Galway-Mayo Institute of Technology

Semester 2 Examinations 2018/2019

MODULE: COMP08015 – Theory of Algorithms

PROGRAMME(S):

GA_KSOAG_H08 B.Sc. (Honours) Software Development

YEAR(S) OF STUDY: 4

EXAMINERS:

Dr. Ian McLoughlin (Internal)
Dr. Des Chambers (External)
Mr. Tom Davis (External)

TIME ALLOWED: 2 hours

INSTRUCTIONS: **Answer 3 questions. All questions carry equal marks.**

Please do not turn this page until you are instructed to do so.
The use of programmable or text storing calculators is expressly forbidden. Please note that where a candidate answers more than the required number of questions, the examiner will mark all questions attempted and then select the highest scoring ones.

There are no additional requirements for this paper.

Question 1 (100 total marks)

Consider the Turing machine given by the following state table.

State	Input	Write	Move	Next
q_0	$\sqcup$	1	R	q_a
q_0	0	0	R	q_1
q_0	1	1	R	q_0
q_1	$\sqcup$	0	R	q_f
q_1	0	0	R	q_0
q_1	1	1	R	q_1

(a) Determine the number of steps taken by the above Turing machine on each of the four following inputs: ϵ, 0101, 11111, and 000000. (40 marks)

(b) Define the term *big-O* in the context of Turing machines. (40 marks)

(c) Is the language decided by the above Turing machine in $O(n)$? Explain your reasoning. (20 marks)

Question 2 (100 total marks)

Consider the language $L = \{0^i 1^j \mid i, j \in \mathbb{N}, 0 < i \leq j\}$ over the alphabet $A = \{0, 1\}$.

(a) List the six shortest strings in L. (40 marks)

(b) Explain what is meant by A^* (where * is the Kleene star) and list the six shortest strings that are in A^* but not in L. (40 marks)

(c) State whether A^* and L^* are equivalent and explain your reasoning. (20 marks)

Question 3 (100 total marks)

The following question is about the 256-bit version of the Secure Hash Algorithm, SHA-256, and the map described by it.

(a) Explain the difference between a one-to-one map and a one-way map. (40 marks)

(b) State whether or not the SHA-256 algorithm describes a one-to-one map and explain your reasoning. (40 marks)

(c) There is a test to determine whether or not the SHA-256 algorithm describes an *onto* map: try all possible inputs and check that all outputs are generated. Explain why we can't perform this test. (20 marks)

Question 4 (100 total marks)

Consider the following scenario. You have a Linux account where your password is "gmit123". Your friend tells you that they have broken into your account by guessing your password. They demonstrate this to you, and sure enough they can log in as you. However, the password they are using is different from "gmit123". Answer the following questions related to this scenario.

(a) Explain how and why passwords on a modern Linux system are stored as hashed values. (40 marks)

(b) In the above scenario, two different passwords can be used to access the same account. Is this a bug in the authentication system? Explain your reasoning. (40 marks)

(c) Explain what the term *salt* means in password hashing and explain why salts are used. (20 marks)