15110 PRINCIPLES OF COMPUTING – EXAM 3A – SPRING 2014

1________________

2________________

3________________

4________________

5________________

6________________

7________________

TOTAL

Name Section

Directions: Answer each question neatly in the space provided.

Please read each question carefully. You have 50 minutes for

this exam. No electronic devices allowed. Good luck!

1. [12 pts] This question concerns generating random numbers.

Using the Python `randint` function, show how to compute the following using one Python expression, that is, without using assignments, loops, or anything other than function calls and arithmetic:

1a. [1 pt] A random integer between -5 and -1, including -5 and -1.

1b. [2 pts] A random **even** integer between 13 and 38, including 38.

1c. [2 pts] A random **odd** integer between 13 and 38, including 13

1d. [2 pts] A random integer between 1 and 31 that is a multiple of 7. Write one expression involving `randint`.

1e. [2 pts] A random string from the array `days` below. You are **not** allowed to use variables or any function other than `randint` from the module `random`.

```
days=["Sunday","Monday","Tuesday","Wednesday","Thursday","Friday","Saturday"]
```

For the next two questions, recall the linear congruential generator (LCG) formula:

$$x_{i+1} = (a \cdot x_i + c) \bmod m$$

As described in class, there are certain conditions that should be obeyed for the LCG to have its maximum period:

i. *c* and *m* must be relatively prime;
ii. *a*-1 must be divisible by every prime factor of *m*; and
iii. if *m* is divisible by 4, then *a*-1 must be divisible by 4.

1f. [2 pts] Consider only values of a and c that are less than m. If $c = 3$ and $m = 8$, what are the possible values of a that yield the maximum period?

1g. [1 pt]. What is the period obtained with any of your values for a above and $c = 3$ and $m = 8$?

2.[13 pts] This question concerns using randomness.

2a. [1 pt] Write a function called `fair_die()` that simulates rolling a fair die to obtain a number from 1 to 6 inclusive. With a fair die, the outcomes from 1 to 6 are equally likely. Assume that any necessary functions from the `random` module have been imported.

2b. [8 pts] Write a function called `loaded_die()`that simulates a loaded die that rolls a one 55% of the time; two, three, four, or five 10% of the time each, and six 5% of the time. Your function should return an integer. Assume that any necessary functions from the `random` module have been imported.

2c. [2 pts] Suppose you are assigned to write the code for a game that uses dice, but you are required to use a function `die()` whose code you cannot see. Describe in one or two sentences what method you would use to determine whether `die()` is a reasonable simulation of rolling a fair die.

2d. [2 pts] Name two common real-world uses for random numbers in computing, **not including games**.

3. [13 pts] This question concerns networking and the Internet.

3a. [2 pts] Which Internet protocol is used to provide "best-effort" packet-switching? Circle your answer.

TCP IP UDP SMTP

3b. [2 pts] What is the purpose of changing the IP addressing scheme between IPv4 and IPv6?

3c. [2 pts] A web browser needs to obey the HTTP protocol in order to transfer web pages. When the switch to IPv6 from IPv4 happens, do web browsers need to be reprogrammed? Explain. (Hint: think about the organizational principle of network protocols.)

3d. [2 pts] Here is a typical *Uniform Resource Locator* (URL) that identifies a web page:

```
http://arstechnica.com/author/jon-brodkin
```

Briefly (in one sentence) explain how the host name arstechnica.com is converted into an IP address.

3e. [2 pts] What service is provided by the TCP protocol in the Internet? Please limit your answer to one or two sentences.

3f. [2 pts] Where is a web cookie stored, on the client machine or the server machine?

3g. [1 pt.] Why do banking web sites need to use cookies for customer logins?

4. [12 pts] This question concerns cryptography.

4a. [8 pts] Alice and Bob want to communicate by encrypting messages using the RSA algorithm. Alice chooses the following values for her messages: decryptionkey d= 2179, encryptionkey e = 19, n = 4747. Suppose Bob wants to send the numerical message 15110 to Alice using RSA. Eve is the adversary trying to eavesdrop.

Which value(s) does Alice make public?

Why is it considered “secure” to make that value public?

When Bob creates the encrypted message to send to Alice, which key does he use?

If Eve gets a copy of Bob's encrypted message, which value does she need to factor into the product of two primes in order to determine Alice's decryption formula?

4b. [1 pt] We discussed encryption using one-time pads, which is considered to be unbreakable by cryptanalysis. Based on the lecture and your reading of Blown to Bits. State one of the reasons that make general use of one-time pads impractical.

4c. [2 pts] Briefly describe the difference between a symmetric encryption system and an asymmetric encryption system.

