Introduction to Cyber Security

What you will do

This is a practical course.

You will have hands-on, technical experience with:

Copyright of BlockCyber Pte Ltd. All rights reserved

What you will do

What it actually means working with the “cloud”

Copyright of BlockCyber Pte Ltd. All rights reserved

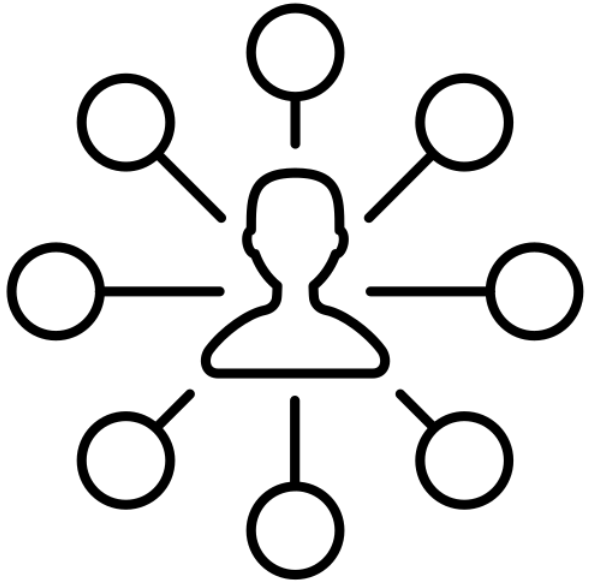
What you will do

Working and controlling Open Source Linux Operating Systems

Copyright of BlockCyber Pte Ltd. All rights reserved

What you will do

Using network controls and basic networking



Copyright of BlockCyber Pte Ltd. All rights reserved

What you will do

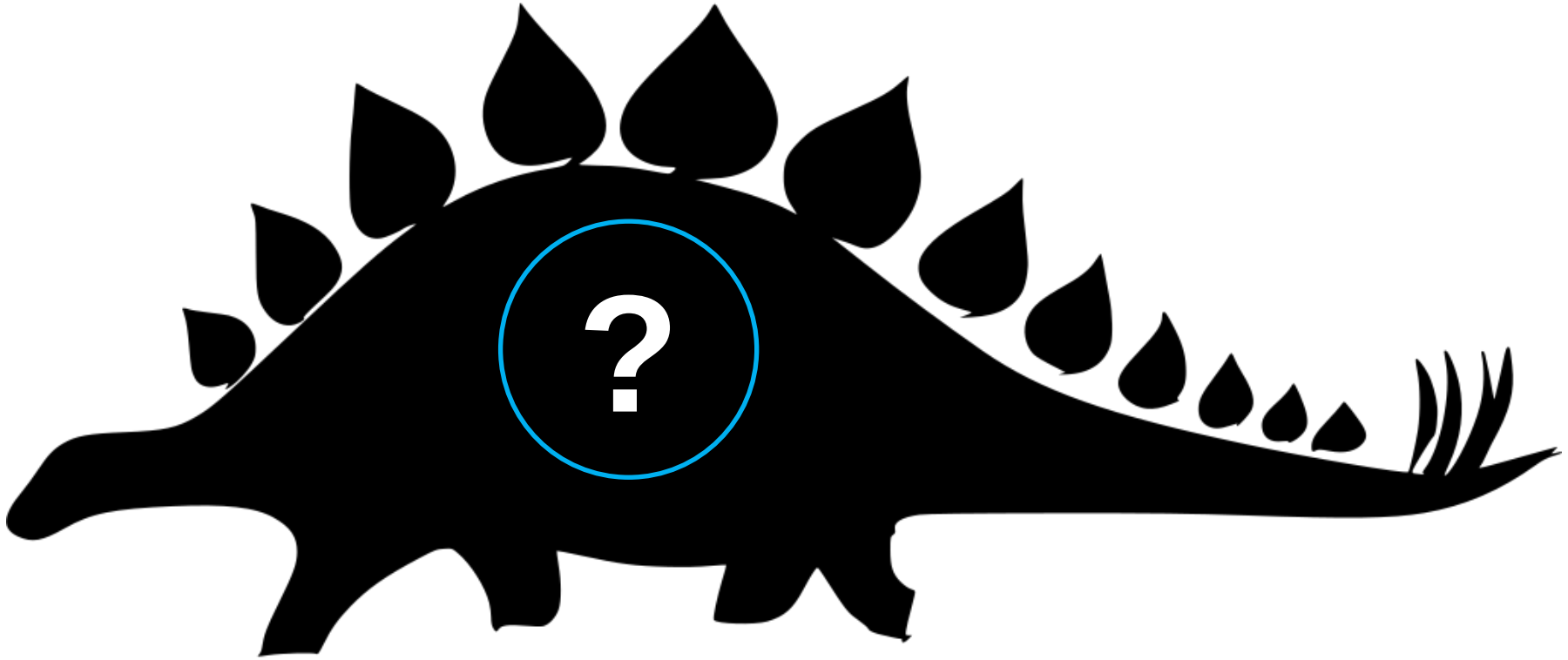
Cryptography: How our data can stay secure

Our Data

Copyright of BlockCyber Pte Ltd. All rights reserved

What you will do

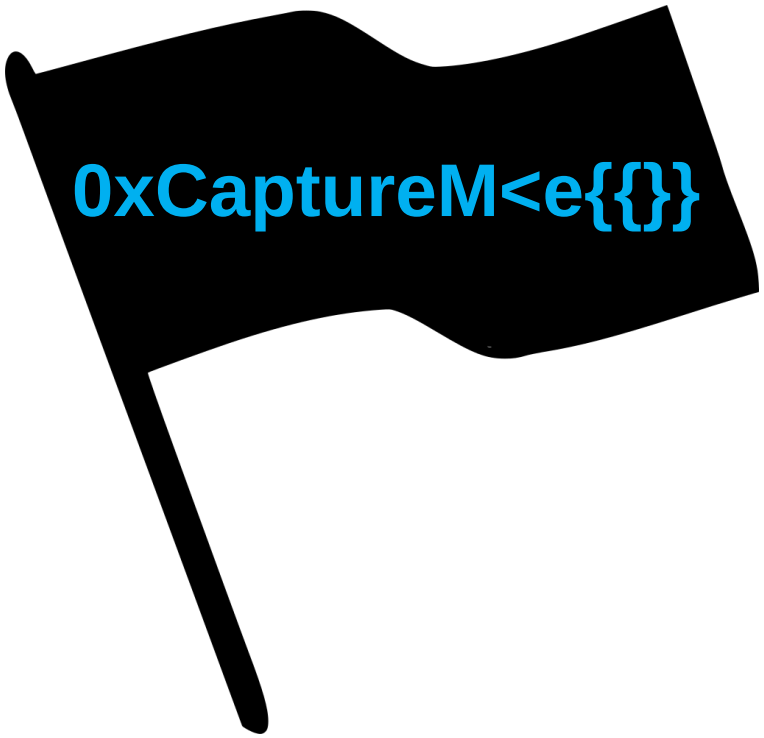
Steganography: Hiding data in plain sight!



Copyright of BlockCyber Pte Ltd. All rights reserved

What you will do

Challenge yourself: Mini Capture the flag competition!



Copyright of BlockCyber Pte Ltd. All rights reserved

Relevance

Copyright of BlockCyber Pte Ltd. All rights reserved

Relevance

Copyright of BlockCyber Pte Ltd. All rights reserved

Topics covered

-

Session	Content
1	Introduction to Virtualization Introduction to Linux and various Linux distros Using Linux command line for basic operation in Linux file and folder operations Linux permissions and access control Linux basic networking
2	Bash scripting Cron scheduling Linux Service / System Control
3	Introduction to Cryptography - Encoding and encryption - Symmetric, Asymmetric - Cryptography Tools
4	Introduction to Cryptography - Hashing - Steganography
5	Challenges (Formative Assessment) - Attempt given tasks and challenges - Network, Linux, Cryptography tasks

Copyright of BlockCyber Pte Ltd. All rights reserved

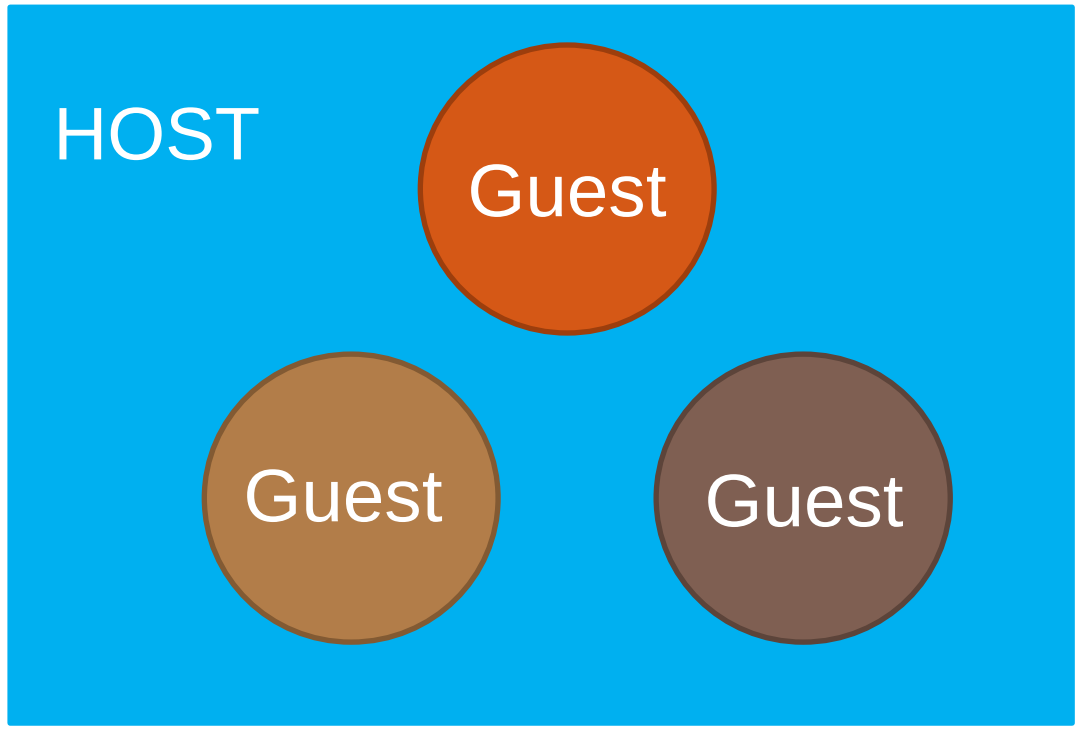
Virtualization

Virtualization

A computer within a computer

Host – the main computer

Guest – the virtual computer



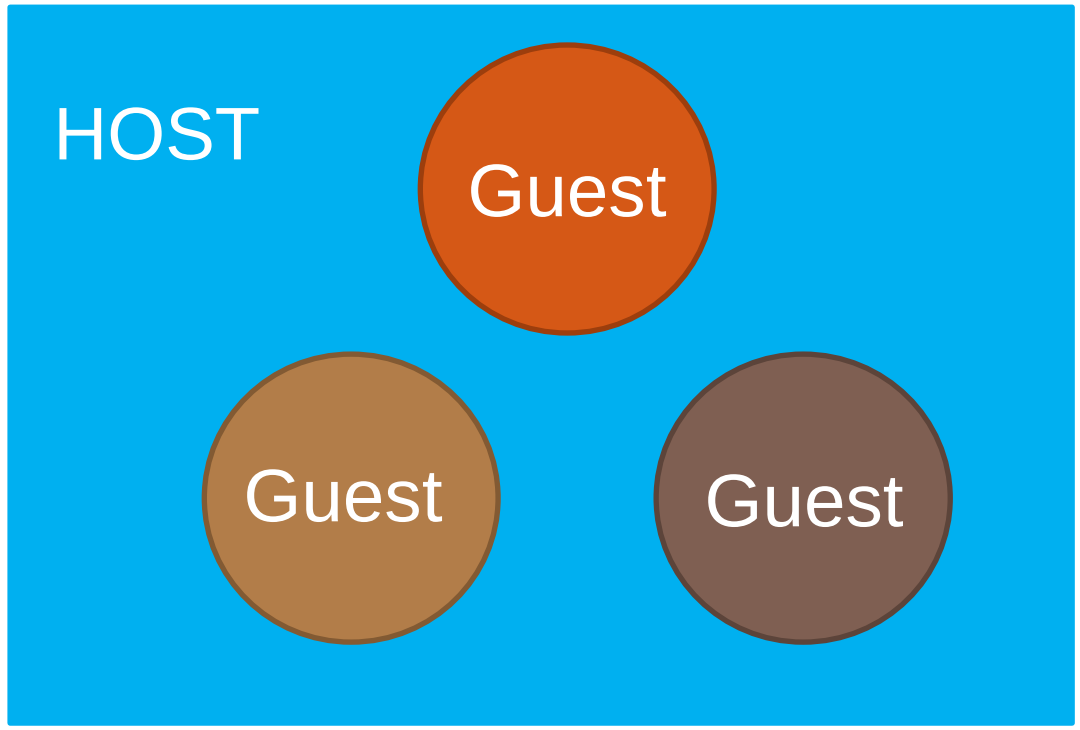
Copyright of BlockCyber Pte Ltd. All rights reserved

Virtualization

Benefits?

We can run different operating systems. We can even run Android.

