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 2009
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. D. J. J. 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: $1\frac{1}{2}$
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 mapping depicted in Table 1.

Table 1: Character to decimal conversion

Character	Number	Comment		Character	Number	Comment
'a'	0			'o'	14	
'b'	1			'p'	15	
'c'	2			'q'	16	
'd'	3			'r'	17	
'e'	4			's'	18	
'f'	5			't'	19	
'g'	6			'u'	20	
'h'	7			'v'	21	
'i'	8			'w'	22	
'j'	9			'x'	23	
'k'	10			'y'	24	
'l'	11			'z'	25	
'm'	12			' '	26	space
'n'	13					

(a) Determine the keyspace $\mathcal{K}$ of the cipher $\mathcal{E}_k(P)$, where

$$\begin{aligned} C &= \mathcal{E}_k(P) \\ C &= (P \times k) \mod 27, \end{aligned}$$

with k an integer number, P the plaintext character ($P \in \{0, 1, 2, \ldots, 26\}$) and C the resulting ciphertext. Motivate your answer.

(5 marks)

(b) Prove that the ciphertext $C = \mathcal{E}_k(P)$ is decrypted by $\mathcal{D}_{k^{-1}}(C)$, where

$$\begin{aligned} P &= \mathcal{D}_{k^{-1}}(C) \\ P &= (C \times k^{-1}) \mod 27, \end{aligned}$$

with k^{-1} the multiplicative inverse of k satisfying $1 \equiv (k \times k^{-1}) \mod 27$.

(2 marks)

(c) Consider the block cipher $\mathcal{C}_T(p_1, p_2, p_3)$, with key $K_T = (k_1, k_2, k_3)$ and output $C_T = (c_1, c_2, c_3)$, where $c_i = (p_i \times k_i) \mod 27$. Determine the size of the keyspace $\mathcal{K}_T$.

(1 marks)

(d) Describe, with the aid of sketches, how cipher block chaining mode works. Show both encryption and decryption.

(2 marks)

(e) What is the advantage of cipher block chaining mode, when compared to electronic block mode?

(2 marks)

(f) Encrypt the message 'blue fox' using $\mathcal{C}_T$ in cipher block chaining mode. Make use of ciphertext stealing. Clearly indicate the order in which the messages are transmitted over the channel.

Parameters to be used:

- Initialisation Vector (IV) = (25, 3, 12)
- $k_1 = 10$, $k_2 = 14$, $k_3 = 23$
- Replace all XOR operations with addition $\mod 27$
- The message to be encrypted has 8 characters

(10 marks)

(Total 22 marks)

Question 2

The matrix C is the result after the ShiftRows operation of a round during AES encryption.

$$C = \begin{bmatrix} d4 & e0 & b8 & 1e \\ bf & b4 & 41 & 27 \\ 5d & 52 & 11 & 98 \\ 30 & ae & f1 & e5 \end{bmatrix}$$

Compute x, the missing element of the matrix D, where D is the output after the MixColumns operation.

$$D = \begin{bmatrix} 04 & e0 & 48 & 28 \\ 66 & x & f8 & 06 \\ 81 & 19 & d3 & 26 \\ e5 & 9a & 7a & 4c \end{bmatrix}$$

Hints:

$$M = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

$m(x) = x^8 + x^4 + x^3 + x + 1$

(Total 10 marks)

Question 3

Alice and Bob wish to communicate securely over an open channel using a public-key scheme. They decide to use the RSA algorithm.

(a) Bob generates two primes, $p = 127$ and $q = 131$, to be used with the RSA algorithm. From this determine n, $\varphi(n)$ and the decryption key d, given that $e = 121$.

(18 marks)

(b) Using pseudocode implement the RSA encryption function $m^e \mod n$ for a processor with a word size limited to z bits, such that the largest values for m, e and n can be used. Specify the values for m, e and n which will ensure that no overflows occur. (Assume that the processor has a function $a \mod p$, where a and $p \leqslant 2^z - 1$).

(5 marks)

(Total 23 marks)

(Test Total 55 marks)

(100%=50 marks)
