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 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. D.J.J. Versfeld (x7212)
External examiner(s)	Dr. T.G. Swart
Special materials required (graph/music/drawing paper) maps, diagrams, tables, computer cards, etc)	None

Time allowance

Course Nos	ELEN3015	Hours	Three

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.
Total marks: 115 - Full marks: 100

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 a $(n,\ k)$ Reed-Solomon code with the following parameters:

- $n = 7$, and
- $g(x) = x^4 + \alpha^3 x^3 + x^2 + \alpha^1 x^1 + \alpha^3$.

Table 1 lists some primitive polynomials.

Table 1: Primitive polynomials

$1 + x + x^3$
$1 + x + x^4$
$1 + x^2 + x^5$
$1 + x + x^6$

(a) Generate the appropriate Galois field to be used in the rest of the calculations.

(8 marks)

(b) Determine the root of lowest power for $g(x)$. (Hint: The root of lowest power is one of the following $\{\alpha^0, \alpha^1, \alpha^2\}$.)

(4 marks)

(c) Assuming that a code polynomial $c(x)$ is transmitted and the polynomial $r(x)$ is received, where the coefficients corresponding to x^3 and x^5 are in error, determine:

i. the error-locator polynomial $\sigma(x)$,

(4 marks)

ii. the error polynomial $E(x)$, given that $Z_0(x) = \alpha^3 + x$.
Hint:

$$\delta_k = \frac{-Z_0(\beta_k^{-1})}{\sigma'(\beta_k^{-1})}$$

(6 marks)

iii. Given that

$$G = \begin{bmatrix} \alpha^3 & \alpha^1 & 1 & \alpha^3 & 1 & 0 & 0 \\ \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 & \lambda_5 & \lambda_6 & \lambda_7 \\ \alpha^5 & \alpha^4 & 1 & \alpha^4 & 0 & 0 & 1 \end{bmatrix},$$

and $r(x) = \alpha^4 + \alpha^1 x + \alpha^5 x^2 + \alpha^6 x^3 + \alpha^1 x^4 + 0x^5 + \alpha^4 x^6$, confirm that $E(x)$ is correctly calculated by making use of erasure decoding. (Note that λ_i indicates values to be calculated.)

(10 marks)

Show all intermediate steps.

(Total 32 marks)

Question 2

Consider the hash function

$$\mathcal{H}_{(k_1,k_2,k_3,k_4)}(x_1, x_2, x_3, x_4, x_5) = (x_1 \cdot k_1 + x_2 \cdot k_2 + x_3 \cdot k_3 + x_4 \cdot k_4 + x_5 \cdot (k_3 \cdot k_4)) \mod 26,$$

where the inputs x_1, x_2, x_3, x_4, $x_5 \in \{0, \ldots 25\}$ represent the numerical values for the letters of the alphabet.

(a) Derive an equation for the probability that a message has the same hash as M_1 and determine the number of messages needed in order to find another message with hash M_1 with probability greater than 50 %.

(6 marks)

(b) Derive an equation for the probability that that any two messages share the same hash and determine the number of messages needed in order to find two messages with same hash with probability greater than 50 %.

(6 marks)

(c) Explain the significance of the two answers.

(5 marks)

(Total 17 marks)

Question 3

A random number generator outputs the list of numbers depicted in Table 2 as candidates for prime numbers. Table 3 lists a number of values and their relationships with the numbers in Table 2. Using the witness $a = 623$ for all your calculations, encrypt the message 1023 using RSA and write down the corresponding decryption function. When selecting or rejecting a number from Table 2, clearly motivate your decision with supporting calculations. (Table 4 lists some modulo computations.)

Table 2: Candidate primes

Number	Is prime?
1513	Not confirmed
1013	Not confirmed
1721	Confirmed

Table 3: Possible values for e

Number	Property
407	$1 = (-664537) \cdot 407 + 104 \cdot 2600640$
507	$3 = 394969 \cdot 507 + (-77) \cdot 2600640$
417	$1 = (-743007) \cdot 417 + 178 \cdot 1740640$
425	$5 = 32765 \cdot 425 + (-8) \cdot 1740640$
415	$1 = (-549377) \cdot 415 + 149 \cdot 1530144$
427	$7 = 75253 \cdot 427 + (-21) \cdot 1530144$

Table 4: Some calculations

$\mod (623^{756}, 1513) = 89$	$\mod (623^{506}, 1013) = 1012$
$\mod (1023^{405}, 2603873) = 1635371$	$\mod (1023^{505}, 2603873) = 1678271$
$\mod (1023^{415}, 1743373) = 1647067$	$\mod (1023^{423}, 1743373) = 1306262$
$\mod (1023^{413}, 1532669) = 653050$	$\mod (1023^{425}, 1532669) = 1425141$

(Total 24 marks)

Question 4

(a) The string $0x\ 0y\ 2y\ 1x\ 2x\ 4x\ 5y\ 4y\ 6x$ is the output after a message has been encoded with a Lempel-Ziv encoder. Find the original message and determine the entropy of the source.

(5 marks)

(b) Let X be the source which emits heads with a probability 0.7 and tails with a probability 0.3. Find an optimal encoding for X^3, the third extension of X. What is the average word length of X^3?

(10 marks)

(Total 15 marks)

Question 5

Your company has been tasked to develop a medium-security solution for access control where embedded devices are used to read fingerprints, encrypt the data and send the data over a potentially open channel, where the fingerprint will then be matched against data stored in a database. Preliminary studies have narrowed down the underlying cryptographic algorithm to be either AES or DES. Compare the two cryptographic algorithms, and then finally propose one, in terms of suitability for this particular application where speed, limited processing power and limited memory resources are the main considerations. Assuming that the output from the fingerprint reader is 1024 bits, develop a scheme (at blockdiagram level, i.e., you can treat one encryption or decryption as a block) that encrypts each fingerprint read as a unique ciphertext message, in order to prevent an intruder from intercepting valid messages and replaying them over the open channel. The length of the ciphertext message that is to be transmitted over the channel should not exceed 1152 bits.

(Total 12 marks)

Question 6

Discuss the JPEG still image compression standard. (Hint: Sketch the block diagram and discuss why each step in the compression process is needed and how each step is performed.)

(Total 15 marks)

(Exam Total 115 marks)

(100%=100 marks)
