Homework 3

Problem 1
Consider the ciphertext given in Figure 1, which resulted from a periodic polyalphabetic substitution cipher applied to an English plaintext. Word breaks are indicated by blanks.

a) Using the C programming language, write programs to compute the Index of Coincidence (I.C.) and to apply the Kasiski test. Hand in a documented copy of your source code.

b) Apply your programs to the given ciphertext. What period is suggested by each test?

c) In high-level pseudocode, state your algorithm for applying the Kasiski test. Analyze the time and space complexity of your algorithm. State your answers in big-Oh notation in terms of the three parameters n, L, and k, where n is the number of ciphertext letters, L is the number of letters in the alphabet (for English, $L = 26$), and k is the length of the longest repeating string for which your algorithm looks. Can you think of a faster algorithm?

```
CT OSB UHGI TP IPEWF H CEWIL NSTTLE FJNVX XTYLS FWKKHI
BJLSI SQ VOI BKSM XMKUL SK NVPONPN GSW OL. IEAG NPSI HYJISFZ
CYY NPUXQG TPRJA VXMSI AP EHVPPR TH WPPNEL. UVZUA MMYVSF
KNTS ZSZ UAJPQ DLMMJXL JR RA PORTELOGJ CSULTWNI XMKUHW
XGLN ELCPOWY OL. ULJTL BVJ TLBWTPZ XLD K ZISZNK OSY DL
RYJUAJSSGK. TLFNS UVD VV FQGCYL FJHVSI YJL NEXV PO WTOL PYYYHSH
GQBOH AGZTIQ EYFAX YPMP SQA CI XEYVXNPPAII UV TLFTWMC FU
WBWXGUHIWU. AIIWG HSI YJVTI BJV. XMQN SFX DQB LRTY TZ
QTXLNISVZ. GIFT AII UQSJGJ OHZ XFOWFV BKAI CTWY DSWTLTTTPKFRHG
IVX QCAFV TP DIIS JBF ESF JSC MCCF HNGK ESBP DJPQ
NLU CTW ROSB CSM.
```

Figure 1: Ciphertext produced by a periodic polyalphabetic substitution cipher.

Problem 2
What is the plaintext for the ciphertext of Figure 1? Explain in how you arrived at your solution.