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

3 shifts to the left: I THINK THAT I SHALL NEVER SEE A BILLBOARD LOVELY AS A TREE

- UXENRBWXCUXENFQRLQJUCNABFQNWRCJUCNAJCRXWORWMB

9 shifts to the right: LOVE IS NOT LOVE WHICH ALTERS WHEN IT ALTERATION FINDS

- BGUTBMBGZTFHNLXMKTIPBMAVAXXLXTEPTRLEXTOXKHHFYHKMAXFHNLX

7 shifts to the left: IN BAITING A MOUSE TRAP WITH CHEESE ALWAYS LEAVE ROOM FOR THE MOUSE

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

abcdefghijklmnopqrstuvwxyz

SCJAXUFBQKTPRWEZHVLIGYDNMO

(a) Encrypt the plaintext message

The gold is hidden in the garden.

IBXFE PAQLB QAAXW QWIBX FSVAX W

(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

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

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

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

(4) (1.5) Suppose that you have an alphabet of 26 letters.

(a) How many possible simple substitution ciphers are there?

If simple substitution cipher is defined as, “A substitution cipher is a method of encryption where each letter in the plaintext is replaced by another letter, symbol, or number,” (https://caesarcipher.net/substitution-cipher/) then there are 26! - 1 different permutations of a simple substitution cipher. This includes shifts as well as just randomly assigning letters to one another, including all letters being fixed. The ‘-1’ takes into account all of the alphabet becoming fixed.

(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?

26!

All possible permutations of the alphabet without repetition.

(ii) At least one letter fixed?

4.b.ii.

!26 a derangement of the alphabet

A is a permutation of the elements of a set in which no element appears in its original position, hence why it is useful for this problem. One possible solution would be (25)((!25)+(!24) = 16,131,658,445,064,225,423,360,000.

One thing I will say is that there appears to be multiple variations of a derangement equation, however this one was the most common:

!n = (n-1) * (!(n-1) + !(n-2))

(iii) Exactly one letter fixed?

26! - !26

(iv) At least two letters fixed?

26! - (26! - !26)

(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.)