Mathematics for Computing
Summer 2014
Suggested Solutions

Question One

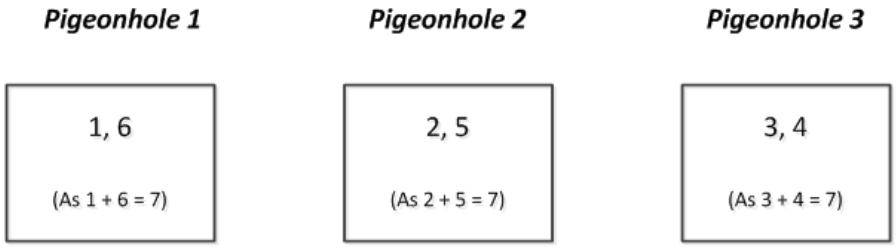
(a)

i. $52 \times 52 \times 52 \times 52 \times 52 \times 10 \times 19 \times 19 = 1.373 \times 10^{12}$ different passwords.

ii. $52 \times 51 \times 50 \times 49 \times 48 \times 10 \times 19 \times 18 = 1.067 \times 10^{12}$ different passwords.

(b)

There are three pairs – 1 and 6, 2 and 5, 3 and 4 – that add up to 7. Each element in the set belongs to one of these pairs. Apply the Pigeonhole Principle, where the pairs are the pigeonholes and the four chosen numbers are the items to be allocated to the three pigeonholes.



(c)

i. The first six terms in the binomial expansion of $(1 + x)^{32}$ are:
$$1 + \binom{32}{1} x + \binom{32}{2} x^2 + \binom{32}{3} x^3 + \binom{32}{4} x^4 + \binom{32}{5} x^5$$

ii. The first six terms in the binomial expansion of $(1 + 0.05)^{32}$ are:
$$1 + \binom{32}{1} 0.05 + \binom{32}{2} 0.05^2 + \binom{32}{3} 0.05^3 + \binom{32}{4} 0.05^4 + \binom{32}{5} 0.05^5$$
$$= 1 + 1.6 + 1.24 + 0.62 + 0.22475 + 0.06293$$
$$= 4.74768$$

iii. $1.05^{32} = 4.76494$ correct to five decimal places.

Error in estimate = 4.76494 - 4.74768 = 0.01726

(d)

Recurrence relation (assuming no repayments):
Debt after n years = $D_n = €1{,}000 \times 1.12^n$

i. Amount owed after three years = $€1{,}000 \times 1.12^3 = €1{,}404.93$

ii. Seven years (see following table)

n	0	1	2	3	4	5	6	7
D_n	€1,000	€1,120	€1,254.40	€1,404.93	€1,573.52	€1,762.34	€1,973.82	€2,210.68

Question Two

(a)

i.

16-digit number	4	0	1	2	8	8	8	8	8	8	8	8	1	8	8	1
Revised "odd" digits	8		2		7		7		7		7		2		7	
"Even" digits		0		2		8		8		8		8		8		1

Sum = (8+2+7+7+7+7+2+7) + (0+2+8+8+8+8+8+1) = 90.
As the sum mod 0 = 0, this is a valid credit card number.

ii.

16-digit number	5	1	0	5	1	0	5	1	0	5	1	0	5	1	0	5
Revised "odd" digits	1		0		2		1		0		2		1		0	
"Even" digits		1		5		0		1		5		0		1		5

Sum = (1+0+2+1+0+2+1+0) + (1+5+0+1+5+0+1+5) = 25.
As the sum mod 0 = 5, this is not a valid credit card number. Change the check digit from 5 to 0 and it becomes a valid credit card number.

(b)

i. Find the greatest common divisor (gcd) of 2926 and 8265.

gcd(2926, 8265) = gcd(2413, 2926)
= gcd(513, 2413)
= gcd(361, 513)
= gcd(152, 361)
= gcd(57, 152)
= gcd(38, 57)
= gcd(19, 38)
= gcd(0, 19) so 19 is the greatest common divisor.

ii. Find the greatest common divisor of 2468 and 3579.

gcd(2468, 3579) = gcd(1111, 2468)
= gcd(246, 1111)
= gcd(127, 246)
= gcd(119, 127)
= gcd(8, 119)
= gcd(7, 8)
= gcd(1, 7)
= gcd(0, 1) so 1 is the greatest common divisor.

