HOMEWORK 1 ANSWERS

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) Decrypted Caesar Cyphers, obtained using a brute-force Java program and looking through all 25 possible shifts

- `ithinkthatishallneverseeabillboardlovelyasatree (With Shift 23)`
- `loveisnotlovewhichalterswhenitalterationfinds (With Shift 17)`
- `inbaitingamousetrapwithcheesealwaysleaveroomforthemouse (With Shift 7)`

(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`

(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).

(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.)