ELEN 330 – Information Engineering Techniques
Examination, June 2001

Instructions to candidates:

1. Answer all questions. 80 marks (out of the 100 possible) represents full marks.
2. Show all working: marks will be allocated for all working and logical reasoning and not just for the correct answer.
3. Give reasons for any assumptions that are made.
4. Type 2 exam – this is a closed book exam. Candidates are allowed to use an engineering calculator and one handwritten A4 information sheet.

Question 1

(a) Explain why it is considered important for the security of a cipher to reside in the key and *not* in the algorithm. Explain also the difference between classic and modern ciphers. **(4 marks)**

(b) (i) Encrypt the following sample plaintext using a first columnar transposition cipher of 7 columns and then a monoalphabetic substitution cipher formed by a 5-position left rotation of the alphabet.

(5 marks)

```
LONG TIME THE MANXOME FOE HE SOUGHT
```

(ii) Tabulate the likely letter frequency distribution of a large ciphertext sample produced by the above cipher (assuming that the plaintext is English) – show entries only for the 6 most frequent characters in your table.

(3 marks)

(iii) Explain precisely what steps a cryptanalyst, knowing only that one columnar transposition cipher and one monoalphabetic substitution had been used, would take in recovering the plaintext from the ciphertext.

(6 marks)

(c) Explain the terms “confusion” and “diffusion” and give examples of classical ciphers which make use of each.

(3 marks)

(d) Double encryption *may* be used to improve the security of a basic cipher. Write a few lines contrasting the notion of using this method for a monoalphabetic substitution vs. a transposition cipher.

(4 marks)

Question 2

(a) Explain and give a mathematical definition of the term “closed cipher”. **(2 marks)**

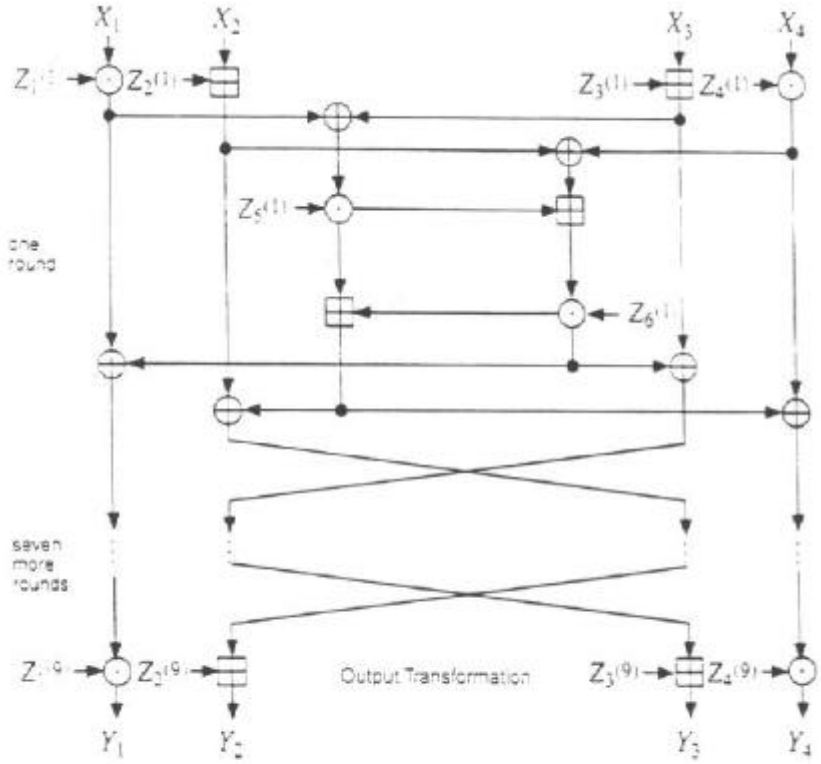
(b) A cryptographer proposes to improve the security of a cipher by using the cipher twice in succession, with two different keys (double-encryption). Explain, with the aid of rudimentary equations, why it is advisable to know whether or not the cipher is *closed*, and what the implication is for the proposed scheme.

