15-110 Hw5 - Written Portion

Name:

AndrewID:

#1 - Simultaneous Execution - 6pts

Which of the following concepts does **NOT** involve running multiple tasks at exactly the same time?

- ❑ Circuit-level concurrency
- ❑ Multitasking
- ❑ Multiprocessing
- ❑ Distributed Computing

For each answer you select, write up to 20 words about what that concept does instead.

#2 - Concurrency Tree - 5pts

How many steps would it take to compute 10! concurrently?

#3 - Multiprocessing - 6pts

Explain 2 ways multiprocessing can improve how quickly programs seem to run on a computer.

Explain 2 reasons why multiprocessing can be a challenge to implement.

#4 - MapReduce - 8pts

Suppose we implement a MapReduce task to compute how many words in a collection of files have the string "the" in them (e.g., "them"). Describe at a high level what the mapper function would input and output (not the algorithm for the function), what the collector function would do, and what the reducer would input and output.

Mapper:

Collector:

Reducer:

#5 - The Internet - 6pts

List 3 reasons covered in lecture that your web browser may not be able to display a website that you type in. In other words, what are 3 things that could go wrong when your browser goes to retrieve a website.

1.

2.

3.

#6 - Websites in your Browser - 2pts

How is a website sent across the internet to your web browser?

- ❑ The server creates a packet of the whole website and sends it as fast as possible to your browser
- ❑ The server zips up the website to make it as small as possible so none of the data gets lost
- ❑ The server splits the website into packets and makes sure they all get there in the right order
- ❑ The server creates packets and sends them all to your browser, which puts them in the right order

#7 - Security Attacks - 6pts

Identify the correct meaning(s) of each security attack. Select all that apply.

In a Distributed Denial of Service (DDOS) attack, the attacker does the following to overload the server and make the server stop replying to data requests:

- ❑ Sends a really large message
- ❑ Sends many many messages
- ❑ Sends a bad data request
- ❑ Sends a request for a lot of data

In a Malware attack, the attacker writes a program that:

- ❑ Infects your home computer and sends back your usernames and passwords
- ❑ Deletes computer data so that you can't use it any more
- ❑ Encrypts your data and holds it hostage until you pay
- ❑ Hides in a PDF or other popular format so you are likely to open it

In a Man in the Middle attack, the attacker:

- ❑ Writes a virus that listens to data passed between your operating system and regular programs
- ❑ Listens on computer networks for unencrypted usernames and passwords or other data
- ❑ Runs on distributed systems to listen for unencrypted data passed between programs

#8 - RSA Encryption - 5pts

Prof. Rivers wants to send Prof. Rosenthal a message encrypted using RSA encryption. What would Prof. Rosenthal have to do in order so that Prof. Rivers can encrypt a message that she can then decrypt?

#10 - The Cloud - 6pts

The benefits of cloud software are that it is commoditized and remotely hosted. Define the two terms in 20 words or less (each).

Commoditized:

Remotely Hosted:

Programming Problems

Each of these problems should be solved in the starter file available on the course website. They should be submitted to the Gradescope assignment Hw5 Full (Programming) to be autograded.

Part A - Caesar Cipher

Encryption: A caesar cipher shifts the characters in a string by a set amount. For example, a shift of 5 would mean all a's would become f's, b's become g's, and z's would become an e's, because we shift the value back around. All characters that are not letters should not be shifted for this assignment.

Decryption: To decrypt a Caesar Cipher, you would need to know the shift and reverse it. However, this shift could be easily stolen. One can repeatedly shift the encoded string over and over and look for common words that appear. For example, the word "the" is a short word and very common. If we find many instances of common words, we probably have the right shift.

caesar_encrypt(string,shift) - 10pts
Write a function caesar_encrypt(string,shift) that takes a string of characters and an integer shift between 0-25, makes the string lowercase, and returns a new string with the letters shifted and all other characters left alone. For example:
caesar_encrypt("The dog jumps over the fox.",4) returns "xli hsk nyqtw sziv xli jsb."

Note 1: you should be using ord(letter) to get the ASCII value of a letter and chr(int) to get the letter associated with an ASCII integer.

caesar_decrypt(string) - 10pts
Write a function caesar_decrypt(string) which takes a string of letters and spaces and repeatedly shifts the message until the string "the " appears in the string, which means it is decrypted. Then return this decrypted message. For example:
caesar_decrypt("xli hsk nyqtw sziv xli jsb.") returns "the dog jumps over the fox."

Note 1: you should look for "the " including the space because it is possible for other words to include "the" in them when encrypted. For example, caesar_encrypt("drop",18) returns "thef" which includes "the" as a substring, but is not as popular a word.

Note 2: you may find it helpful to use caesar_encrypt() in your decrypt function.

Part B - Substitution Cipher

Generate Substitution List: If two people agree that they have encrypted messages to send each other, they can create a random shuffle (permutation) of all the letters in the alphabet and share it between them. This is the secret list that they will use to encrypt and decrypt their messages.

Encryption: When they have a message to send, for each letter of their message, if the letter is the i'th letter of the alphabet, they'll substitute in the i'th letter of their secret list.

Decryption: When receiving an encrypted message, they look in the secret list for the index of each letter of their message, and substitute it for the letter at that index in the normal alphabet.

generate_cipher_alphabet() - 10pts
Write a function generate_cipher_alphabet() which returns a list of letters that represents a random shuffle of the alphabet. You should use the function random.sample(alphabet,length) which takes a string containing each and every lowercase letter in the English alphabet and the length of that string, and returns a list of the letters in a random order.

substitution_encrypt(message,secret) - 10pts
Write a function substitution_encrypt(message,secret) that returns the cipher (encrypted string) of the message string encoded using the secret list. In particular, first make the message lower case and then for each letter of the message (if the letter is the i'th letter of the alphabet), substitute it for the i'th letter of their secret list. Any characters that are not letters should be kept the same.
For example: substitution_encrypt("The dog jumps over the fox.", ["e","f","g","h","i","j","k","l","m","n","o","p","q","r","s","t","u","v","w","x","y","z","a","b","c","d"]) returns "xli hsk nyqtw sziv xli jsb."

substitution_decrypt(cipher,secret) - 10pts
Write a function substitution_decrypt(cipher,secret) that decrypts the cipher string using the secret list and returns the original message. In particular, for each letter of the cipher (if the letter is the i'th letter of the secret list), substitute in the i'th letter of the original alphabet. Any characters that are not letters should be kept the same.
For example: substitution_decrypt("xli hsk nyqtw sziv xli jsb.", ["e","f","g","h","i","j","k","l","m","n","o","p","q","r","s","t","u","v","w","x","y","z","a","b","c","d"]) returns "The dog jumps over the fox."