15110 PRINCIPLES OF COMPUTING – SAMPLE EXAM 3

1	_____
2	_____
3	_____
4	_____
5	_____
TOTAL	_____

Name _____ Section _____

Andrew ID _____

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. (20 pts)

(a) (4 pts) Match the layer from the TCP/IP reference model with its purpose.

(A) application layer _____ transmission between adjacent hosts

(B) internet layer _____ logical transmission of packets between two hosts

(C) link layer _____ logical connection between application processes

(D) transport layer _____ communication of the application

(b) (2 pts) Of the four layers specified above, which is the lowest layer? Answer: _____

(c) (2 pts) What protocol is used to turn names, such as www.cmu.edu, into IP addresses?
(A) HTTP (B) DNS (C) SMTP (D) SSH Answer: _____

(d) (4 pts) When a message is transmitted using TCP and is split into packets what two pieces of information must be stored in each packet (besides the data)?

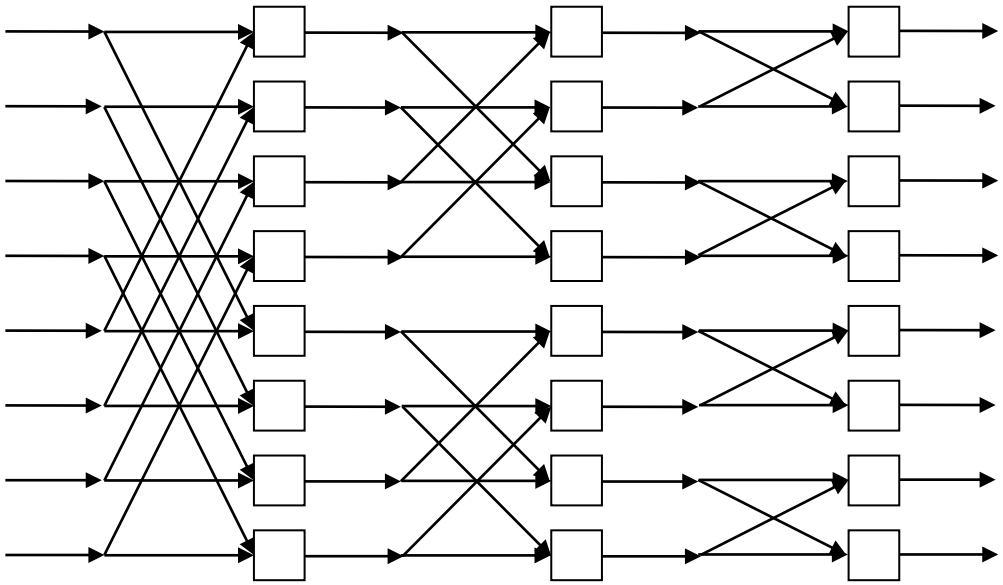
_____ _____

(f) (2 pts) Suppose you are creating a new application-layer network protocol and you want to rely on your requests reaching the server, would you layer your protocol on top of TCP or UDP (User Datagram Protocol)? Answer: _____

(g) (3 pts) In IPv4, a company is assigned addresses of the form 143.17.___.___.
How many unique addresses can the company use with this assignment? Answer: _____

(h) (3 pts) In IPv6, an address is given by eight 16-bit numbers usually written in hexadecimal. For example, here is an IPv6 address:
3001:0DE5:CA14:AD0F:0000:0000:0000:0000.
Suppose a company gets a set of IPv6 addresses of this form:
3001:0DE5:CA14:AD0F:152F:9AA1:E6__:____
How many unique addresses does this company get to use? Answer: _____

2. (20 pts) An 8-input butterfly network has the following structure:



