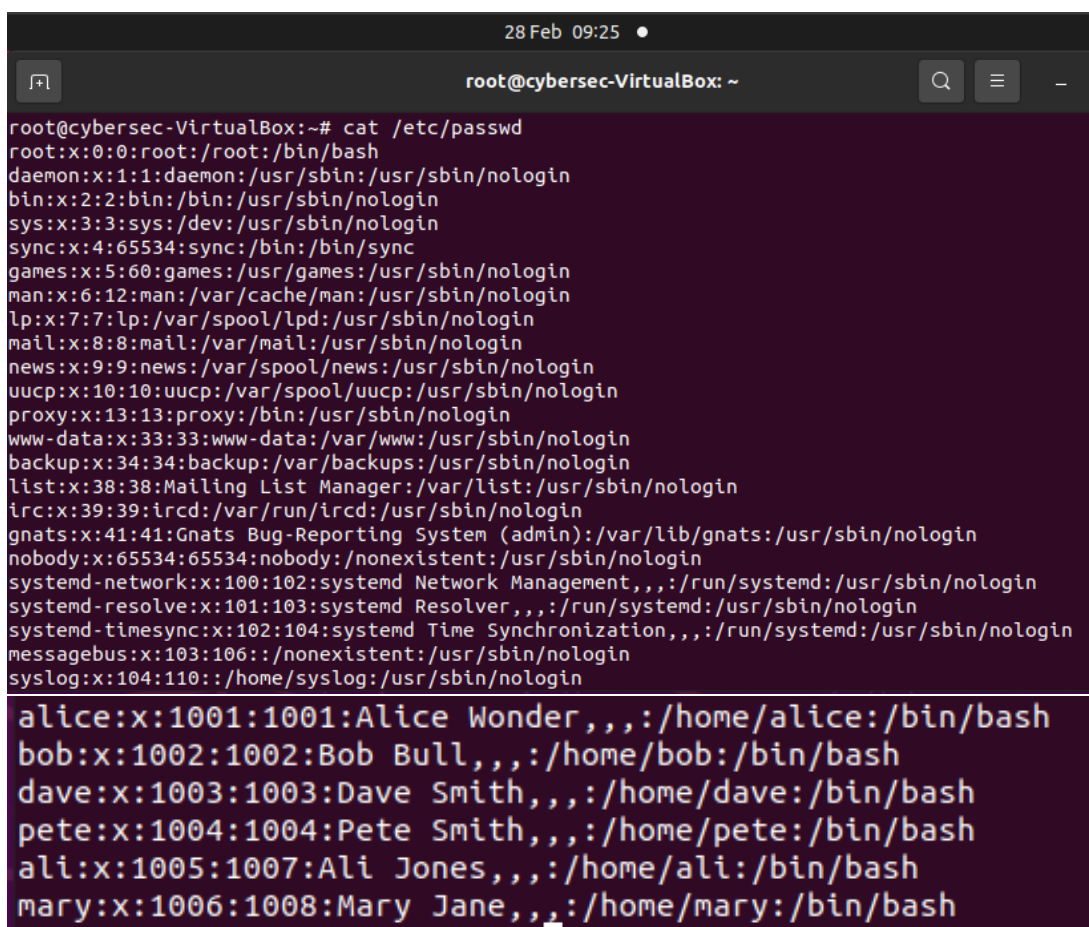
Ali still can't access the directory because he is not part of the "Pete" group, but he (and any other users) would be able to use permissions given to "others".

Password Cracking

In this lab, a simple brute-force attack program written in C was used to crack a hashed account password.

