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 2015
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. 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: 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

A columnar transposition cipher scheme is used for two parties who communicate securely over an open channel. The eavesdropper knows that the number of columns used in this cipher is not more than eight (8). The following ciphertext is captured by an eavesdropper:

itaeini nratnim tetneex otdfope icrhxcu methrcr wseithe

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

(5 marks)

(b) Show the sums of frequency of 5 different possible solutions (widths).

(3 marks)

(c) Show the most likely plaintext and number of letters in each cipher block. A non-continuous plaintext could be obtained if the eavesdropped sequence is composed of two fractions from two consecutive cipher blocks.

(7 marks)

(Total 15 marks)

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

Question 2

This question concerns the Discrete Cosine Transform (DCT) based lossy scheme which is part of the Joint Photographic Experts Group (JPEG) standard.

(a) Draw the block diagram of JPEG compression process.

(3 marks)

(b) Explain why the above-mentioned compression process is a lossy process and why the lossy scheme is valid for image compression.

(3 marks)

(c) In an application of steganography, one tries to store secret data in a JPEG image. Give a solution by using the standard JPEG compression process.

(5 marks)

(Total 11 marks)

Question 3

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

(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)

(Total 15 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 unit per hertz. The noise in the band is additive white Gaussian noise with double-sided power spectral density $N_0 = 1/2$ 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 100 kHz and 110 kHz, and transmission data rate of 10^5 bits/sec, what is the required signal-to-noise ratio in decibels (dB)?

(5 marks)

(Total 10 marks)

Question 5

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

(5 marks)

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

(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 6

(a) Draw a data-flow diagram 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 7

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.

(Total 12 marks)

Question 8

Consider a (7, 4) Hamming code with 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 all the existing 7 bits.

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

(5 marks)

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

(5 marks)

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

(7 marks)

(Total 17 marks)

(Exam Total 100 marks)

(100%=100 marks)