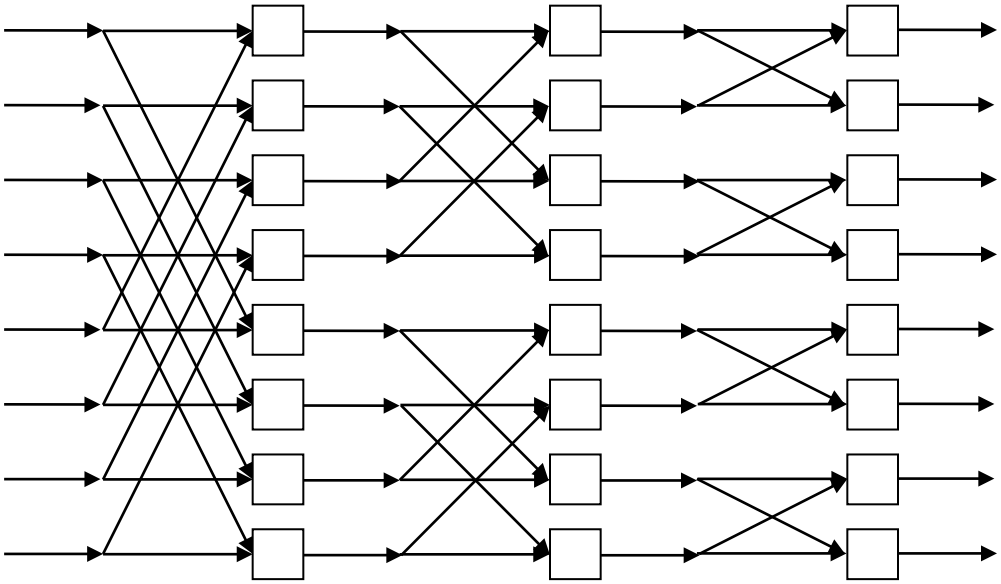
8 data values enter from the left side. Each data value is sent to two nodes. Once the node does its computation, its output is sent to two nodes to its right. The final results exit the network on the right. Butterfly networks are used for computations in signal processing.

(a) (2 pts) If the network operates sequentially (i.e. only one node at a time), and each node takes time t to do its computation, how long does it take to perform the entire computation for this network? _____

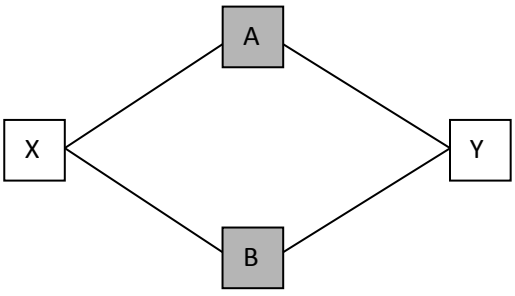
(b) (4 pts) If the network operates with maximum concurrency and each node takes time t to do its computation, how long does it take to perform the entire computation for this network? _____

(c) (4 pts) Based on your answer for part (b), if the network operates concurrently and is required to process 10 sets of 8 data inputs, how long does it take to process all of the data if pipelining is used? Show your work for maximum credit.

(d) (5 pts) Using the principle of *abstraction*, show to implement an 8-input butterfly network out of two 4-input butterfly networks by drawing two boxes on the diagram below to represent the two 4-input butterfly networks that would be used to build the 8-input butterfly network.



(e) (5 pts) In the simple circuit switching network below, there are two switches shown in gray, A and B, between two devices shown in white, X and Y. To establish a connection between the two devices, a switch must establish a connection with each of the devices, one at a time, to form a complete path between the devices. Once a switch establishes a connection with a device, it does not drop the connection until after a complete circuit is established. If a device is already connected to another switch, the switch waits until that pre-existing connection is dropped. Explain <u>in at most two sentences</u> how this network can become deadlocked.



3. (20 pts) This question deals with random number generators.

(a) (10 pts) Recall that the Python `randint(m,n)` function returns a random integer between `m` and `n`, inclusive. Using this `randint` function, show how to compute the following:

A random integer from the set {0, 1, 2, 3, 4, 5, 6, 7} _____
without storing these values in an array first.

A random integer from the set {7, 8, 9, 10, 11} _____
without storing these values in an array first.

A random integer from the set {-2, 0, 2, 4, 6, 8, 10, 12} _____
without storing these values in an array first.

A random integer from the set {1, 3, 9, 27, 81, 243} _____
without storing these values in an array first.

A random integer from the array below. _____

```
primes = [2, 3, 5, 7, 11, 13, 17, 19, 23, 27, 29]
```

(b) (10 pts) Let spin() be a helper function that simulates a game wheel and returns a random integer between 1 and 10 inclusive. Complete the function below that simulates a game of WHAM. In this game, a player spins the wheel until the player spins a 10. The function returns the maximum number that was spun before the 10 was spun. (If the player spins 10 on the first spin, the function should return 1.)

```
def spin():
    return randrange(_____,______)
def wham():
    maximum = ____________
    number = spin()
    while  _________________________________:
        if ____________________________________________:
            maximum = number
        number = ____________________________
   return maximum
```

4. (20 pts) The following question involves cryptography. For your convenience, the Vigenère table is given below.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	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
E	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
F	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	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

(a) (4 pts) Decode the following word that was encoded using a Caesar cipher. (HINT: The letter J decodes to a vowel.)