We can replicate a whole computer with a click of a button.



Copyright of BlockCyber Pte Ltd. All rights reserved

Virtualization

Virtualization tools:

VMWare (professional)

VirtualBox (Free)

Copyright of BlockCyber Pte Ltd. All rights reserved

Cloud and Virtualization

What is the cloud?

It is essentially a bunch of virtual computers running on powerful hosts in data centers.

Copyright of BlockCyber Pte Ltd. All rights reserved

Cloud and Virtualization

BLOCKCYBER

Google Data Center in Jurong West slated to start in 2020

https://www.straitstimes.com/business/companies-markets/google-building-third-data-centre-in-singapore-with-likely-added
PHOTO:GOOGLE

Copyright of BlockCyber Pte Ltd. All rights reserved

Cloud and Virtualization

Inside a data center

https://www.google.com/about/datacenters/gallery/#!#%2Ftech%2F1

Copyright of BlockCyber Pte Ltd. All rights reserved

Virtualization

VirtualBox (Free)

We can simulate a data center in our own computers. With virtualbox

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to Linux

Linux

Linux: What is it?
https://www.linux.org/

Linux is an open-source operating system that is favored by many in the world.

It is often used as the base of server and desktop systems. Sometimes it is also referred to as GNU/Linux

Alternative: FreeBSD https://www.freebsd.org/

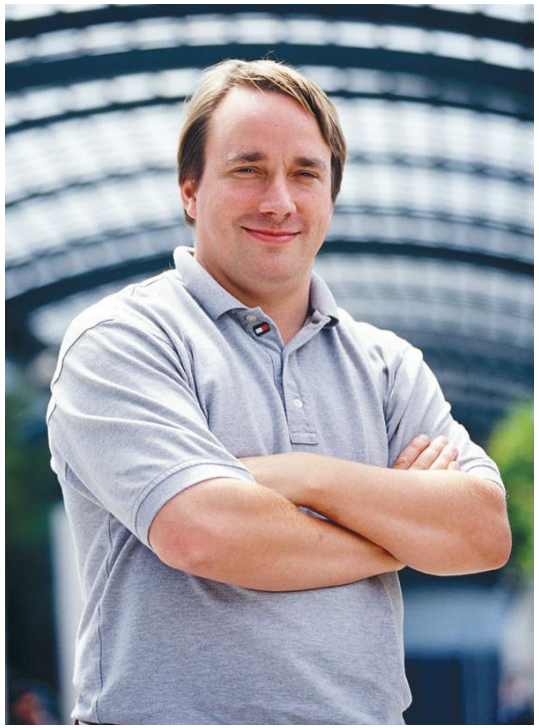
Copyright of BlockCyber Pte Ltd. All rights reserved

Linux

About Linux:

Linux kernel was first released in 17 September, 1991 by Linux Torvalds.

Currently used in servers, desktops, mobile phones, embedded systems(IoT)



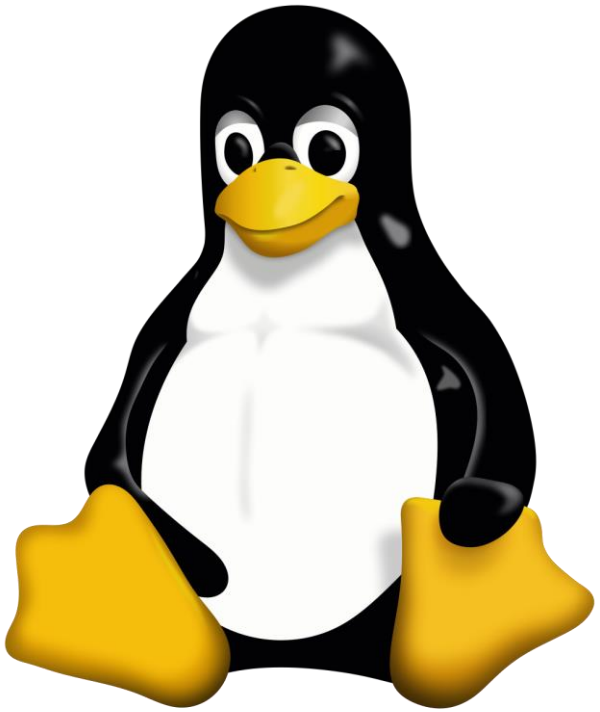
Copyright of BlockCyber Pte Ltd. All rights reserved

Linux

The Linux Kernel:

The Linux kernel is the core of the operating system.

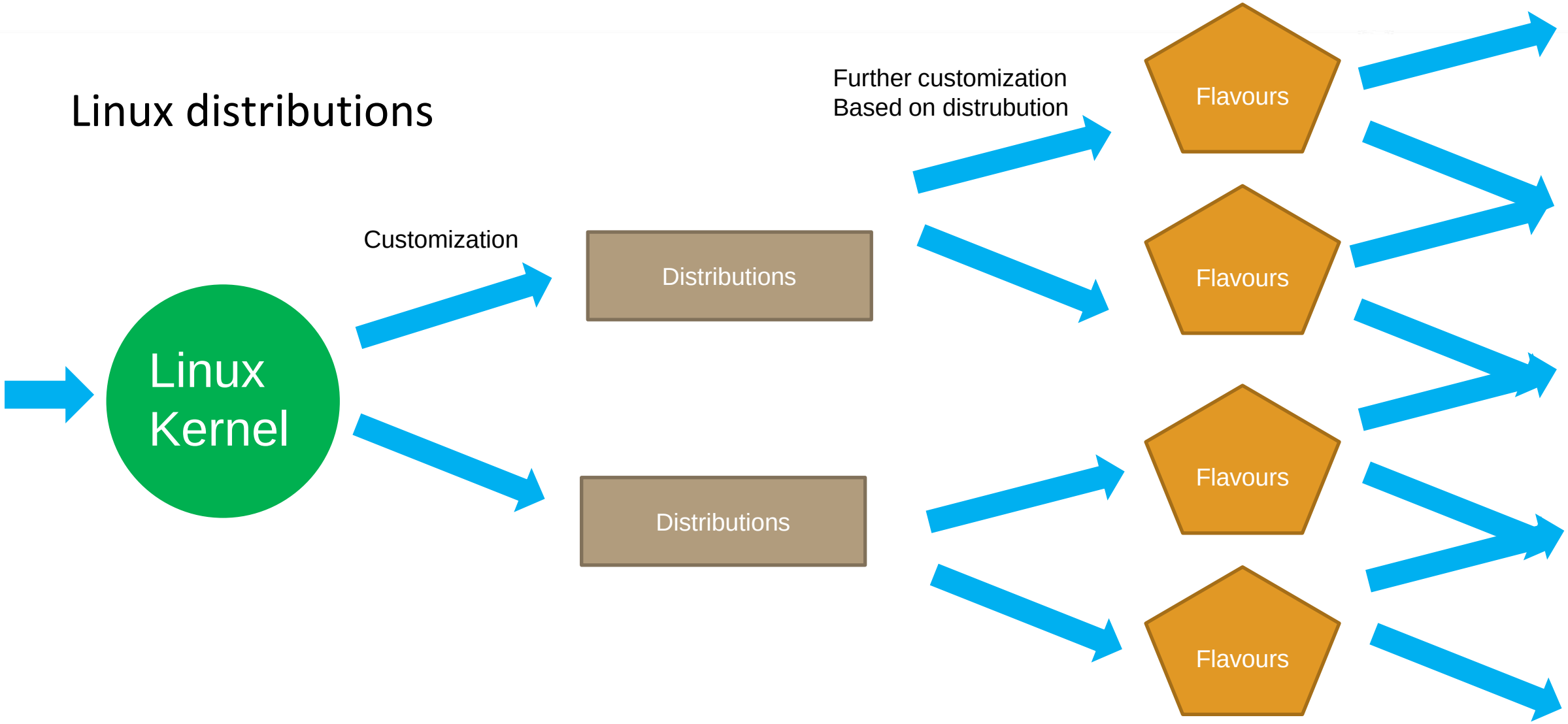
Because it is open sourced, there are many variations called **distributions**.



Copyright of BlockCyber Pte Ltd. All rights reserved

Linux

Linux distributions



Copyright of BlockCyber Pte Ltd. All rights reserved

Linux

BLOCKCYBER

Popular Linux distributions

Ubuntu
Debian
Red Hat
Alpine
Arch Linux
Fedora
CentOS

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux

What is the difference?

They have different packages to suit different needs.

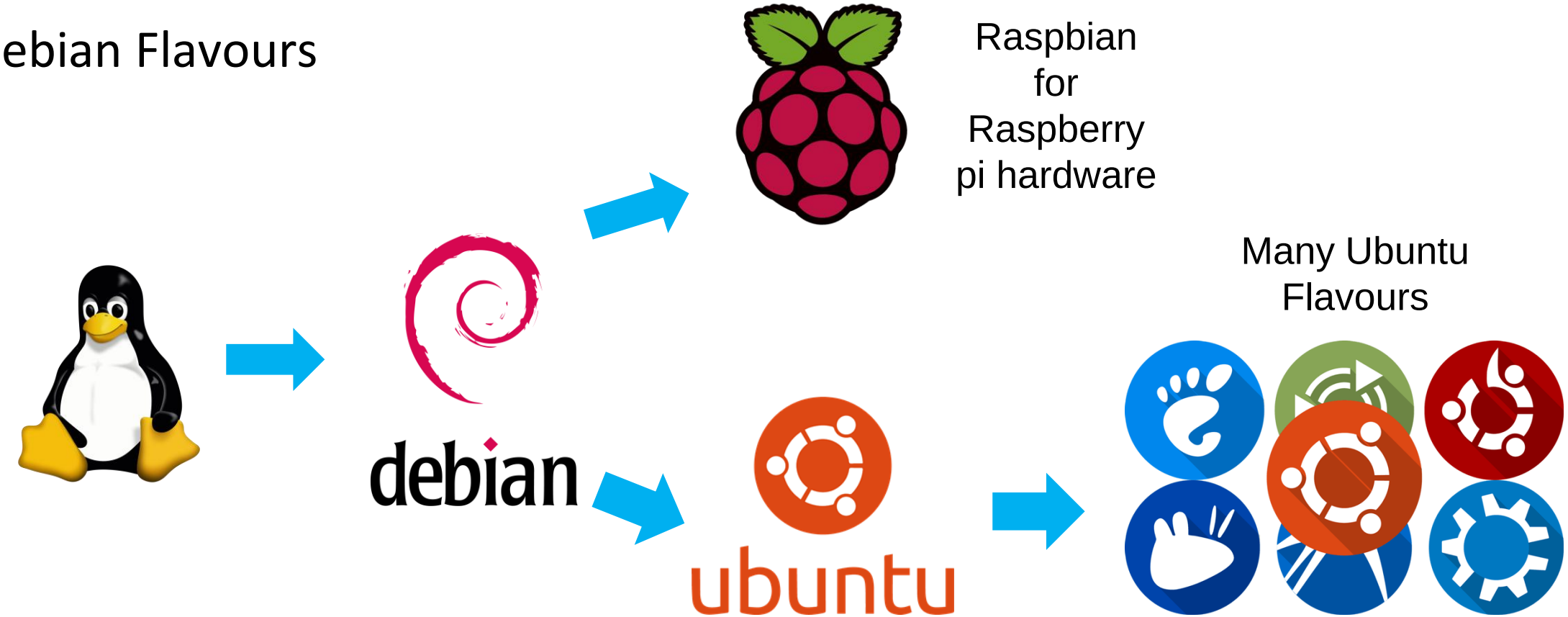
Some, like Alpine and Raspbian, needs to be light weight.

Ubuntu has desktop and non-GUI flavours.

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux

Debian Flavours



Copyright of BlockCyber Pte Ltd. All rights reserved

Linux

Learning Linux will greatly boost our technical skills!

