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.

Recall that the Python function `randint(0, n)` returns a random integer between 0 and n, inclusive. Using the `randint` function, show how to compute the following using one Python expression:

1a. [1 pt] A random integer between -5 and -1, including -5 and -1. **`randint(-5, -1)`**

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

`randint(7, 19) * 2`

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

`randint(6, 18) * 2 + 1`

1d. [2 pts] A random integer between 1 and 31 that is a multiple of 7. Write one expression involving `randint`. **`randint(1, 4) * 7`**

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[randint(0, 6)]`**

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

1f. [2 pts] 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.

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?

$a = 1$ or 5

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

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.

```
def fair_die() :
  return randint(1,6)
```

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.

```
def loaded_die():
  p = randint(0, 99)
  if p < 55 :
    return 1
  elif p < 65 :
    return 2
  elif p < 75 :
    return 3
  elif p < 85 :
    return 4
  elif p < 95 :
    return 5
  else :
    return 6
```

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.

Use a Monte Carlo method: call die() a large number of times and count the number of times each result is obtained.

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

simulation, Monte Carlo methods, cryptography/security

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

IP

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

To allow for more IP addresses

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.)

No, because the HTTP protocol is at a higher layer than the IP protocol, which handles addressing.

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.

A DNS server has a database of matching names and addresses and is queried for the address

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

Provide a reliable two-way stream of data / a "circuit"

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

Client

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

Because http is stateless, the server can't remember that the customer is logged in unless it stores a cookie on the customer's computer.

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? **19 , n = 4747**

Why is it considered "secure" to make that value public? **The message can only be decrypted with the secret decryption key 2179**

When Bob creates the encrypted message to send to Alice, which key does he use? (**19, 4747) the public encryption key**

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?

4747

4c. [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.

Two parties need a secure way to exchange or share one-time pads, which are as large as the secret messages to be exchanged.

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

In a symmetric encryption system the two parties share a secret key, which is used to encrypt and decrypt messages. In an asymmetric system different keys are used to encrypt and decrypt and only the decryption key needs to be secret.

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

To generate a secret key in an unpredictable way.

5. [20 pts] This question concerns simulation.

Recall the simulation for the spread of a flu virus in a population. 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.

```
def contagious(matrix, i, j):
    return matrix[i][j] ==  DAY1 or matrix[i][j] == DAY2 or matrix[i][j]
== DAY3 or matrix[i][j] == DAY4
```

Below answer is also acceptable because the constants DAY1 .. DAY4 are 2,3,4,5 in the code we showed in class.

```
def contagious(matrix, i, j):
    return matrix[i][j] >= DAY1 and matrix[i][j] <= DAY4
```

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. Use the contagious function from part 5a for full credit.

```
def terminate(matrix):
    for i in range(len(matrix)):
        for j in range(len(matrix[i])):
            if matrix[i][j] == INFECTED or contagious(matrix, i, j):
                return False
    return True
```

Also acceptable but for less credit since it does not use contagious

```
def terminate(matrix):
    for i in range(len(matrix)):
        for j in range(len(matrix[i])):
            if matrix[i][j] != IMMUNE and matrix[i][j] != HEALTHY:
                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 < len(matrix) - 1:
        if contagious(matrix, i+1, j):
            infected = True
    if j > 0:
         if contagious(matrix, i, j-1):
            infected = True
    if j < len(matrix[0]) - 1:
         if contagious(matrix, i, j+1):
            infected = True
    if infected and randint(0,99) < 40
        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.

Stock is initially 60. The execution may go as follows.

1. Store A checks and verifies that the stock is greater than 50.

2. Store B checks and verifies that the stock is greater than 30.

3. 50 is subtracted from stock. Stock becomes 10

4. 30 is subtracted from stock. Stock becomes -20.

6b. [7 pts] The programs below employ the idea of critical sections to deal with the race condition described in 5a. 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
```

Both processes can end up in a state where both freeA and freeB are false and wait in their while loops forever. This could happen, for example, when they strictly alternate their execution steps.

6c. [5 pts] If we graded this 7 question exam using 7 graders and pipelining such that each grader is responsible for grading a single question 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 the order 1, 2, ..7. Show your work.

199 + 7 = 206 minutes

The first exam in the pipeline is completed in 7 minutes. Then every minute, one of the remaining 199 is completed.

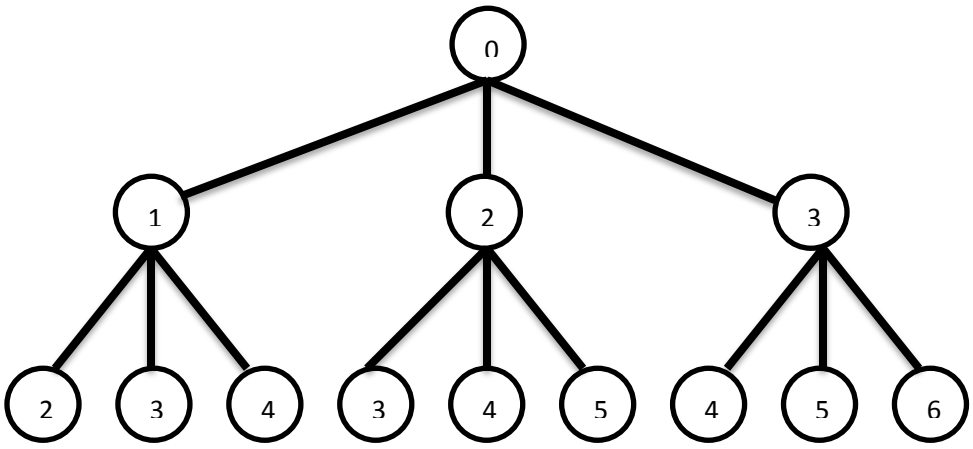
7. [10 pts] This question concerns state space search.

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.

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?

27 7c. [2 pts.] What is the number of moves in the shortest game of "21"? How many nodes are in the game tree at that level?

7 moves, 3^7 nodes 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.

13 moves, 3^{13} nodes