J Q J H Y N A J

___ ___ ___ ___ ___ ___ ___ ___

(b) (4 pts) The message PITTSBURGH is encoded using the Vigenère table and becomes the encoded message GCURJVVPXB. What keyword was used?

(c) (6 pts) From your reading in *Blown To Bits*, Alice uses a secret key to encrypt a message destined for Bob. Bob uses the secret key to decode the message. If an eavesdropper Eve intercepts the encrypted message, it should be hard for her to decrypt the message without knowing the secret key.

The following algorithm allows Alice to transmit the secret key to Bob without Eve being able to determine what it is. It depends on a function ○ that is a one-way function that is commutative (i.e. $x \circ y = y \circ x$) and associative (i.e. $x \circ (y \circ z) = (x \circ y) \circ z$).

1. Alice and Bob agree on a very large number g.
2. Alice chooses a random number a and tells no one.
3. Bob chooses a random number b and tells no one.
4. Alice calculates $A = g \circ a$.
5. Bob calculates $B = g \circ b$.
6. Alice sends A to Bob, and Bob sends B to Alice, on a public channel.
7. Alice then computes $B \circ a$, and Bob computes $A \circ b$.

Show that $B \circ a = A \circ b$.

Thus, the secret key Alice and Bob can use is $K = A \circ b = B \circ a$. Suppose Eve knows g and overhears A and B when Alice and Bob transmit them publicly. Why can't Eve determine their secret key K easily?

(d) (6 pts) Alice and Bob communicate using the RSA algorithm. Alice's public key pair is (e_A, n_A) and her private key pair is (d_A, n_A). Bob's public key pair is (e_B, n_B) and his private key pair is (d_B, n_B).

Bob wants to send message M to Alice.
Complete the following Python formula that Bob uses to compute
the encrypted message C that he wants to send to Alice:

C = (_____**_____) % _____

Complete the following Python formula that Alice uses to decrypt
the encrypted message from Bob to get the original message M:

M = (_____**_____) % _____

5. (20 pts) In a simulation of the spread of a flu virus among a population of 500 individuals, information about individuals' health is stored as integers in a 25x20 matrix using 4 for healthy (but not immune), 3 for infected (but not yet contagious), 1 or 2 for contagious, and 0 for immune. For the individual at column j of row i, the following code is used during each update to determine if the person becomes infected:

```
if healthy(matrix, i, j):
   for k in range(1,5) do
      # contact a random person in the matrix
      if contagious(matrix, randint(0,24), randint(0,19)):
         newmatrix[i][j] = 3
```

(a) (2 pts) Based on the code given above, how does a healthy (but not immune) person get infected?

(A) If at least one of four random individuals is contagious, the individual gets infected.
(B) If exactly one of four random individuals is contagious, the individual gets infected.
(C) If exactly four random individuals are contagious, the individual gets infected.
(D) None of the above.

Answer: _____

(b) (2 pts) Based on the code given above, can a healthy individual get infected by contacting himself/herself? Yes or no? Answer: _____

(c) (4 pts) Write a Python function `healthy(matrix, i, j)` that returns true if and only if the individual in column j of row i is healthy (but not immune). Otherwise, it returns false.

(d) (4 pts) Define a Python function `contagious(matrix, i, j)` that returns true if and only if the individual in column j of row i is contagious. Assume `i` and `j` are valid matrix indices.

(e) (4 pts) **[CORRECTION}** Complete the following statement that sets an individual in the matrix at row i column j to immune with a probability of 35%.

```
if randint(_______,_______) < _____________:
    newmatrix[i][j] = 0
```

(f) (4 pts) A new feature of this simulation is assigning a score to a person to indicate how healthy the surrounding neighbors are. The neighbors are the people immediately to the north, south, east and west of the person being scored. Suppose we compute this score as follows for the person in the matrix at row i column j:

```
score = matrix[i-1][j] + matrix[i+1][j] + matrix[i][j-1] + matrix[i][j+1]
```

For what value(s) of i and for what value(s) of j does this computation fail for a matrix of people of size 25 X 20? (Be careful.)