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.`

`IBXFEPAQLBQAAXWQWIBXFSVAXW.`

(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.

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

`IBXLX JVXIZ SLLDE VAQLL DEVAU QLB`

`thesecretpasswordisswordfish` $\rightarrow$ `The secret password is swordfish.`

(3) (1.4.c)

"A Brilliant Detective"

```
iamfa irlyf amili arwit hallf ormso fsecr etwri tinga ndamm yself
autho rofat rifli ngmon ograp hupon subje ctinw hichi analy zeone
hundr edsep arate ciphe rsbut iconf essth atthi sisen tirel ynewt
omeob jecto fthos ewhoi nvent edthi ssyst emhas appar ently beent
oconc ealth atthe secha racte rscon veyam essag eandt ogive ideat
          hatth eyare merer andom sketc hesof child ren
```

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

Process: V seemed obvious to be 'e'. XCSXXC appears 3 times, using the letter frequencies the most likely deciphering was 'thatth'. From there G was likely to be

'i' to make 'this' a few times, and Z to be 'm' to make "I am". B → 'y' and N → 'r' creates the phrase 'they are'. U → 'l' creates some adverbs and other familiar combinations, E → 'f' makes almost the entire first line make sense. From there it was trivial to replace the few remaining letters with the only things that make sense.

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

(4) (1.5) Suppose that you have an alphabet of 26 letters.
(a) How many possible simple substitution ciphers are there?

$$26!$$

The total number of ciphers is the product of the number of ways we can map each letter. There are 26 ways we can remap A (yes, we can map it to itself), there are 25 ways to remap B given that we have mapped A, ect. This will include the mapping of the alphabet to the alphabet. If we don't want that, just subtract 1.

(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?
We will need to exclude all ciphers that leave at least one letter fixed. We can subtract the number that fix one letter: $26! - \binom{26}{1}25!$ but because this includes the ciphers that fix 2 letters, counting each set of 2 letters twice, we need to add back in $\binom{26}{2}24!$ and because this includes the ciphers that keep 3 letters fixed, we need to subtract $\binom{26}{3}23!$ and so on. Giving $\sum_{k=0}^{26}(-1)^k * \binom{26}{k} * (n-k)!$ = $26!\sum_{k=0}^{26}(-1)^k/k!$
(ii) At least one letter fixed?

$$26!\sum_{k=1}^{26}(-1)^{(k-1)}/k!$$

This is 26! - the sum from (i) by removing the k = 0 term (26!) and flipping the signs so it is now the ciphers fixing 1 - the ciphers fixing 2 double count etc.

(iii) Exactly one letter fixed?

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

We can pick 26 letters to be the fixed one. Then we have to count the ways that the other 25 can be mapped with none of them fixed, which is like (i) but with 25 instead of 26.

(iv) At least two letters fixed?

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

This is the total number of ciphers minus the number that have 0 fixed minus the number that have 1 fixed (using the numbers from (i) and (iii)).

(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.)