6.1 Linux password storage

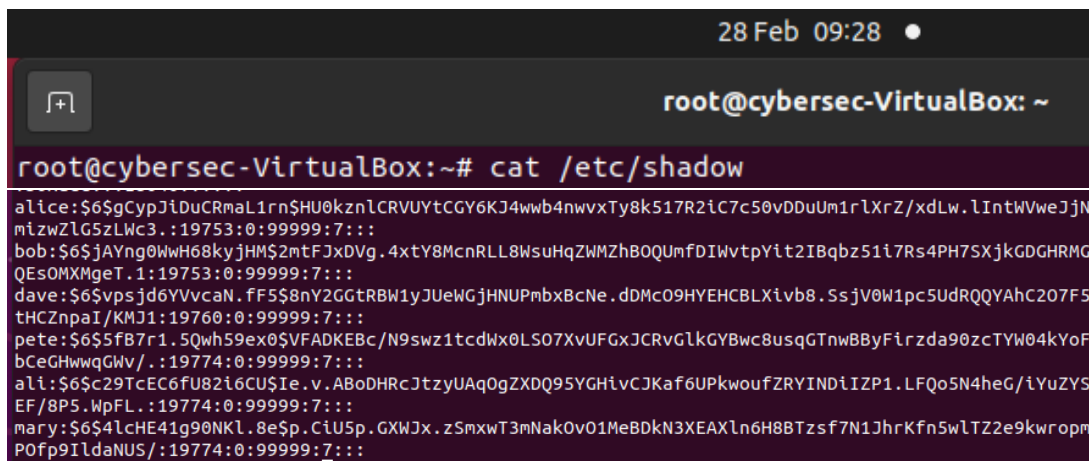
Linux systems store user account details across two files, */etc/passwd* and */etc/shadow*. I learned information about this from [this site](#) (Gite, 2024), which states that the public unencrypted ASCII file */etc/passwd* contains a line for each user on the system, with publicly accessible information such as username, user ID and group ID, whereas the encrypted */etc/shadow* file contains the encrypted passwords of users on the system.

A terminal window titled 'root@cybersec-VirtualBox: ~' with a search icon and a menu icon. The terminal shows the command 'cat /etc/passwd' and its output. The output lists system users (daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, nobody, systemd-network, systemd-resolve, systemd-timesync, messagebus, syslog) and regular users (alice, bob, dave, pete, ali, mary) in the format 'username:x:UID:GID:full_name:home_directory:shell'.

```
root@cybersec-VirtualBox:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:/nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:/home/syslog:/usr/sbin/nologin

alice:x:1001:1001:Alice Wonder,,,:/home/alice:/bin/bash
bob:x:1002:1002:Bob Bull,,,:/home/bob:/bin/bash
dave:x:1003:1003:Dave Smith,,,:/home/dave:/bin/bash
pete:x:1004:1004:Pete Smith,,,:/home/pete:/bin/bash
ali:x:1005:1007:Ali Jones,,,:/home/ali:/bin/bash
mary:x:1006:1008:Mary Jane,,,:/home/mary:/bin/bash
```

Figure 6.1: Some of the contents of */etc/passwd*, with the created users from earlier labs.



```

28 Feb 09:28 ●
root@cybersec-VirtualBox: ~
root@cybersec-VirtualBox:~# cat /etc/shadow
alice:$6$gCypJiDuCRma1rn$HU0kzn1CRVUYtCGY6KJ4wwb4nwvxTy8k517R21c7c50vDDuUm1rLXrZ/xdLw.lIntWVweJJN
mizwZLG5zLwc3.:19753:0:99999:7:::
bob:$6$jAYng0WwH68kyjHM$2mtFJxDVg.4xtY8McnRLL8WsuHqZWMZhBOQumfDIWvtpYit2IBqbz51i7Rs4PH7SXjkGDGHRMG
QESOMXMgeT.1:19753:0:99999:7:::
dave:$6$ypsjd6YVvcaN.fF5$8nY2GGtRBW1yJUeWgJHNUPmbxBcNe.dDMc09HYEHCBXLxib8.SsjV0W1pc5UDRQQYAhC207F5
tHCZnpaI/KMJ1:19760:0:99999:7:::
pete:$6$5fB7r1.5Qwh59ex0$VFADKEBc/N9swz1tcdWx0LS07XvUFGxJCRvGlkGYBwc8usqGTnwBBYfirzda90zcTYW04kyoF
bCeGHwwqGWv/.:19774:0:99999:7:::
ali:$6$c29TcEC6fU82i6CU$ie.v.ABoDHrcJtzYUAQOgZXDQ95YGHlvcJKaf6UPkwoufZRYINDiIZP1.LFQo5N4heG/iYuZYS
EF/8P5.WpFL.:19774:0:99999:7:::
mary:$6$4lcHE41g90NKL.8e$P.CiU5p.GXWJx.zSmxwT3mNakOv01MeBDkN3XEAXln6H8BTzsf7N1JhrKfn5wLTZ2e9kwropm
POfp9IldaNUS/:19774:0:99999:7:::

