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
Examination/Test* to be held during month(s) of (*delete as applicable)	June 2012
Year of Study (Art & Sciences leave blank)	Third
Degrees/Diplomas for which this course is prescribed (BSc (Eng) should indicate which branch)	BSc (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	3

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. Closed book Engineering calculator permitted A4 handwritten information sheet Total marks: 100 - Full marks: 90

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

1. As the Internal Examiner/Head of School, 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 School, 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)

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.All terms and symbols are as defined in the course handouts. Answers written on your question paper will NOT be marked. Answers written in pencil will NOT be marked.

Question 1

The minimum polynomials of the Galois field GF(2^4) based on the primitive polynomial $h(x) = 1 + x + x^4$ are given in Table 1.

(a) What is the generator polynomial of a Bose-Chaudhuri-Hocquenghem (BCH) code with two errors correcting capability?

(5 marks)

(b) What is the code rate of this two-error-correcting code?

(5 marks)

Table 1: Minimal polynomials of the elements in $GF(2^4)$

Elements of $GF(2^4)$ using $h(x)$	Minimal polynomial
0	x
1	$x + 1$
α, α^2, α^4, α^8	$x^4 + x + 1$
α^3, α^6, α^9, α^{12}	$x^4 + x^3 + x^2 + x + 1$
α^5, α^{10}	$x^2 + x + 1$
α^7, α^{11}, α^{13}, α^{14}	$x^4 + x^3 + 1$

(Total 10 marks)

Question 2

The frequency band between 200 and 201 MHz is allocated to a communication system. The signal power is $S = 1023$ power unit. The noise in the band is additive white Gaussian noise with signal-sided power spectral density $N_0 = 1$ power unit per hertz.

(a) What is the Shannon limit on the achievable data rate (bits/sec)?

(5 marks)

(b) For a given bandwidth between 200 and 210 MHz, and transmission data rate of 10^7 bits/sec, what is the required signal-to-noise ratio in decibel (dB)?

(5 marks)

(Total 10 marks)

Question 3

A (7, 5) Reed-Solomon code used for erasure decoding is defined by the generator polynomial $g(x) = (x + \alpha)(x + \alpha^2)$ in GF(2^3). The GF(2^3) is specified by Table 2.

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

Codeword	Polynomial in x (mod $h(x)$)	Power of α
000	–	
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

(a) Complete the following procedure to encode a message.

i. $g(x) = (x + \alpha)(x + \alpha^2) =$ ________.

(3 marks)

ii. Given message $m(x) = \alpha x^3 + \alpha^2 x^2 + \alpha^3$, the codeword is $m(x)x^2 + m(x)x^2 \pmod{g(x)} =$ ________.

(6 marks)

(b) An unknown codeword encoded by this generator polynomial is sent over the noisy channel. The coefficients of the terms of degree 4, 5 of the codeword are erased. The two erased coefficients of the terms of degree 4, 5 are represented by A and B respectively. Then the received codeword can be represented as

$$r(x) = Bx^5 + Ax^4 + x^2 + x + \alpha^3.$$

Complete the following procedure to correct two erasure errors.

i. Substitute root α into $r(x)$ and obtain _________.

(3 marks)

ii. Substitute root α^2 into $r(x)$ and obtain _________.

(3 marks)

iii. Determine A and B by solving the two simultaneous equations.

(10 marks)

(Total 25 marks)

Question 4

Consider the key expansion procedure for AES encryption. If the given four subkeys are w_0 = 01 23 45 67, w_1 = 89 ab cd ef, w_2 = 01 23 45 67 and w_3 = 89 ab cd ef, complete the following procedure to generate the next subkey w_4. (Hints: all subkeys are in their hexadecimal formats and $\oplus$ is a bitwise exclusive-OR operator.)

(a) Generate temporary subkey $w_t = w_{\underline{?}}$.

(2 marks)

(b) Rotate (round-end) the binary sequence w_t to the left for 8 positions and obtain $w_t =$ ________.

(3 marks)

(c) Substitute w_t byte by byte according to Table 3 and obtain $w_t =$ ________.

(3 marks)

Table 3: AES S-Box

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

(d) Generate round constant $r_4 =$ ________ for w_4.

(3 marks)

(e) $w_t = w_t \oplus r_4 =$ ________.

(2 marks)

(f) $w_4 = w_t \oplus w_0 =$ ________.

(2 marks)

(Total 15 marks)

Question 5

(a) Draw a data flow digram of the encryption and decryption process of a cipher block chain. What is the significance of using an initialization vector?

(5 marks)

(b) Draw a data flow diagram to show the ciphertext stealing technique for a cipher block chain. What is the significance of using ciphertext stealing?

(5 marks)

(Total 10 marks)

Question 6

Consider a binary sequence. Given the input stream

111000111100001111000111000011

(read left to right), answer the following.

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

(10 marks)

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

(2 marks)

(c) Calculate the entropy of this sequence.

(3 marks)

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

(11 marks)

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

(4 marks)

(Total 30 marks)

(Exam Total 100 marks)

(100%=90 marks)