Practice Final Exam Solutions

12 December 2012

You have up to 2 hours. 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
   • kernel • minimax • operating system • password • primary key • public key
   • shell • table

   (a) HTTP is the way that web browsers and servers communicate with each other.

   (b) Cryptography based on a(n) public key was a breakthrough because it meant we no longer need to establish a *shared secret* with our comrades.

   (c) A(n) primary key is an attribute that uniquely identifies each row in a database table.

   (d) A(n) operating system is responsible for providing an interface between the computing hardware and multiple software applications.

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

   (a) A four-digit number, like a bank PIN.

   (b) A three-character password, using only lowercase letters.

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

   There are $10^4 = 10,000$ four-digit PINs.

   There are $26^3 = 17,576$ three-character passwords.

   Therefore, the more secure mechanism is the three-character lowercase password.

3. 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, born in 1993

(b) Which user has the most friends? Alice has 4 friends. (Dee has 3 approved plus 1 requested.)

(c) The oldest friendship in the database is between which two users? Alice and Edward, since 2007.

(d) Name all the friends of Dee Doe.

Dee is friends with Alice, Bob, Carl. Friendship with Edward has been requested, but not approved.

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

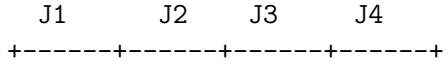
Yes, there is a message between Carl and Alice, but they are not friends.

4. Below is a table of jobs that we must schedule on a batch operating system. **Note the arrival times — a job cannot be scheduled before it has arrived!**

Job	Arrival time	Run time
J1	0	5 seconds
J2	0	4 seconds
J3	3	2 seconds
J4	5	4 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.

   FCFS takes them all in order:



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

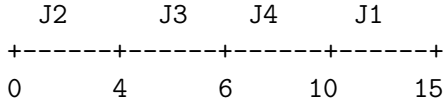
   Turnaround time is completion time minus arrival time. Then you take the average of all the jobs.

   J1: 5 – 0 = 5
   J2: 9 – 0 = 9
   J3: 11 – 3 = 8
   J4: 15 – 5 = 10

   The average is (5+9+8+10)÷4 = 32÷4 = 8.

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

   SJN means we choose the job with the shortest run time, but choosing only from those jobs already available when we're making the decision.



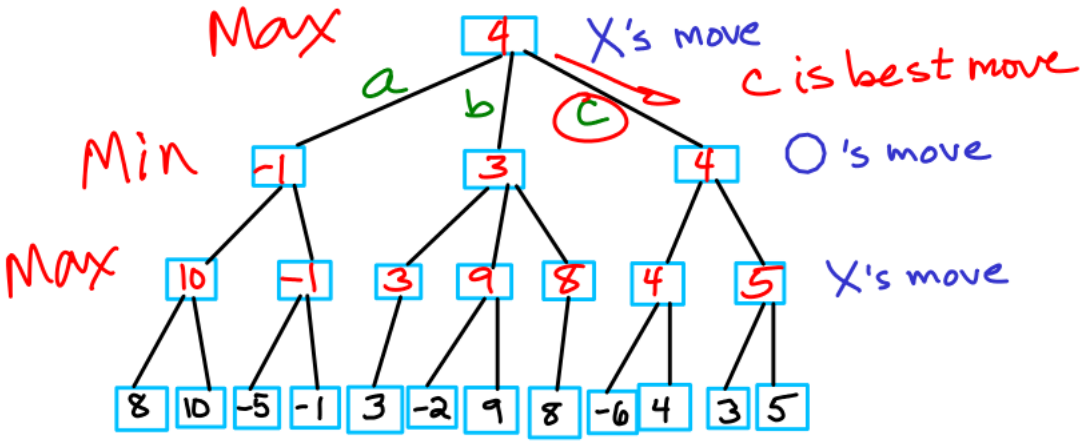
   (d) Compute the average **turnaround** time of the four jobs using your SJN time-line from the previous question.

   J1: 15 – 0 = 15
   J2: 4 – 0 = 4
   J3: 6 – 3 = 3
   J4: 10 – 5 = 5

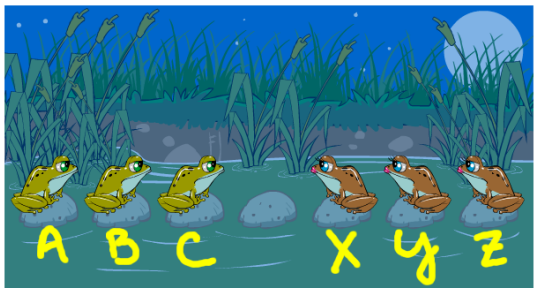
   The average is (15+4+3+5)÷4 = 27÷4 = 6.75.