```

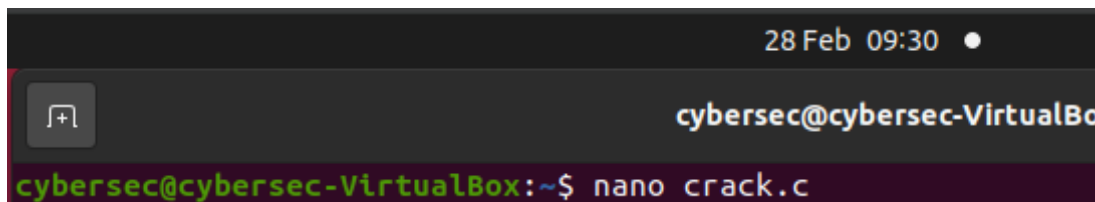
Figure 6.2: Some of the contents of `/etc/shadow`, with the created users from earlier labs.

6.2 crack.c

The provided code in `crack.c` is a small program that performs a dictionary attack, cracking hashed passwords by hashing each word in the dictionary, adding the salt and comparing the product to the hashed password. The Ubuntu dictionary is located in `/usr/share/dict/words`.

6.2.1 Importing and compilation

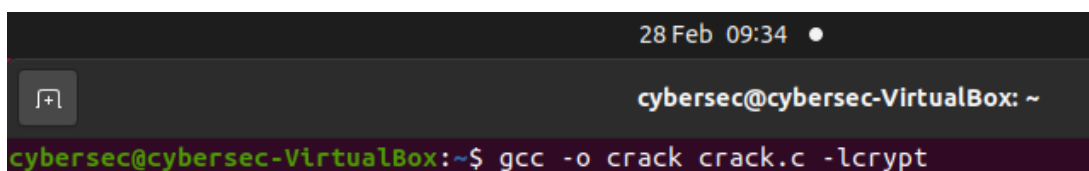
First, this code must be ported into the Ubuntu VM using "nano `crack.c`", and pasting the code from Moodle.



```

28 Feb 09:30 ●
cybersec@cybersec-VirtualBo
cybersec@cybersec-VirtualBox:~$ nano crack.c

```

Figure 6.3: Porting `crack.c` into the VM.


```

28 Feb 09:34 ●
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ gcc -o crack crack.c -lcrypt

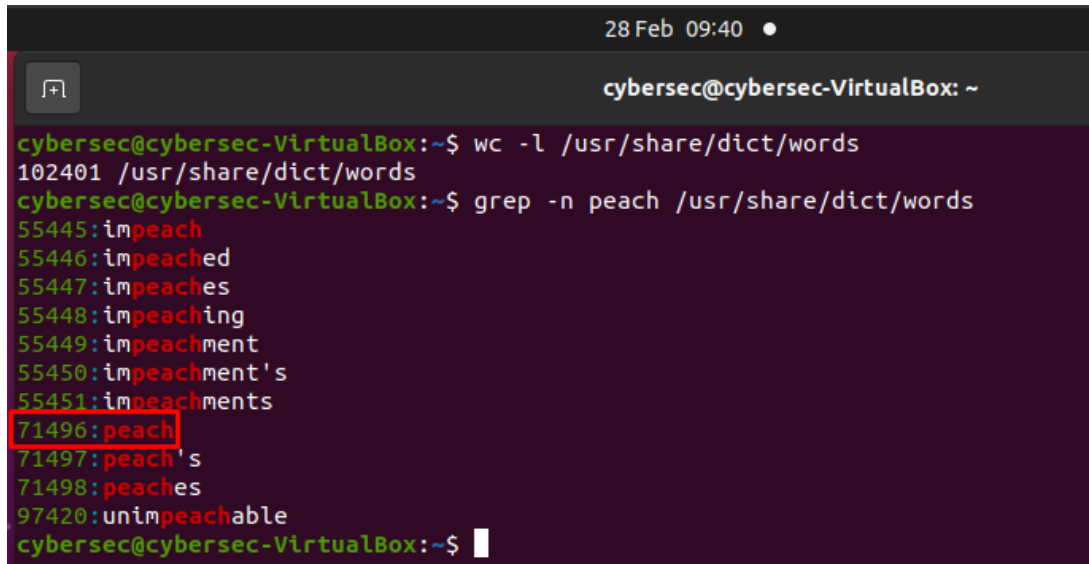
```