(c)

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149

Exact value (count from sieve): $\pi(150) = 35$ to the nearest integer.
Estimated value: $\pi(150) \approx 150/\ln(150) = 30$.

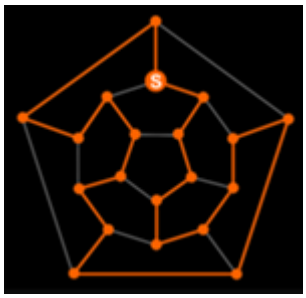
(d)

i. $12{,}321 = 3 \times 3 \times 37 \times 37$
ii. $1{,}234{,}567 = 127 \times 9{,}721$

Question Three

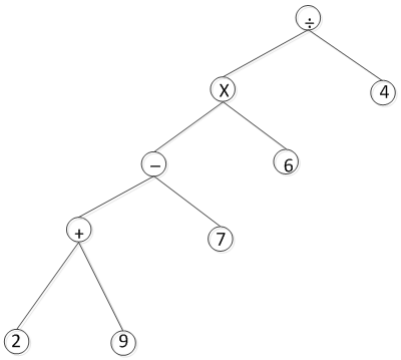
(a)

One possible solution is:

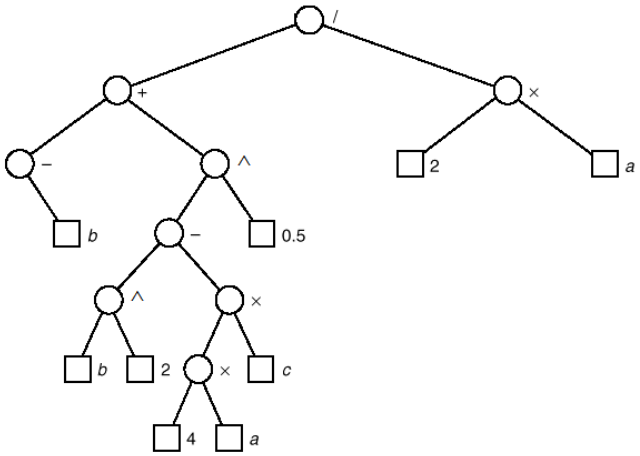


(b)

(i)



(ii)



(c)

An *Eulerian walk* is a walk that goes through every edge in a graph exactly once.

Vertex	*A*	*B*	*C*	*D*	*E*	*F*	*G*
Degree	4	4	4	4	4	4	4

As there are no vertices of odd degree in the graph (and the graph is connected), a closed Eulerian walk exists.

One such walk is: *A-B-C-D-E-F-G-A-C-F-B-D-G-E-A*.

Question Four

(a)

Each plaintext letter has been shifted six positions to the right, so the deciphered message is:

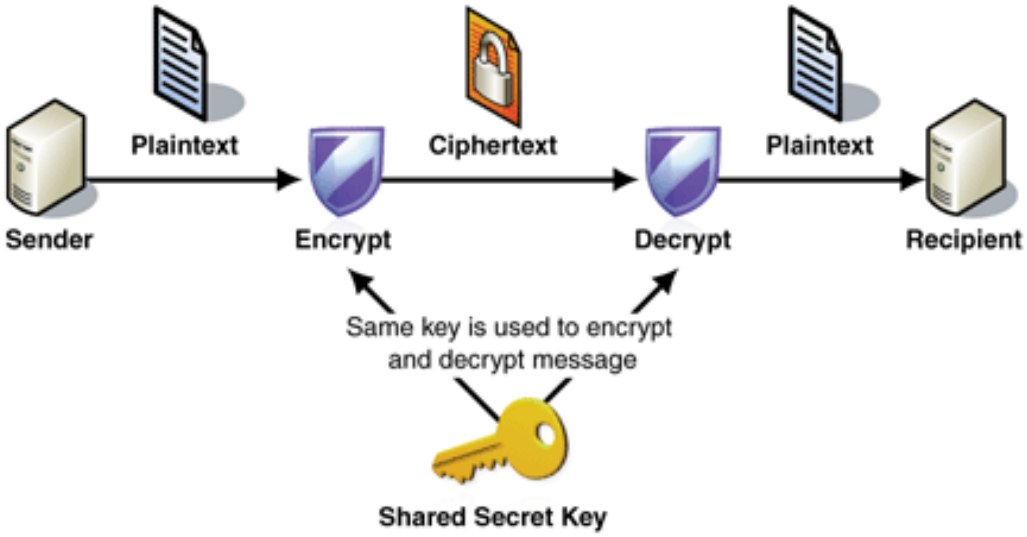
> Walking on water and developing software from a specification are easy if both are frozen.

