Practice final solutions

14 December 2016

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 • 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) 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?

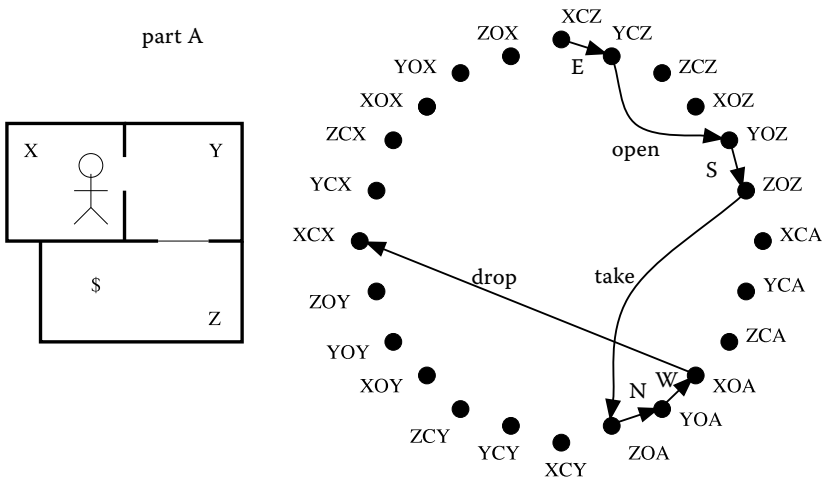
```
xy = 5
zq = 3
print(xy*2)
if xy > 7:
    print("yes")
print(xy + zq)
print("xy")
```

```
10
8
xy
```

9. This question is about 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 entire state of this world using just three letters:

- 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.

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"