Figure 6.4: Compiling `crack.c`.

The `-lcrypt` argument supplies the Linux `crypt` library when compiling, allowing the `crypt()` function to be used more securely.

6.2.2 Creating a test user

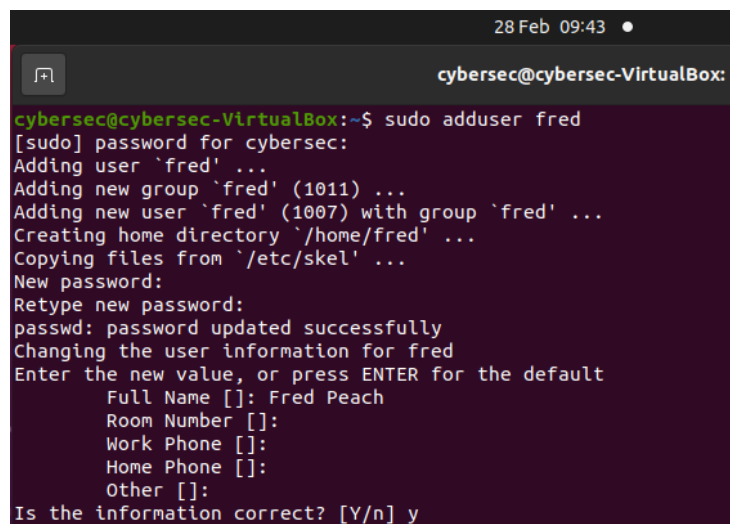
To use the program, it will be necessary to create a new user, whose password can be found in the dictionary. For this, the user 'fred' will be created, and his password will be 'peach'. We can see if 'peach' appears in the dictionary, as well as the overall dictionary word count.



```
28 Feb 09:40 ●
cybersec@cybersec-VirtualBox: ~

cybersec@cybersec-VirtualBox:~$ wc -l /usr/share/dict/words
102401 /usr/share/dict/words
cybersec@cybersec-VirtualBox:~$ grep -n peach /usr/share/dict/words
55445:impeach
55446:impeached
55447:impeaches
55448:impeaching
55449:impeachment
55450:impeachment's
55451:impeachments
71496:peach
71497:peach's
71498:peaches
97420:unimpeachable
cybersec@cybersec-VirtualBox:~$
```

Figure 6.5: Checking the dictionary for the word 'peach', which is the 71496th entry.

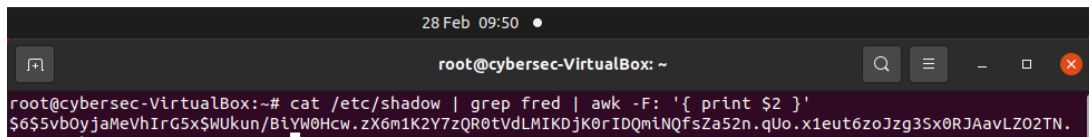


```
28 Feb 09:43 ●
cybersec@cybersec-VirtualBox: ~

cybersec@cybersec-VirtualBox:~$ sudo adduser fred
[sudo] password for cybersec:
Adding user `fred' ...
Adding new group `fred' (1011) ...
Adding new user `fred' (1007) with group `fred' ...
Creating home directory `/home/fred' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for fred
Enter the new value, or press ENTER for the default
  Full Name []: Fred Peach
    Room Number []:
    Work Phone []:
    Home Phone []:
      Other []:
Is the information correct? [Y/n] y
```

Figure 6.6: Creating the 'fred' user, with the password 'peach'.