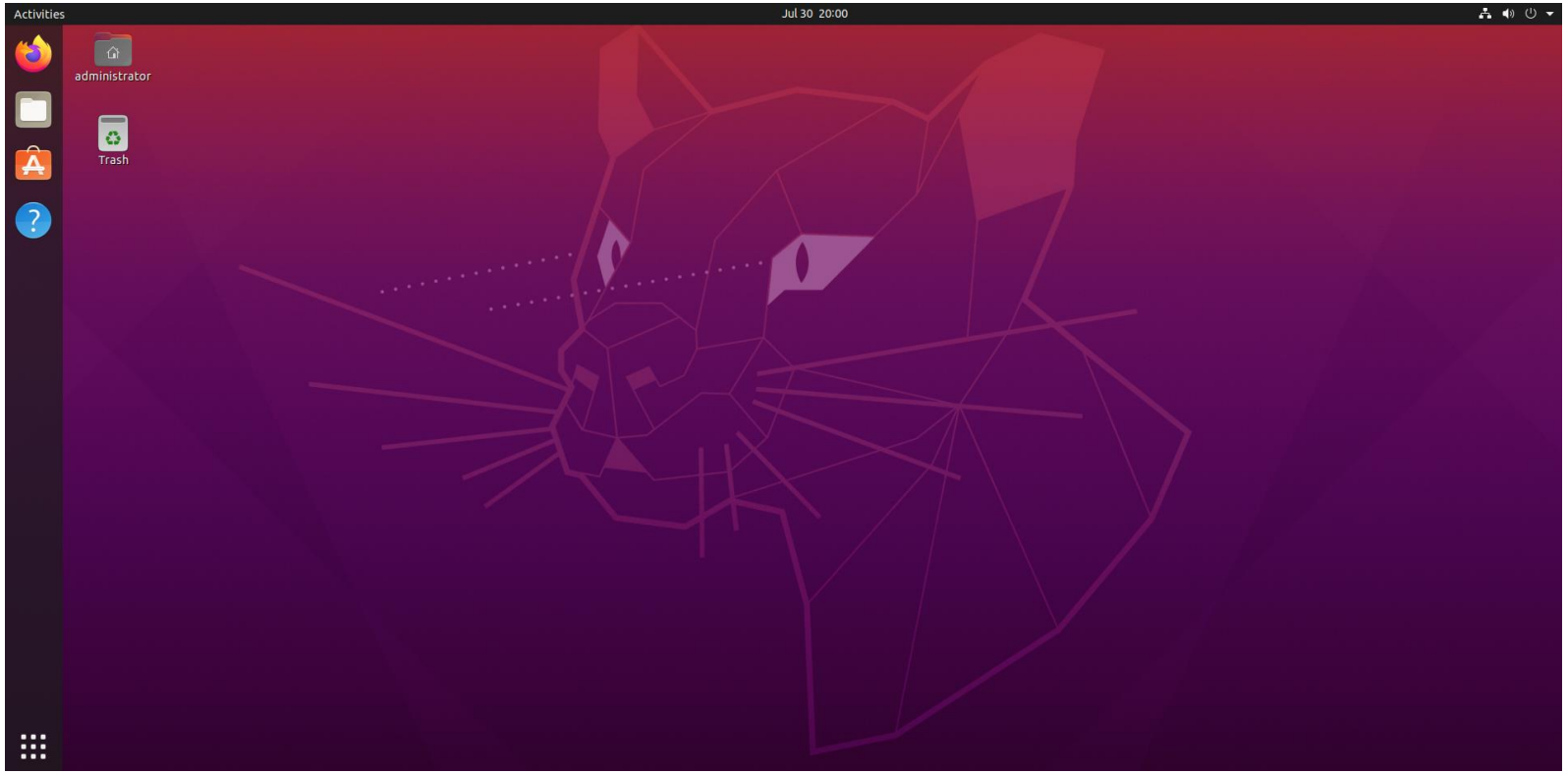
Copyright of BlockCyber Pte Ltd. All rights reserved

Ubuntu

Linux - Basic commands

Ubuntu:

Latest version 20.04



Copyright of BlockCyber Pte Ltd. All rights reserved

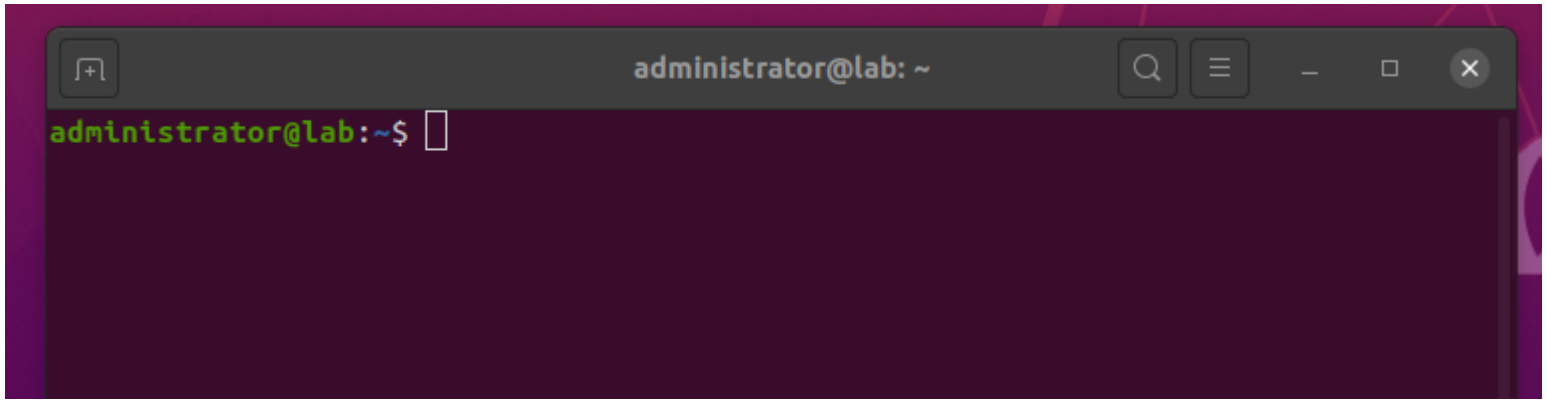
Linux - Basic commands

Ubuntu:

Console / Terminal

This is where we control the computer from.

Let’s get to it.

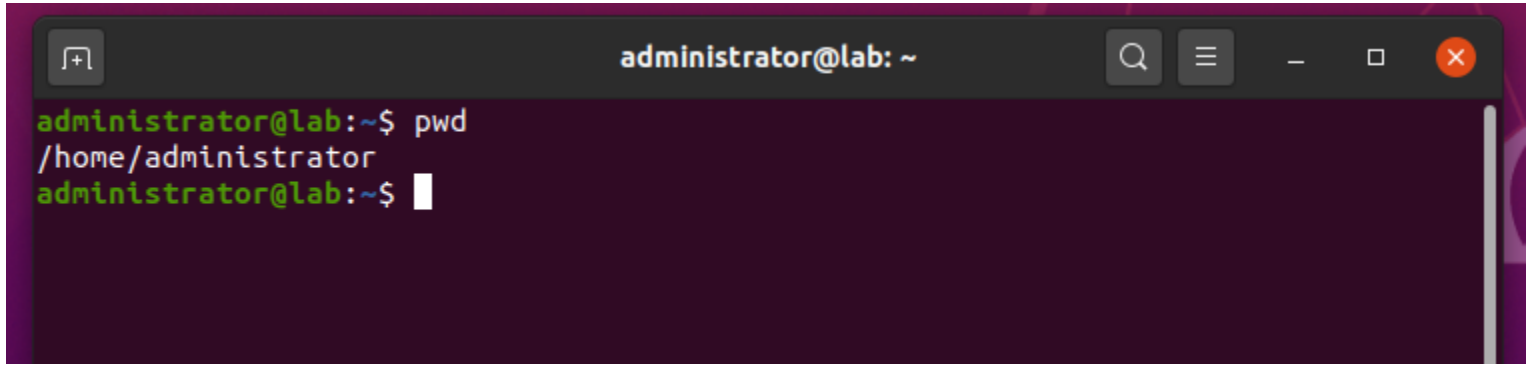


Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

pwd:
Present working directory.

This gives us the full path of the current directory the terminal is in.



Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

cd:
Change directory

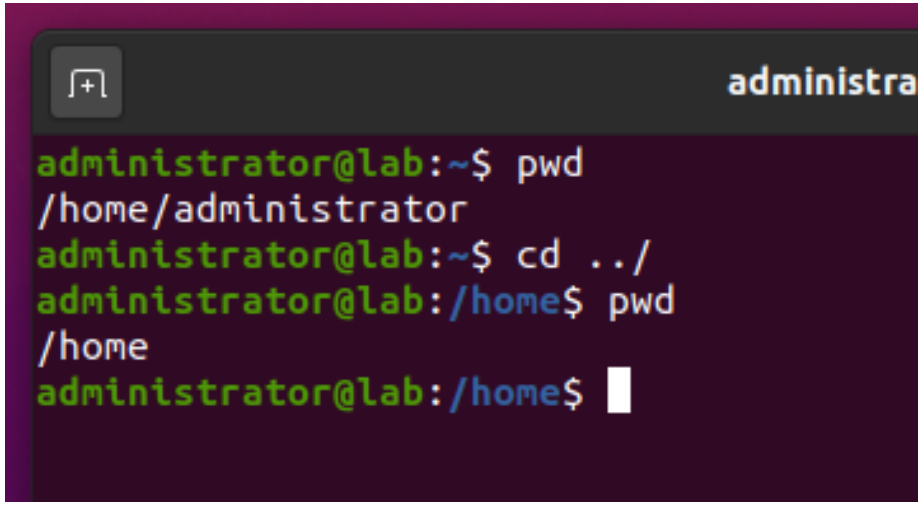
```
# go to previous directory

cd ../

# go to the root directory

cd /
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

cd:
Change directory

```
# go to previous directory

cd ../

# go to the root directory

cd /
```



Copyright of BlockCyber Pte Ltd. All rights reserved

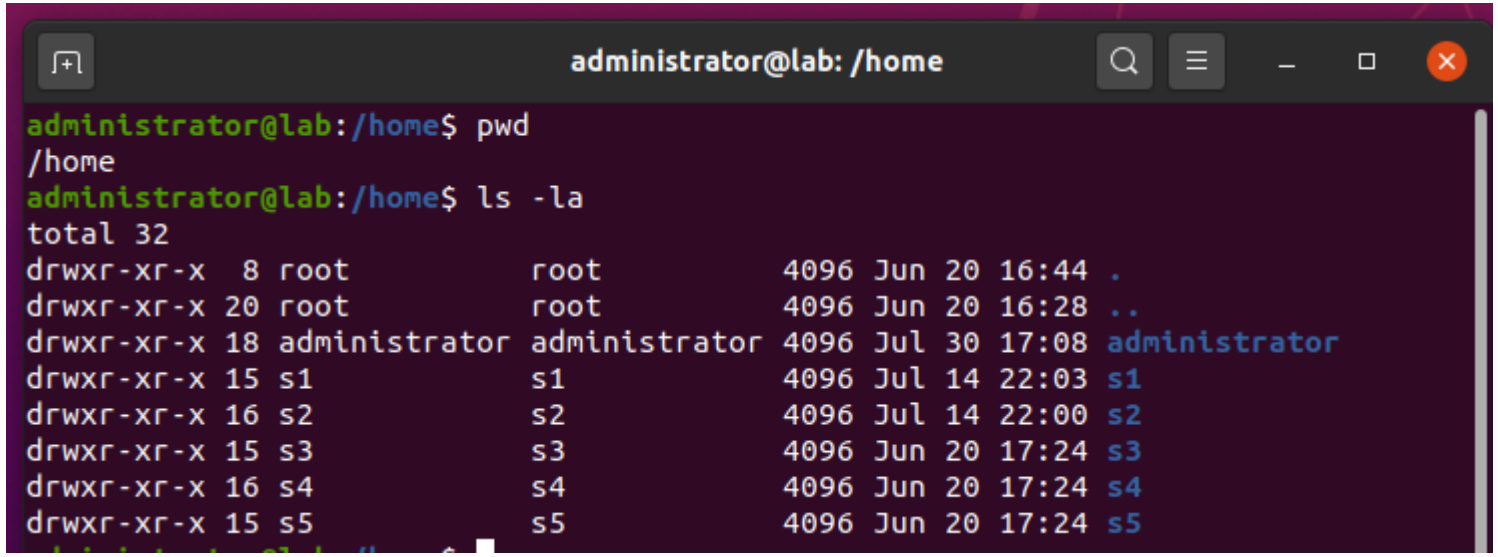
Linux - Basic commands

ls:

List

Lists items in the directory

```
# list

ls

# list all

ls -la
```



Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

What is –la?

Dashes indicate options. We can find out usually with --help

```
ls --help
```

```
administrator@lab:/home$ ls --help
Usage: ls [OPTION]... [FILE]...
List information about the FILEs (the current directory by default).
Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.

Mandatory arguments to long options are mandatory for short options too.
  -a, --all                  do not ignore entries starting with .
  -A, --almost-all           do not list implied . and ..
      --author               with -l, print the author of each file
  -b, --escape               print C-style escapes for nongraphic characters
      --block-size=SIZE      with -l, scale sizes by SIZE when printing them
```

It's usually --help or –h.

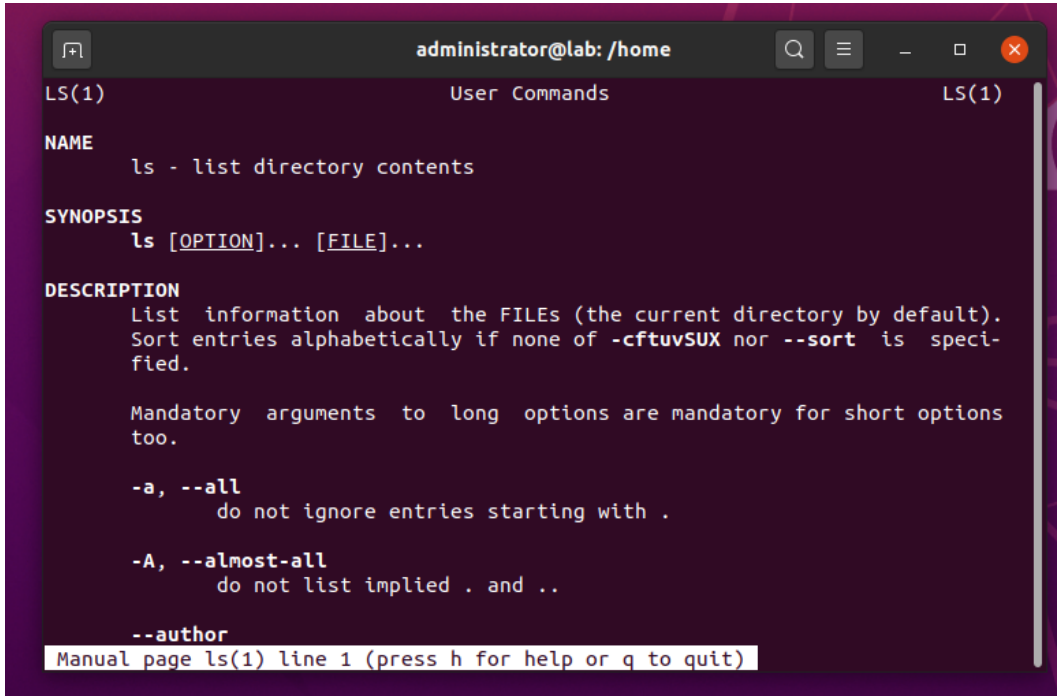
Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

man page

The manual page will give the full information of any command in the terminal.

