The Command Line

Tuesday, April 8, 2025   11:58 PM

Command Line Interface (CLI): a scary black and white screen with a bunch of lines. Unfortuna

How to access with macOS: Open your Applications > Utilities folder and find “Terminal”. You c
Press Cmd + Space to open Spotlight, and search for “Terminal”. Press Enter to open it.

Programmers are lazy. CLI Shortcuts:

- Cmd C and Cmd V
- Tab completion
- Opening project folders/files in one go with "."

```
git add . // adds all files in a directory to the staging area
```

- "code" to open vscode from command line

To change default shell from Zsh to Bash:	chsh -s /bin/bash	// this is what I currently have r

- Other way around: chsh -s /bin/zsh

To ensure we start in home directory on the CLI:	cd RETURN

Unix Shell -> The Unix shell is both a command-line interface (CLI) and a scripting language

- Most popular Unix shell is Bash (the Bourne Again Shell)
- ‘Git Bash’ is a piece of software that enables Windows users to use a Bash like int
- I have a Mac though so idc
- Mac shell prompt: %

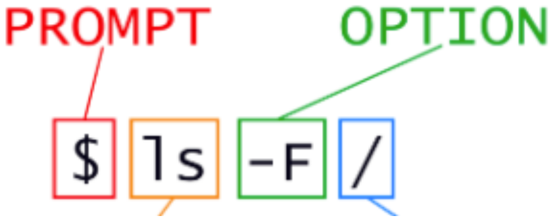
Shell: a program whose primary purpose is to read commands and run other programs
File system: part of the operating system responsible for managing files and directories

tely, it's also an indispensable skill.

an also use Spotlight search to open Terminal.

ow!

erface when interacting with Git.



/ before a folder implies that this folder is directly inside the home directory (ex /Users)

Most Common Commands: general syntax of a shell command -->

Command	Function	Note
`Ls`	Lists contents of current directory	Lots of
`Ls -F`	Classify listing output by adding a marker (in note)	• a trai • `@` indi • `*` indi
`Ls -R`	Lists all subdierctories within a given directory	Can do
`Ls --help`	Can be passed to any command	
`Man ls`	Read command's manual	To quit
`Pwd`	Prints working directory	
`Clear`	Clears terminal	Up and
`Cd`	Change directory (.. To move up/back a level)	Cd - to
`~`	Current user's home directory	
`Mkdir`	Creating a directory in current working directory	
`Mkdir -p ..`	Create dir and subdir in one operation	mkdir -
`Nano`	Creates a plan text document	nano w
`Touch`	Creates new files from terminal in current dir	
`Rm`	Removing a specified file	rm wor
`Mv`	Moving files - 1st cmd is what, 2nd is where	mv the
`Cp`	Copying file (similar to mv)	Recursi
`Wc`	Word count, bytes, etc	

Shell Wildcards

Command	Function	Note
*	Wildcard of any length	*.pdb = any file th

possible -? options for many cmds
ling / indicates that this is a directory icates a link icates an executable
ls -FR in one go, and others
man page, press q
down arrows for previous cmds
move to previous directory (not back)
p ../project/data ../project/results
ords.txt
ds.txt (use rm -I for safety prompt)
sis/draft.txt thesis/quotes.txt
ve copying with cp -r for directories

at ends in .pdb

?	Wildcard of a single character, can be successive	???ane.pdb = thr

SSH Key Pairs

SFTP, or Secure File Transfer Protocol, is a network protocol that uses Secure Shell (SSH) to sec

In every SSH/SFTP connection, there are four keys (or two key pairs) involved.

- The SSH employs public key cryptography. A public-key cryptography, also known as asy algorithms which requires two separate keys, one of which is secret (private) and one of
- First key pair = host (server) key
- Second key pair = user (client) key

Key descriptions

1. User private key: secret key kept by the user, never reveal this to anyone for user identit
2. User public key: counterpart to ^, to allow user authorization on a server this key is regis
3. Host private key: generated when the server is set up, accessible by server admin only - u
4. Host public key: counterpart to ^, user should be provided with this key in advance to co connection and then it's registered automatically for further connections

Asymmetric Encryption

Encryption in a nutshell: taking a message and scrambling it so only certain people can read you

- Two types: sym and asym

Symmetric	Uses the same key to encrypt and decrypt the data	Problem? Security iss
Asymmetric	Aims to solve this issue using two key-pairs	Generated using the R

RSA Algorithm: basis - easy to multiply prime numbers, but deriving factors of large numbers is

1. *Key Generation:*

- Choose two large prime numbers (p and q): These primes must be kept secret.
- Calculate n (the modulus): $n = p * q$.
- Calculate the totient function ($\phi(n)$): $\phi(n) = (p-1) * (q-1)$.
- Choose an integer e (the public exponent): $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$ (e and $\phi(n)$ a
- Find the modular multiplicative inverse of e modulo $\phi(n)$, which is d (the private exponent

ree single letter wildcards (cubane.pdb, etc)

urely transfer files between a client and a server

mmetric cryptography, is a class of cryptographic
which is public. Together they are known as a key pair.

y safety
tered - can be revealed to anyone
user does not need to care abt this
nnection - typically user is prompted for this on first

ur message

ues and risk of external interception
RSA algorithm

difficult (encrypt good, decrypt hard!)

re relatively prime).
t) e * d = 1 (mod l(n))

- Find the modular multiplicative inverse of e modulo φ(n), which is d (the private exponen
    - Public key: (n, e).
    - Private key: (n, d).

2. *Encryption*:

- Convert the plaintext message (m) to a number (m < n):
- Calculate the ciphertext (c): c = m^e mod n.

3. *Decryption*:

- Calculate the plaintext (m): m = c^d mod n.

Key-Pair features: although the keys are linked, they aren't derivable - you can't get the private

- Mailbox address = public key, mailbox key = private key

Ex: sending a file over email with asymmetric encryption

Action	Analogy
A encrypts the file with B's public key	A sends a letter to B's ma
A sends it to B, and B uses his private key to unlock the file	B uses his private mailbox

Strength of encryption depends on security of private keys- but even A's private key cannot de

Some YT comment:

The part that was really confusing me was that EVERYONE has a public key that they give out to want to send me encrypted data? Here take my public key and use it to encrypt the data. Now s data, I will use my private key to decrypt it. Very straight forward.

nt): $e * d \equiv 1 \pmod{\varphi(n)}$.

key from the public

ilbox address
x key to unlock the mailbox and retrieve A's letter

crypt messages meant for B.

o anyone who wants to send them encrypted data. Hi, you send me the encrypted data. Now I have the encrypted