HOMEWORK 1

For this week, please answer the following questions from the text. I've copied the problem itself below and the question numbers for your convenience.

(1) (1.2) Decrypt each of the following Caesar encryptions by trying the various possible shifts until you obtain readable text.
- LWKLQNWKDWLVKDOOQHYHUVHHDELOOERDUGORYHOBDVDWUHH
- UXENRBWXCUXENFQRLQJUCNABFQNWRCJUCNAJCRXWORWMB
- BGUTBMBGZTFHNLXMKTIPBMAVAXXLXTEPTRLEXTOXKHHFYHKMAXFHNLX

Decrypted text
- I think that I shall never see a billboard lovely as a tree.
- Love is not love which alters when it alteration finds.
- In baiting a mouse trap with cheese always leave room for the mouse.

(2) (1.3) Use the simple substitution table below

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
S	C	J	A	X	U	F	B	Q	K	T	P	R	W	E	Z	H	V	L	I	G	Y	D	N	M	O

(a) Encrypt the plaintext message

`The gold is hidden in the garden.`

(b) Make a decryption table, that is, make a table in which the ciphertext alphabet is in order from A to Z and the plaintext alphabet is mixed up.

(c) Use your decryption table from (b) to decrypt the following message.

`IBXLX JVXIZ SLLDE VAQLL DEVAU QLB`

Solutions

(a) IBX FEPA QL BQAAXW QW IBX FSVAXW

(b) Decryption table

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
d	h	b	w	o	g	u	q	t	c	j	s	y	x	z	l	i	m	a	k	f	r	n	e	v	p

(c) the secret password is swordfish

(3) (1.4.c) Each of the following messages has been encrypted using a simple substitution cipher. Decrypt them. For your convenience, we have given you a frequency table and a list of the most common bigrams that appear in the ciphertext. (If you do not want to recopy the ciphertexts by hand, they can be downloaded or printed from the web site listed in the preface.) In order to make this one a bit more challenging, we have removed all occurrences of the word "the" from the plaintext.

"A Brilliant Detective"

```
GSZES GNUBE SZGUG SNKGX CSUUE QNZOQ EOVJN VXKNG XGAHS AWSZZ BOVUE
SIXCQ NQESX NGEUG AHZQA QHNSP CIPQA OIDLV JXGAK CGJCG SASUB FVQAV
CIAWN VWOVP SNSXV JGPCV NODIX GJQAE VOOXC SXXCG OGOVA XGNVU BAVKX
QZVQD LVJXQ EXCQO VKCQG AMVAX VWXCG OOBOX VZCSO SPPSN VAXUB DVVAX
QJQAJ VSUXC SXXCV OVJCS NSJXV NOJQA MVBSZ VOOSH VSAWX QHGMV GWVSX
          CSXXC VBSNV ZVNVN SAWQZ ORVXJ CVOQE JCGUW NVA
```

The ciphertext contains 313 letters. Here is a frequency table:

	V	S	X	G	A	O	Q	C	N	J	U	Z	E	W	B	P	I	H	K	D	M	L	R	F
Freq	39	29	29	22	21	21	20	20	19	13	11	11	10	8	8	6	5	5	5	4	3	2	1	1

The most frequent bigrams are: XC (10 times), NV (7 times), and CS, OV, QA, and SX (6 times each). Decrypted text:

Decrypted: I am fairly familiar with all forms of secret writing and am myself author of a trifling monograph upon subject in which i analyze one hundred separate ciphers but i confess that this is entirely new to me object of those who invented this system has apparently been to conceal that these characters convey a message and to give idea that they are mere random sketches of children

To decrypt this code, I first looked at the frequency tables for the individual digits and the bigrams. I was able to immediately determine that 'V' corresponded to 'e'. I then looked at the common bigrams and noted which letters were repeated. I then looked at the frequency of digits within bigrams to make a couple of educated guesses. Afterwards, I looked up common trigrams as well as letters that appear most often in pairs. This is how I discovered the identities of 's' and 'l'. In addition, I knew that my predictions were correct when, early on, I had solved for 'hundred seParate'. I was then able to infer the rest of the letters from context clues.

(4) (1.5) Suppose that you have an alphabet of 26 letters.
   (a) How many possible simple substitution ciphers are there?
   (b) A letter in the alphabet is said to be fixed if the encryption of the letter is the letter itself. How many simple substitution ciphers are there that leave:
      (i) No letters fixed?
      (ii) At least one letter fixed?
      (iii) Exactly one letter fixed?
      (iv) At least two letters fixed?

   (Part (b) is quite challenging! You might try doing the problem first with an alphabet of four or five letters to get an idea of what is going on.)

Problem 4 Solutions

(a) This is equivalent to the number of permutations of the alphabet, which is $26! = 403291461126605635584000000$

(b) (i) This can be counted using the principle of inclusion-exclusion. We begin with 26! total simple substitution ciphers. We then subtract all of the ciphers with one fixed element, which is $\binom{26}{1} * 25!$, as we are choosing 1 of 26 letters to fix and permuting the others in any other way. However, this subtracted the case where 2 letters are fixed, so this is added back as $\binom{26}{2} * 24!$. This pattern of alternating addition and subtraction continues with terms matching the form

$$\binom{26}{i} * (26-i)!.$$

which by the definition of $\binom{n}{k}$ is equal to

$$\frac{26!}{k!(26-k)!} * (26-k)! = \frac{26!}{k!}$$

This simplifies our expression to be

$$26! - \frac{26!}{1!} + \frac{26!}{2!} - \cdots + \frac{26!}{26!}$$

which is equivalent to the sum

$$26! \sum_{k=0}^{26} \frac{(-1)^k}{k!} \approx 1.48362637 \times 10^{26}$$

(ii) All possible simple substitution ciphers can be broken into either having no fixed letters or having at least one fixed letter. We can then subtract the number without any fixed letters from the total:

$$26! - (26! \sum_{k=0}^{26} \frac{(-1)^k}{k!}) \approx 2.54928824 \times 10^{26}$$

(iii) We begin by choosing a letter to fix, which is equal to $\binom{26}{1=26}$. We can then multiply this by the number of ciphers on 25 letters without any fixed letters, which is

$$25! \sum_{k=0}^{25} \frac{(-1)^k}{k!}$$

, so the total with one fixed is

$$26! * (25! \sum_{k=0}^{25} \frac{(-1)^k}{k!})$$

(iv) The number of ciphers with at least two letters fixed is the number with at least one fixed minus the number with exactly one fixed:

$$26! - (26! \sum_{k=0}^{26} \frac{(-1)^k}{k!}) - (26! * (25! \sum_{k=0}^{25} \frac{(-1)^k}{k!}))$$