```
man ls
```



Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

man page

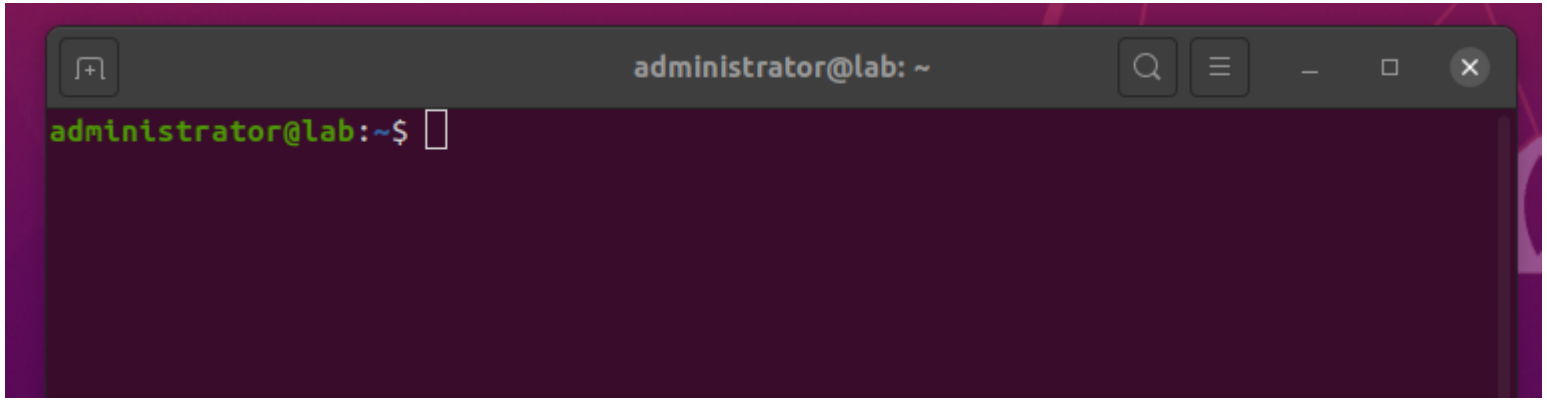
We can also google the man page.

https://man7.org/linux/man-pages/man1/ls.1.html

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

clear:
Clears the terminal if it gets too messy

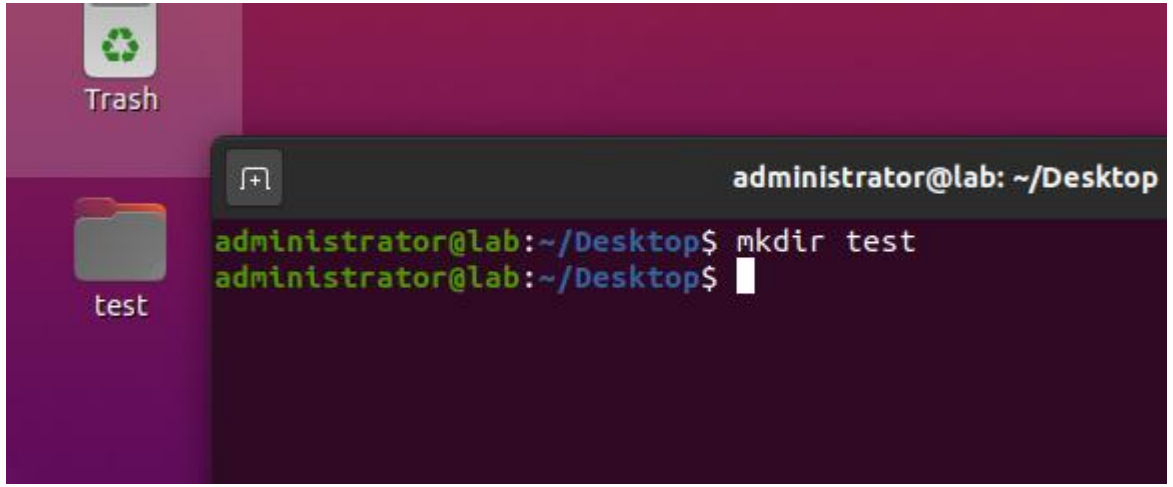


Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

mkdir:
Make directory (folder)

```
mkdir test
```



Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

echo:
Show something on screen

```
echo hi there
```

```
administrator@lab:~/Desktop$ echo hi there
hi there
administrator@lab:~/Desktop$
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

">" save output into a file:

The arrow key

```
echo hi there > words.txt
```

```
administrator@lab:~/Desktop/test$ echo hi there > words.txt
administrator@lab:~/Desktop/test$ ls
words.txt
administrator@lab:~/Desktop/test$
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

cat:

Reading files with cat. Displays content of files in console.

```
cat sample.txt
```

```
s1@ip-172-31-38-241:~/Desktop/lab$ cat sample.txt
this is a textfile
s1@ip-172-31-38-241:~/Desktop/lab$
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

rm:
Remove a file

Current directory is in the test folder

```
rm words.txt
```

```
administrator@lab:~/Desktop/test$ rm words.txt
administrator@lab:~/Desktop/test$ ls
administrator@lab:~/Desktop/test$
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

We can use commands with the directory syntax.

If our current directory is in Desktop, we can do the following

```
rm test/words.txt
```

```
administrator@lab:~/Desktop$ rm test/words.txt
administrator@lab:~/Desktop$
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

Tab:

If we are unsure of the file name, we can type an incomplete name and press tab. It will help us find compatible names

```
rm test/wo
```

Press tab

```
administrator@lab:~/Desktop$ rm test/words.txt
administrator@lab:~/Desktop$
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

rm –rf foldername:

We cannot use rm to remove a folder. It will give us an error.
We use the rm options –rf to “recursively remove”

Options
-r is to recursively remove
-f is to force

```
rm –rf test
```

```
administrator@lab:~/Desktop$ rm -rf test
administrator@lab:~/Desktop$ ls
administrator@lab:~/Desktop$
```

https://man7.org/linux/man-pages/man1/rm.1.html

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

./program_name:

We use ./ to execute a program

```
./echo_program.sh
```

```
administrator@lab:~/Desktop$ ./echo_program.sh
the program is running!
administrator@lab:~/Desktop$
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Basic commands

LAB Session 1

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux Permissions

Linux - Linux permissions

We can find out about the file permissions with ls -la

```
administrator@lab: /home
administrator@lab:/home$ pwd
/home
administrator@lab:/home$ ls -la
total 32
drwxr-xr-x  8 root          root          4096 Jun 20 16:44 .
drwxr-xr-x 20 root          root          4096 Jun 20 16:28 ..
drwxr-xr-x 18 administrator administrator 4096 Jul 30 17:08 administrator
drwxr-xr-x 15 s1            s1            4096 Jul 14 22:03 s1
drwxr-xr-x 16 s2            s2            4096 Jul 14 22:00 s2
drwxr-xr-x 15 s3            s3            4096 Jun 20 17:24 s3
drwxr-xr-x 16 s4            s4            4096 Jun 20 17:24 s4
drwxr-xr-x 15 s5            s5            4096 Jun 20 17:24 s5
```

Permissions

owner

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Linux permissions

Permissions

Read
Write
Execute

Full permissions

```
# directory
d rwx rwx rwx
# file
- rwx rwx rwx
```

user | group | others

No execution

```
# directory
d rw- rw- rw-
# file
- rw- rw- rw-
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Linux permissions

Sometimes files do not run with ./ because it does not have the execution permission.

We can put users in the same group to manage permissions. That will be for more advanced management

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Linux permissions

chmod:

We can use chmod to change permissions.

I have a secret file that can only be read by the administrator.
I want to change it to read only

```
administrator@lab:~/Desktop$ ls -la
total 12
drwxr-xr-x  2 administrator administrator 4096 Jul 30 20:50 .
drwxr-xr-x 18 administrator administrator 4096 Jul 30 17:08 ..
-rw-rw-r--  1 administrator administrator   18 Jul 30 20:50 confidential_secret
administrator@lab:~/Desktop$
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Linux permissions

chmod:

```
chmod 444 confidential_secret
```

```
administrator@lab:~/Desktop$ chmod 444 confidential_secret
administrator@lab:~/Desktop$ ls -la
total 12
drwxr-xr-x  2 administrator administrator 4096 Jul 30 20:50 .
drwxr-xr-x 18 administrator administrator 4096 Jul 30 17:08 ..
-r--r--r--  1 administrator administrator   18 Jul 30 20:50 confidential_secret
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Linux permissions

chmod:
We use binary calculations to come to the 444 number

If we want read-only, it is:

```
# file
- r-- r-- r--
```

Binary 100 is 4 in base 10.

```
# file
- 100 100 100
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Linux permissions

chmod:

Base 10	128	64	32	16	8	4	2	1
Binary	0	0	0	0	0	1	0	0

```
# file
- r-- r-- r--
```

```
# Full permissions
- rwx rwx rwx
```

```
# file
- 100 100 100
```

```
# What is the number
- 111 111 111
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Linux permissions

chmod:

Base 10	128	64	32	16	8	4	2	1
Binary	0	0	0	0	0	1	1	1

```
4 + 2 + 1 = 7
```

The number for full permissions is 777.

Copyright of BlockCyber Pte Ltd. All rights reserved

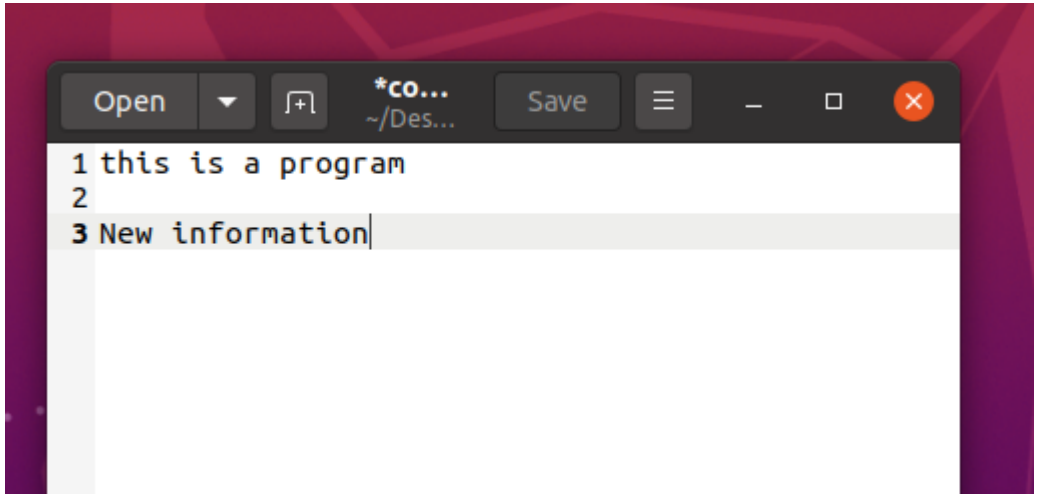
Linux - Linux permissions

Let’s try using a text editor to change the contents of the file.

The save button is blurred out.

We cannot save.

In this case, we do not have the **Write** permission.



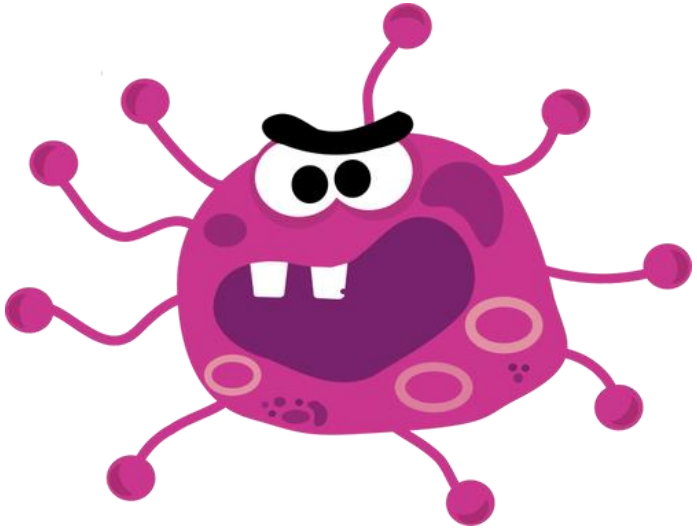
Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Linux permissions

Generally, giving files full permission 777 is a security hole.

If we have a text file, we should disable the execution flag.

Or we could do 600 do give current user Read and Write, and nobody else can read or edit.



Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Linux permissions

SUDO:

Somethings we need to run certain commands with higher privileges

