Problem Set 1

In both of the problems below, use frequency analysis to decipher the given ciphertext. In each case, the ciphertext was created from an English language plaintext using a substitution cipher. Different substitutions were used in the two cases. The line breaks have no significance.

See Stinson, p.40, for probabilities of occurrence of the 26 letters in an English text; and see pp.42-44 for a sample analysis of a substitution cipher.

1.

IEEIPYEQKVZJRPDPKAPRPVAIFZPKJB

FLPJTBEWFZPIAIPFPPIFZNPIFQTLFZ

JFFZABYETKVYJBDPAIOYJFNZPVXPPI

KLJIVNKEBPKLDLAIFPKKAOPINPBOTP

JFPTFZJIGJIBIEEIPOJRPJFZEQOZFF

EFZPEKVPTYETKVBEWBSJNPJBBEQTNP

BEWZQGJIVJIOPTETFZEQOZFEWFZPGE

IKLFEVABGABBFZPAVPJEWKAWPQSEIF

ZPGJBAGSEBBADKP

A first step in analyzing a ciphertext such as this one is to look at the numerical distribution of characters in the text. The characters for the given ciphertext are distributed as follows:

A: 13	J: 18	S: 3
B: 18	K: 14	T: 10
C: 0	L: 6	U: 0
D: 4	M: 0	V: 10
E: 23	N: 6	W: 6
F: 23	O: 7	X: 1
G: 6	P: 35	Y: 5
H: 0	Q: 7	Z: 17
I: 20	R: 3	

P jumps out as the most frequently occurring ciphertext character. It is reasonable (and, in this case, correct) to surmise that P encodes the plaintext e.

Note furthermore that the digram (two-character sequence) FZ occurs several times in the ciphertext. FZ is in fact the encryption of a common English digram (again, see p.27 of Stinson).

After P, the most frequently occurring ciphertext characters are E, F, I. It is reasonable (and again correct, in this case) to assume that E, F, I each encode letters in the set $\{t,a,o,i,n,s,h,r\}$.

2.

ESKAGWJNSESRAVRFEKADWIHWGEKDYL

VVLWDOKRGFRDAESKGKLNDWHESKEKGG

LZVKVLQRGAFSRAVWDNFLDXKKDAKASK

GKWDESKKTJREWGLDESKXWDELDKDEIS

LXSIWJVAWDKAROZKUDWIDRFRHGLXRE

SKZREEVKHWGKBLFEKDXKSRAGKRXSKA

RDKIXVLYRBWHHKGWXLEORDAESKPLXE

WGIRFDWEOKELDFLNSE

Distribution of ciphertext characters:

A: 13	J: 3	S: 16
B: 2	K: 31	T: 1
C: 0	L: 16	U: 1
D: 21	M: 0	V: 9
E: 22	N: 4	W: 17
F: 8	O: 4	X: 9
G: 14	P: 1	Y: 2
H: 6	Q: 1	Z: 3
I: 6	R: 18	

Due: February 13