Practice final

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) ____________________ is the main language in which the structure and content of a web page is specified.

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

   (c) ____________________ is a notation for arithmetic in which the operator is written *after* the operands, such as `3 5 +`

   (d) ____________________ is a technique for trying to decrypt a message without requiring access to the shared secret. It's especially effective in a monoalphabetic code.

   (e) A(n) ____________________ 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.

3. Explain how withdrawing cash from an ATM employs *two-factor authentication.*

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

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

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

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

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")
```

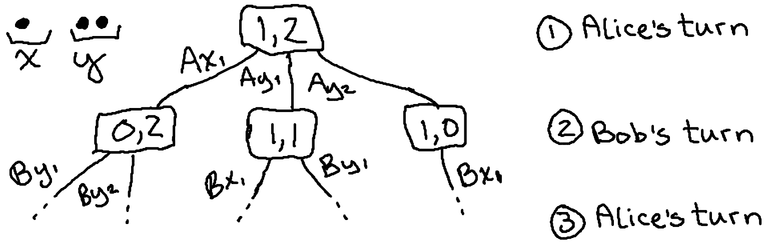
8. What is the output of the following Python program?

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

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.



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