```
administrator@lab:~/Desktop$ ip link set enp0s3 down
RTNETLINK answers: Operation not permitted
administrator@lab:~/Desktop$
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux Networking

Linux - Linux networking

We can check our network status with

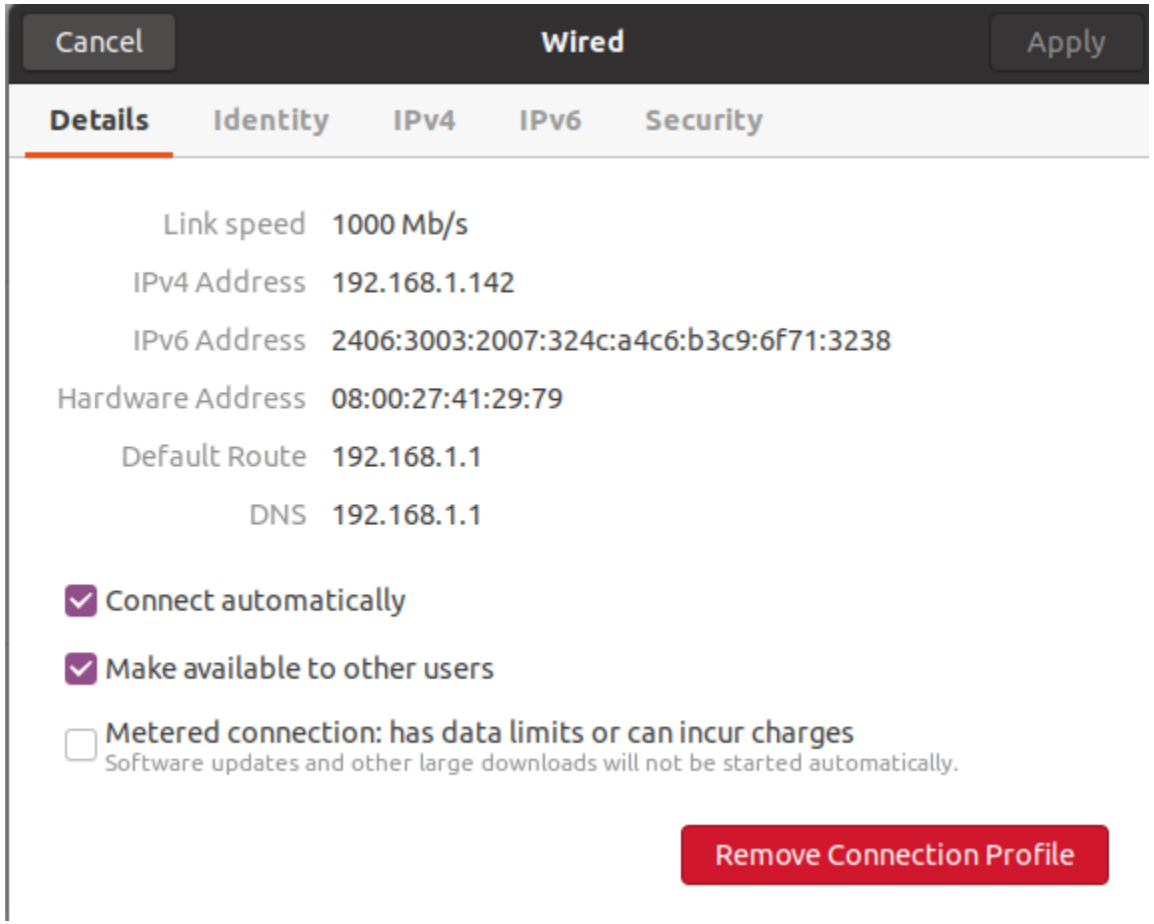
```
ip a
```

```
administrator@lab: ~/Desktop
administrator@lab:~/Desktop$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:41:29:79 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.142/24 brd 192.168.1.255 scope global dynamic noprefixroute e
np0s3
       valid_lft 71898sec preferred_lft 71898sec
    inet6 2406:3003:2007:324c:a4c6:b3c9:6f71:3238/64 scope global temporary dyna
mic
       valid_lft 154930sec preferred_lft 71701sec
    inet6 2406:3003:2007:324c:3a20:6947:f86d:151a/64 scope global dynamic mngtmp
addr noprefixroute
       valid_lft 154930sec preferred_lft 154930sec
    inet6 fe80::aabc:4f2f:93c9:8fcf/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Linux networking

We can see similar information using the GUI settings menu



Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Linux networking

To start and stop the network:

```
ip link set enp0s3 up
```

```
ip link set enp0s3 down
```

```
s1@lab:~/Desktop$ ip l show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel s
    link/ether 08:00:27:41:29:79 brd ff:ff:ff:ff:ff:ff
```

Status is up

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Linux networking

To use higher privileges, we use the sudo command at the start of the command:

```
sudo ip link set enp0s3 up
```

```
sudo ip link set enp0s3 down
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Linux networking

To use higher privileges, we use the sudo command at the start of the command:

```
administrator@lab: ~/Desktop
administrator@lab:~/Desktop$ ip link set enp0s3 down
RTNETLINK answers: Operation not permitted
administrator@lab:~/Desktop$ sudo ip link set enp0s3 down
[sudo] password for administrator:
administrator@lab:~/Desktop$ ip l show enp0s3
2: enp0s3: <BROADCAST,MULTICAST> mtu 1500 qdisc fq_codel state DOWN mode DEFAULT group default qlen 1000
    link/ether 08:00:27:41:29:79 brd ff:ff:ff:ff:ff:ff
administrator@lab:~/Desktop$
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Linux networking

SUDO:

Some users might not have sudo permissions too.

```
s1@lab:/home/administrator/Desktop$ sudo ip link set enp0s3 down
[sudo] password for s1:
s1 is not in the sudoers file.  This incident will be reported.
s1@lab:/home/administrator/Desktop$
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Linux - Wrap up

BLOCKCYBER

So why do we bother to learn with command line?

In cyber security, most of the time we are working in command line.

When we take control or access a computer, it is with the command line.

Windows and MacOS has their own terminal as well, the commands are slightly different but the concepts are similar.

Copyright of BlockCyber Pte Ltd. All rights reserved

Bash Scripting

Bash Scripting

We have covered Linux command lines using the terminal in Ubuntu.

The terminal is a GNU Bash shell

Copyright of BlockCyber Pte Ltd. All rights reserved

Bash Scripting

We can automate our commands using bash scripting.

Basic template:
Save the code as a .sh file

Initialize. This is path of the bash program.

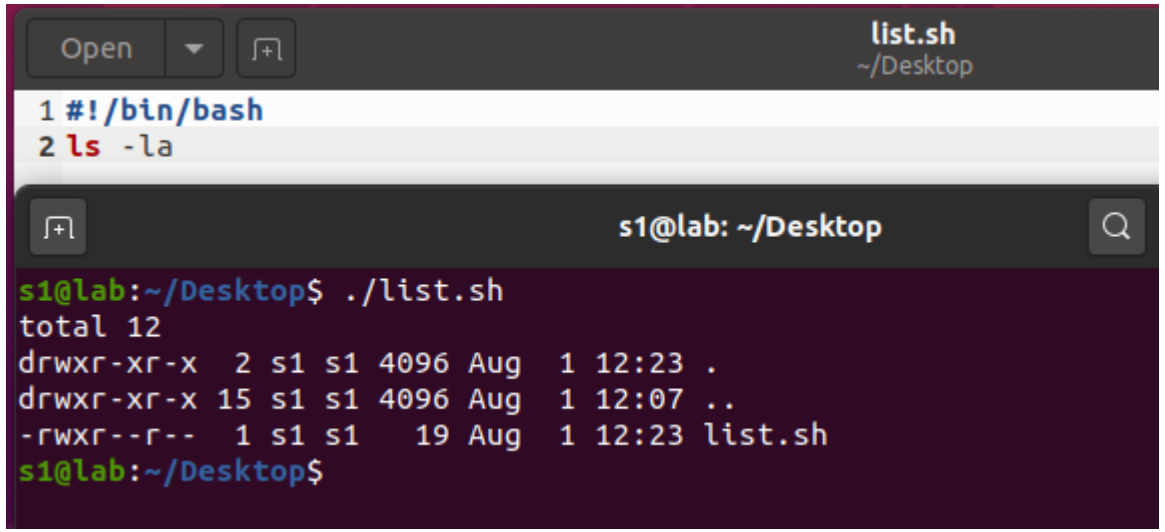
```
#!/bin/bash
Ls -la
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Bash Scripting

We have a script called list.sh. Using ./list.sh, we run the bash script.

```
./list.sh
```



If we cannot run the script, check the file permissions and enable execute. In this case I used 744.

Copyright of BlockCyber Pte Ltd. All rights reserved

Bash Scripting

BLOCKCYBER

Bash scripting is Turing complete, so it can function as a full programming language.

Bash scripting can help us automate PC administration tasks.

E.g., if we want to empty out a folder at noon every day, every start up

Copyright of BlockCyber Pte Ltd. All rights reserved

Bash Scripting

Example: Write a script that checks if our network is up or down

Using “ip a”, my network is on the adapter enp0s3.

We just need to check status of enp0s3

```
ip a
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Bash Scripting

To turn on or off enp0s3, we have the following commands:

```
ip link set enp0s3 up
```

```
ip link set enp0s3 down
```

```
s1@lab:~/Desktop$ ip l show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel s
    link/ether 08:00:27:41:29:79 brd ff:ff:ff:ff:ff:ff
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Bash Scripting

GREP:
We use GREP to extract out information with keywords

PIPE: pipe passes the output data from the first command into another command.

```
administrator@lab:~/Desktop$ ip l show enp0s3 | grep "state UP"
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mo
de DEFAULT group default qlen 1000
```

```
ip l show enp0s3 | grep "state UP"
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Bash Scripting

There are no results if we search for “state Down”. Because the current state is “UP”.

```
administrator@lab:~/Desktop$ ip l show enp0s3 | grep "state DOWN"
administrator@lab:~/Desktop$
```

```
ip l show enp0s3 | grep “state DOWN”
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Bash Scripting

In bash scripting, we can do if, else, while loops, for loops, and everything a programming language can.

Script logic:
We can check for “state DOWN”. If the response if empty “”, then the state is up. Else, the state is down.

Copyright of BlockCyber Pte Ltd. All rights reserved

Bash Scripting

The script:

We save it as start_network.sh

```
#!/bin/bash

OUTPUT=$(ip l show enp0s3 | grep 'state DOWN')

# if output equals to empty
if [ "$OUTPUT" = "" ]; then
      echo "enp0s3 is UP";
else
      echo "enp0s3 is DOWN";
fi
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Bash Scripting

The script:

```
administrator@lab: ~/Desktop
administrator@lab:~/Desktop$ ./start_network.sh
enp0s3 is UP
administrator@lab:~/Desktop$ sudo ip link set enp0s3 down
administrator@lab:~/Desktop$ ./start_network.sh
enp0s3 is DOWN
administrator@lab:~/Desktop$
```

We have successfully check for network

Copyright of BlockCyber Pte Ltd. All rights reserved

Bash Scripting

Next, if network interface is down, start the network interface!

Copyright of BlockCyber Pte Ltd. All rights reserved

System Services

System Services

What are system services?

Services are programs and processes that the computer is currently running. They may be running in the background without us knowing.

Web servers and databases can be start/off using system services.

Copyright of BlockCyber Pte Ltd. All rights reserved

System Services

We use the following command to check for running services

```
service --status-all
```

```
administrator@lab:~/Desktop$ service --status-all
 [ + ]  acpid
 [ + ]  alsa-utils
 [ - ]  anacron
 [ + ]  apparmor
 [ + ]  apport
 [ + ]  avahi-daemon
 [ - ]  bluetooth
```

Copyright of BlockCyber Pte Ltd. All rights reserved

System Services

We can check status and control with **systemctl**

```
systemctl status cron
```

```
administrator@lab:~/Desktop$ systemctl status cron
● cron.service - Regular background program processing daemon
     Loaded: loaded (/lib/systemd/system/cron.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2020-08-01 12:02:28 +08; 1h 32min ago
       Docs: man:cron(8)
   Main PID: 587 (cron)
      Tasks: 1 (limit: 4656)
     Memory: 1.5M
     CGroup: /system.slice/cron.service
             └─587 /usr/sbin/cron -f

Aug 01 12:17:01 lab CRON[2545]: pam_unix(cron:session): session opened for user root by (uid=0)
Aug 01 12:17:01 lab CRON[2553]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
```

Copyright of BlockCyber Pte Ltd. All rights reserved

System Services

Press CTRL+C to exit the systemctl. This will pass the console back to the bash shell.

Other than checking status, we can **start**, **stop**, **restart**, **enable**, and more commands.

Copyright of BlockCyber Pte Ltd. All rights reserved

Cron Scheduling

CRON scheduling

Cron is a program that helps us schedule tasks.

For example, we can ask our program to check for network interface every minute

Copyright of BlockCyber Pte Ltd. All rights reserved

CRON scheduling

Cron is a program that helps us schedule tasks.

