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

Class Test – 6 May 2002

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

(a) Derive the two translation tables corresponding to the following permutation functions for monoalphabetic substitution ciphers:

$P_1(a) = (3 * a) \bmod 26$
$P_2(a) = (5 * a + 13) \bmod 26$

Hence double-encipher the following plaintext using first a five-column transposition cipher, and then the two-alphabet polyalphabetic cipher defined by the permutation functions above. Pay close attention to your choice of padding characters – explain why and how you have chosen them. **(6 marks)**

THE SANDY SHORE

(b) Explain briefly how the method of Kasiski, along with the index of coincidence, can be used to cryptanalyse polyalphabetic ciphers. **(4 marks)**

Question 2

(a) In the translation table shown below, each plaintext character is enciphered by moving a certain number of blocks in the vertical, and then the horizontal direction, to determine the ciphertext character. The number of positions moved changes from character to character in order to hide patterns. These moves can be represented graphically – an example of a repeating pattern of 3 move sequences (which can be thought of as a rudimentary key) is shown below the block. There is no plaintext for "Z", in order to make the plaintext alphabet fit into a square grid. Z's in the plaintext are replaced by "S". Spaces are not coded – they are removed from the plaintext before encipherment.

An example encryption using this cipher is (spaces shown only for clarity):

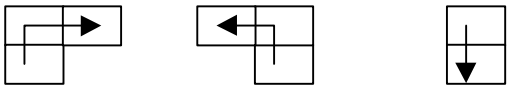
```
SHE SELLS SEA SHELLS
obj oxqfm xuy xdxqhm
```

Ignoring the anomaly introduced by the Z being treated as an S, this cipher is equivalent to (possibly a combination) of ciphers you have learned about. Determine and state the precise details of this equivalence. **(5 marks)**

(b) What kind of ciphertext-only attack would you use on this cipher? **(2 marks)**

(c) Describe an adaptive chosen plaintext attack you would use on this cipher. **(3 marks)**

S	T	P	Q	R	S	T	P	Q
X	Y	U	V	W	X	Y	U	V
D	E	A	B	C	D	E	A	B
I	J	F	G	H	I	J	F	G
N	O	K	L	M	N	O	K	L
S	T	P	Q	R	S	T	P	Q
X	Y	U	V	W	X	Y	U	V
D	E	A	B	C	D	E	A	B
I	J	F	G	H	I	J	F	G



Question 3

(a) The Caesar cipher can be thought of as a monoalphabetic substitution cipher with a fixed key (the "key" is effectively built into the algorithm). Explain how this cipher may be operated with a selectable key and how the users could go about choosing a key. What is the keyspace for your method of key selection? **(4 marks)**

(b) Prove that a closed cipher is also a pure cipher. **(2 marks)**

(c) The diagram below shows a particular technique associated with a cipher mode. What is the name of the technique and why is it used? Write down which information is transmitted and the order in which it is transmitted. **(4 marks)**