Mathematics for Computing
Summer 2015
Suggested Solutions

Question One

(a)

Suppose that no two people have the same age so that there are at least 51 different ages in the room. Let box 1 correspond to integers 1 and 2, box 2 correspond to integers 3 and 4, …, box 50 to integers 99 and 100. Assigning ages to boxes, by the pigeonhole principle, some box contains two ages. This says that ages of the two people are consecutive integers as required (consecutive integers show that the two people, whose ages are those values, were born within one year of each other).

(b)

If there are 12 different letters, we have 12! different anagrams. But some letters are repeated twice (S and O). Therefore, there are 12!/2!2! = 119,750,400 different anagrams.

(c)

i. There are nine terms in the expansion.

ii. As there is an odd number of terms in the expansion, there is a single middle term. This term is $\binom{8}{4}(2x)^4(-y)^4 = 70 \times 16x^4 \times y^4 = 1{,}120x^4y^4$.

(d)

i. The first four terms in the sequence are:

n	1	2	3	4
R_n	3	7	11	15

ii. <u>Recursion formula</u>

By observation, a beam of length one unit requires three rods. This is the required initial condition.

Initial condition $R_1 = 3$.

By observation, when the beam length increases by one unit, four more rods must be added onto the diagram of the beam. This reasoning allows us to identify the recursion formula.

$R_n = R_{n-1} + 4$ for all $n \geq 2$.

Question Two

(a)

i. Find the greatest common divisor (gcd) of 252 and 660.

gcd(252, 660) = gcd(156, 252)
= gcd(96, 156)
= gcd(60, 96)
= gcd(36, 60)
= gcd(24, 36)
= gcd(12, 24)
= gcd(0, 12) so 12 is the greatest common divisor.

ii. Find the greatest common divisor of 2415 and 3289.

gcd(2415, 3289) = gcd(874, 2415)
= gcd(667, 874)
= gcd(207, 667)
= gcd(46, 207)
= gcd(23, 46)
= gcd(0, 23) so 23 is the greatest common divisor.

(b)

i. $q = 74$; $r = 5539$.

ii. $q = 279$; $r = 15$. Note that $q = 278$; $r = -4$ is not a valid solution as the remainder r must be non-negative as stated in the Division Algorithm.

(c)

i. $2^{10} - 1 = 1{,}023 = 3 \times 11 \times 31$.

ii. $\sqrt{503}$ rounded down = 22. As there are no prime numbers between 2 and 22 inclusive that are factors of 503, then 503 is a prime number and so has only one prime factor, itself (503).

(d)

i. **sum** = (9+8+4+1+3+ 9) + 3×(7+1+7+1+8+4) mod 10 = 118 mod 10 ≡ 8.

Check digit = 10 – **sum** = 10 – 8 = 2.

As ***D*** is the check digit in this book, ***D*** = 2.

ii. **sum** = (9+8+8+***D***+8+ 9) + 3×(7+1+4+8+2+1) mod 10 = ***D*** + 111 mod 10.

Check digit = 5 so 10 – **sum** mod 10 ≡ 5.

As ***D*** + 111 mod 10 ≡ 5 then ***D*** = 4.

Question Three

(a)

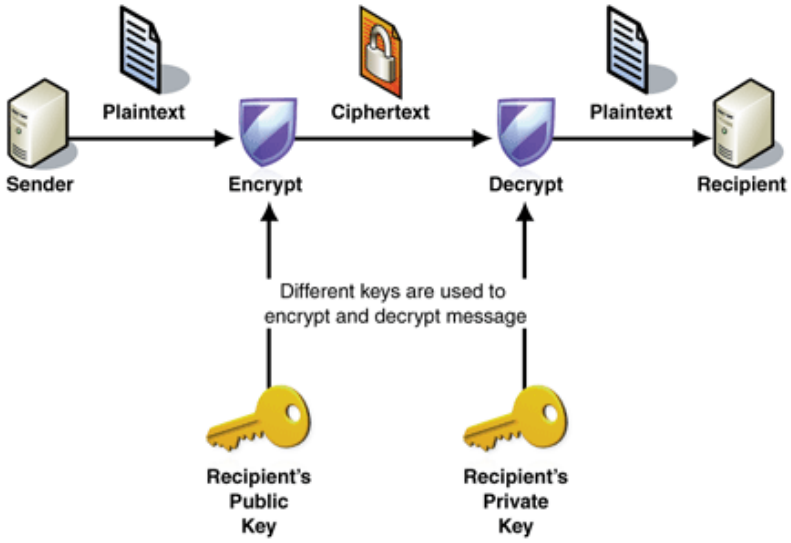
Yes, it is possible. Here's what you can do: Pick two enormous primes at random. Suppose the primes are p = 47,287 and q = 48,869. (In reality you'd want them much bigger, say 300 digits.) Then multiply the primes to get a composite number, in this case $n = p \times q$ = 2,310,868,403. Finally, print that composite number n in an appendix to the book. Later, when it's safe, you can prove you're the author by revealing the primes you multiplied. It's easy to check that those are the right primes (just multiply them), but for anyone who didn't know them, they'd be pretty hard to find!

The key here is the following:

- There are quick ways to test whether a number n is prime or composite.
- But if n is composite, then actually finding its factors takes a huge amount of time by any current method.

(b)

In public key cryptography, the sender encrypts data with one key, and the recipient uses a different key to decrypt ciphertext. The encryption key and its matching decryption key are often referred to as a public/private key pair. The public key of the recipient is used to encrypt data. It can be openly distributed to those who want to encrypt a message to the recipient. The private key of the recipient is used to decrypt messages, and only the recipient must be able to access it.