For example, we can ask our program to check for network interface every minute

```
crontab -e
```

Copyright of BlockCyber Pte Ltd. All rights reserved

CRON scheduling

We will be asked to choose a terminal text editor, we can start with NANO

```
sudo crontab -e
```

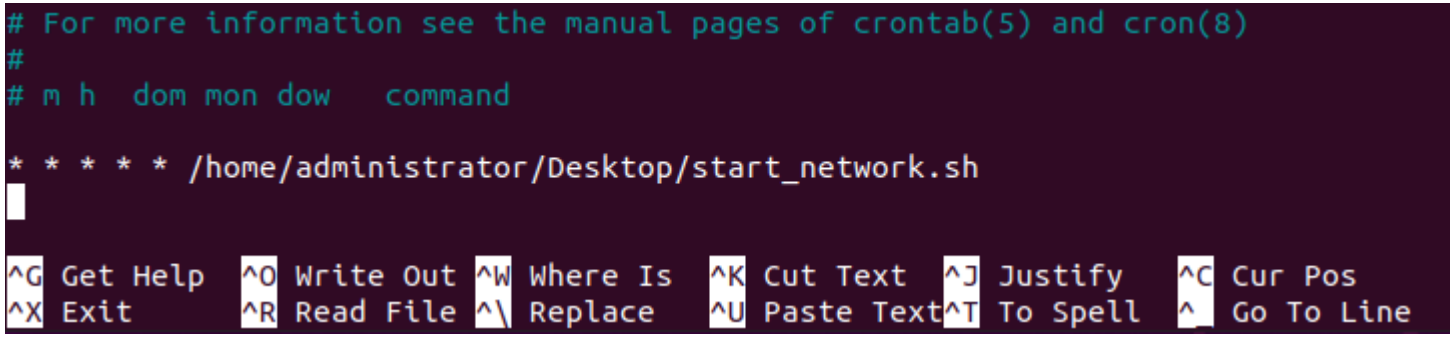
```
administrator@lab:~/Desktop$ crontab -e
no crontab for administrator - using an empty one

Select an editor.  To change later, run 'select-editor'.
  1. /bin/nano        <---- easiest
  2. /usr/bin/vim.tiny
  3. /bin/ed

Choose 1-3 [1]: 1
```

Copyright of BlockCyber Pte Ltd. All rights reserved

CRON scheduling

Fill in the following line, CTRL+ O to save, CTRL + X to exit.

```
* * * * * /home/administrator/Desktop/start_network.sh
```



Copyright of BlockCyber Pte Ltd. All rights reserved

CRON scheduling

Once we reboot, if we turn off enp0s3, it will check and start the network automatically every minute.

So what was the * * * * * in the command?

Copyright of BlockCyber Pte Ltd. All rights reserved

CRON scheduling

Once we reboot, if we turn off enp0s3, it will check and start the network automatically every minute.

So what was the * * * * * in the command?

Copyright of BlockCyber Pte Ltd. All rights reserved

CRON scheduling

Legend:
* stands for any value.

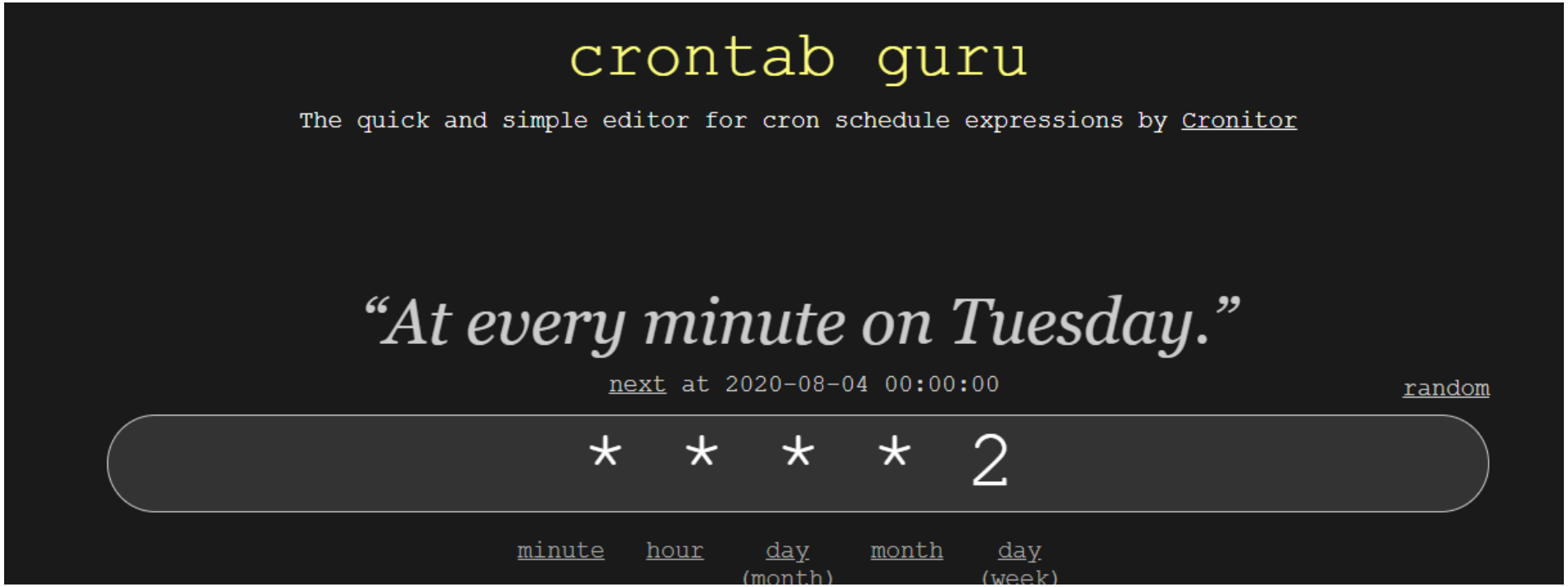
This stands for all minutes, all hours, all days and all months.

minute	hour	day	month	Day(of the week)
*	*	*	*	*

Copyright of BlockCyber Pte Ltd. All rights reserved

CRON scheduling

We can use online resources to find out more:
https://crontab.guru/



Copyright of BlockCyber Pte Ltd. All rights reserved

CRON scheduling

Let’s practice!

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography

Intro to Encoding

Intro to cryptography

Cryptography is a means of protecting information with cipher. Feel free to look at the math behind cryptography, but we will look at practical applications only.

2 Main Concepts in cryptography

- Encoding
- Encryption

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encoding

BLOCKCYBER

Encoding

Encoding is changing data from one form to another. With encoding, different systems are able to understand the data that you sent.

Text encoding formats:
ASCII, Unicode(UTF-8, 16, 32) and many more!
HTML/URL encoding

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encoding

BLOCKCYBER

Base64 Encoding

Base64 text encoding is the most common in modern web communications.

It is used in

- Authentication Encoding image files for display on web
- Many other variations

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encoding

BLOCKCYBER

Encoding

When developing a web application, we must know which text encoding to use in our app and database.

For example, if we save text in Chinese, but encoding is in ASCII, then your data will be ruined because ASCII does not support Chinese language. A Unicode UTF-8 will be better suited.

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encoding

BLOCKCYBER

HTML Encoding / HTML

If we display the following on a web page, it will become a XSS attack

```
str = <script>alert("attack")</script>
```

HTML encoding will turn characters like < > into safe characters to display

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encoding

BLOCKCYBER

HTML Encoding

HTML Encoding will turn the string into:

str = <script>alert(“attack”)</script>

Str_encoded = <script>alert(“attack”)</script>

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encoding

BLOCKCYBER

HTML Encoding in PHP

Input:

```
<?php
$str = '<script>alert("attack")</script>';
echo htmlspecialchars($str);
?>
```

```
<!DOCTYPE html>
<html>
<body>
&lt;script&gt;alert("attack")&lt;/script&gt;
</body>
</html>
```

Browser Text Output

```
<script>alert("hi")</script>
```

SAFE
!

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encoding

BLOCKCYBER

URL Encoding / URL

URLs only encoding ASCII character set.
Most of our user inputs, or database text encoding is not in ASCII, so we need to URL encode

For example, we sent a “Hello there” string through a GET request, we get a %20 instead of a space

Mywebsite.com?message=hello%20there

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encoding

BLOCKCYBER

Unicode Encoding

Is mainly used for multi-language text data. It is also safer to set your database to encode data in UTF-8 to prevent data loss.

What is the difference between Unicode and UTF-8?

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encoding

BLOCKCYBER

What is the difference between Unicode and UTF-8?

UTF-8, UTF-16, UTF-32 and other encoding schemes can change a character to a binary number for storage.

Unicode is a Character set, which maps the binary number stored to a character in the character set
https://home.unicode.org/

Copyright of BlockCyber Pte Ltd. All rights reserved

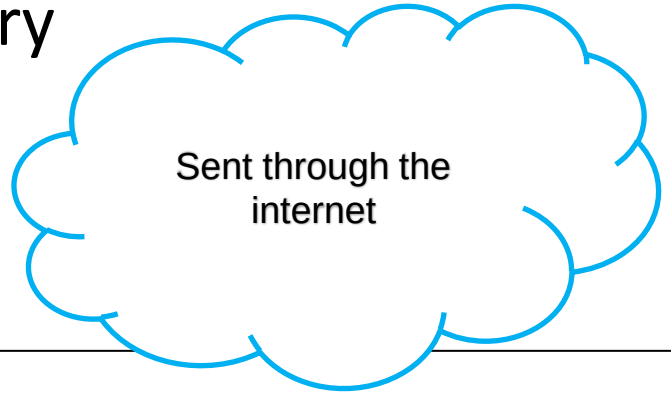
Intro to Encryption

Intro to cryptography: Encryption

Encryption data + Cipher Key = ciphertext

Server

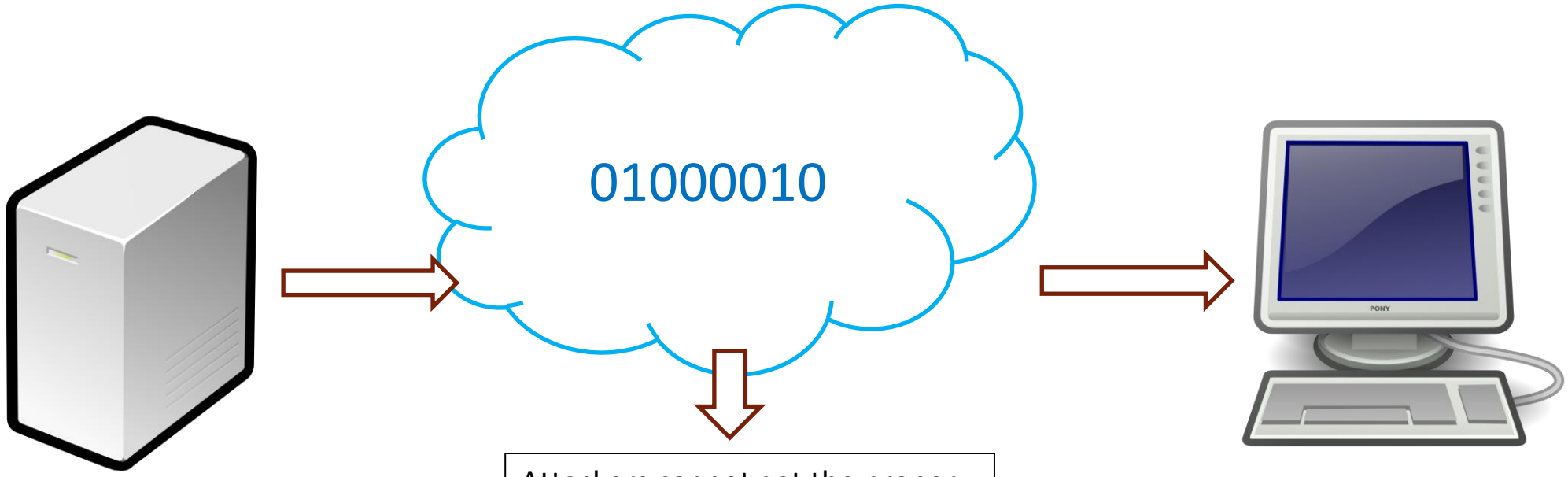
// 01000001 is the character “A” in binary
// binary addition
01000001 + 1 = 01000010



Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encryption

Encryption



Attackers cannot get the proper data because they do not have the decryption key, the cipher

