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 2014/4/14 CBEH
Examination/Test* to be held during month(s) of (*delete as applicable)	April 2014
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)	Dr. L. Cheng (x7228)
External examiner(s)	Dr. 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: 50 - 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 14, 2014 Test Venue: CBEH
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

A columnar transposition cipher scheme is used for two parties who communicate securely over an open channel. The eavesdropper knows that the number of columns used in this cipher is not more than eight (8). The following ciphertext is eavesdropped:

itaeini nratnim tetneex otdfope icrhxcu methrcr wseithe

(a) Show the method to cryptanalyze the ciphertext by using the bigram.

(5 marks)

(b) Show the sums of frequency of 5 different possible solutions (widths).

(3 marks)

(c) Show the most likely plaintext and number of letters in each cipher block (hint: a non-continuous plaintext could be obtained if the eavesdropped sequence is composed of two fractions from two consecutive cipher blocks).

(7 marks)

(Total 15 marks)

th	1.52%	*en*	0.55%	*ng*	0.18%
he	1.28%	*ed*	0.53%	*of*	0.16%
in	0.94%	*to*	0.52%	*al*	0.09%
er	0.94%	*it*	0.50%	*de*	0.09%
an	0.82%	*ou*	0.50%	*se*	0.08%
re	0.68%	*ea*	0.47%	*le*	0.08%
nd	0.63%	*hi*	0.46%	*sa*	0.06%
at	0.59%	*is*	0.46%	*si*	0.05%
on	0.57%	*or*	0.43%	*ar*	0.04%
nt	0.56%	*ti*	0.34%	*ve*	0.04%
ha	0.56%	*as*	0.33%	*ra*	0.04%
es	0.56%	*te*	0.27%	*ld*	0.02%
st	0.55%	*et*	0.19%	*ur*	0.02%

(Total 15 marks)

Question 2

Given the two primes 13 and 17, answer the following.

(a) Describe how to use these two primes to setup an RSA public-key cryptosystem.

(5 marks)

(b) Is 33 a valid key for the above system? Why?

(5 marks)

(c) Determine the corresponding public key for the private key 35.

(7 marks)

(d) Encrypt integer 2 with private key 35, and show how to decrypt the ciphertext.

(8 marks)

(Total 25 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 6 bits.

(4 marks)

(b) Derive the expression of number of HASH calculations, n, required to have a 50% chance of generating two different messages with the same HASH. Determine the approximate value of n (try values below 15).

(6 marks)

(Total 10 marks)

(Exam Total 50 marks)

(100%=50 marks)
