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 2013
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. K. Ouahada
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: 100

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 three (3) errors correcting capability?

(5 marks)

(b) What is the code rate of this three-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

Consider the key expansion procedure for AES encryption. If the given four subkeys are $w_4 = a0fafe17$, $w_5 = 88542cb1$, $w_6 = 23a33939$ and $w_7 = 2a6c7605$, complete the following procedure to generate the next subkey w_8.

(a) Generate the temporary subkey $w_t = w\_\_\_\_\_\_$.

(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 using Table 2 and obtain $w_t =$ ________

(3 marks)

(d) Generate the round constant $r_8 =$ ________ for w_8.

(3 marks)

(e) $w_t = w_t \oplus r_8 =$ ________.

(2 marks)

(f) $w_8 = w_t \oplus w_4 =$ ________.

(2 marks)

(Total 15 marks)

Table 2: 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

Question 3

Given the two primes 23 and 29, answer the following.

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

(5 marks)

(b) Is 7 a valid key for the above system? Why?

(7 marks)

(c) Determine the corresponding private key for the public key 9.

(7 marks)

(d) Encrypt integer 8 with public key 9, and show how to decrypt the ciphertext.

(6 marks)

(Total 25 marks)

Question 4

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)

Question 5

For a double DES encryption system,

(a) Explain the meet-in-the-middle attack and give the computational complexity of the cryptanalytic method for the double DES system.

(8 marks)

(b) Describe a scheme that can be used to circumvent the meet-in-the-middle attack.

(2 marks)

(Total 10 marks)

Question 6

Consider a binary sequence. Given the input stream

0001110000011110001111111000011

(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%=100 marks)