It will then be necessary to get the hashed version of Fred's password, which can be done using "`cat /etc/shadow | grep fred | awk -F: '{ print $2 }'`". This command will read the shadow file, selecting the row starting with 'fred'. Then, it will extract his hash by selecting the second column.



```
28 Feb 09:50 •
root@cybersec-VirtualBox: ~
root@cybersec-VirtualBox:~# cat /etc/shadow | grep fred | awk -F: '{ print $2 }'
$6$5vb0yjaMeVhIrG5x$WUkun/BiYW0Hcw.zX6m1K2Y7zQR0tVdLMIKDJk0rIDQmiNQfsZa52n.qUo.x1eut6zoJzg3Sx0RJAavLZ02TN.
```

Figure 6.7: Viewing fred's hashed password.

6.2.3 Cracking the password

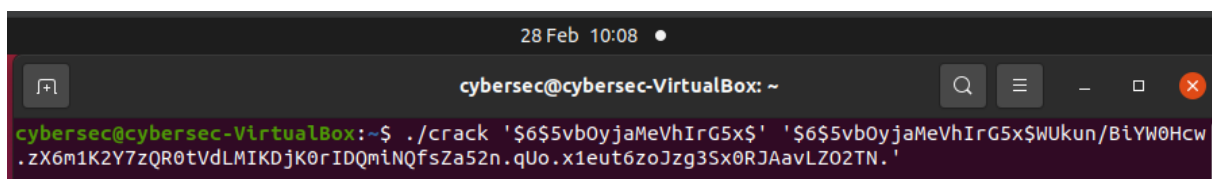
The program takes two arguments, with the first being the salt used on the password and the second being the entire hashed password. It requires the salt as an argument because it will apply the salt to each password it checks. As seen in Figure 6.7, Fred's entire hashed password is

```
$6$5vb0yjaMeVhIrG5x$WUkun/BiYW0Hcw.zX6m1K2Y7zQR0tVdLMIKDJk0rIDQmiNQfsZa52n.qUo.x1eut6zoJzg3Sx0RJAavLZ02TN.
```

We can figure out the salt used on this password by looking at how it starts. The first 20 characters of this password are the salt, noticeable by how they are between two dollar signs. This can be supplied as the first argument for the compiled crack program, and the second argument would be the entire password, including the salt as well. Ultimately, this forms the following command:

```
./crack '$6$5vb0yjaMeVhIrG5x$'
'$6$5vb0yjaMeVhIrG5x$WUkun/BiYW0Hcw.zX6m1K2Y7zQR0tVdLMIKDJk0rIDQmiNQfsZa52n.qUo.x1eut6zoJzg3Sx0RJAavLZ02TN.'
```

It is imperative to use **quotation** marks rather than speech marks, as Linux will otherwise incorrectly interpret the arguments given due to there being dollar signs in the hash, meaning that the crack will be unsuccessful.



```
28 Feb 10:08 •
cybersec@cybersec-VirtualBox: ~
cybersec@cybersec-VirtualBox:~$ ./crack '$6$5vb0yjaMeVhIrG5x$' '$6$5vb0yjaMeVhIrG5x$WUkun/BiYW0Hcw.zX6m1K2Y7zQR0tVdLMIKDJk0rIDQmiNQfsZa52n.qUo.x1eut6zoJzg3Sx0RJAavLZ02TN.'
```