Ciphertext	A	B	C	D	E	F	G	H	I	J	K	L	M
Plaintext	U	V	W	X	Y	Z	A	B	C	D	E	F	G

Ciphertext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plaintext	H	I	J	K	L	M	N	O	P	Q	R	S	T

(b)

With symmetric key cryptography, both parties use the same key for encryption and decryption purposes. Each user must possess the same key to send encrypted messages to each other. The sender uses the key to encrypt their message, and then transmits it to the receiver. The receiver, who is in possession of the same key, uses it to decrypt the message. The security of this encryption model relies on the end users to protect the secret key properly.



The advantages of symmetric key cryptography are that:

1. Computational time is very fast.
2. It has been well tested.
3. Uses less computing resources.
4. A different key for each different user means a comprised key only affects one sender/receiver pairing.

The disadvantages are that:
1. The key must remain secret.
2. Exchanging keys with someone must be done in secret.
3. Each communicating pair of people needs to share a key.
4. Large number of keys to manage.

(c)

i. $e = 5$ and $\Phi = (p - 1)(q - 1) = 4 \times 6 = 24$ – we must find positive integers d and v so that $de - v\Phi = 1$, i.e. $5d - 24v = 1$. Examining multiples of both 5 and 24 and substituting into the equation yields a minimum value of $d = 5$ when $v = 1$.

	1	2	3	4	5
5*d* (Multiples of 5)	5	10	15	20	**25**
24*v* + 1 (Multiples of 24, plus 1)	**25**				

ii. The decrypted message is "Kiss me Kate".

Ciphertext *C*	16	04	24	24	13	10	16	01	20	10
Plaintext C^5 mod 35	11	09	19	19	13	05	11	01	20	05
Letter	K	I	S	S	M	E	K	A	T	E

iii. (1) Making $n = 35$ and $e = 5$ publicly available, makes it easy to determine $p = 5$ and $q = 7$ and hence that $\Phi = 24$. From this, it is pretty easy to find the decryption key. Hence using a small value of n is not very secure.
(2) Encrypting one character at a time means that there will be a lot of repetition of numbers in your message. A long message can be easily broken using knowledge about common letters and letter patterns. Hence, encrypting one letter at a time can be broken without using RSA methods at all.

Question Five

(a)

Propositions:

- S = "security is a problem".
- R = "regulation is increased".
- B = "business on the internet grows".

The argument is: $(S \rightarrow R) \wedge (\sim S \rightarrow B) \rightarrow (\sim R \rightarrow B)$.

A proof sequence is:
(i) $S \rightarrow R$ is equivalent to $\sim R \rightarrow \sim S$,
(ii) $\sim S \rightarrow B$,
(iii) $\sim R$,
from (i) and (ii) we arrive at: (iv) $\sim R \rightarrow B$,
from (iii) and (iv) B.

(b)

One possible intermediate statement is shown under each predicate formula.

i. $\forall x\,[S(x) \rightarrow L(x)]$

For all items x, x being a spy novel implies that it (x) is long.

ii. $\exists x\,[M(x) \wedge \sim S(x)]$

There exists an item x such that x is a mystery novel and it (x) is not a spy novel.

iii. $\forall x\,[L(x) \rightarrow M(x)]$

For all items x, x being long implies that it (x) is a mystery novel.

iv. $\exists x\,[M(x) \wedge \forall y\,(S(y) \rightarrow B(x, y))]$

There exists an item x such that x is a mystery novel and for all items y, such that y are spy novels, mystery novel (x) is better than spy novels (y).

(c)

There are 3×2×1 = 6 different arrangements of the top 3 teams at the World Cup as shown in the following table:

First	Second	Third	Feasible?
Brazil	Italy	Spain	No (from 3rd piece of information – Spaniard's comment)
Brazil	Spain	Italy	No (from 1st piece of information – radio commentary)
Italy	Brazil	Spain	No (from 1st piece of information – radio commentary)
Italy	Spain	Brazil	No (from 1st piece of information – radio commentary)
Spain	Brazil	Italy	No (from 2nd piece of information – Italian's comment)
Spain	Italy	Brazil	Yes (by elimination)

So Spain placed first, Italy placed second, and Brazil placed third.