Practice final solutions

11 December 2013

You have up to 1 hour, 45 minutes. You may use a calculator, but no text book or notes.

1. For each statement below, fill in the blank with the *best* term from the following list. Some terms might be used more than once; some might not be used at all.

   • domain name • foreign key • frequency analysis • HTML • HTTP • IP address • minimax • operating system • password • primary key • public key • table

   (a) HTML is the main language in which the structure of a web page is specified.

   (b) A(n) foreign key is an attribute in a database table whose value references a record in a different table.

   (c) frequency analysis is a technique for trying to decrypt a message without requiring access to the shared secret. It's especially effective in a mono-alphabetic code.

   (d) A(n) IP address is a numeric identifier for each machine on the Internet. The current version is 32 bits.

2. Which of the following schemes is the more secure authentication mechanism?

   (a) A three-character password, using upper- and lower-case letters and digits.

   (b) A four-character password, using just lower-case letters.

   Explain why. Recall that we can quantify the security of a password using the number of *possible* passwords.

   Password scheme (a) has 62 possibilities for each character (26 upper plus 26 lower plus 10 digits). There are three characters, so $62^3 = 238,328$ possible passwords. Password scheme (b) has 26 possibilities for each character, and there are four characters so $26^4 = 456,976$ possible passwords. That means that (b) is the more secure scheme, which may be counter-intuitive. (Of course, they're both pretty bad.)

3. Explain how presenting a photo ID in the physical world is an example of *two-factor authentication.*

   The categories are:

   - Something you **know**
   - Something you **have**
   - Biometric

   So a photo ID is something you **have,** and the photo allows humans to authenticate based on your facial features **(biometric).**

4. The three tables below are a simplification of the database for a social networking web site, like Facebook. There is one main table, 'User', and two other tables that contain foreign keys to 'User'.

User:

ID*	Name	Birthday	Password hash
1	Alice Ann	1974/08/18	cf6a52053ff904bca9d96fd4e7740d7d
2	Bob Björk	1989/11/07	75e22f4965738386cbe02bca10d3120d
3	Carl Carlson	1993/05/03	61aa5b6c78fa4e3636069347ae39df10
4	Dee Doe	1989/12/21	98246ef16a87c12407e5fada044f591e
5	Edward Eng	1990/11/19	1ca30cd59f0b566f9ef3a8208679585e
6	Francine Fuentes	1992/03/25	e5dbb7657f770fad038220f5c69d806c

Friendship — indicates which users are friends with which other users:

User 1 (ref. User)	User 2 (ref. User)	Status	Date
1	2	approved	2012/12/10
1	4	approved	2012/03/24
1	5	approved	2007/05/06
1	6	approved	2010/03/08
2	3	approved	2012/11/01
2	4	approved	2011/08/03
3	4	approved	2008/09/04
4	5	requested	2009/08/04

Wall Messages — sent between users:

Sender (ref. User)	Receiver (ref. User)	Date/time	Message
1	2	2012/12/05 11:51	"Hey man!"
1	5	2012/12/05 16:40	"What r u doing tonite?"
2	1	2012/12/05 17:45	"Send me some tunez"
2	3	2012/12/05 21:18	"Love that pic, LOL"
4	2	2012/12/05 23:00	"This prof is trying my patience."
3	1	2012/12/06 00:05	"Ugh, tired"
2	4	2012/12/06 06:37	"You rock!"

(a) Which user is the youngest? Carl Carlson

(b) Which user has the most friends? Alice Ann has four friends. (Dee Doe has three approved and one more requested.)

(c) The oldest friendship in the database is between which two users? Alice Ann Edward Eng

(d) Name all the friends of Dee Doe.

Dee's approved friends include Alice, Bob, and Carl.

(e) Are there any wall messages between users who are *not* friends? Which ones?

Yes, there's a message from Carl to Alice and they are not friends.

5. Below is a table of jobs that we must schedule on a batch operating system. All jobs are available from the start.

Job	Arrival time	Run time
J1	0	8 seconds
J2	0	3 seconds
J3	0	4 seconds
J4	0	5 seconds

   (a) Create a time-line to illustrate the First-Come First-Served (FCFS) strategy. It should include the start/stop times of each job.

```
  J1    J2    J3    J4
+-----+-----+-----+-----+
0     8    11    15    20
```

   (b) Compute the average **turnaround** time of the four jobs using your FCFS time-line from the previous question.

```
Subtract arrival time from completion time.
  J1:  8 - 0 =  8
  J2: 11 - 0 = 11
  J3: 15 - 0 = 15
  J4: 20 - 0 = 20
Sum of these is 54, average is 54÷4 = 13.5
```