Figure 6.8: Entering the command.


```

28 Feb 10:11 •
cybersec@cybersec-VirtualBox: ~
pwhash: $6$5vb0yjaMeVhIrG5x$WUkun/BiYW0Hcw.zX6m1K2Y7zQR0tVdLMIKDjK0rIDQmInQfsZa52n.qUo.x1eut6zoJzg3Sx0RJAavLZO2TN.
hashguess: $6$5vb0yjaMeVhIrG5x$vo.XwPCwkcA0sFl15WgcKKKPS0JPA4142vCvLFjLyF6/X8sPbQVBah2SxqozxgyL8yMN.SKMFn5CB6P1TdsIz/
word: parries
salt: $6$5vb0yjaMeVhIrG5x$
pwhash: $6$5vb0yjaMeVhIrG5x$WUkun/BiYW0Hcw.zX6m1K2Y7zQR0tVdLMIKDjK0rIDQmInQfsZa52n.qUo.x1eut6zoJzg3Sx0RJAavLZO2TN.
hashguess: $6$5vb0yjaMeVhIrG5x$LzEQBxzLw49JyUr7HwDC70KVyLylppoIUBMFEQUZ4zRoWFS1WkL/6uTI7Dc9mhaIPU2sHI3s69sv2x80HDUR/
word: partisanship's
salt: $6$5vb0yjaMeVhIrG5x$
pwhash: $6$5vb0yjaMeVhIrG5x$WUkun/BiYW0Hcw.zX6m1K2Y7zQR0tVdLMIKDjK0rIDQmInQfsZa52n.qUo.x1eut6zoJzg3Sx0RJAavLZO2TN.
hashguess: $6$5vb0yjaMeVhIrG5x$6Lu9/6uaZ2btS67l44YUImrBlLLZc37A.ELALmbnDBaHJlwwMOXJhVx3qeWH1pr6YX6tV4UjtjRGITGvWzKL.Q0
word: pastern's
salt: $6$5vb0yjaMeVhIrG5x$
pwhash: $6$5vb0yjaMeVhIrG5x$WUkun/BiYW0Hcw.zX6m1K2Y7zQR0tVdLMIKDjK0rIDQmInQfsZa52n.qUo.x1eut6zoJzg3Sx0RJAavLZO2TN.
hashguess: $6$5vb0yjaMeVhIrG5x$0kyCZzVqKZGceuwkoHVMEMv7rZ4I01PkP95Q7c8N8kymcKYlv6pKIN/7n59NIwUHCz.KpImX8UqujcdD54iJp1
word: patience's
salt: $6$5vb0yjaMeVhIrG5x$
pwhash: $6$5vb0yjaMeVhIrG5x$WUkun/BiYW0Hcw.zX6m1K2Y7zQR0tVdLMIKDjK0rIDQmInQfsZa52n.qUo.x1eut6zoJzg3Sx0RJAavLZO2TN.
hashguess: $6$5vb0yjaMeVhIrG5x$lgIS2jCfWZcsnDw0q8Gtcw7sNzY.tUaYic3bFe///19zNvz3jbLwBZ7n1b8HtXWfbU5ki7csQdfNBULAEuu5H/
word: pauperizing
salt: $6$5vb0yjaMeVhIrG5x$
pwhash: $6$5vb0yjaMeVhIrG5x$WUkun/BiYW0Hcw.zX6m1K2Y7zQR0tVdLMIKDjK0rIDQmInQfsZa52n.qUo.x1eut6zoJzg3Sx0RJAavLZO2TN.
hashguess: $6$5vb0yjaMeVhIrG5x$AUJwbI1Y2CNA2CJeNigrq/K4ZMFskE7PRt.BGnnGN41jWqC14wbdKYH80wdsF9xdRoapCyQny9kmnJCot26Gm/
the password is: peach

```

Figure 6.9: The hashed password is revealed as 'peach'.

Note the differing timestamps, showing how this took around 3 minutes to execute. This is because the word 'peach' occurs so late in the dictionary as seen in Figure 6.5.

Reflective report

Cryptography and Access Control

With the world moving forward into an increasingly digital age, the security of data is paramount for corporations, businesses and general end-users alike. Sensitive data such as bank details and important corporate documents being stored on digital servers inspires countless threat agents to gain unauthorised access to all kinds of devices with each passing year. In 2016, the Identity Theft Resource Center and Cyber Scout reported 1,093 data breach incidents, up 40% from the 780 reported in 2015 (Xu et al., 2018).

It is for this reason that many strategies are employed to secure digital systems, such as cryptography. Cryptography is defined as the technique of obfuscating or coding data (Kaspersky, n.d.), and often refers to encryption in a cybersecurity context, wherein data transmitted and stored on systems is encrypted as an additional layer of security that ensures data cannot be read by anyone other than its intended recipient, even if it is intercepted during transmission or stolen. Asymmetric encryption is especially important, as it allows for non-repudiation, which provides assurance to the sender that its message was delivered, as well as proof of the sender's identity to the recipient. As a result, neither the sender nor the receiver can deny the message was sent and received (Awati, 2021).

