HOMEWORK 1

GROUP 2

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

- `LWKLQNWKDWLVKDOOQHYHUVHHDELOOERDUGORYHOBDVDWUHH`
- `UXENRBWXCUXENFQRLQJUCNABFQNWRCJUCNAJCRXWORWMB`
- `BGUTBMBGZTFHNLXMKTIPBMAVAXXLXTEPTRLEXTOXKHHFYHKMAXFHNLX`

Solution.
I deciphered all of the following by hand on an iPad.

- `LWKLQNWKDWLVKDOOQHYHUVHHDELOOERDUGORYHOBDVDWUHH`
  This cipher took 3 shifts.
  `I THINK THAT I SHALL NEVER SEE A BILLBOARD LOVELY AS A TREE`
- `UXENRBWXCUXENFQRLQJUCNABFQNWRCJUCNAJCRXWORWMB`
  This cipher took 9 shifts.
  `LOVE IS NOT LOVE WHICH ALTERS WHEN IT ALTERATION FINDS`
- `BGUTBMBGZTFHNLXMKTIPBMAVAXXLXTEPTRLEXTOXKHHFYHKMAXFHNLX`
  This cipher took 19 shifts.
  `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`

Solution.

(a) The encrypted message is

`IBXFE PAQLB QAAXW QWIBX FSVAX W`

(b) The decryption table for the given cipher:

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).

Solution.

After a fair amount of trial and error (including confusion as to why the string "the" was appearing and then realizing it was a substring of a word) and looking at common bigrams and trigrams, we noticed that "XCSXXC" appears 3 times. Comparing this with the common bigrams, we tried assigning this string to "thatth", and then assigning 'V' to 'e' since it was the most frequent and followed "thatth" twice. We then used the letter frequencies to start tentatively adding in other vowels, and by this point enough was filled in that it was fairly clear how to fill in the rest of the letters based on strings looking like certain words. We believe this is the decryption key (excluding 'T' and 'Y' since they never appear):

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

Thus, the decrypted message (with adding instances of "the" where they seem to have been removed) is:

```
I am fairly familiar with all forms of secret writing, and am myself
  the 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 sketches of children.
```

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

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

Solution.

There are 26! different simple substitution ciphers: there are 26 choices for 'A', 25 choices for 'B', and so on until there is one choice left for 'Z'.

(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?

Solution.
This is the number of derangements of a 26-element set, written !26. There are various ways to compute this: one is

$$26! \sum_{i=0}^{26} \frac{(-1)^i}{i!}.$$ [1]

(ii) At least one letter fixed?

Solution.
This is all the ciphers except for the ciphers with no fixed points, both values of which we have already computed. So there are 26!−!26 such ciphers.

(iii) Exactly one letter fixed?

Solution.
We first choose a letter to fix, and then permute the others with no fixed points. There are 26 choices for the letter to fix, and then !25 ways to permute the other letters with no fixed points. So there 26(!25) such ciphers.

(iv) At least two letters fixed?

Solution.
This is all the ciphers except for the ciphers with no fixed points or exactly one fixed point, all three of which we have already computed. So there are $26! - 26(!25) - !26$ such ciphers.

(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.)

[1] See the proof of this here.