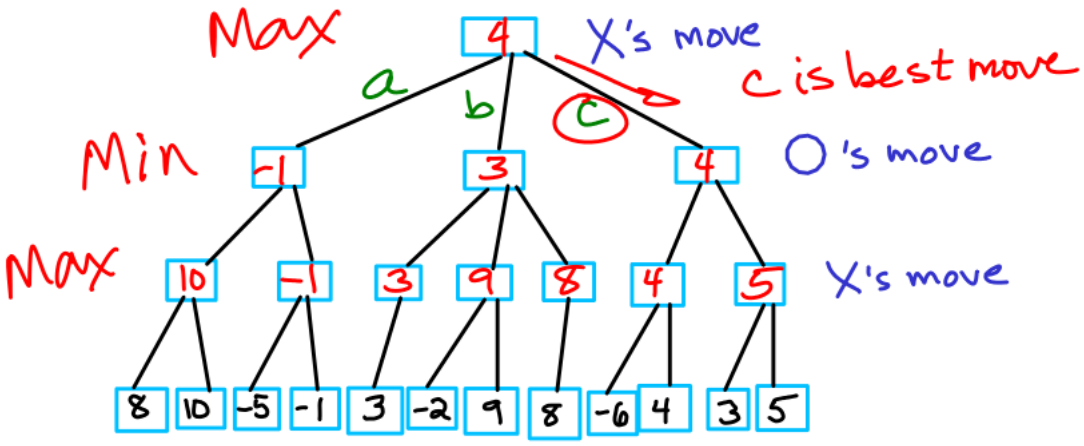
   (c) Create a time-line to illustrate the Shortest Job Next (SJN) strategy. It should include the start/stop times of each job.

```
  J2    J3    J4    J1
+-----+-----+-----+-----+
0     3     7    12    20
```

   (d) Compute the average **turnaround** time of the four jobs using your SJN time-line from the previous question.

```
  J1: 20 - 0 = 20
  J2:  3 - 0 =  3
  J3:  7 - 0 =  7
  J4: 12 - 0 = 12
Sum of these is 42, average is 42÷4 = 10.5
```

6. Below is a game tree in which player X is deciding which move to make: a, b, or c. The scores across the bottom are the relative value of that game state for player X. Use the *minimax* algorithm to propagate the scores and **determine the best move** for player X.



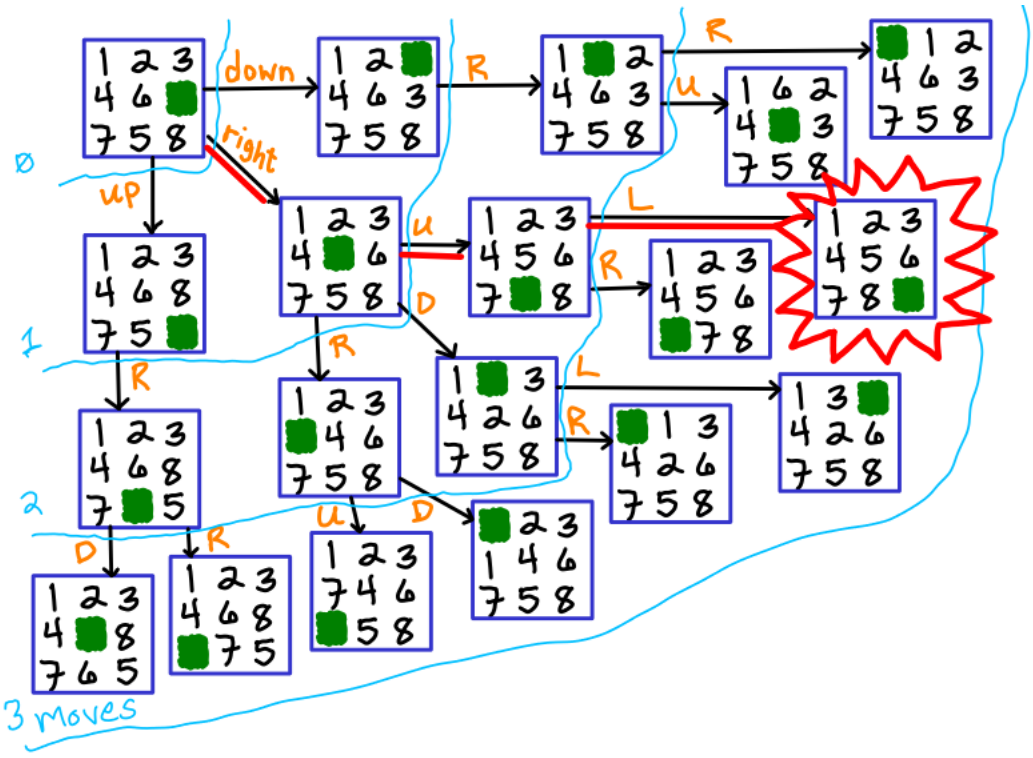
7. What is the output of the following Python program?

```
four = 4
six = four + 2
print "six is six"
six = six - 3
print six+1
four = four * four
print four+4
print "five * four"
```

```
six is six
4
20
five * four
```

8. This question is about planning by searching a state graph in AI. We will study the *8-puzzle,* in which the player slides eight tiles around on a 3×3 grid. The goal is to put the numbers in order, with the `hole' in the lower right.

   Below is the start of a state space graph. The directions labeling the arrow transitions indicate that a numbered tile is moved *down* (or *up, left, right*) into the blank space. Complete the graph to show two more moves, and thus the path to the goal state: a solved puzzle.



9. In an attempt to conceal the character frequencies that are the downfall of a monoalphabetic substitution, the Vigenère technique (1553) switches the alphabet used on each letter, according to a secret keyword. We start with a table of shifted alphabets:

	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

Below is a secret message encoded with the keyword `blimp`. Work backwards to discover the message. The result should be two actual English words.

message:								
key:	b	l	i	m	p	b	l	i
encrypted:	h	l	u	q	d	w	p	z

The message is "gameover"