5. 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.

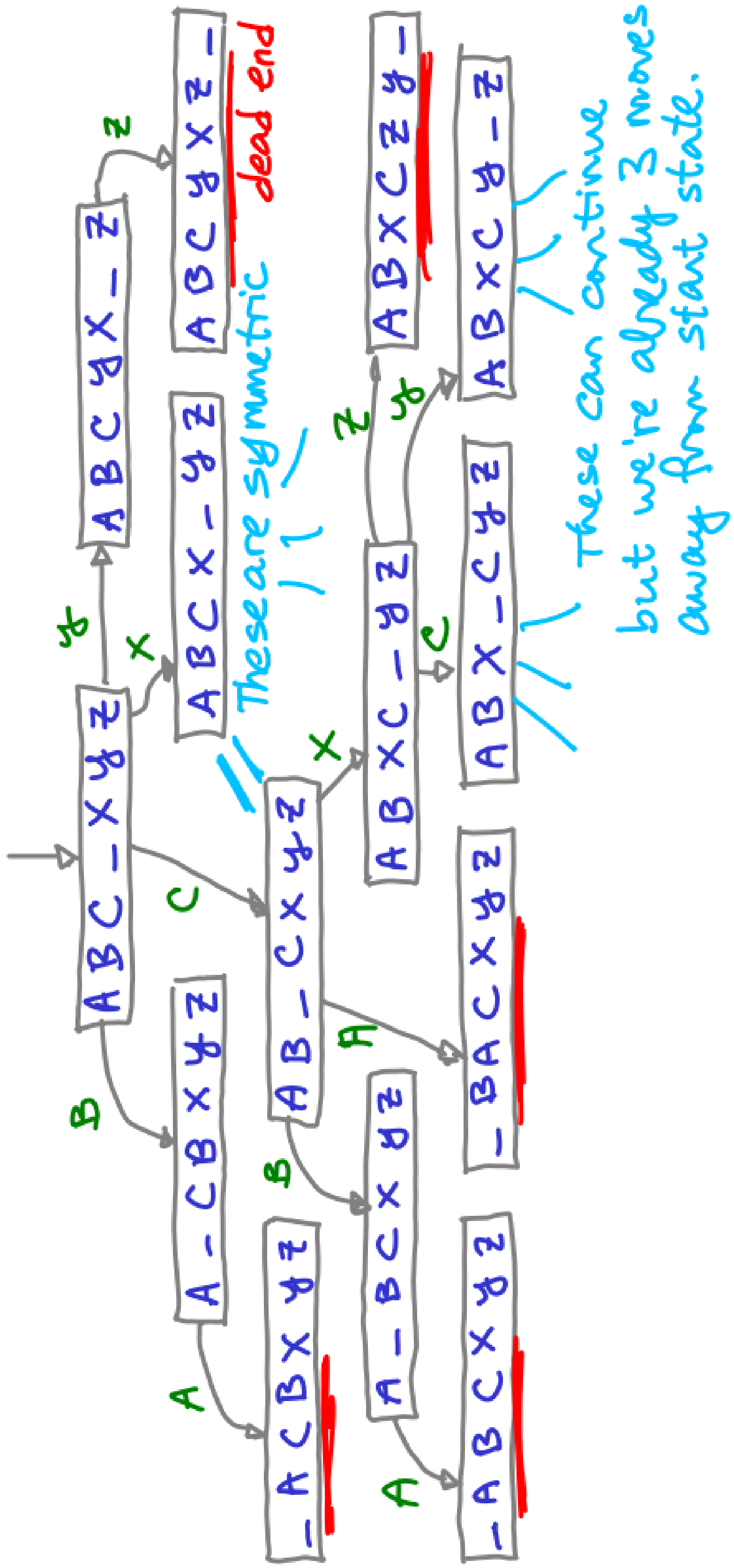
   Because player X starts, the scores are in terms of player X, and X's moves are where we maximize. The opponent, O, wants to minimize.



6. Six frogs are trying to cross a pond by jumping between stones. Alma, Ben, and Carl are heading East; while Xavier, Yolanda, and Zanjoe are heading West. Each frog can jump just onto an adjacent stone, or jump *over* another frog if there is an empty stone behind it. The frogs are stubborn, however, and are **not** willing to change direction.



   Design a simple representation for the state of the world, and draw a graph showing all possible moves **three** steps out from the start state, as illustrated.


dead end
These are symmetric
These can continue but we're already 3 moves away from start state.