While cryptography is essential in the security and integrity of data, it does not come without some disadvantages of its own, especially on portable and/or older, low-performance devices. Constant encryption and decryption of data using strong encryption algorithms such as AES256 can be performance-intensive, causing these devices to lag. Additionally, an unavoidable consequence of the security provided by strong encryption is that the data cannot be recovered without the key. Though this is intentional, there are likely to be scenarios wherein a user has lost their key and therefore all of their encrypted data, as cracking stronger encryption methods is not feasibly possible with current computational power in finite time (Popat and Mehta, 2019).

An additional cybersecurity measure utilised across a wide variety of systems is access control. One variant of this known as Discretionary Access Control (DAC) was showcased and explained in detail in Lab 5 of this logbook. Access control is defined as "an essential element of security that determines who is allowed to access certain data, apps, and resources." (Microsoft, n.d.). By limiting user access to only what is strictly necessary, risk can be significantly mitigated due to users being unable to modify or delete data they are not entitled to, intentionally or not.

Access control is also not without some issues of its own. Access control is predicated on authentication, meaning that if a threat agent were to gain access to an account with superior access than their own via methods such as phishing or password cracking via tools like Hashcat or John the Ripper, they could then access privileged data via impersonation.

These two techniques are typically used in conjunction with each other on the vast majority of IT systems, which is known as Cryptographic Access Control. This is a vastly superior option to using just one of these techniques, as each technique amplifies the other. Cryptography mitigates access control's impersonation drawback because account passwords would be hashed and salted, making them much harder to brute force. It can also assist in role-based access control, assigning keys dependent upon a user's role and associated privilege level. With the application of cryptographic access control, digital systems can be much more secure and robust in the face of constantly evolving threats.

Bibliography

- Awati, R. (1st Aug. 2021). *What is nonrepudiation?* URL: <https://www.techtarget.com/searchsecurity/definition/nonrepudiation> (visited on 19/03/2024).
- Gite, V. (19th Feb. 2024). *Understanding /etc/passwd File Format*. URL: <https://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/> (visited on 02/03/2024).
- Heinlein, P. (13th Sept. 2016). *OpenSSL Command-Line HOWTO*. URL: <https://www.madboa.com/geek/openssl/#how-do-i-simply-encrypt-a-file> (visited on 24/01/2024).
- Kaspersky (n.d.). *What is Cryptography?* URL: <https://www.kaspersky.com/resource-center/definitions/what-is-cryptography> (visited on 19/03/2024).
- Kolletzki, S. (1996). ‘Secure internet banking with privacy enhanced mail — A protocol for reliable exchange of secured order forms’. In: *Computer Networks and ISDN Systems* 28 (14), pp. 1891–1899. DOI: [https://doi.org/10.1016/S0169-7552\(96\)00089-X](https://doi.org/10.1016/S0169-7552(96)00089-X).
- Microsoft (n.d.). *What is access control?* URL: <https://www.microsoft.com/en-gb/security/business/security-101/what-is-access-control> (visited on 19/03/2024).
- Popat, J. and U. Mehta (2019). ‘Statistical security analysis of AES with X-tolerant response compactor against all types of test infrastructure attacks with/without novel unified countermeasure’. In: *IET circuits, devices & systems* 13 (8), p. 1117. DOI: [10.1049/iet-cds.2019.0083](https://doi.org/10.1049/iet-cds.2019.0083).
- Unix File Permissions* (n.d.). URL: <https://docs.nersc.gov/filesystems/unix-file-permissions/> (visited on 21/02/2024).
- Xu, M., K. M. Schweitzer, R. M. Bateman and S. Xu (2018). ‘Modeling and Predicting Cyber Hacking Breaches’. In: *IEEE Transactions on Information Forensics and Security* 13 (11), pp. 2856–2871. DOI: [10.1109/TIFS.2018.2834227](https://doi.org/10.1109/TIFS.2018.2834227).