(5 marks)

(c) Give a clear explanation of the *meet-in-the-middle* attack. What kind of cryptosystem is it applied to and how it is implemented? Describe a scheme that can be used to circumvent the *meet-in-the-middle* attack.

(5 marks)

(d) Figure 1 depicts IDEA, a 64 bit symmetric block cipher that uses a 128 bit key.



IDEA weak keys

0000 0000 0x00 0000 0000 000x xxxx x000

Figure 1 The IDEA Symmetric Cipher

(i) Reproduce the second round of this diagram in your answer book, labelling the widths of the data paths shown and explaining the function of the symbols shown in the diagram. **(5 marks)**

(ii) Given that 2^{128} = 340282366920938463463374607431768211456, and the information given in Figure 1 about IDEA weak keys (keys that would not be used), determine the *exact* keyspace of IDEA (write down the numerical value in full).

(3 marks)

(iii) Part of IDEA's key schedule specifies a 25 bit left rotation in deriving subkeys. Using this information and the information given in Figure 1, write the first four subkeys for the *second* round into your diagram, given the primary key (in binary notation) below. Specify the required subkeys in hexadecimal notation.

```
10011001100101110011101011101001110000111111100101010100110101110
10011010111010010111011101001010111010001010101011010001101110001
```

(5 marks)

Question 3

(a) OFB (output feedback mode) is useful in data streaming applications such as Secure Sockets Layer (SSL). Draw a block diagram showing how OFB may be implemented using a symmetric block cipher. Discuss any attack(s) which CFB mode is resistant to, what special provisions have to be made to ensure this resistance.

(8 marks)

(b) What are two most important properties of a secure hash function?

(2 marks)

(c) With reference to hash algorithms, explain what the birthday attack is and how the threat of this attack affects the choice of a hash algorithm's hash size. (Note: probability calculations are not required).

(6 marks)

(d) The accompanying information sheet includes data on the MD5 hash algorithm. Use this information to implement the first iteration of the first round, up to the input of the shifting stage only, using the plaintext block given below. Only the least significant byte of the result is required.

```
A493 23FF 5B90 B1E8 2C8A F924 BA5C 3267 B2AC 0126 6CA5 78BA
6679 5580 DF89 AF66 6DC0 53DD 38AC 3D86 AE93 6494 3BFE BD49
B68A 0655 D579 21F7 15CB B22C 1BE7 BBC6
```

(9 marks)

Question 4

(a) Mallory cryptanalyses a popular hash function and discovers that it is seriously flawed. Describe how he can use this flaw to defraud Bob. **(6 marks)**

(b) In the proof that the Rivest Shamir Adleman (RSA) deciphering function is the inverse of its enciphering function, the following use is made of Euler's Theorem:

$$M_i^{\ \ddot{o}(n)} \bmod n = 1$$

Where ö(n) is the Euler Totient function and the other symbols have their usual meaning. Euler's theorem requires both that Mi and n are relatively prime and that $M_i < n$. Explain why these assumptions are valid in the context of RSA. **(4 marks)**

