University of the Witwatersrand, Johannesburg
School of Electrical and Information Engineering
ELEN 330 – Information Engineering Techniques

Class Test – 19 May 2003

Time: 1 hour
Full Marks: 30

Instructions to candidates:
1. Answer all questions.
2. Show all working: marks will be allocated for all working and logical reasoning and not just for the correct answer.
3. State and give reasons for any assumptions that are made.
4. Candidates are allowed to use one handwritten A4 information sheet.

Question 1

The table below shows the first of two stages of the "adfgvx" cipher. All 26 letters of the alphabet and digits 0 to 9 are present in the 6 by 6 grid, giving a total of 36 entries. The arrangement of the 36-character alphabet in this table is arbitrary and may be varied as required by the users of the cipher.

	a	**d**	**f**	**g**	**v**	**x**
a	3	V	Q	K	2	M
d	L	C	I	A	G	S
f	P	0	Y	7	X	N
g	F	W	B	1	D	9
v	U	Z	O	R	4	8
x	6	E	J	5	H	T

In this stage, a plaintext character is translated by finding it in the table and writing down the letters (from the set "adfgvx") representing its row and column. A short example translation (spaces shown only for clarity) is:

```
A  T  T  A  C  K      A  T      1  1  P  M
dg xx xx dg dd ag     dg xx     gg gg fa ax
```

In the second stage a keyword is chosen and used to form the first row of a new grid. The first-stage ciphertext is then used to fill this grid row by row as shown in the table below left. Finally, the keyword is re-arranged alphabetically as shown in the table below right. The entire column associated with each key word letter is moved along with it during the alphabetical re-arrangement.

D	**A**	**V**	**E**
d	g	x	x
x	x	d	g
d	d	a	g
d	g	x	x
g	g	g	g
f	a	a	x

A	**D**	**E**	**V**
g	d	x	x
x	x	g	d
d	d	g	a
g	d	x	x
g	g	g	g
a	f	x	a

The final ciphertext is then obtained by reading off the table column by column, giving:

```
gxdggadxddgfxggxgxxdaxga
```

(a) Use the information given above to decipher the following ciphertext:

```
dxvggxgdfvgddxvg
```
(2 marks)

(b) Where are the elements of confusion and diffusion introduced in this cipher? **(2 marks)**

(c) As an expert in cryptography what two rules about stage-2 keyword generation would you make for users of the cipher? **(2 marks)**

(d) Devise and describe a method of specifying the stage-1 table by means of a key/keyword. Assuming that your key is able to generate every possible stage-1 translation table, what is the keyspace for stage-1? (Note: the method you specify does not necessarily have to be capable of generating every possible translation table). **(4 marks)**

Question 2

(a) The following equation represents a translation table for a monoalphabetic substitution cipher where X is a value from 0 to 25 representing a plaintext character from "a" to "z". C_1 and C_0 are integers. Under what condition(s) will C_1 and C_0 give valid translation tables? Determine and list all of the values of C_1 and C_0 which yield valid translation tables. **(2 marks)**

$$P_1(X) = (C_1 * X + C_0) \bmod 26$$

(b) Using your knowledge of probability and the frequency table for English given in the information sheet, determine the frequency table for ciphertexts produced using the ADFGVX cipher described in Question 1. Check your result by adding up the values in your table of frequencies. (Assume that plaintexts do not have the digits 0 to 9 in them, as the frequency table does not list values for the digits). Hence determine the IC (index of coincidence) for the short alphabet ADFGVX associated with this cipher. **(6 marks)**

(c) It will be apparent from your result in (b) that the frequency distribution of the ADFGVX is fairly non-uniform and depends on the chosen translation table. How could a cryptographer use this fact to flatten the frequency distribution? (Precise details not required, just an allusion to the method will do). What effect would this have on the keyspace? **(2 marks)**

Question 3

The attached information sheet gives block diagrams representing the Blowfish algorithm.

(a) What are the two operations (represented by the small circles and squares containing crosses) present in this algorithm? Demonstrate your understanding of these operations by applying each of them in turn to the following two 4-bit operands: 1101 and 1110. Assume for the sake of this exercise that the 32-bit data paths of blowfish are 4 bits wide. **(2 marks)**

(b) Where is the element of diffusion introduced in this cipher? (Describe the point, which is either in figure 1 or 2, precisely) **(1 mark)**

(c) Different cryptographic algorithms have "weak keys" which are weak in different senses. Approximately 1 in 2^{14} blowfish keys is weak in the sense that the ciphertext cannot subsequently be deciphered by the algorithm. Given that the Blowfish cipher has a key length of 448 bits, approximately how many weak keys (in total) are there? Devise and describe, possibly with the aid of a block diagram, a method for deciding whether or not a prospective key is weak. **(3 marks)**

(d) A wireless mouse generates one byte of movement information at a time. To minimise latency, the movement bytes are transmitted immediately after being enciphered with the Blowfish algorithm, leaving the scheme open to the dictionary attack. Draw a block diagram that shows how the cipher scheme can be modified to eliminate the possibility of a dictionary attack. What is the tolerance of your scheme to single-bit errors and synchronisation errors? **(4 marks)**

Information Sheet

Letter frequency distribution for the English Language:

A	B	C	D	E	F	G
0.0749	0.0129	0.0354	0.0362	0.1400	0.0218	0.0174
H	I	J	K	L	M	N
0.0422	0.0665	0.0027	0.0047	0.0357	0.0339	0.0674
O	P	Q	R	S	T	U
0.0737	0.0243	0.0026	0.0614	0.0695	0.0985	0.0300
V	W	X	Y	Z		
0.0116	0.0169	0.0028	0.0164	0.0004		

Index of Coincidence:

$$IC = \sum_{i=a}^{i=z} \frac{(Freq_i)(Freq_i - 1)}{N(N-1)}$$

Blowfish Cipher: (function F is shown on the right-hand side)