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

Class Test – 3 May 2001

Time: 1 hour
Full Marks: 50

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) The cryptographer "A Kerckhoffs" (last century) was noted for some valuable advice relating to the use of non-restricted vs. restricted cryptographic algorithms. What (in your own words) was this advice? How is this advice generally put into practise today? **(4 marks)**

(b) Double-encrypt the following sample plaintext using a first a Caesar cipher and then a columnar transposition cipher of 5 columns. **(8 marks)**

```
TWAS BRILLIG, AND THE SLITHY TOVES
```

(c) Give the name of, and describe, a classical cipher other than mono/polyaphaphetic substitution & transposition ciphers. **(3 marks)**

Question 2

(a) The following sample of ciphertext has been generated from a plaintext which makes use of the usual 26 character alphabet. Determine the index of coincidence (IC) of this sample (note: normally a much longer sample would be used to obtain a useful result). **(8 marks)**

```
wkhir oorzl qjvkr uwvdp sohri flskh
```

(b) What does the IC of a ciphertext tell us about the substitution cipher that produced it? **(2 marks)**

(c) Suppose a given ciphertext is known to have been produced by either a monoalphabetic substitution or a double-columnar transposition cipher. What simple test or analytical method can be used to determine which cipher was used? – explain fully. Use this method, showing any analysis you do, to determine which cipher was probably used to produce the following ciphertext : (hint: extensive analysis of the sample below is not required – it should take you just a few minutes to glean the information you need) **(10 marks)**

```
stolh detru oaeac rhoph lctaw obpap osnad aovhl ibstb seaum
euole bbmpu sdyae enlse euget aeedt sinir tdeee vpcte txrde
rsrso pmtno uatdl iocdb noean piuss rtier pctpa enwoh eionr
fhded tsamu iurbu ililc ctytt ynlhe eeiit eyctx iooiw uihtt
nnchs peiho caieh fseri lcteo krapm hhrln adhec iwlom oetis
aowou rhpms wnnbw ohepi
```

Question 3

a) Figure 1 shows parts of the DES symmetric cipher, which has a key size of 56 bits and a block size of 64 bits. With reference to the blocks in Figure 1, explain briefly how DES achieves the goals of confusion and, in particular, diffusion effectively. **(4 marks)**

b) The IDEA symmetric cipher uses a block size of 64 bits and a key size of 128 bits. What is the key space of this algorithm? Does this in itself make the algorithm more secure than DES? – explain. **(3 marks)**

c) Explain, with the aid of sketches, how a block cipher can be used with feedback or feedforward to produce a non-repeating ciphertext stream, regardless of the nature of the plaintext input. Explain why such schemes are used. **(8 marks)**.

The Index of Coincidence:

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

Mnemonic Popular with Amateur Cryptographers:

ETAOIN

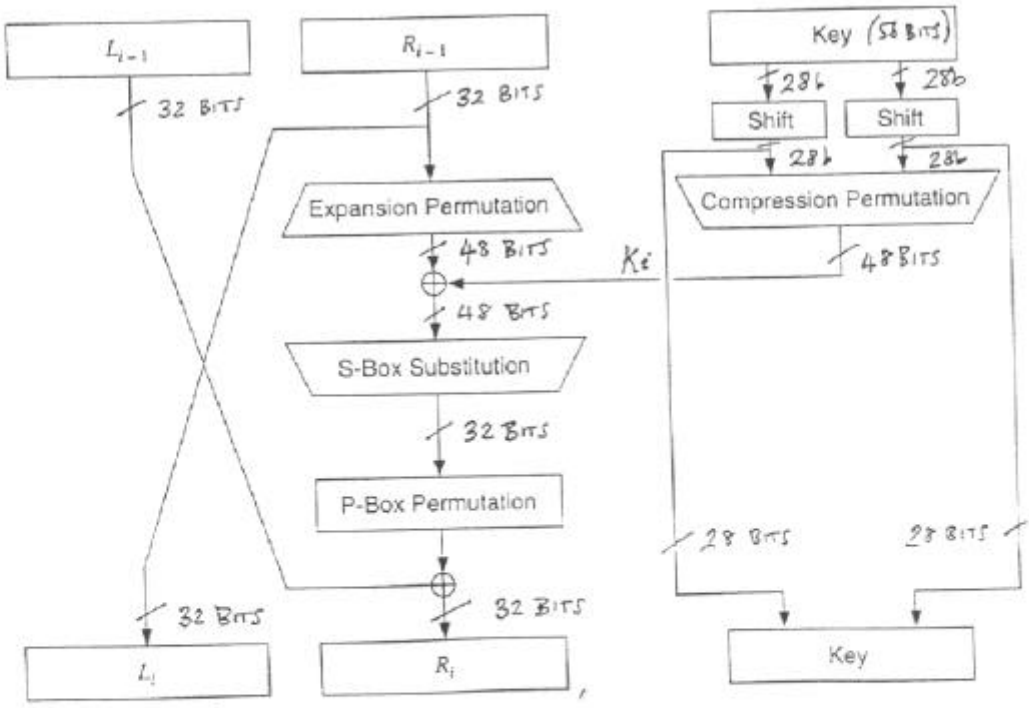

Figure 1 – One Round of DES