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encryption

Decryption

Ciphertext and decipher key = Data

User

// 01000001 is the character “A” in binary

// binary substract

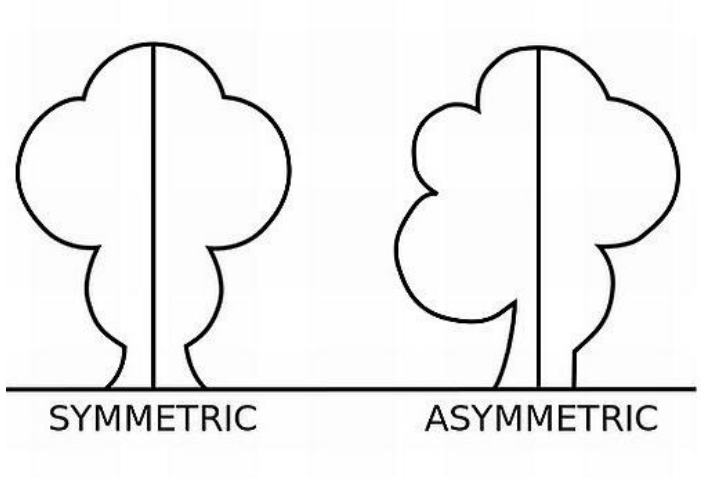
01000010 – 1 = 01000001

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encryption

There are 2 types of encryption

Symmetric and Asymmetric

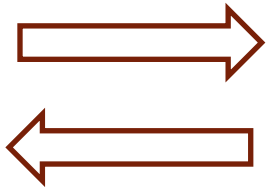


Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encryption

Symmetric Encryption

Server



End-point

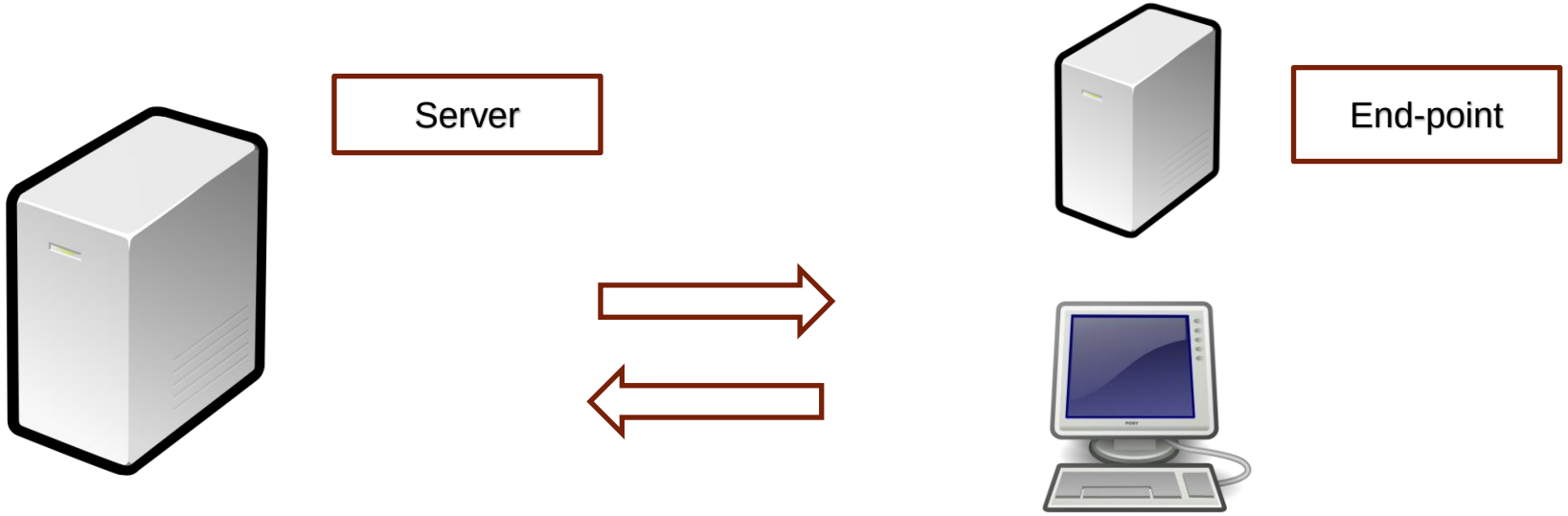
Server uses SAME KEY

Endpoints uses SAME KEY

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encryption

Asymmetric Encryption



Server has Public Key and private key

Endpoints has Public key only

*can have other variations

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encryption

Important <u>Asymmetric</u> Encryption in web tech

RSA Algorithm

MATH!

Here is an example of RSA encryption and decryption. The pa

1. Choose two random prime numbers.
2. :$p = 61$ and $q = 53$;Compute $n = pq$
3. :$n = 61 * 53 = 3233$
4. Compute the totient $\phi(n) = (p-1)(q-1)$
5. :$\phi(n) = (61-1)(53-1) = 3120$
6. Choose $e > 1$ coprime to 3120
7. :$e = 17$
8. Choose d to satisfy $de \bmod \phi(n) \equiv 1$
9. :$d = 2753$
10. :$17 * 2753 = 46801 = 1 + 15 * 3120$.

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Encryption

BLOCKCYBER

Other important encryption standards to know:

Wired Equivalency Privacy (WEP) – 1990s
Advanced Encryption Standard (AES) – 2001
Wi-Fi Protected Access (WPA) – 2003
Wi-Fi Protected Access 2(WPA2) – 2004
Wi-Fi Protected Access 3(WPA3) – 2018

Copyright of BlockCyber Pte Ltd. All rights reserved

Cryptography tools

Cryptography tools

There are many tools we can use.

We will look at OpenSSL

OpenSSL
Cryptography and SSL/TLS Toolkit

Copyright of BlockCyber Pte Ltd. All rights reserved

Cryptography tools

OpenSSL can help us encrypt and decrypt data.

```
openssl help
```

```
Cipher commands (see the `enc' command for more details)
aes-128-cbc        aes-128-ecb        aes-192-cbc        aes-192-ecb
aes-256-cbc        aes-256-ecb        aria-128-cbc       aria-128-cfb
aria-128-cfb1      aria-128-cfb8      aria-128-ctr       aria-128-ecb
aria-128-ofb       aria-192-cbc       aria-192-cfb       aria-192-cfb1
aria-192-cfb8      aria-192-ctr       aria-192-ecb       aria-192-ofb
aria-256-cbc       aria-256-cfb       aria-256-cfb1      aria-256-cfb8
aria-256-ctr       aria-256-ecb       aria-256-ofb       base64
bf                 bf-cbc             bf-cfb             bf-ecb
bf-ofb             camellia-128-cbc   camellia-128-ecb   camellia-192-cbc
camellia-192-ecb   camellia-256-cbc   camellia-256-ecb   cast
cast-cbc           cast5-cbc          cast5-cfb          cast5-ecb
cast5-ofb          des                des-cbc            des-cfb
des-ecb            des-ede            des-ede-cbc        des-ede-cfb
des-ede-ofb        des-ede3           des-ede3-cbc       des-ede3-cfb
des-ede3-ofb       des-ofb            des3               desx
rc2                rc2-40-cbc         rc2-64-cbc         rc2-cbc
rc2-cfb            rc2-ecb            rc2-ofb            rc4
rc4-40             seed               seed-cbc           seed-cfb
```

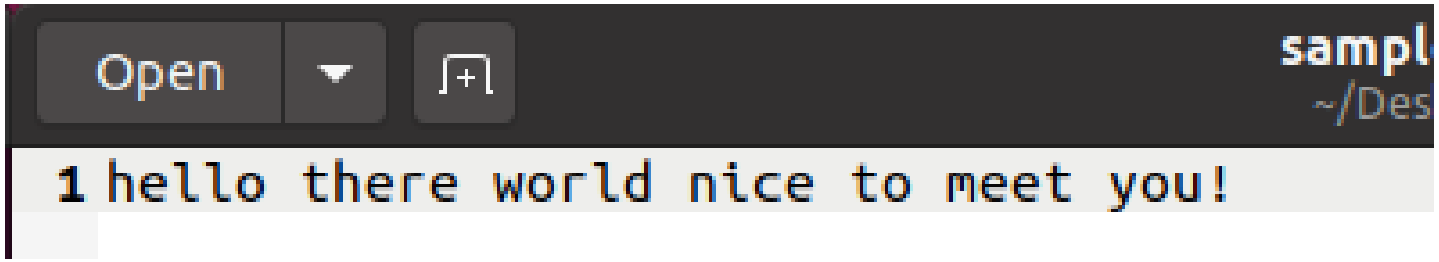
List of ciphers that we can use to encrypt

Copyright of BlockCyber Pte Ltd. All rights reserved

Cryptography tools

Let’s say we have a text file with some words in it, called plaintext.txt.

We want to encrypt it to keep the data safe.



Copyright of BlockCyber Pte Ltd. All rights reserved

Cryptography tools

We choose a cipher that we want and choose the output file name.

Let's choose **aes-256-cbc** and let's choose a password **lab**.

```
# Check for ciphers we can use
openssl list -cipher-algorithms
```

```
# encryption command
openssl enc -k lab -AES-256-cbc -e -in plaintext.txt -out
encrypted.txt
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Cryptography tools

BLOCKCYBER

What does the commands mean?

```
# encryption command
openssl enc -k lab -AES-256-cbc -e -in plaintext.txt -out output.txt
```

Use enc function of openssl

-k is for password (optional)

Cipher we choose

-e for encrypti on

-in and –out for input filename and output filename

Copyright of BlockCyber Pte Ltd. All rights reserved

Cryptography tools

Let’s look at the new encrypted text file!

*Salted__ indicates the use of a password

```
1 Salted__82 81ºAÃ98 7 82é 8E 8E2ÅèõÚÞt 15ÿ 93 88Ü'~Ë:    âhà,âWQŸ` 97 8C 8EË 95úÜ 8E 17ôë 8EJçóà&2Ö
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Cryptography tools

BLOCKCYBER

Let's decrypt!

```
# encryption command
openssl enc -k lab -AES-256-cbc -d -in encrypted.txt -out
decrypted.txt
```

Use enc function of openssl

-k is for password (optional)

Cipher we choose

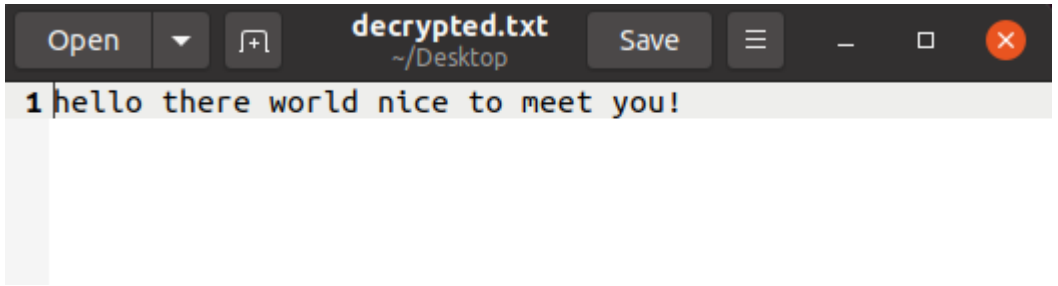
-d for decrypti on

-in and –out for input filename and output filename

Copyright of BlockCyber Pte Ltd. All rights reserved

Cryptography tools

We get back the original data!



Copyright of BlockCyber Pte Ltd. All rights reserved

Cryptography tools

Cipher strength

AES-256 is the current strongest.

We can estimate that it takes 1 billion-billion years to crack a AES-128 key with current computing power

https://www.eetimes.com/how-secure-is-aes-against-brute-force-attacks/#

Copyright of BlockCyber Pte Ltd. All rights reserved

Cryptography tools

We can encrypt all kinds of files with this method, like pictures, videos etc.

Copyright of BlockCyber Pte Ltd. All rights reserved

Hashing

Intro to cryptography: Hashing

Hashing

Data and hash function = hashed-data(called Checksum)

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Hashing

BLOCKCYBER

Hashing

Hashing is a one way function that cannot decrypted. This is commonly used to protect passwords, or check for data integrity.

There are a few common hashing algorithms:

- MD5
- SHA-2
- CRC32

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Hashing

Scenario

Downloading install file for games online.

Official site has a download file, a checksum, and hashing method.

The checksum is 28EDujsakO

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Hashing

Hashing

Checking for data integrity:
File A is official copy.
File B is my copy.

File A -> hash = 28EDujsakO
File B -> hash = 28EDujsakO

File A and File B is the same! Safe to use!

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Hashing

Hashing

Checking for data integrity:
File A is official copy.
File B is my copy.

File A -> hash = 28EDujsakO
File B -> hash = 28EDujsakP

File A and File B is not same! Data is suspicious!
不安全！

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Hashing

BLOCKCYBER

Hashing

Not just for files downloaded on the internet.

Networks and applications check and confirm data integrity with hashes all the time!

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Hashing

Example:
Using OpenSSL to verify the data.

Previously, we have the encrypted data. We want to share the data with our friends, and we want to make sure that the file our friends downloaded is the same file that I have.

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Hashing

Example:
Using OpenSSL to verify the data.

```
openssl dgst -md5 encrypted.txt
```

```
administrator@lab:~/Desktop$ openssl dgst -md5 encrypted.txt
MD5(encrypted.txt)= ea69919de8109330b9fb57e82ee4137f
administrator@lab:~/Desktop$
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Hashing

Example:
We will tell our friends that we have
ea69919de8109330b9fb57e82ee4137f
as the correct hash.

Our friends can then use the same method to verify the MD5 hash of the file they have received.

If the hash is different, then we know that the file has been modified in some ways.

