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 2019
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)	Prof. L. Cheng (x7228)
External examiner(s)	Prof. 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: 111 - 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

Alice and Bob wish to communicate securely over an open channel using a columnar transposition cipher scheme. Eva eavesdrops on 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.

(5 marks)

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

(5 marks)

(c) Show the most likely plaintext.

(5 marks)

$$\begin{pmatrix}
th & 1.52\% & en & 0.55\% & ng & 0.18\% \\
he & 1.28\% & ed & 0.53\% & of & 0.16\% \\
in & 0.94\% & to & 0.52\% & al & 0.09\% \\
er & 0.94\% & it & 0.50\% & de & 0.09\% \\
an & 0.82\% & ou & 0.50\% & se & 0.08\% \\
re & 0.68\% & ea & 0.47\% & le & 0.08\% \\
nd & 0.63\% & hi & 0.46\% & sa & 0.06\% \\
at & 0.59\% & is & 0.46\% & si & 0.05\% \\
on & 0.57\% & or & 0.43\% & ar & 0.04\% \\
nt & 0.56\% & ti & 0.34\% & ve & 0.04\% \\
ha & 0.56\% & as & 0.33\% & ra & 0.04\% \\
es & 0.56\% & te & 0.27\% & ld & 0.02\% \\
st & 0.55\% & et & 0.19\% & ur & 0.02\%
\end{pmatrix}$$

(Total 15 marks)

Question 2

Consider the key expansion procedure for AES encryption. The given four subkeys are $w_4 = a0fafe17$, $w_5 = 88542cb1$, $w_6 = 23a33939$ and $w_7 = 2a6c7605$ using hexadecimal notation.

(a) Complete the following procedure to generate the next subkey w_8.

i. Generate the temporary subkey $w_t = w$_______.

(2 marks)

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

(3 marks)

iii. Substitute w_t byte by byte using Table 1 and obtain $w_t =$ _________.

(3 marks)

iv. Generate the round constant $r_8 =$ _________ for w_8.

(3 marks)

v. $w_t = w_t \oplus r_8 =$ _________.

(2 marks)

vi. $w_8 = w_t \oplus w_4 =$ _________.

(2 marks)

(b) Let the irreducible polynomial for GF(2^8) be $m(x) = x^8 + x^4 + x^3 + x + 1$ (not primitive). The MixColumn Transformation is defined as

$$MC = \begin{pmatrix} \alpha & \alpha+1 & 1 & 1 \\ 1 & \alpha & \alpha+1 & 1 \\ 1 & 1 & \alpha & \alpha+1 \\ \alpha+1 & 1 & 1 & \alpha \end{pmatrix} \begin{pmatrix} B_{0,0} & B_{0,1} & B_{0,2} & B_{0,3} \\ B_{1,1} & B_{1,2} & B_{1,3} & B_{1,0} \\ B_{2,2} & B_{2,3} & B_{2,0} & B_{2,1} \\ B_{3,3} & B_{3,0} & B_{3,1} & B_{3,2} \end{pmatrix}.$$

Given $B_{0,0} = 89_{16}$, $B_{1,1} = 0_{16}$, $B_{2,2} = AB_{16}$ and $B_{3,3} = CD_{16}$, calculate the four elements in the first column of the resultant matrix.

(12 marks)

(Total 27 marks)

Question 3

(a) A memoryless information source has a countably infinite symbol alphabet $\mathbf{S} = \{S_1, S_2, \ldots\}$ with $P_i = b\alpha^i$ for $i = 1, 2, \ldots$. Express b in terms of α.

(5 marks)

(b) Calculate the entropy of $\mathbf{S}$ as a function of α.

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

(5 marks)

Hint: $\sum_{i=1}^{\infty} a^i = \frac{a}{1-a}$ and $\sum_{i=1}^{\infty} ia^i = \frac{a}{(1-a)^2}$ given $|a| \leq 1$.

(Total 10 marks)

Question 4

The frequency band between 100 kHz and 101 kHz is allocated to a communication system. The signal power is $S = 31$ power units per hertz. The noise in the band is additive white Gaussian noise with single-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 800 MHz and 850 MHz, and transmission data rate of 10^5 bits/sec, what is the minimum signal-to-noise ratio required in decibels (dB)?

(5 marks)

(Total 10 marks)

Question 5

Consider a (7, 4) Hamming code with a parity-check matrix,

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Add one more parity check bit with the binary-sum value of the existing all 7 bits.

(a) What is the new parity-check matrix?

(2 marks)

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

(4 marks)

(c) If the received sequence is [0 0 1 0 1 E 0 0] (E denotes erasure error), determine the codeword that was sent using the syndrome decoding algorithm.

(6 marks)

(Total 12 marks)

Question 6

Consider a Galois field GF(2^3) based on the primitive polynomial $h(x) = 1 + x^2 + x^3$.

(a) Derive the Galois field based on the given primitive polynomial in terms of binary sequences, polynomial notations and powers of the primitive element (α).

(5 marks)

(b) Derive the corresponding minimum polynomials.

(5 marks)

(c) Derive the generator polynomial of a single-error-correcting code based on the minimum polynomials. What is the rate of the code generated by the derived generator polynomial?

(5 marks)

(d) If the received sequence is [0 E 1 0 1 E 0] (E denotes erasure error), determine the codeword that was sent using the syndrome decoding algorithm.

(7 marks)

(Total 22 marks)

Question 7

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. Provide the proof.

(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 111 marks)

(100%=100 marks)