The advantages of public key cryptography are that:

1. Private keys never need to be transmitted or revealed to anyone, leading to increased security compared to private key systems.
2. Digital signatures are provided that cannot be repudiated (the digital signature *guarantees* that the sender is who he/she claims to be).
3. The inconvenience of sharing keys with someone (either manually or through a communication channel) as required in private key cryptography is avoided. The sender/recipient never need to meet.
4. A digitally signed message cannot be tampered with without invalidating the digital signature, making it easy to detect tampering.

The disadvantages are that:
1. Private key encryption systems are significantly faster than public key encryption systems.
2. Public key encryption systems are vulnerable to *impersonation*, even if users' private keys are not available.
3. More powerful computers are needed to perform the encryption/decryption.
4. If a person's private key is compromised, all of his/her messages can be read.

(c)

i. Plaintext $P = 0511$ as E is the 5^{th} letter and K is the 11^{th} letter in the alphabet.

Ciphertext $C = P^e \bmod n = 511^3 \bmod 2773 = 1617$.

ii. $\Phi = (p-1)(q-1) = 46 \times 58 = 2668$. Solve $de - v\Phi = 1$ to find the decryption key d, i.e. solve $3d = 2668v + 1$. We get $d = 1779$ and $v = 2$. Decrypting: The plaintext message $P = C^d \bmod n = C^{1779} \bmod 2773$.

Question Four

(a)

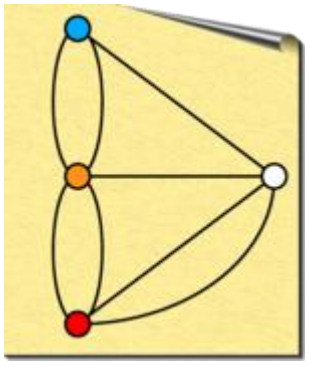
Original graph (as it has more than two vertices of odd degree, it does not have an Eulerian walk i.e. one cannot "walk the bridges").

Vertex	Degree
Blue castle	3
Inn	5
Red castle	3
Church	3

i.

An open Euclidean walk requires exactly two vertices of odd degree, one at the start and one at the end. Add a new bridge between the red castle and the church to meet this requirement.

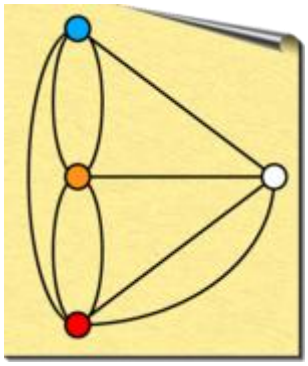
Vertex	Degree
Blue castle	3
Inn	5
Red castle	4
Church	4



ii.

An open Euclidean walk requires exactly two vertices of odd degree, one at the start and one at the end. Add a new bridge between the blue castle and the red castle to meet this requirement.

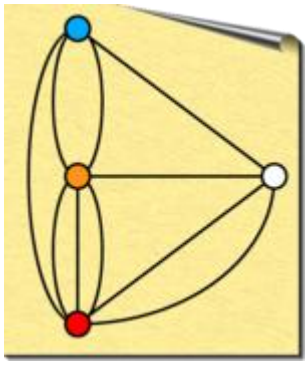
Vertex	Degree
Blue castle	4
Inn	5
Red castle	5
Church	4



iii.

A closed Euclidean walk requires all vertices to be of even degree. Add a new bridge between the inn and the red castle to meet this requirement

Vertex	Degree
Blue castle	4
Inn	6
Red castle	6
Church	4



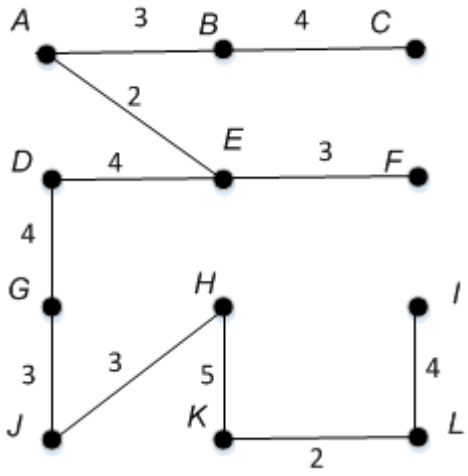
(b)

As there are 12 vertices in the graph, 11 edges are needed to span the graph. One possible sequence of steps from Kruskal's algorithm is:

Step	Edge	Weight
1	AE	2
2	KL	2
3	AB	3
4	EF	3
5	HJ	3
6	GJ	3
7	BC	4
8	DE	4
9	DG	4
10	IL	4
11	HK	5

Minimum weight is 37.

Spanning tree:



Question Five

(a)

The argument is invalid. An analysis of the argument must take into account the fact that "nothing" is being used in two different ways.

(b)

Propositions:

- G = "I have a good round of golf".
- C = "the wind is calm".
- D = "the weather is dry".

The argument in symbolic form is: $[(G \rightarrow (C \vee D)) \wedge (C \wedge D)] \rightarrow G$

G	C	D	$(C \vee D)$	$(G \rightarrow (C \vee D))$	$(C \wedge D)$	$[(G \rightarrow (C \vee D)) \wedge (C \wedge D)]$	Argument
T	T	T	T	T	T	T	T
T	F	F	T	F	F	F	T
T	T	T	T	T	F	F	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	F
F	F	F	T	F	F	F	T
F	T	T	T	T	F	F	T
F	F	F	F	T	F	F	T

The truth table shows that the argument is not always valid (it is a contingency), therefore the argument is invalid. (The fifth row of the table shows that if G is false while both C and D are true, then the hypotheses of the argument are true while the conclusion is false.)

(c)

i. Some days are not rainy.

ii. Every day that is sunny is not rainy.

iii. No day is both sunny and rainy.

iv. No day is sunny.