hrs	/ /20		Exams Office Use Only

University of the Witwatersrand, Johannesburg

Course or topic No(s)	ELEN330
Course or topic name(s) Paper Number & title	Information Engineering Techniques
Examination/Test* to be held during month(s) of (*delete as applicable)	June 2006
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. S. Mohamed x77236 Prof. T. Marwala x77217
External examiner(s)	Dr. W. A. Clarke
Special materials required (graph/music/drawing paper) maps, diagrams, tables, computer cards, etc)	Refer to the attached information sheet for any extra information that is needed.

Time allowance

Course Nos	ELEN330	Hours	Two

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 and 1 Handwritten A4 Information Sheet
There is a total of 70 marks, but 60 marks is 100%

Internal Examiners or Heads of Department are requested to sign the declaration overleaf

State any assumptions that are made. Marks will be allocated for all working and logical reasoning and not just for the correct answer.

Question 1

(a) Consider the following cryptosystem. The elements 0, 1, ..., 25 of $\mathbb{Z}_{29}$ represent the letters A,B, ..., Z in the usual order, and 26, 27, 28 represent the comma, space and full stop. A key is a pair (a, b) with $a, b \in \mathbb{Z}_{29}$ and $a \neq 0$. Encryption consists of replacing each symbol x, by $e(x)$ defined as follows:

$$e(x) = (ax + b) \bmod 29$$

What is the decryption function? Discuss the possibility of discovering the key to this system by using

i. an exhaustive key search

ii. a chosen plaintext attack. (4 marks)

(b) A variation of the Vigenère cipher is the auto key cipher which s described as follows: Sender and receiver have agreed on a secret keyword K with p letters. The first p letters of the plaintext are encrypted as in the standard Vigenère cipher. The rest of the encryption differs: The shift to be used at position k is decided not by the keyword letter at position k mod p as in standard Vigenère, but instead by the *ciphertext* letter at position $k - p$, which has already been determined. This implies that the Vigenère can be used with a potentially infinite key consisting of K followed by the ciphertext.

Decrypt the ciphertext `WFMBHJ` that has been encrypted using the keyword `EXAM`. Make use of the Vigenère table that appears at the end of the question paper.

(4 marks)

(Total 8 marks)

Question 2

(a) Present a time/memory tradeoff known plaintext attack against an "EEEE" DES mode; a mode which uses 4 independent keys (each 56 bits; 224 total) to encrypt a 64-bit block by applying DES 4 times. An attack is considered effective if $max(time, memory)$ is less than the time/memory required for an exhaustive key search. (6 marks)

(b) We are trying to break a variable-strength secret key encryption system (such as Secure Sockets Layer, SSLv3). Exhaustive key search through the keyspace is the only available way of breaking the cipher. A standard PC CPU + motherboard costing R3200.00 can check about 15 million keys per second. We wish to have a solution within 30 days. How much will such a setup cost (excluding labour, etc) for the following effective key sizes?

i. "Low–grade" encryption: 40-bit keyspace.

ii. "Export–grade" encryption 56-bit keyspace.

iii. 64-bit key–space. (6 marks)

(Total 12 marks)

Question 3

(a) Answer the following questions in relation to public–key cryptography:

i. In a public-key cryptosystem you do not need to keep the encryption key a secret. Why is it essential to keep the encryption key secret in a symmetric cryptosystem. (2 marks)

ii. Describe the RSA (Rivest Shamir Adleman) pubic key cryptosystem. Your answer should include:

1. The generation of public and private keys
2. The encryption algorithm
3. The decryption algorithm
4. The basis for the security of RSA (6 marks)

iii. Bob has public RSA key $(n, e) = (77, 7)$. Show that Bobs private key is $d = 43$. (2 marks)

iv. Alice wants to send the message $M = 13$ to Bob. She encrypts the message using Bob's public key. What is the value of the ciphertext that Alice sends to Bob? (2 marks)

(b) The following questions relate to the popular cryptosystem PGP (Pretty Good Privacy):

i. PGP combines public and symmetric key cryptography to provide confidentiality as follows:

1. Alice creates a message M
2. Alice generates a random session key k.
3. Alice encrypts the session key using Bob's public key and public key cryptosystem to obtain k'.
4. Alice encrypts the message M using a symmetric cryptosystem with session key k to obtain ciphertext c.
5. Alice sends Bob the values of k' and c.