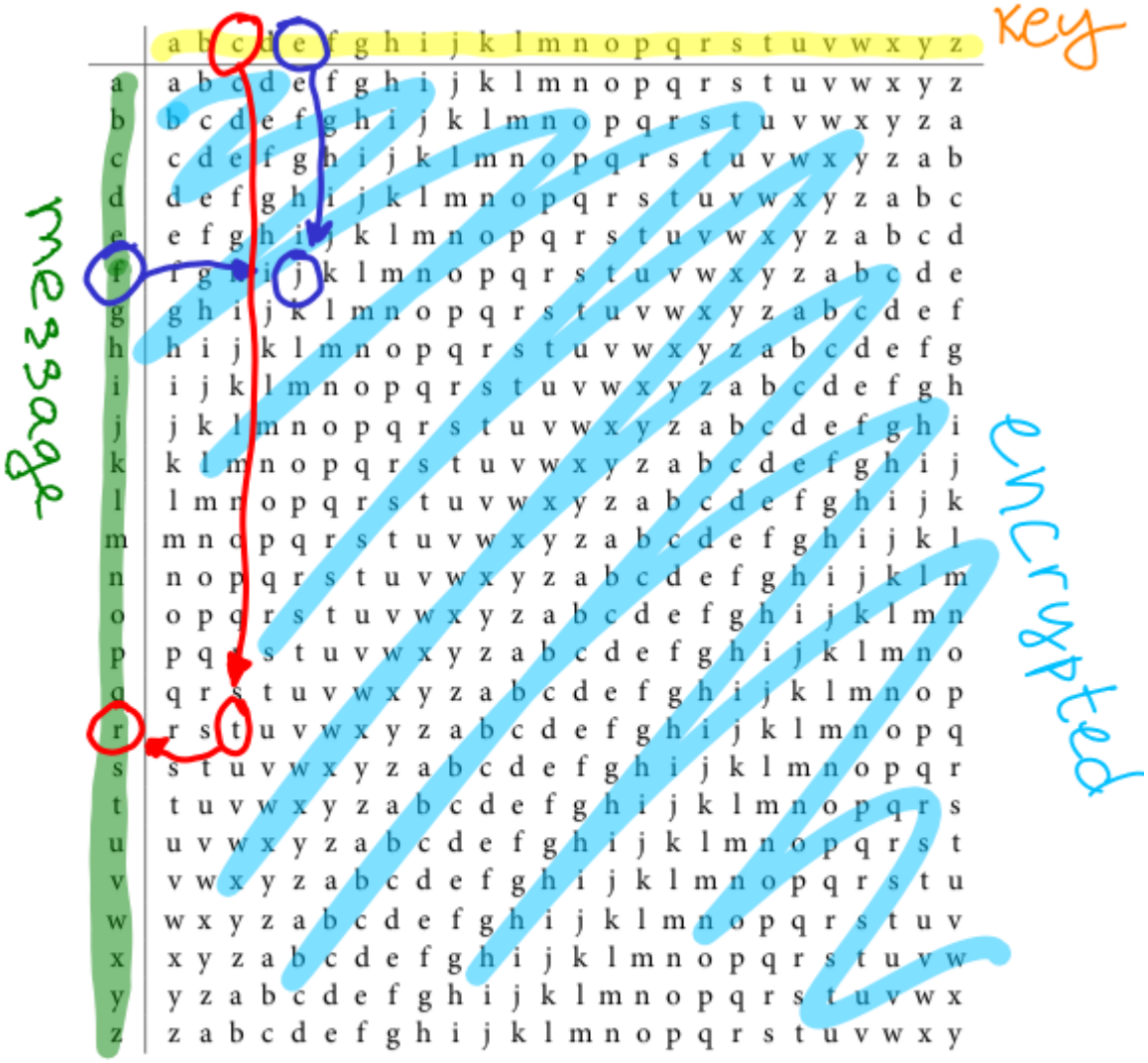
7. In an attempt to conceal the character frequencies that are the downfall of a monoalphabetic substitution, the Vigenère technique (1553) switches the alphabet used on each letter, according to a secret keyword. We start with a table of shifted alphabets:

	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 'face'. Work backwards to discover the message. The result should be two actual English words.

message:	e	n	j	o	y	b	r	e	a	k
key:	f	a	c	e	f	a	c	e	f	a
encrypted:	j	n	l	s	d	b	t	i	f	k

See next page...



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

message:	e	n	j	o	y	b	r	e	a	k
key:	f	a	c	e	f	a	c	e	f	a
encrypted:	j	n	l	s	d	b	t	i	f	k