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)	April 2010
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)	Mr. DJJ Versfeld x7212
External examiner(s)	Prof ASJ Helberg
Special materials required (graph/music/drawing paper) maps, diagrams, tables, computer cards, etc)	None
Time allowance	Course Nos: ELEN3015 — Hours: One
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. Type '2' Examination.

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

Consider the following cryptographic system. The elements $0, 1, \ldots, 25$ of $\mathbb{Z}_{26}$ represent the letters A, B, ..., Z. Encryption consists of replacing each element x, by $\mathcal{E}(x)$ defined as follows:

$$\mathcal{E}_{k_e}(x) = (x \cdot k_e + k_e) \mod 26.$$

(a) Determine the size of the keyspace of the encryption function $\mathcal{E}_{k_e}(x)$.

(5 marks)

(b) Determine the function $\mathcal{D}_{k_d}(x)$ which will decrypt the ciphertext generated by $\mathcal{E}_{k_e}(x)$. Verify that $\mathcal{D}_{k_d}(x)$ is working as expected by encrypting the character C using the key $k_e = 5$ and then decrypting the resulting ciphertext with $\mathcal{D}_{k_d}(x)$.

(5 marks)

(c) Determine whether the cipher $\mathcal{E}_{k_e}(x)$ forms a groups (the cipher is closed).

(4 marks)

(d) What is the perceived keyspace and the effective keyspace of the double cipher consisting of $\mathcal{E}_{k_1}(\mathcal{E}_{k_2}(x))$? Determine the keys k_1 and k_2 for the following plaintext and ciphertext pairs:

- plaintext1 = 'BK' , ciphertext1 = 'FA', and
- plaintext2 = 'FI', ciphertext2 = 'XE'.

(16 marks)

(Total 30 marks)

Question 2

The following vector is received on a channel that introduces a maximum of one error per codeword:

$$\overline{r} = \left(\alpha^5,\ \alpha^1,\ 1,\ \alpha^2,\ \alpha^4,\ \alpha^2,\ \alpha^5\right).$$

Assume that the original codeword was generated with the generator matrix

$$G = \begin{bmatrix} \alpha^3 & \alpha^1 & 1 & \alpha^3 & 1 & 0 & 0 \\ \alpha^6 & \alpha^6 & 1 & \alpha^2 & 0 & 1 & 0 \\ \alpha^5 & \alpha^4 & 1 & \alpha^4 & 0 & 0 & 1 \end{bmatrix}.$$

Determine whether $\overline{r}$ is a valid codeword or not. If $\overline{r}$ is not a valid codeword, determine the position of the error, as well as the correct value of the element in error. Assume that the elements are from the Galois field GF(2^m), generated by $p(x) = x^3 + x + 1$.

Show all intermediate steps.

(25 marks)

(Test Total 55 marks)

(100%=50 marks)
