15-110 Quiz4 Notes Sheet

Levels of Concurrency

CPU: a piece of hardware that runs the actions taken by a program

Circuit-level Concurrency: run concurrent actions on a single CPU by running multiple simple circuits at the same time
Multitasking: alternate rapidly between programs on a single CPU to simulate concurrency
Multiprocessing: run multiple programs concurrently on multiple CPUs on the same computer
Distributed Computing: run multiple programs concurrently on multiple computers that are connected together

Concurrency tree: a tree that represents how an expression can be broken down into individual actions, and how those actions can be organized to minimize time spent computing. The leaves are initial values, the root is the final result.

Total steps: the actual number of steps taken in a concurrent process
Time steps: the number of concurrent steps taken by a concurrent process

Parallel Programming

Design difficulty: you have to figure out how to split up steps in a program so they can happen concurrently
Resource sharing: two programs that run concurrently might both want to access the same resource. Resolved using locks.
Deadlock: occurs when 2+ programs are both waiting on resources that one of the other programs in the group already has

Pipelining: make an algorithm concurrent by splitting the process into steps. Each step is assigned to one worker (CPU), data is passed between CPUs.

MapReduce: make an algorithm concurrent by splitting the data into many smaller datasets.
Mapper: part of MapReduce. Takes a small piece of data, processes it, and returns a result.
Reducer: part of MapReduce. Takes a collection of results and processes them into the final result.
Manager: part of MapReduce. The manager moves data through the system and outputs the final result.

How the Internet Works

Browser: program that receives data from the internet and displays it as a webpage
Router: a device that can send data to other machines connected to it via cables. Routers form the core of the internet.
ISP: a service that connects individuals' computers to the internet
IP Address: a series of numbers that forms the 'real name' of a computer. Can be used to find a computer on the internet
DNS Server: a computer on the internet that can map URLs to IP Addresses.
Protocol: a standard for communicating information between machines. Examples include HTML and HTTP.
Packet: a small piece of data that is sent from one computer to another across the internet. Has sender, receiver, and data.
Fault tolerance: the internet is designed to be error-tolerant by being decentralized with many redundancies.

15-110 Quiz4 Notes Sheet

Authentication and Encryption

Data Privacy: we may want to have control over who has access to our data and what others do with it
Data Security: we may want to keep some communications accessible only by the sender and receiver

DDOS: a security attack where a server is overwhelmed by a large number of messages, which blocks regular traffic
Man-in-the-middle: a security attack where a router intercepts data that passes through it to read and/or change it

Authentication: a process to verify someone's identity. Can be done with passwords and certificates.
Encryption: a process to encode data so that only the sender and receiver can read it. Original messages are plaintext; encrypted messages are ciphertext.

Key: a piece of information used to encode a message. Keys can be symmetric (known by both parties) or asymmetric (split into public/private parts)

Encrypt: take plaintext and change it with a key into ciphertext.
Decrypt: take ciphertext and change it back to plaintext using the key.
Break: an attempt to decipher plaintext out of ciphertext without the key

Caesar Cipher: an encryption algorithm where you shift each letter by a set amount. The shift amount is the key.

RSA: an encryption algorithm where you raise the message to a power e and mod by n to encrypt, then raise it to a power d and mod by n to decrypt. Uses asymmetric keys. Public key is (e, n); private key is (d, n).

Keyspace: the number of possible keys that could be used to encrypt a message. Represented as a power of 2 (power is # bits needed to represent key). Caesar Cipher has a keyspace of 2^5; RSA has a keyspace of 2^b.

Managing Large Code Projects

```
f = open(fname, mode) # open file
f.read() # read contents as string
f.readlines() # read list of lines
f.write(text) # write text to file
f.close() # close file when done
```

```
try:
    # try body
except:
    # what to do if error raised
```

Helper functions: when given a complicated task, break it into subtasks and assign each subtask to a separate function to simplify the program.

Learning about Libraries

External library: a library outside of the main Python language that can be installed into Python.
Documentation: instructions on how to use a library available online. Describes existing functions and what they do.

```
pip install name
```