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 2011/4/8 CM5
Examination/Test* to be held during month(s) of (*delete as applicable)	April 2011
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: 47 - Full marks: 45

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 8, 2011 Test Venue: CM5
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

Given a (7, 4) Hamming code,

(a) If we add one more parity-check bit, which is the binary-sum of all the existing 7 bits, what is the parity-check matrix of the new code?

(b) What is the minimum Hamming distance of the new code? Prove it.

(Total 12 marks)

Question 2

For a 3-error-correcting (15, 9) Reed-Solomon code with the generator polynomial

$$\begin{aligned} g(x) =&(x+1)(x+\alpha)(x+\alpha^2)\dots(x+\alpha^5) \\ =&1+\alpha^4x+\alpha^2x^2+\alpha x^3+\alpha^{12}x^4+\alpha^9x^5+x^6 \end{aligned}$$

Suppose the received word is $10\alpha^2\alpha\alpha^{12}\alpha^9\alpha^8 00000000$, complete the following decoding process by using the Berlekamp-Massey algorithm:

The received sequence can be written in the polynomial

$$w(x) = \rule{6cm}{0.4pt}.$$

(a) We get the syndrome polynomials as:

$$\begin{aligned} s_0 =& w(\alpha^0) = \underline{?}, \\ s_1 =& w(\alpha^1) = \alpha^4, \\ s_2 =& w(\alpha^2) = \alpha^8, \\ s_3 =& w(\alpha^3) = \alpha^{13}, \\ s_4 =& w(\alpha^4) = \alpha^7, \\ s_5 =& w(\alpha^5) = \alpha^{11} \end{aligned}$$

(b)

$$\begin{aligned} q_{-1}(x) =& \rule{2.5cm}{0.4pt}, \\ q_0(x) =& \rule{2.5cm}{0.4pt}, \\ p_{-1}(x) =& x^7, \\ p_0(x) =& x^6, \\ d_{-1} =& -1, d_0 = 0, z_0 = -1. \end{aligned}$$

(c) Preceding the step 3, we can get the following table:

Table 1: Calculation results of step (c)

i	$q_i - p_i$									d_i	z_i
-1	α^0	α^{10}	α^4	α^8	α^{13}	α^7	α^{11}	–	α^0	-1	
0	α^{10}	α^4	α^8	α^{13}	α^7	α^{11}	–	α^0		0	-1
1	α^8	α^6	α^8	α^{11}	α^9	–	α^0	α^{10}		0	0
2	$\underline{?}$	α^{14}	0	α^6	–	α^0	α^9			1	1
3	α^7	α^3	0	–	α^0	$\underline{?}$	α^5			1	2
4	0	0	–	α^0	α^{11}	α^7				2	3
5	0	–	α^0	α^{11}	α^7					3	3
6	–	α^0	α^{11}	α^7						4	3

Finally, we obtain:

$$\sigma(x) = \rule{2cm}{0.4pt}.$$

(d) According to $\sigma(x)$, we get the error location numbers as __ and __.

(e) Solve the following function

$$\begin{pmatrix} 1 & 1 \\ \_ & \_ \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} \_ \\ \alpha^4 \end{pmatrix}$$

and we get $b_1 = \_$ and $b_2 = \_$.

The most likely error pattern is:

$$e = \_\_\_\_\_\_\_.$$

Then

$$c = w + e = \_\_\_\_\_\_\_.$$

(Total 20 marks)

Question 3

Alice and Bob wish to communicate securely over an open channel using a columnar transposition cipher scheme with the column width no more than 8. Eva eavesdrops a ciphertext as follows:

ddh rat snt ode srh udo nla ode bqa oef fsy tun tif wfa lig mna ior ece eti zre akr

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

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

(c) Show the most likely plaintext.

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)

(Exam Total 47 marks)

(100%=45 marks)