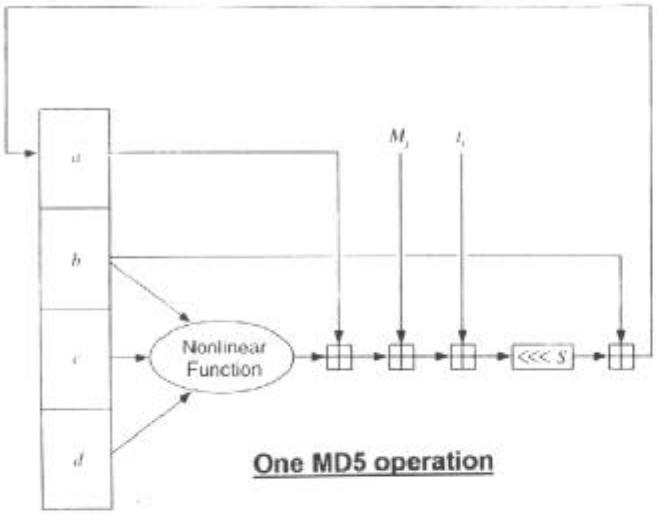
(c) Alice wishes to send Bob instructions and files by email in such a way that firstly: no one else intercepting the email will know what the instructions and file contents are and secondly: Bob knows with certainty that Alice sent the email. They have decided to use the RSA public key algorithm, the SHA hash algorithm and the AES symmetric algorithm in their scheme. Draw a complete block diagram of Alice and Bob's possible implementation, showing the flow of data and keys, and processes such as encryption and hashing. **(8 marks)**

(d) Given the product of two prime numbers 11 * 7 = 77 and the choice of RSA private key (77,43), determine and write down the public key for this cryptosystem. Table 1 provides the data you need to do this. Hence write down the encryption and decryption functions for the cryptosystem.

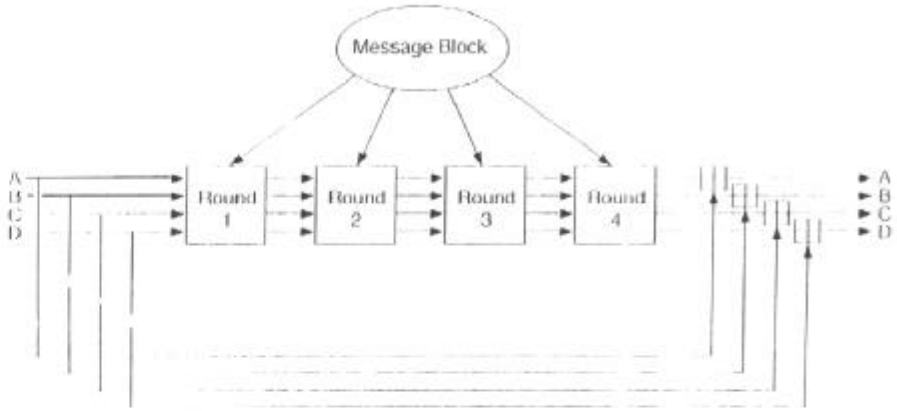
```
43 * 1  = 0 * 60 + 43
43 * 2  = 1 * 60 + 26
43 * 3  = 2 * 60 +  9
43 * 4  = 2 * 60 + 52
43 * 5  = 3 * 60 + 35
43 * 6  = 4 * 60 + 18
43 * 7  = 5 * 60 +  1
43 * 8  = 5 * 60 + 44
43 * 9  = 6 * 60 + 27
43 * 10 = 7 * 60 + 10
```

Table 1 **(5 marks)**

(e) Identify Dave's motives for the following actions: he uses his private key to encrypt a file containing Alice's name, email address and public key. He then encrypts the whole with Bob's public key and sends the result to Bob (who trusts Dave). **(2 marks)**



One MD5 operation



MD5 Main Loop

$F(X,Y,Z) = (X \wedge Y) \vee ((\neg X) \wedge Z)$
$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge (\neg Z))$
$H(X,Y,Z) = X \oplus Y \oplus Z$
$I(X,Y,Z) = Y \oplus (X \vee (\neg Z))$

($\oplus$ is XOR, $\wedge$ is AND, $\vee$ is OR, and $\neg$ is NOT.)