With the aid of a diagram, list the steps that Bob must take to recover the message M. (4 marks)

ii. Why does PGP use both public and symmetric key cryptography and not just one or the other? (2 marks)

(c) Alice and Bob are using a public-key cryptosystem and both have their own public and private key pairs. Describe how they can use the public key system in conjuction with MD5 to produce and verify digital signatures. (5 marks)

(Total 23 marks)

Question 4

(a) A zero memory information source produces the following sequence of symbols:

`01100111111001101101011110`

Determine the entropy $H(M)$ of this source. Show all workings. (3 marks)

(b) Two types of error correction can be applied when transferring data across a communications medium (eg. network), viz., the Automatic Repeat Request (ARQ) or the Forward Error Correction (FEC). Describe briefly how these types of error correction schemes operate. (4 marks)

(c) The School of Electrical and Information Engineering is now placing the management of all the laboratories under a new automated and on-line system. This system allows for the booking of lab times and for monitoring and control of the lab usage. An initial system specification for the information that is to be stored in a database for each lab is given in table 1, with some representative information:

Table 1: Sample table showing key fields of the lab management database system

Code	Supervisor	Lab Name	Courses Using Lab
1	Dr. Anderson	B- Lab	ELEN 100, ELEN 224, ELEN 324
2	Prof. Parks	C-Lab	ELEN 442, ELEN 326, ELEN 456

Normalise the above database up to the second normal form (2NF), showing how you move from one stage to the next. Explain the logic that you use in moving from one normal form to the next and the logic of the particular database arrangement that you have chosen. (8 marks)

(Total 15 marks)

Question 5

(a) Describe the key elements associated with crawler–based search engines. Discuss how each of the elements you have identified are related and what the function of each is. Make use of diagrams and an explanation in your answer. Mention a software tool that can be used to implement one of these systems practically. (6 marks)

(b) Students of the biological sciences are increasingly faced with the problem of large amounts of measurement and survey data that is acquired, with no means or methodology of understanding this data. As an Information Engineer working with many scientists from the life sciences, explain what the benefit and impact of using data mining tools are for the analysis of data sets. In your answer, give an explanation of what you understand data mining to be, as well as examples of the types of understanding that data mining can give to the scientist using these tools. (6 marks)

(Total 12 marks)

(Exam Total 70 marks)

(100%=60 marks)

Additional Information

TABLE 2.5 VIGENÈRE TABLEAU

```
   0         1         2
   01234567890123456789012345

   abcdefghijklmnopqrstuvwxyz
A  abcdefghijklmnopqrstuvwxyz   0
B  bcdefghijklmnopqrstuvwxyza   1
C  cdefghijklmnopqrstuvwxyzab   2
D  defghijklmnopqrstuvwxyzabc   3
E  efghijklmnopqrstuvwxyzabcd   4
F  fghijklmnopqrstuvwxyzabcde   5
G  ghijklmnopqrstuvwxyzabcdef   6
H  hijklmnopqrstuvwxyzabcdefg   7
I  ijklmnopqrstuvwxyzabcdefgh   8
J  jklmnopqrstuvwxyzabcdefghi   9
K  klmnopqrstuvwxyzabcdefghij  10
L  lmnopqrstuvwxyzabcdefghijk  11
M  mnopqrstuvwxyzabcdefghijkl  12
N  nopqrstuvwxyzabcdefghijklm  13
O  opqrstuvwxyzabcdefghijklmo  14
P  pqrstuvwxyzabcdefghijklmop  15
Q  qrstuvwxyzabcdefghijklmnop  16
R  rstuvwxyzabcdefghijklmnopq  17
S  stuvwxyzabcdefghijklmnopqr  18
T  tuvwxyzabcdefghijklmnopqrs  19
U  uvwxyzabcdefghijklmnopqrst  20
V  vwxyzabcdefghijklmnopqrstu  21
W  wxyzabcdefghijklmnopqrstuv  22
X  xyzabcdefghijklmnopqrstuvw  23
Y  yzabcdefghijklmnopqrstuvwx  24
Z  zabcdefghijklmnopqrstuvwxy  25
```

Figure 1: Vignere Table