This question paper consists of 2 printed pages, each of which is identified by the Code Number COMP5710M01.

School of Computing

January 2018

COMP5710M01

Algorithms

Answer all 3 questions.

Time allowed: 2 hours

TURN OVER FOR QUESTIONS

Question 1

(a) What is meant by

(i) a randomised algorithm? **[1 mark]**

(ii) a Monte Carlo algorithm? **[2 marks]**

(iii) a Las Vegas algorithm? **[2 marks]**

(b) Which basic operations are efficiently supported in 2-4 trees? What is their running time? **[4 marks]**

(c) Which cryptosystem becomes insecure if quantum computers become practicable? Just name one system. **[1 mark]**

(d) Does every false formula in CNF have a polynomial-size Resolution refutation? Give reasons. **[2 marks]**

[question 1 total: 12 marks]

Question 2

(a) State the extended Euclidean algorithm in pseudocode. **[6 marks]**

(b) Explain the RSA cryptosystem, including full details on public and private keys. **[6 marks]**

(c) Let $n = 85$, $e = 19$ be Bob's public key in the RSA cryptosystem. Use the extended Euclidean algorithm to compute Bob's private key. State all steps of the computation. **[6 marks]**

[question 2 total: 18 marks]

Question 3

(a) Define Horn formulas. **[2 marks]**

(b) State the satisfiability test for Horn formulas in pseudocode. **[5 marks]**

(c) What is the running time of your algorithm? Give reasons. **[3 marks]**

(d) Use the algorithm to determine whether the formula

$$(p_1 \wedge p_2 \to p_3) \wedge (p_2 \to p_1) \wedge (p_2 \wedge p_4 \to 0) \wedge (1 \to p_2)$$

is satisfiable. State all steps of the algorithm. **[5 marks]**

[question 3 total: 15 marks]
[grand total: 45 marks]

END