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 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	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: 110 - Full marks: 100

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)

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) Consider voice transmission over a telephone line. Each channel has a bandwidth $B = 3$ kHz. We assume the analogue channel distorted by Additive White Gaussian Noise (AWGN). If the power signal-to-noise ratio is 20 dB, what is the channel capacity?

(10 marks)

(b) Consider Wideband Code Division Multiple Access (W-CDMA). For a given bandwidth $B = 5$ MHz, and transmission data rate of 25 kbps (kbits/sec), what is the required signal-to-noise ratio in decibel (dB)?

(5 marks)

(Total 15 marks)

Question 2

Given a (7, 4) cyclic code defined by the generator polynomial $g(x) = 1 + x + x^3$ used for Cyclic Redundancy Check (CRC),

(a) determine the maximum number of burst substitution errors that the code can detect.

(3 marks)

(b) justify the value obtained in (a) above.

(12 marks)

(Total 15 marks)

Question 3

Consider the key expansion procedure for AES encryption. If the given four subkeys are $w_0 = 2b7e1516$, $w_1 = 28aed2a6$, $w_2 = abf71588$ and $w_3 = 09cf4f3c$, complete the following procedure to generate the next subkey w_4.

(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 1 and obtain $w_t =$ _____

(3 marks)

(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)

Table 1: 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 4

Given the two primes 23 and 17, answer the following.

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

(5 marks)

(b) Is 9 a valid key for the above system? Why?

(7 marks)

(c) Determine the corresponding public key for the private key 7.

(7 marks)

(d) Encrypt integer 8 with private key 7, and show how to decrypt the ciphertext.

(6 marks)

(Total 25 marks)

Question 5

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 8 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 25).

(6 marks)

(Total 10 marks)

Question 6

Consider an alphabet with two letters x and y. Given the input stream

$$yxxxyyxyyyyxyxyyxyyyy,$$

answer the following.

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

(10 marks)

(b) If it takes 8 bits to encode a symbol (a–z) in ASCII and 5 bits to encode a digit (0–31), calculate the compression ratio of the Lempel-Ziv algorithm in this case.

(5 marks)

(c) Calculate the probabilities of letters x and y of the given sequence.

(4 marks)

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

(11 marks)

(Total 30 marks)

(Exam Total 110 marks)

(100%=100 marks)