```
openssl dgst -md5 received_file.txt
```

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Hashing

BLOCKCYBER

In web applications, passwords are saved as hashes.

This is for security's sake.

However, we often still hear that passwords are still saved in plaintext on lousy made apps.

Copyright of BlockCyber Pte Ltd. All rights reserved

Intro to cryptography: Hashing

Popular types of hashes

MD5
SHA-256

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)
MD5 (as reference)		128	128 (4 × 32)	512
SHA-0		160	160 (5 × 32)	512
SHA-1				
SHA-2	*SHA-224* *SHA-256*	224 256	256 (8 × 32)	512
	SHA-384 *SHA-512*	384 512	512 (8 × 64)	1024
	SHA-512/224 *SHA-512/256*	224 256		
SHA-3	*SHA3-224* *SHA3-256* *SHA3-384* *SHA3-512*	224 256 384 512	1600 (5 × 5 × 64)	1152 1088 832 576
	SHAKE128 *SHAKE256*	*d* (arbitrary) *d* (arbitrary)		1344 1088

How hashed passwords are attacked

Attacking hashed passwords

Rainbow Table attack

Generate list of hashes to match with the password hash.

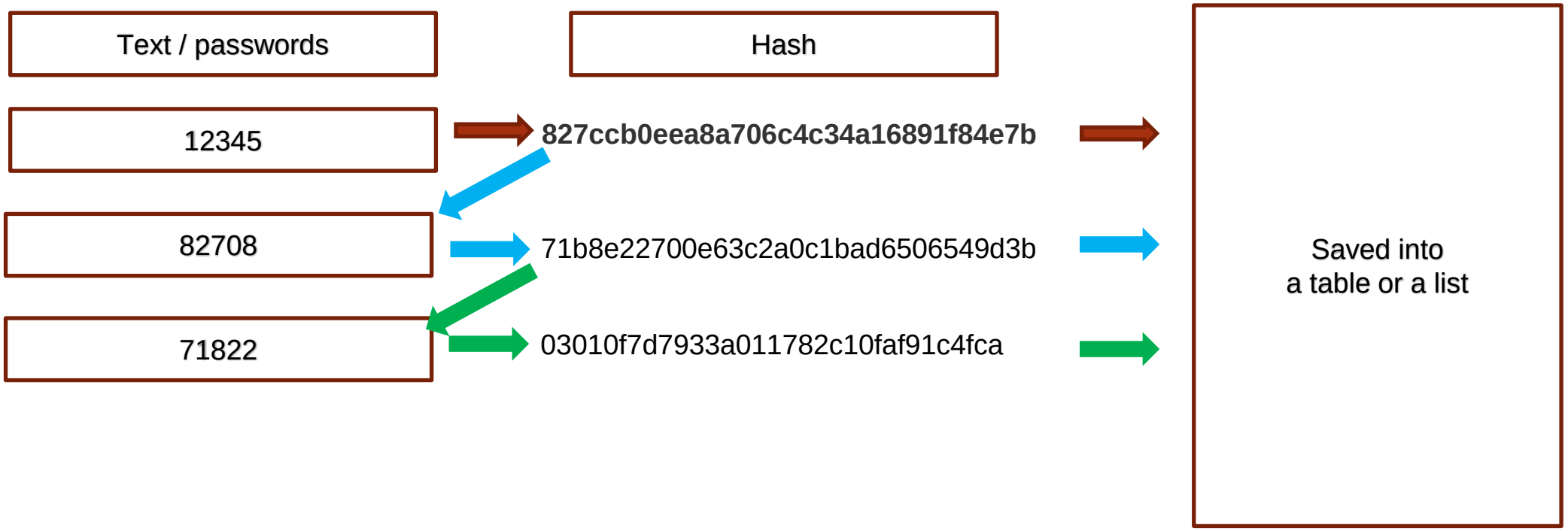
CASE: A web app that saves only 5 digit numerical data for passwords

- For example, 12345, 49732
- Hashing Function MD5

Copyright of BlockCyber Pte Ltd. All rights reserved

Attacking Hashed passwords

RT Attack(**MD5 hash, reduction function** -> take first 5 integer)



Copyright of BlockCyber Pte Ltd. All rights reserved

Attacking Hashed passwords

Rainbow Table attack:

If we have the hashed password, we can just compare it to our hash table.

Copyright of BlockCyber Pte Ltd. All rights reserved

Attacking Hashed passwords

BLOCKCYBER

Fast and efficient compared to brute forcing attack(i.e. testing from 00000 to 99999).

Less processing power but needs more storage space for large tables.

If 2 users have the same password,
The 2 hashes will be the same!

Copyright of BlockCyber Pte Ltd. All rights reserved

Defending against Rainbow Table attack

BLOCKCYBER

Password salting

Salt = time now (HHMM)
e.g. 10.21pm => 2221
Password = 12345

Admin sets password at 10.21pm

12345 → 123452221 → 6147e0f00b30355cfa4f2f64f684d418

User B sets password at 9.32am

12345 → 123450932 → 0d3615fb21d56334e8b6d6cd3371eba4

Copyright of BlockCyber Pte Ltd. All rights reserved

Defending against Rainbow Table attack

BLOCKCYBER

Password salting
Same password, different hash
Harder for rainbow tables to attack because of the added salt

Salt and Reduction function can any condition

Salt is saved along with the hash into the database in plain text

Copyright of BlockCyber Pte Ltd. All rights reserved

Steganography

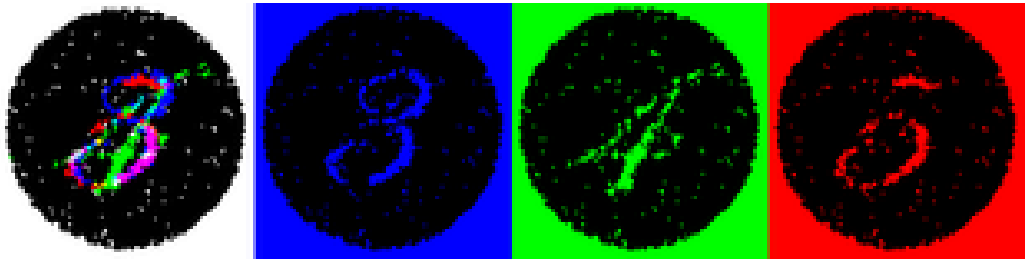
Steganography

Content
What is Steganography
Types of Steganography
Digital representation of images(RGB)
Least-Significant Bits(LSB) Steganography
LSB demonstration with Python

Steganography

What is Steganography?

It is the practice of concealing data in all sorts of media.
e.g. an image hidden in another image



BLOCKCYBER

Steganography

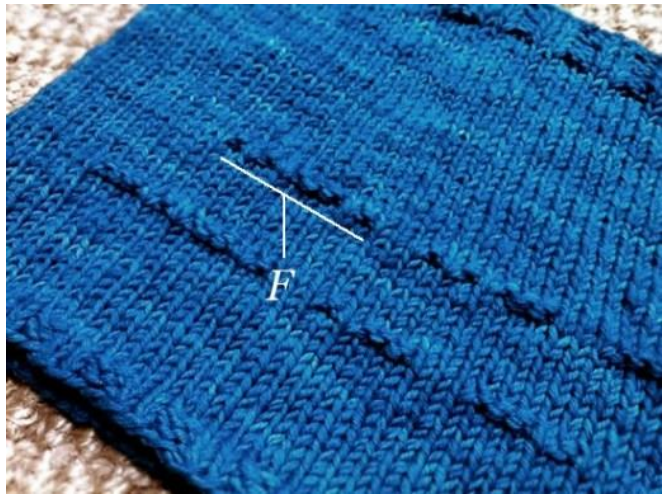
Instead of encrypting messages with ciphers or hashes, the messages are hidden within other messages, looking **unsuspicious**.

H T T P
T E L N
R S L A
H T T P

Steganography

Physical Steganography

Morse code on yarn
Invisible Inks
Sign Language in photos
Blinking morse code in video

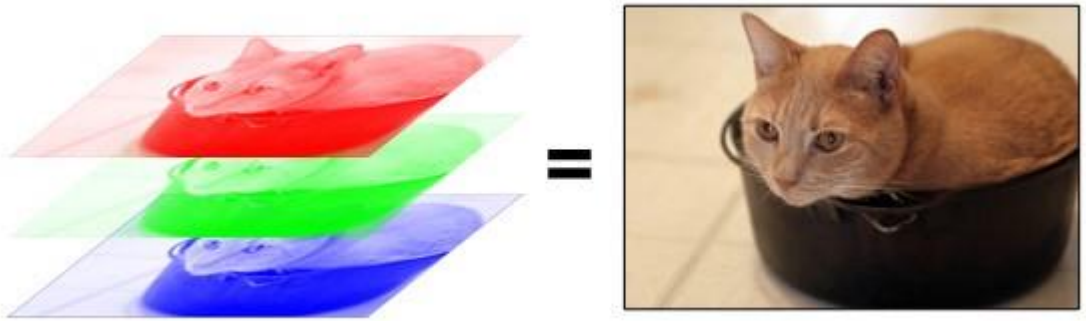


Steganography

Image Steganography – Least Significant Bits(LSB) Steganography

Digital Steganography – Images

Digital raster images are made of pixels. And to add color, each pixels has 3 values: **Red**, **Green** and **Blue**.

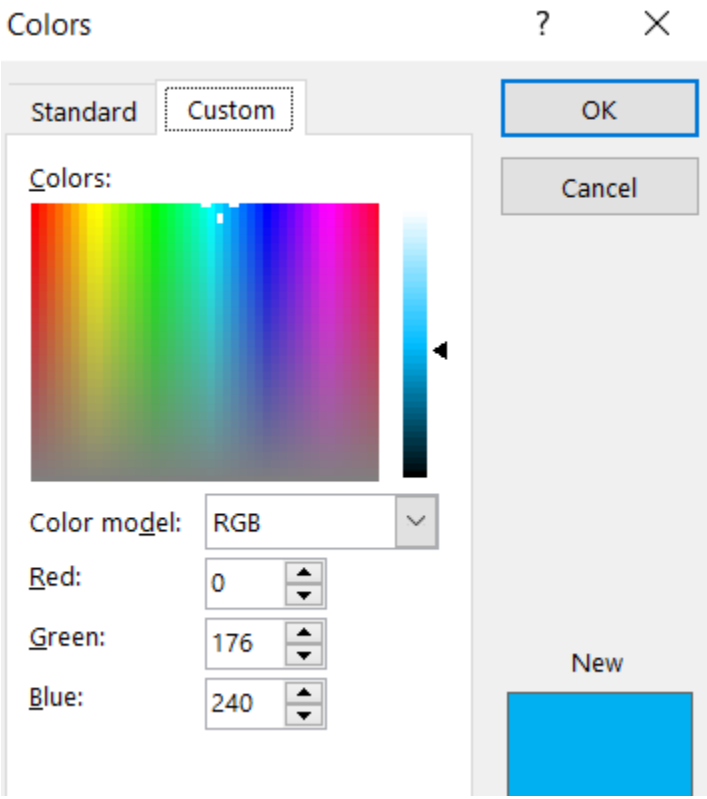


Steganography

Digital Steganography – Images

Each pixel is represented by RGB(0-255,0-255,0-255)

RGB(0,176,240)



Steganography

Digital Steganography – Images

Each color is represented by 8-bit data

Red = 0000 0000

Green = 10110000

Blue = 11110000

	128	64	32	16	8	4	2	1
Binary	1	0	1	1	0	0	0	0

128 + 32 + 16 = 176

Steganography

Combining 2 images

Img 1 pixel

Img 2 pixel (to hide)
(112,48,180)

Steganography

Img 1 pixel

R(0000 0000)
R(1011 0000)
B(1111 0000)

Img 2 pixel

R(0111 0000)
R(0011 0000)
B(1011 0100)

Img 3 merged pixel

R(0000 0111)
G(1011 0011)
B(1111 1011)

Steganography

Img 1 pixel

Img 2 pixel

Img 3 merged pixel

R(7)
G(179)
B(251)

Steganography

We have successfully hidden image 2 into image 1.

There is a slight only difference in the pixel color
Can you tell which is which?

Steganography

Let’s extract the hidden image in image 3 We will take out the least significant bits (last 4 bits)

(0000 0111)
(1011 0011)
(1111 1100)

(0111 0000)
(0011 0000)
(1100 0000)

R(112)
G(48)
B(192)

Extracted pixel

Steganography

There is only a slight change in color.

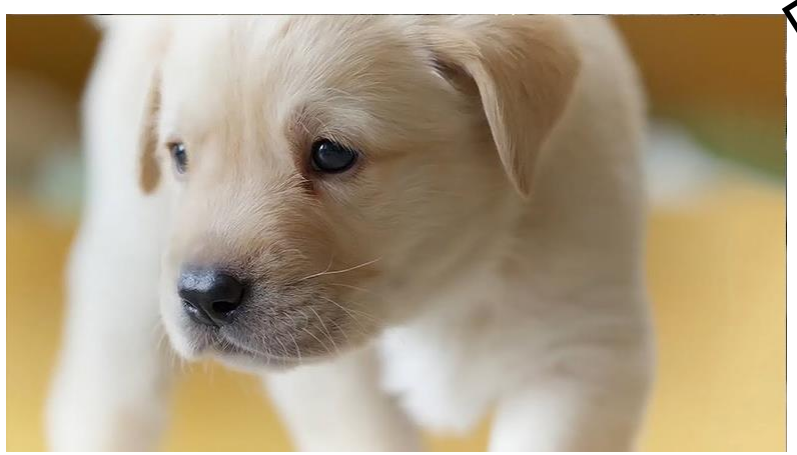
Img 2 pixel

Extracted pixel

Steganography

Can you spot the difference?

Merge



Extracted

Steganography

BLOCKCYBER

Steg vs Crypto

Steganography hides the data in plain sight, will not arouse suspicion.

Why not use both together to secure some information?

Steganography

BLOCKCYBER

Steg tools

- OpenSteg
- StegoSuite
- Xiao Steganography
- Not many stego tools from trusted sources just yet