Homework 1

Note: Always, carefully justify all answers and explain your reasoning clearly. Write in complete sentences. Unjustified answers risk receiving no credit.

Problem 1

Consider the following ciphertext, which resulted from a monoalphabetic substitution cipher applied to an English plaintext. The ciphertext is arranged in blocks of five letters for convenience only.

```
SFDZF IOGHL PZFGZ DYSPF HBZDS GVHTF UPLVD FGYVJ VFVHT GADZZ AITYD

ZYFZJ ZTGPT VTZBD VFHTZ DFXSB GIDZY VTXOI YVTEF VMGZZ THLLV XZDFM

HTZAI TYDZY BDVFH TZDFK ZDZZJ SXISG ZYGAV FSLGZ DTHHT CDZRS VTYZD

OZFFH TZAIT YDZYG AVDGZ ZTKHI TYZYS DZGHU ZFZTG UPGDI XWGHX ASRUZ

DFUID EGHTV EAGXX
```

a) What evidence supports the hypothesis that the encryption process is monoalphabetic substitution?

b) Are there any sequences of three or more ciphertext letters that have distinctive patterns? What is the significance of such sequences, if any?

c) Try to distinguish the vowels from the consonants. What techniques are useful for accomplishing this task?

d) What is the plaintext? Explain the highlights of how you arrived at your solution.

e) Can you explain how the key was chosen?

Problem 2

In a brief and thoughtful essay, discuss how one might break monoalphabetic substitution ciphers automatically. Creativity, insightfulness, and careful analysis will be rewarded.