Crypto Engineering Quiz 1

Problem 1

a.

```
> python .\109550076.py -1f
{'A': 2, 'B': 2, 'C': 12, 'D': 6, 'E': 4, 'F': 0, 'G': 5, 'H': 3, 'I': 4, 'J': 0, 'K': 2, 'L': 1, 'M': 19, 'N': 5, 'O': 1, 'P': 12, 'Q': 2, 'R': 9, 'S': 3, 'T': 1, 'U': 6, 'V': 7, 'W': 9, 'X': 6, 'Y': 12, 'Z': 9}
```

A	B	C	D	E	F	G	H	I	J	K	L	M
2	2	12	6	4	0	5	3	4	0	2	1	19
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
5	1	12	2	9	3	1	6	7	9	6	12	9

b.

Because C is a phrase with one letter, so it can be A or I. But the phrase I do not consisted in the middle of sentences, so C <-> A. Second, Y often used as the beginning of different two-character phrases, so I guess Y <-> O and since YV is also the beginning of another five-character phrase, so I guess YV <-> OF and YVRMP <-> OFTEN.

After some trial and error:

CIPHER	A	B	C	D	E	F	G	H	I	J	K	L	M
PLAIN	U	X	A	D	G	J	M	P	S	Q	Y	B	E
CIPHER	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
PLAIN	H	K	N	V	T	W	Z	C	F	I	L	O	R

The Plaintext:

A COMPUTER SCIENTIST MUST OFTEN
EXPERIENCE A FEELING OF NOT FAR
REMOVED FROM ALARM ON ANALYZING AND EXPLORE
THE FLOOD OF ADVANCED KNOWLEDGE WHICH EACH
YEAR BRINGS WITH IT

c.

Calculate the function using YVRMP <-> OFTEN:

Let $C_1 = P = 15, C_2 = R = 17$

And $P_1 = N = 13, P_2 = T = 19$

Since $\begin{cases} P_1 = aC_1 + b \\ P_2 = aC_2 + b \end{cases}$

We can get $\begin{cases} P_2 - P_1 = 6 \\ C_2 - C_1 = 2 \end{cases} \rightarrow a = 3$

and $\begin{cases} C_1 = 15, P_1 = 13 + 26n \\ P_1 = 3C_1 + b \end{cases} \rightarrow b = 20$

$$P = 3 * C + 20 \blacksquare$$

d.

Let $X_1 = E, X_2 = F, X_1 + 1 = X_2$

Since $\begin{cases} Y_1 = M \\ Y_2 = V \\ Y_1 = aX_1 + b \\ Y_2 = aX_2 + b \end{cases}$

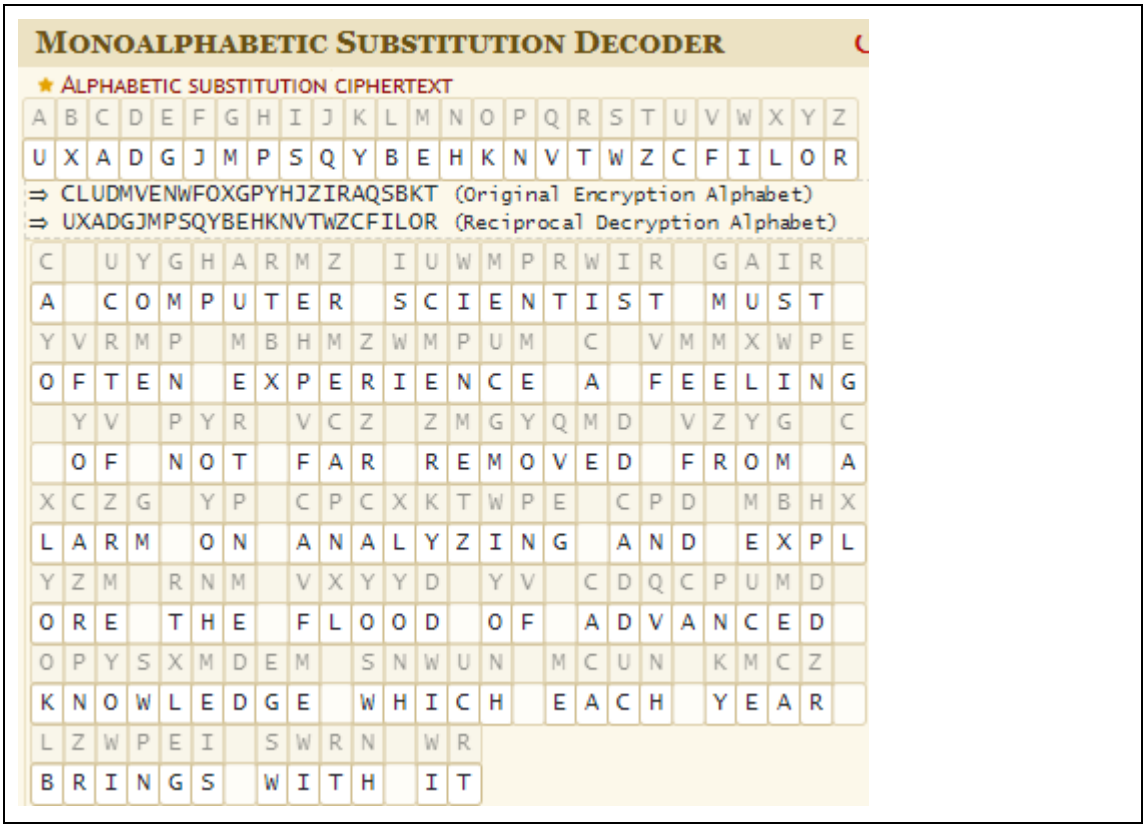
We can get $\begin{cases} X_2 - X_1 = 1 \\ Y_2 - Y_1 = 9 \end{cases} \rightarrow a = 9$ and $\begin{cases} X_3 = A = 0 \\ Y_3 = C = 2 \\ Y_3 = 9X_3 + b \end{cases} \rightarrow b = 2$

$$f(x) = 9x + 2 \blacksquare$$

e.

the key space size is $26! \fallingdotseq 2^{88}$ and this big space make search difficult. But we can break this kind of cipher with the frequency analysis.

f. https://www.dcode.fr/monoalphabetic-substitution can decrypt easily.



Problem 2

a.

the key space is $\phi(30) * 30 = 8 * 30 = 240$

b.

calculated using python

```
E:\Code\CryptoEngineering\Lab1
→ python .\109550076.py -2b
[(1, 1), (7, 13), (11, 11), (13, 7), (17, 23), (19, 19), (23, 17), (29, 29)]
```

	1	7	11	13	17	19	23	29
inverse	1	13	11	7	23	19	17	29

c.

$$\begin{cases} 8 + 30n = 4a + b \\ 26 + 30n = 10a + b \\ 7 + 30n = 27a + b \end{cases}$$

Finding the a whose differences of the results of different x would fit the difference of different y.

```
E:\Code\CryptoEngineering\Lab1
→ python .\109550076.py -2c
a: 13, b: 0
[22, 10, 21]
```

The answer $a = 13$, and the y when $(a, b) = (13, 0)$ are 22, 10, 21.

Which can easily get the offset b should be 16.

$$k_{enc} = (a, b) = (13, 16)\blacksquare$$

d.

$$D(x) = a^{-1}(x - b)\ mod\ 30 = 7(x - 16)\ mod\ 30 = 7(x + 14)\ mod\ 30$$
$$= 7x + 8\ mod\ 30\blacksquare$$
$$k_{dec} = (7, 8)$$