hrs	/ /20		Exams Office Use Only

University of the Witwatersrand, Johannesburg

Course or topic No(s)	ELEN3015
Course or topic name(s) Paper Number & title	Data and Information Management 2018/4/9 RW 5
Examination/Test* to be held during month(s) of (*delete as applicable)	April 2018
Year of Study (Art & Sciences leave blank)	Third
Degrees/Diplomas for which this course is prescribed (BSc (Eng) should indicate which branch)	B.Sc (Eng) Elec.
Faculty/ies presenting candidates	Engineering
Internal examiners and telephone number(s)	Prof. L. Cheng (x7228)
External examiner(s)	Prof. T. G. Swart
Special materials required (graph/music/drawing paper) maps, diagrams, tables, computer cards, etc)	None

Time allowance	Course Nos	ELEN3015	Hours	1.5

Instructions to candidates (Examiners may wish to use this space to indicate, inter alia, the contribution made by this examination or test towards the year mark, if appropriate)	Answer *ALL* questions. Type '2' Examination. Total marks: 53 - Full marks: 50

Internal Examiners or Heads of Department are requested to sign the declaration overleaf

1. As the Internal Examiner/Head of Department, I certify that this question paper is in final form, as approved by the External Examiner, and is ready for reproduction.

2. As the Internal Examiner/Head of Department, I certify that this question paper is in final form and is ready for reproduction.

(1. is applicable to formal examinations as approved by an external examiner, while 2. is applicable to formal tests not requiring approval by an external examiner—Delete whichever is not applicable)

Name:____________________________ Signature:____________________________

(THIS PAGE NOT FOR REPRODUCTION)

Course of topic: ELEN3015 Data and Information Management
Test Date: April 9, 2018 Test Venue: RW 5
Time allowance: 1.5 hours

Note: Show all workings, complete with the necessary comments. Marks will be allocated for all working and logical reasoning and not just for the correct answer.

Question 1

Consider a binary sequence. Given the input stream

100000000010010100011000110101000110

(read left to right), answer the following.

(a) Compress the above sequence by using the Lempel-Ziv algorithm.

(5 marks)

(b) Calculate the probabilities of digits 0 and 1 of the given sequence.

(1 marks)

(c) Calculate the entropy of this sequence in the second extension.

(3 marks)

(d) Implement Huffman coding based on the second extension of the alphabet.

(5 marks)

(e) Based on the answers in (a) and (d), compare the compression rates and comment on the trade-off between complexity and efficiency.

(2 marks)

(Total 16 marks)

Question 2

Given the two primes 197 and 199 for the RSA public-key crypto-system in this question, answer the following.

(a) Describe how to use these two primes to set up the RSA public-key crypto-system.

(5 marks)

(b) Is 7 a valid key? Why?

(3 marks)

(c) Determine the corresponding private key for the public key 25.

(5 marks)

(d) Show how to decrypt ciphertext 32 with the private key 23285, and determine the plaintext.

(5 marks)

(Total 18 marks)

Question 3

When determining the security of a HASH system, the cryptanalyst tries the following attacks.

(a) If the attacker is NOT allowed to modify the original message, determine the number of HASH calculations that would be required to have a 50% chance of generating a new message with the same HASH as the original message. In your calculations, assume the HASH length is 8 bits.

(4 marks)

(b) Derive the expression of number of HASH calculations, n, required to have a 20% chance of generating two different messages with the same HASH. Determine the approximate value of n.

(6 marks)

(Total 10 marks)

Question 4

Consider a known-plaintext attack performed on a double DES cryptosystem.

(a) Determine the maximum number of times the DES algorithm needs to be run when using the brute-force strategy.

(3 marks)

(b) Determine the maximum number of times the DES algorithm needs to be run when using the meet-in-the-middle strategy.

(6 marks)

(Total 9 marks)

(Exam Total 53 marks)

(100%=50 marks)
