

1 Problem 1

1. Please write a program to find out the frequencies of letters in the ciphertext.

```

1 def cypher_freq(f_path):
2     freq = {}
3     with open(f_path, "r") as file:
4         for l in file:
5             for c in l:
6                 if c.isalpha():
7                     freq[c] = freq.get(c, 0) + 1
8
9     return freq
10
11 f_path = "./Quiz1/cyphertext.txt"
12 unsorted_freq = cypher_freq(f_path)
13 sorted_freq = {k: v for k, v in sorted(unsorted_freq.items(),
14                                     key=lambda item: item[1], reverse=True)}
15 print(sorted_freq)

```

Output: {'M': 19, 'C': 12, 'Y': 12, 'P': 12, 'R': 9, 'Z': 9, 'W': 9, 'V': 7, 'U': 6, 'X': 6, 'D': 6, 'G': 5, 'N': 5, 'I': 4, 'E': 4, 'H': 3, 'S': 3, 'A': 2, 'B': 2, 'Q': 2, 'K': 2, 'T': 1, 'O': 1, 'L': 1}

2. Use the plaintext frequency count information below as a reference to break this encrypted messages.

Ciphertext	A	B	C	D	E	F	G	H	I	J	K	L	M
	0	1	2	3	4	5	6	7	8	9	10	11	12
Plaintext	U	X	A	D	G	Q	M	P	S	J	Y	B	E
	20	23	0	3	6	16	12	15	18	9	24	1	4
Ciphertext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	13	14	15	16	17	18	19	20	21	22	23	24	25
Plaintext	H	K	N	V	T	W	Z	C	F	I	L	O	R
	7	10	13	21	19	22	25	2	5	8	11	14	17

Ciphertext: C UYGHARMZ IUWMPRWIR GAIR YVRMP MBHMZWMPUM C VMMXWPE YV
 PYR VCZ ZMGYQMD VZYG CXCZG YP CPCXKTWPE CPD MBHXYZM RNM VXYD YV
 CDQCPUMD OPYSXMDM SNWUN MCUN KMCZ LZWP EI SWRN WR

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

Step :

- (a) Guess M corresponds to E and C corresponds to A based on the common frequency of letters appearance.
 - (b) Guess RNM corresponds to THE based on context.
 - (c) And so on to get the final result.
3. Assume C is ciphertext, and P is plaintext. Can you find a particular relationship between C and P?
 It can be observed that most of the index of ciphertext increases by 1, the index value of plaintext will increase by 3, and the maximum index is not greater than 25.

4. Suppose " $f(x) = ax + b \bmod 26$ ", where x is plaintext, please solve the value of a and b .

From the observation of the question 3, we can get $f(x) = \begin{cases} 9x + 2 \bmod 26 & (x \neq 9, 21) \\ 9 & (x = 9) \\ 16 & (x = 21) \end{cases}$

5. What is the key size of the Mono-Alphabetic Substitution Cipher? Such a size makes exhaustive search becomes difficult?

Key size: $26!$

Exhaustive search time: $\frac{26!}{60 \times 60 \times 24 \times 365 \times 10^7} \approx 1.28 \times 10^{12}$ years (Suppose checking 10^7 keys/second).

6. (Bonus) Please try to see if it is possible to decipher this problem with ChatGPT or another tool.

(a) Substitution Solver (Possible)

Substitution Solver

This tool solves [monoalphabetic substitution ciphers](#), also known as [cryptograms](#). These are ciphers where each letter of the clear text is replaced by a corresponding letter of the cipher alphabet.

As an example here is an English cryptogram this tool can solve:

Rbo rpktdgo vcrb bwucja wj kloj hcjd, km sktpqo, cq rbwr loklgo
vcgg cjqcqr kj skhcja wgcja wjd rpycja rk ltr rbcjaq cj cr.
— Roppy Lpwrbsorr

A Python implementation of this breaker is provided on [GitLab](#).

If you want to break a [polyalphabetic cipher](#) instead try the [Vigenère Solver](#).

Input

Cipher Text *

C UYGHARMZ IUWMPRIW GAIR YVRMP MBHMZWMPUM C VMMXWPE YV PYR VCZ ZMGYQMD VZYG CX CZG
YP CPCXKTWE CPD MBHXYZM RNM VXYD YV CDQCPUMD OPYSXMDM SNWUN MCUN
KMCZ LZWPEI SWRN WR

Language

English

Break Cipher Clear Cipher Text

Result

Key	abcdefghijklmnopqrstuvwxyz	This clear text ...
	uxadqmps j ybehknvtwzcfilor	... maps to this cipher text

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

Details

Runtime: 0.010 seconds

(b) ChatGPT (Impossible)

ChatGPT 4

You

Solve this substitution encrypted message:
C UYGHARMZ IUWMPRWIR GAIR YVRMP MBHMZWMPUM C VMMXWPE YV PYR VCZ
ZMGYQMD VZYG CXZG YP CPCXKTWPE CPD MBHXYZM RNM VXYD YV CDQCPUMD
OPYSXMDM SNWUN MCUN KMCZ LZWPEI SWRN WR

ChatGPT

To solve this substitution cipher, we need to identify a pattern or key for the substitution. Since there's no direct key provided, one approach is to use frequency analysis, which involves looking at the most common letters in the cipher and comparing them to the most common letters in the English language. Let's start by analyzing the frequency of each letter in the encrypted message.