A = 0x01234567
B = 0x89abcdef
C = 0xfedcba98
D = 0x76543210

MD5 initial values

$FF(a,b,c,d,M_j,s,t_i)$ denotes $a = b + ((a + F(b,c,d) + M_j + t_i) <<< s)$
$GG(a,b,c,d,M_j,s,t_i)$ denotes $a = b + ((a + G(b,c,d) + M_j + t_i) <<< s)$
$HH(a,b,c,d,M_j,s,t_i)$ denotes $a = b + ((a + H(b,c,d) + M_j + t_i) <<< s)$
$II(a,b,c,d,M_j,s,t_i)$ denotes $a = b + ((a + I(b,c,d) + M_j + t_i) <<< s)$

MD5 INFORMATION SHEET

Round 1:

FF (*a*, *b*, *c*, *d*, M_0, 7, 0xd76aa478)
FF (*d*, *a*, *b*, *c*, M_1, 12, 0xe8c7b756)
FF (*c*, *d*, *a*, *b*, M_2, 17, 0x242070db)
FF (*b*, *c*, *d*, *a*, M_3, 22, 0xc1bdceee)
FF (*a*, *b*, *c*, *d*, M_4, 7, 0xf57c0faf)
FF (*d*, *a*, *b*, *c*, M_5, 12, 0x4787c62a)
FF (*c*, *d*, *a*, *b*, M_6, 17, 0xa8304613)
FF (*b*, *c*, *d*, *a*, M_7, 22, 0xfd469501)
FF (*a*, *b*, *c*, *d*, M_8, 7, 0x698098d8)
FF (*d*, *a*, *b*, *c*, M_9, 12, 0x8b44f7af)
FF (*c*, *d*, *a*, *b*, M_{10}, 17, 0xffff5bb1)
FF (*b*, *c*, *d*, *a*, M_{11}, 22, 0x895cd7be)
FF (*a*, *b*, *c*, *d*, M_{12}, 7, 0x6b901122)
FF (*d*, *a*, *b*, *c*, M_{13}, 12, 0xfd987193)
FF (*c*, *d*, *a*, *b*, M_{14}, 17, 0xa679438e)
FF (*b*, *c*, *d*, *a*, M_{15}, 22, 0x49b40821)

Round 2:

GG (*a*, *b*, *c*, *d*, M_1, 5, 0xf61e2562)
GG (*d*, *a*, *b*, *c*, M_6, 9, 0xc040b340)
GG (*c*, *d*, *a*, *b*, M_{11}, 14, 0x265e5a51)
GG (*b*, *c*, *d*, *a*, M_0, 20, 0xe9b6c7aa)
GG (*a*, *b*, *c*, *d*, M_5, 5, 0xd62f105d)
GG (*d*, *a*, *b*, *c*, M_{10}, 9, 0x02441453)
GG (*c*, *d*, *a*, *b*, M_{15}, 14, 0xd8a1e681)
GG (*b*, *c*, *d*, *a*, M_4, 20, 0xe7d3fbc8)
GG (*a*, *b*, *c*, *d*, M_9, 5, 0x21e1cde6)
GG (*d*, *a*, *b*, *c*, M_{14}, 9, 0xc33707d6)
GG (*c*, *d*, *a*, *b*, M_3, 14, 0xf4d50d87)
GG (*b*, *c*, *d*, *a*, M_8, 20, 0x455a14ed)
GG (*a*, *b*, *c*, *d*, M_{13}, 5, 0xa9e3e905)
GG (*d*, *a*, *b*, *c*, M_2, 9, 0xfcefa3f8)
GG (*c*, *d*, *a*, *b*, M_7, 14, 0x676f02d9)
GG (*b*, *c*, *d*, *a*, M_{12}, 20, 0x8d2a4c8a)

Round 3:

