Practice final solutions

8 May 2014

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 and content 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. Describe the main purpose of the Domain Name Service (DNS).

   DNS translates a domain name (a text identifier, like `google.com`) into an IP address (like `124.18.38.3`).

6. 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
```

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

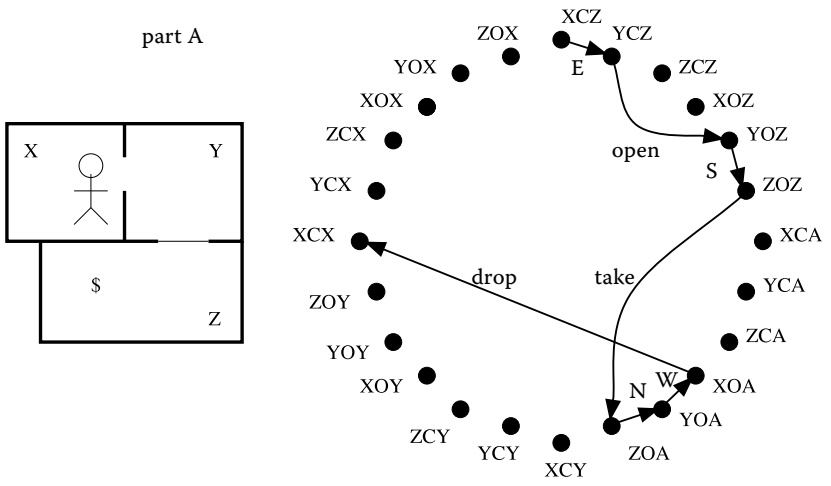
```
xy = 5
zq = 3
print(xy*2)
if xy > 7:
    print("yes")
print(xy + zq)
print("xy")
```

```
10
8
xy
```

8. This question is about planning using graph search in AI. Imagine a castle with 3 rooms, called X, Y, and Z. An adventurer starts in room X, and there is a treasure in room Z. Between rooms Y and Z is a closed (but not locked) door. See the map in the left side of the figure below. We can represent the state of this world with three components:

- the room containing the adventurer (X, Y, or Z);
- the status of the door (O for open, or C for closed); and
- the room containing the treasure (X, Y, Z, or A if the adventurer is carrying it).

That produces a total of 24 states ($3 \times 2 \times 4$). There are eight possible actions: north / south / east / west / open door / close door / take treasure / drop treasure. Of course, not all actions are possible from all states. From the start state, `XCZ`, the only possible action is **east,** which puts us in state `YCZ`.



The right side of the diagram above depicts all 24 states, arrange in a circle so it is easy to draw lines between any two states.

(a) In your own words, describe the meaning of the state `ZCY`.

The adventurer is in room Z, the door is closed, and the treasure is in room Y.

(b) Using the graph above, trace a complete path from the start state `XCZ` to the goal state `XOX`. (This corresponds to fetching the treasure, carrying it back to room X, and dropping it there.) Shown above.

(c) How many states would there be if we added another room, W, to the west of X?

That means there is one more room in both the first and last portions of the state (the room containing the adventurer, and the room containing the treasure). So that makes $4 \times 2 \times 5 = 40$ states.

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”