COMS10003

Mathematical Methods for Computer Scientists

Assignment - Portfolio 1

This assignment is worth 15% of the unit mark

2014-15

Instructions

1. You are required to provide solutions to the following five questions.
2. Each question is worth 10 marks.
3. You are expected to work independently.
4. Clearly state your name and your user name on your submission. The submission can be hand written or typed.
5. All answers should be clearly structured and you should fully explain and justify each and every step.
6. Marks will be deducted if justifications and explanations are not given. Answers without any justification or explanation will be given ZERO MARKS.
7. You should hand-in a hard copy of your answers to the MVSE School Office AND upload an electronic copy to SAFE (PF1). If you produce hand written answers, then these should be scanned and uploaded as a single PDF document. No other format will be accepted.
8. The DEADLINE for submission of both the hard copy and the electronic copy is

5pm on Monday 12th January 2015.

Question 1

a) Determine whether the following sets of connectives are functionally complete:

i) $\{\Rightarrow\}$,

ii) $\{\Rightarrow, \neg\}$.

Clearly state what you need to do and provide details to justify your answer (i.e. in form of a truth table or a proof based on logical equivalences).

Note, you need to consider at least $\vee, \wedge$ and $\Leftrightarrow$.

[4 marks]

b) Transform the following proposition

$$((\neg A \Rightarrow B) \wedge ((A \wedge \neg C) \Leftrightarrow \neg B))$$

both into

i) Disjunctive Normal Form and into

ii) Conjunctive Normal From.

Clearly explain the method you are using step by step. Minimise your answer. Show how you obtained the minimised form.

[6 marks]

Question 2

a) Prove that $n^4 - 1$ is divisible by 5 when n is not divisible by 5. Which proof strategy did you use?

[5 marks]

b) Two integers are said to have the same parity if they are both odd or both even.

Use proof by contrapositive to show that if x and y are two integers for which $x + y$ is even, then x and y have the same parity.

[5 marks]

Question 3:

(a) Use Euclid's algorithm to find the inverse of 11 modulo 40, i.e. find $11^{-1} \pmod{40}$. Write out the lines of Euclid's algorithm in full and show where the final answer comes from.

[6 marks]

(b) Now use your result from part (a) to find x where $x^{11} \mod 41 = 10$ showing how you could get the final answer with a calculator that can manage a maximum of 9 digits.

[4 marks]

Question 4

An enemy organization has encrypted a message with the public key $n = 111$ and $e = 5$. The message is 001101000081025032000101013000067 but the enemy organization has made itself vulnerable to a decryption attack. That's your job. Show how you arrive at the decrypted message based on a simple alphabet encoding starting with 000 ='a', including an argument for how you can deduce the block size from the encoded number.

[10 marks]

Question 5

(a) A network switch has two input links, A and B, and one output link C. Consider time to be divided into successive 10 ms intervals. During each interval a single data packet arrives on each input link at a random time. Each packet is stored in the switch and then put on the output link after a delay of x ms following its arrival, where $x < 10\ ms$. A packet is deleted immediately after it has been put on the output link. If the probability of the two packets which arrive within the same interval being stored in the switch at the same time is 0.5, determine the value of the delay x.

[4 marks]

(b) Packets arriving at the switch are either 128 bytes or 256 bytes long. On input link A, 25% of packets are 128 bytes long, whilst on input link B, 64% of packets are 256 bytes long. If a 256 byte packet is followed by 128 byte packet on the output link, determine the probability that the 256 byte packet arrived on link A and the 128 byte packet arrived on link B. *Hint: consider the observation of both packets as an event and use Bayes' theorem to compute the conditional probability of them orgininating from links A and B given that event.*

[6 marks]