Practice final solutions

3 May 2017

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 • graph • HTML • HTTP
   • IP address • minimax • operating system • password • postfix • prefix
   • primary 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) postfix is a notation for arithmetic in which the operator is written *after* the operands, such as `3 5 +`

   (d) 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.

   (e) 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 withdrawing cash from an ATM employs *two-factor authentication.*

   The authentication categories are:

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

   In an ATM transaction, you present something you **have** (the bank card) and then something you **know** (the PIN).

4. Evaluate the following *prefix* expression. What result does it produce?

```
(* (+ 3 5) (- 6 2))
```

```
⇒ (* 8 (- 6 2))
⇒ (* 8 4)
⇒ 32
```

5. Convert the prefix expression from the previous question into *postfix* notation.

```
3 5 + 6 2 - *
```

6. 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`).

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. What is the output of the following Python program?

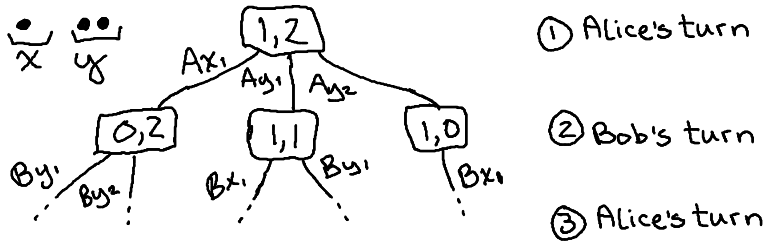
```
xy = 5
zq = 3
print(xy*2)
if xy > 7:
    print("yes")
print(xy + zq)
print("xy")
```

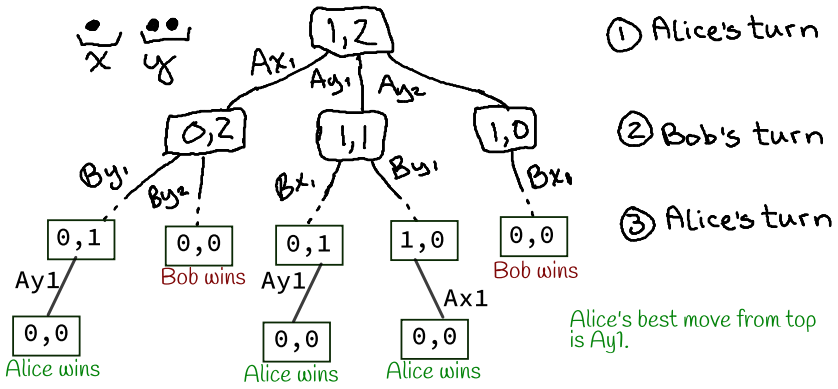
```
10
8
xy
```

9. This question is about a strategy for an ancient game known **Nim.** We start with several piles of stones; let's call the piles x, y, z. On each turn, a player can remove **any number** of stones from a **single** pile. The player to take the very last stone wins.

   We're going to investigate the search tree, as if we were programming a computer player. This is for an end-game, where only two piles remain, pile x with one stone, and pile y with two stones. So we represent that state as $1, 2$. We can represent moves as Ax_1 (which would mean Alice takes one stone from pile x) or By_2 (which would mean Bob takes two stones from pile y). It is Alice's turn.

   Below is a partial tree of moves for each player. Complete the tree to the end of the game, show who wins in each case, and then use those results to determine which is Alice's **best move** for turn #1.




x
y
1,2
Ax1
Ay1
Ay2
0,2
1,1
1,0
By1
By2
Bx1
By1
Bx1
0,1
0,0
0,1
1,0
0,0
Bob wins
Bob wins
Ay1
Ax1
Ay1
0,0
0,0
0,0
Alice wins
Alice wins
Alice wins
① Alice's turn
② Bob's turn
③ Alice's turn
Alice's best move from top is Ay1.

10. 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"