HH (*a*, *b*, *c*, *d*, M_5, 4, 0xfffa3942)
HH (*d*, *a*, *b*, *c*, M_8, 11, 0x8771f681)
HH (*c*, *d*, *a*, *b*, M_{11}, 16, 0x6d9d6122)
HH (*b*, *c*, *d*, *a*, M_{14}, 23, 0xfde5380c)
HH (*a*, *b*, *c*, *d*, M_1, 4, 0xa4beea44)
HH (*d*, *a*, *b*, *c*, M_4, 11, 0x4bdecfa9)
HH (*c*, *d*, *a*, *b*, M_7, 16, 0xf6bb4b60)
HH (*b*, *c*, *d*, *a*, M_{10}, 23, 0xbebfbc70)
HH (*a*, *b*, *c*, *d*, M_{13}, 4, 0x289b7ec6)
HH (*d*, *a*, *b*, *c*, M_0, 11, 0xeaa127fa)
HH (*c*, *d*, *a*, *b*, M_3, 16, 0xd4ef3085)
HH (*b*, *c*, *d*, *a*, M_6, 23, 0x04881d05)
HH (*a*, *b*, *c*, *d*, M_9, 4, 0xd9d4d039)
HH (*d*, *a*, *b*, *c*, M_{12}, 11, 0xe6db99e5)
HH (*c*, *d*, *a*, *b*, M_{15}, 16, 0x1fa27cf8)
HH (*b*, *c*, *d*, *a*, M_2, 23, 0xc4ac5665)

Round 4:

II (*a*, *b*, *c*, *d*, M_0, 6, 0xf4292244)
II (*d*, *a*, *b*, *c*, M_7, 10, 0x432aff97)
II (*c*, *d*, *a*, *b*, M_{14}, 15, 0xab9423a7)
II (*b*, *c*, *d*, *a*, M_5, 21, 0xfc93a039)
II (*a*, *b*, *c*, *d*, M_{12}, 6, 0x655b59c3)
II (*d*, *a*, *b*, *c*, M_3, 10, 0x8f0ccc92)
II (*c*, *d*, *a*, *b*, M_{10}, 15, 0xffeff47d)
II (*b*, *c*, *d*, *a*, M_1, 21, 0x85845dd1)
II (*a*, *b*, *c*, *d*, M_8, 6, 0x6fa87e4f)
II (*d*, *a*, *b*, *c*, M_{15}, 10, 0xfe2ce6e0)
II (*c*, *d*, *a*, *b*, M_6, 15, 0xa3014314)
II (*b*, *c*, *d*, *a*, M_{13}, 21, 0x4e0811a1)
II (*a*, *b*, *c*, *d*, M_4, 6, 0xf7537e82)
II (*d*, *a*, *b*, *c*, M_{11}, 10, 0xbd3af235)
II (*c*, *d*, *a*, *b*, M_2, 15, 0x2ad7d2bb)
II (*b*, *c*, *d*, *a*, M_9, 21, 0xeb86d391)

MD5 INFORMATION SHEET

ETAOIN

Mnemonic Popular Among Amateur Cryptographers

Letter	Count	Percent
a	3312	7.49
b	573	1.29
c	1568	3.54
d	1602	3.62
e	6192	14.00
f	966	2.18
g	769	1.74
h	1869	4.22
i	2943	6.65
j	119	0.27
k	206	0.47
l	1579	3.57
m	1500	3.39
n	2982	6.74
o	3261	7.37
p	1074	2.43
q	116	0.26
r	2716	6.14
s	3072	6.95
t	4358	9.85
u	1329	3.00
v	512	1.16
w	748	1.69
x	123	0.28
y	727	1.64
z	16	0.04
ALL	44232	

English Letter Frequency Distributions

0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

Binary/Hex translation Table

8:30 hrs	18/6/01	HALL 29-GF	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 2001
Year of Study (Art & Sciences leave blank)	Third
Degrees/Diplomas for which this course is prescribed (BSc (Eng) should indicate which branch)	BSc (Eng)
Faculty/ies presenting candidates	Engineering
Internal examiners and telephone number(s)	Mr G D Agnew x77213
External examiner(s)	Mr Willem Clark
Special materials required (graph/music/drawing paper) maps, diagrams, tables, computer cards, etc)	None

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 FOUR* questions.
Type '2' Examination (see instructions overleaf).

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