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 2008
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)	Dr. W. A. Clarke
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

What is ciphertext stealing? Explain how ciphertext stealing can be implemented in Electronic codebook mode (make use of sketches).

(Total 5 marks)

Question 2

Refer to the algorithm depicted in Fig. 1 and the key schedule of Table 1.

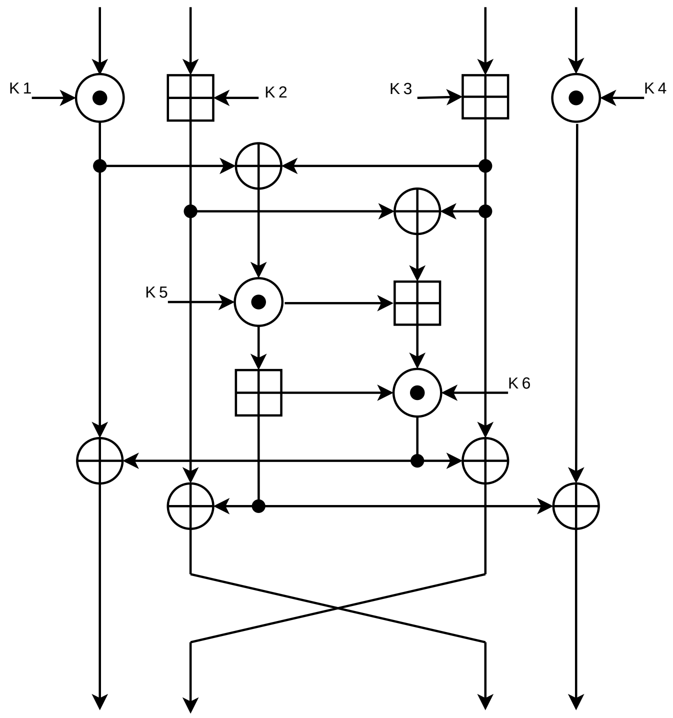

Figure 1: Algorithm

(a) Identify the cryptographic system.

(1 marks)

(b) Determine the output of the top left operation if $K_1 = AB78_{16}$ and the other input is $1AB8_{16}$.

(3 marks)

Table 1: Key Schedule - Decryption

Round	Subkeys					
1st	$Z_1^{(9)-1}$	-$Z_2^{(9)}$	-$Z_3^{(9)}$	$Z_4^{(9)-1}$	$Z_5^{(8)}$	$Z_6^{(8)}$
2nd	$Z_1^{(8)-1}$	-$Z_3^{(8)}$	-$Z_2^{(8)}$	$Z_4^{(8)-1}$	$Z_5^{(7)}$	$Z_6^{(7)}$
3rd	$Z_1^{(7)-1}$	-$Z_3^{(7)}$	-$Z_2^{(7)}$	$Z_4^{(7)-1}$	$Z_5^{(6)}$	$Z_6^{(6)}$
4th	$Z_1^{(6)-1}$	-$Z_3^{(6)}$	-$Z_2^{(6)}$	$Z_4^{(6)-1}$	$Z_5^{(5)}$	$Z_6^{(5)}$
5th	$Z_1^{(5)-1}$	-$Z_3^{(5)}$	-$Z_2^{(5)}$	$Z_4^{(5)-1}$	$Z_5^{(4)}$	$Z_6^{(4)}$
6th	$Z_1^{(4)-1}$	-$Z_3^{(4)}$	-$Z_2^{(4)}$	$Z_4^{(4)-1}$	$Z_5^{(3)}$	$Z_6^{(3)}$
7th	$Z_1^{(3)-1}$	-$Z_3^{(3)}$	-$Z_2^{(3)}$	$Z_4^{(3)-1}$	$Z_5^{(2)}$	$Z_6^{(2)}$
8th	$Z_1^{(2)-1}$	-$Z_3^{(2)}$	-$Z_2^{(2)}$	$Z_4^{(2)-1}$	$Z_5^{(1)}$	$Z_6^{(1)}$
Last	$Z_1^{(1)-1}$	-$Z_2^{(1)}$	$-Z_3^{(1)}$	$Z_4^{(1)-1}$		

(c) Given that $K_2^{(9)} = 2C1B_{16}$, determine the value of K_2 for the first round of decryption.

(2 marks)

(d) Given the key (in the form LSB … MSB):

1001101011101001011101110100101011101000101010101101000110111001
1001100110010111001110101110100111000011111110010101010011010110,

determine the subkeys $K_1^{(2)}$, $K_2^{(2)}$, $K_3^{(2)}$ and $K_4^{(2)}$

(4 marks)

(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) Using the Solovay-Strassen test, determine if the number 11131 is prime, using 121 as a witness. (Indicate all the intermediate steps.)
Hint: $121^{5564} \mod 11131 = 92$

(10 marks)

(b) Bob generates two primes, $p = 113$ and $q = 109$, to be used with the RSA algorithm. From this determine n, $\varphi(n)$ and the decryption key d, given that $e = 101$.

Hint:

$$\begin{aligned}101 \times d_1 &= 78 \times Q + r_1\\101 \times d_2 &= 79 \times Q + r_2\\101 \times d_3 &= 80 \times Q + r_3\\101 \times d_4 &= 81 \times Q + r_4\\101 \times d_5 &= 82 \times Q + r_5\end{aligned}$$

(7 marks)

(c) Encrypt the message 00054.
(Hint: $54^{100} \equiv 5706$, using the specified modular arithmetic)

(3 marks)

(Total 20 marks)

Question 4

Consider the even parity code C used on 8-bit bytes, i.e., a codeword c is in the form $(v_0, u_0, u_1, \ldots, u_6)$, where v_0 is the redundancy and u_i, $i \in \{0, 1, \ldots, 6\}$ is the message. Also, v_0 is equal to 0 if the number of ones in the information part is even, else it is a logical one.

(a) Derive the parity-check equations for the code C.

(2 marks)

(b) Determine the systematic generator matrix G for the code C.

(3 marks)

(c) Determine the parity-check matrix H for the code C.

(2 marks)

(d) Determine the minimum distance of the code C and comment on the error detection and error correction capabilities of C.

(3 marks)

(Total 10 marks)

Question 5

Consider the polynomial $g(x) = 1 + x^3 + x^4 + x^5 + x^8$.

(a) Show that $g(x)$ generates a code C of length $n = 17$.

(3 marks)

(b) Determine the parameter k of the code C.

(2 marks)

(c) Systematically encode the message $(1, 1, \ldots, 1)$.

(5 marks)

(Total 10 marks)

(Test Total 55 marks)

(100%=50 marks)
