EXAM 3 Review

EXAM3Bfinal

Concurrency

6b. [7 pts] The programs below employ the idea of critical sections to deal with the race condition described in 6a. The call to `orderBB(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 `free1` and `free2` 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 1 to
keep
# track of inventory

while True:
    quantity = some_function
    free1 = False
    while not free2:
        pass
    orderBB(quantity)
    free1 = True
```

```
# Program run by Store 2 to
# keep track of inventory

while True:
    quantity = some_function
    free2 = False
    while not free1:
        pass
    orderBB(quantity)
    free2 = True
```

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 21.
- Then the players take turns, decreasing the previous number picked by 1, 2, or 3, but not picking any negative number.
- The first player to pick 0 loses.

For example, a game might result in the following series of picks: 21, 18, 16, 15, 13, 10, 8, 6, 5, 2, 1, 0 (and player 1 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 three moves including the forced move for player 1 described above. So the first (root) node of the tree must be 21.

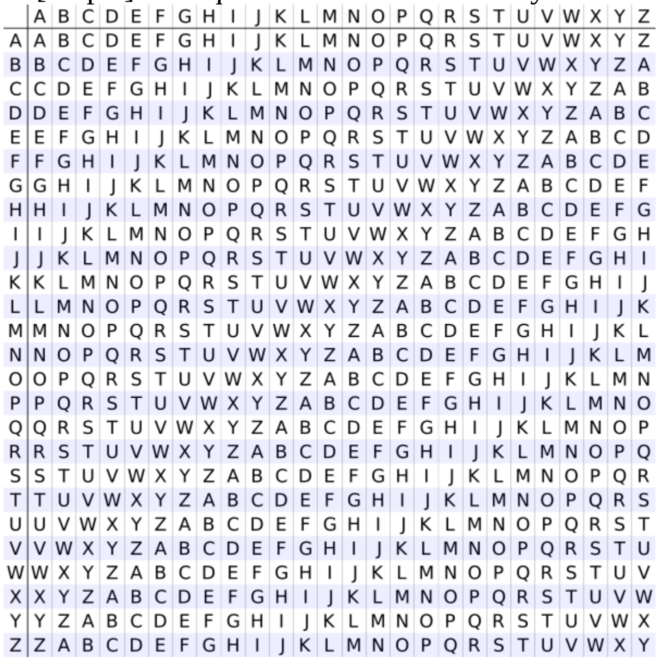
7b. [1 pt.] How many nodes are on the fifth level of the tree (where the root is the first level)?

7c. [2 pts.] What is the number of moves (*counting the first, forced move*) 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 starting number. Answer the previous question for this new game.

Exam3Afinal

4. [15 pts] This question concerns security.



	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

4a. [2 pts] The message AMERICA is encoded using the Vigenère table and becomes the encoded message CAQGCVE. What key was used? For your convenience, the Vigenère table is given above.

____

4b. [8 pts] Alice and Bob want to communicate by encrypting messages using the RSA algorithm. Alice chooses the following values for her messages: decryption_key = 2753, encryption_key = 17, n = 3233. 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?

____ ________________________

4c. [5 pts] 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.

Machine Learning

7b. [6 pts] Suppose CMU wants to use a neural network to select applicants for admissions. CMU has historical data for GPA, SAT, class rank, honors, citizenship at the time of application, as well as information on their GPA and other performance at CMU. Identify or describe the following:

a. Training Data:

b. Features:

c. Neural Network Output:

3. [12 pts] This question concerns networking and the Internet.

3a. [2 pts] In IPv4, a company is assigned addresses of the form 143.17.___.___.
How many unique addresses can the company use with this assignment?

3b. [2 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.
How many unique addresses does IPv6 support overall?

3c. [2 pts] What protocol is used to turn names, such as www.cmu.edu, into IP addresses? Circle your answer.

(A) HTTP (B) DNS (C) SMTP (D) SSH

3d. [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) based on the example done in class?

1. ___ ________________________
2.

3e. [2 pts] What is the role of a router in the Internet protocol? Limit your answer to one sentence.