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 2013/4/15 WSS101
Examination/Test* to be held during month(s) of (*delete as applicable)	April 2013
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. K. Ouahada
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: 55 - 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 15, 2013 Test Venue: WSS101
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

Two parties communicate securely over an open channel using a combined monoalphabetic and columnar transposition cipher scheme. One eavesdrops a ciphertext as follows:

ijwmjtgjjwswdrj tntxcyizmuhlhtw wjtwjtxryxxgjhx xjyqnyktjtmtyas

(a) In the first stage, show the frequency analysis method to cryptanalyze the monoalphabetic ciphertext by using the ETAOIN rule.

(5 marks)

(b) In the second stage, show the method to cryptanalyze the columnar transposition ciphertext by using the bigram (assume the anticipated column width is less than 6).

(5 marks)

i. Show the sums of frequency of different possible solutions.

(5 marks)

ii. Show the most likely plaintext.

(5 marks)

(Total 20 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%

Question 2

Given the encoding polynomial of a Reed-Solomon code $g(x) = (x-\alpha^1)(x-\alpha^2)(x-\alpha^3) = x^3 + \alpha^6 x^2 + \alpha^1 x + \alpha^6$ over GF(8), answer the following.

(a) Generate the systematic generator matrix.

(5 marks)

(b) Encode message $u(x) = 1 + \alpha^6 x^2 + \alpha^3 x^3$ systematically.

(5 marks)

(c) Choose a different input $u(x)$ and encode it in the same way. If the received sequence is $v(x) = 1 + x + x^2 + x^3 + x^4 + Ex^5 + Ex^6$, where E's denote two erasures, retrieve $u(x)$.

(10 marks)

(Total 20 marks)

Table 1: Construction of a $GF(2^3)$ field by $h(x) = 1 + x + x^3$

Codeword	Polynomial in $x \pmod{h(x)}$	Power of α
000	0	–
100	1	1
010	x	α
001	x^2	α^2
110	$1 + x$	α^3
011	$x + x^2$	α^4
111	$1 + x + x^2$	α^5
101	$1 + x^2$	α^6

Question 3

Consider a systematic binary cyclic code with the generator polynomial $g(x) = x + 1$ (Assume the number of inputs is k).

(a) Determine if the weight of any codeword in this code is even. Give a proof of your argument.

(5 marks)

(b) Determine the minimum Hamming distance of this code. Give a proof of your argument.

(5 marks)

(c) Give an implementation as a convolutional encoder with shift-registers. Draw the connections of the shift-registers.

(5 marks)

(Total 15 marks)

(Exam Total 55 marks)

(100%=50 marks)