Finished analyzing

The frequency of the letters in the encrypted message is as follows, with 'M' being the most common:

- M: 19 times
- C, Y, P: 12 times each
- R, Z, W: 9 times each
- V: 7 times
- U, X, D: 6 times each
- G, N: 5 times each
- I, E: 4 times each
- H, S: 3 times each
- A, B, Q, K: 2 times each
- T, O, L: 1 time each

In English, the most common letters are E, T, A, O, I, N, S, H, R, D, L, U. We can start by assuming that the most frequent letters in the ciphertext correspond to these letters. For example, 'M' might be 'E', 'C'/'Y'/'P' might be 'T'/'A'/'O', and so on.

Let's try substituting these and see if we can start making sense of the message. We'll need to adjust as we go, as the first attempt is unlikely to be completely accurate. Let's begin by replacing 'M' with 'E', 'C' with 'T', 'Y' with 'A', and 'P' with 'O' and see what the message starts to look like. [↩]

After making the initial substitutions:

- 'M' to 'E'
- 'C' to 'T'
- 'Y' to 'A'
- 'P' to 'O'

The partially decrypted message looks like this:

"T UAGHAREZ IUWEORWIR GAIR AVREO EBHEZWEQUE T VEEIXWOE AV OAR VTZ ZEGAQED
VZAG TXTZG AO TOTXTWOE TOD EBHXAZE RNE VXAAD AV TDQTOUED OOASXEDEE
SNWUN ETUN KETZ LZWOEI SWRN WR"

This doesn't immediately reveal a clear message, indicating that our initial substitutions might not be entirely accurate. Deciphering substitution ciphers often involves a bit of trial and error, especially without more context. Let's refine our approach by considering other common letter substitutions and looking for common English word patterns in the partially decrypted message. For example, single-letter words are likely to be 'A' or 'I', and 'T' is a common letter to appear twice together in English words.

We'll adjust the substitutions accordingly and continue the process. Let's try a few more adjustments. [↩]

Finished analyzing

After making further adjustments to the substitutions, the message now reads:

"X JZUPYFGM FJWGPFWFF UYFF ZRFGP GYPGMWGPJG X RGGCWPG ZR PZF RXM MGUZVGC
RMZU XCXMU ZP XPXCWXPWG XPC GYPCZMG FMG RCZZC ZR XCVXPJGC ZPZWCXGCGG
WNWJM GXJM WGXM JMWPGF WWFM WF"

This still does not reveal a clear message, suggesting that our substitutions are not yet correct. Deciphering substitution ciphers can be quite challenging without additional context or clues. It often requires iterative adjustments and sometimes even complete reevaluation of the substitution strategy.

Considering the complexity and the need for iterative, nuanced adjustments, it may be more practical to use a computer program that can try multiple combinations quickly or to have more context about the nature of the message or its origin. If you have any additional context or clues about the message, please provide them, as they could be crucial in cracking the code. [↩]

Get citation

Message ChatGPT...

ChatGPT can make mistakes. Consider checking important information.

2 Problem 2

1. Determine the size of the key space (that is, the total number of keys).

We must have $\gcd(30, a) = 1$, and also $1 \leq b \leq 30$. $\varphi(30) = \varphi(2 \times 3 \times 5)$
 $= (2 - 1) \times (3 - 1) \times (5 - 1) = 8$, therefore we have $8 \times 30 = 240$ possible keys.

2. Determine all values in \mathbb{Z}_{30} that have inverses and, by trial-and-error, determine the inverses.

Value	0	1	2	3	4	5	6	7	8	9
Inverse	x	1	x	x	x	x	x	13	x	x
Value	10	11	12	13	14	15	16	17	18	19
Inverse	x	11	x	7	x	x	x	23	x	19
Value	20	21	22	23	24	25	26	27	28	29
Inverse	x	x	x	17	x	x	x	x	x	29

3. Determine the encryption key $k_{enc} = (a, b)$.

$$\begin{cases} 4a + b \bmod 30 = 8 \\ 10a + b \bmod 30 = 26 \\ 27a + b \bmod 30 = 7 \end{cases} \Rightarrow \begin{cases} a = 13 \\ b = 16 \end{cases}$$

4. Determine the decryption key $k_{dec} = (c, d)$, where " $x = cy + d \bmod 30$ ".

$$\begin{cases} 8c + d \bmod 30 = 4 \\ 26c + d \bmod 30 = 10 \\ 7c + d \bmod 30 = 27 \end{cases} \Rightarrow \begin{cases} c = 7 \\ d = 8 \end{cases}$$