4d. [1 pt.] For what purpose do symmetric cryptographic systems use random number generators?

5. [20 pts] This question concerns simulation.

Recall the simulation for the spread of a flu virus in a population that we covered in the lecture. In the simulation code the constants HEALTHY, IMMUNE, and INFECTED represent, respectively, the healthy, immune, and infected states of an individual. The constants DAY1, DAY2, DAY3, and DAY4 represent the various stages of contagiousness.

5a. [4 pts] Define a function `contagious(matrix, i,  j)` that returns True if the individual at row i and column j is contagious, and False otherwise. Assume `i` and `j` are valid matrix indices.

5b. [6 pts] The following is a Python function to check whether the simulation has reached a state where the virus cannot spread any further because there is no one that is infected or contagious. Complete the function. Use the contagious function from part 5a for full credit.

```
def terminate(matrix):
    for i in ______________________________:

        for j in _______________________________:

            if ___________________________________________________:
                return False
    return True
```

5c. [10 pts] Suppose that we changed the simulation model from class so that a person gets infected 40% of the time if at least one of the north, south, east, and west neighbors is contagious, and the person is not immune. The function `get_infected(matrix, i, j)` below returns True if the person at row `i` and column `j` should get infected according to the assumption above and False otherwise. Fill in the blanks.

```
def get_infected(matrix, i, j):
    if matrix[i][j] == IMMUNE:
        return False
    infect = False
    # infected will be set to True if any neighbor is contagious
    if i > 0:
        if contagious(matrix, i-1, j):
            infected = True


    if i < _______________________________________:


        if _______________________________________:
            infected = True
    if j > 0:


         if ______________________________________:
            infected = True


    if j < _______________________________________:


         if ______________________________________:
            infected = True


    if __________________ and ______________________:
        return True
    return False
```

6. [20 pts] This question concerns concurrency.

```
# Assume stock is a global variable that is
# shared by multiple programs

def orderEC(quantity):
    if stock >= quantity:
        stock = stock – quantity
    else:
        print(“Out of stock”)
```

6a. [8 pts] Suppose that Store A and Store B both sell the book “Explorations in Computing” from a shared stock. They get an order request at the same time and two processes are run concurrently to handle the orders. Each process runs the `orderEC` function given above where `stock` is a shared variable that can be read and updated by both of the processes. Suppose that `stock` has value 60 initially. Store A makes a request to get 50 copies and Store B makes a request to get 30 copies. It is possible for both orders to complete **without** an “`Out of stock`” message even though the `stock` ends up with a value less than 0. Give one execution scenario that leads to this result.

6b. [7 pts] The programs below employ the idea of critical sections to deal with the race condition described in 6a. The call to `orderEC(quantity)`is treated as the critical section so that at most one process can be in its critical section at a given time. Assume that the variables `freeA` and `freeB` are shared across the two processes. When the two programs given below are executed concurrently they can end up in a deadlock. Explain how this could happen.

```
# Program run by Store A to keep
# track of inventory

while True:
    quantity = some_function
    freeA = False
    while not freeB:
        pass
    orderEC(quantity)
    freeA = True
```

```
# Program run by Store B to
# keep track of inventory

while True:
    quantity = some_function
    freeB = False
    while not freeA:
        pass
    orderEC(quantity)
    freeB = True
```

6c. [5 pts] If we graded this 7 question exam using 7 graders and pipelining such that each grader is assigned one of the 7 questions to grade and only grades that question throughout, how long would it take us to grade 200 exams assuming that each question takes 1 minute to grade? You can also assume that the questions are graded in order: Question 2 cannot be graded until question 1 is graded, and question 3 cannot be graded until question 2 is graded, and so on. Show your work.

7. [10 pts] This question concerns state space search.

Consider the game “21” (not the card game!) played by two players using the following rules for picking numbers:

- The first player picks 1, 2, or 3.
- Then the players take turns, increasing the previous number picked by 1, 2, or 3, not exceeding 21.
- The first player to pick 21 loses.

For example, a game might result in the following series of picks: 1, 3, 6, 9, 12, 14, 17, 20, 21 (and player 2 wins).

At any point in the game, the state can be represented by a number, recording the last number picked.

7a. [5 pts] Draw the game tree for the first two moves only. Represent the starting state of the game by the number 0.

7b. [1 pt.] How many nodes are on the next level of the tree?

7c. [2 pts.] What is the number of moves in the shortest game of “21”? How many nodes in the game tree are on that level?

7d. [2 pts.] Suppose we played a related game, “39”, where all the rules are the same except that 39 is the limit. Answer the previous question for this new game.