

Problem 1

(a)

| | | | | | | | | | | | | | | | | | | | | | |
|---------------|------------|------|-------|------------|------------|--------|---------|------|-------|----|-----------|-----|---------|-----|------|------------|-----------|-------|------|------|--------|
| C: UYGHARMZ | IUWIMPRWIR | GAIR | YVRMP | MBHMZWMPUM | CVMIXWPEYV | PYRVCZ | ZMGYQMD | VZYG | CXCZG | YP | CPCXKTWPE | CPD | MBHXYZM | RNM | VYYD | YVCDQCPUMD | OPYSXMDEM | SNWUN | MCUN | KMCZ | LZWPEI |
| RN WR | | | | | | | | | | | | | | | | | | | | | |
| A: 1.408451% | | | | | | | | | | | | | | | | | | | | | |
| B: 1.408451% | | | | | | | | | | | | | | | | | | | | | |
| C: 8.450704% | | | | | | | | | | | | | | | | | | | | | |
| D: 4.225352% | | | | | | | | | | | | | | | | | | | | | |
| E: 2.816901% | | | | | | | | | | | | | | | | | | | | | |
| F: 0.000000% | | | | | | | | | | | | | | | | | | | | | |
| G: 3.521127% | | | | | | | | | | | | | | | | | | | | | |
| H: 2.112676% | | | | | | | | | | | | | | | | | | | | | |
| I: 2.816901% | | | | | | | | | | | | | | | | | | | | | |
| J: 0.000000% | | | | | | | | | | | | | | | | | | | | | |
| K: 1.408451% | | | | | | | | | | | | | | | | | | | | | |
| L: 0.704225% | | | | | | | | | | | | | | | | | | | | | |
| M: 13.380282% | | | | | | | | | | | | | | | | | | | | | |
| N: 3.521127% | | | | | | | | | | | | | | | | | | | | | |
| O: 0.704225% | | | | | | | | | | | | | | | | | | | | | |
| P: 8.450704% | | | | | | | | | | | | | | | | | | | | | |
| Q: 1.408451% | | | | | | | | | | | | | | | | | | | | | |
| R: 6.338028% | | | | | | | | | | | | | | | | | | | | | |
| S: 2.112676% | | | | | | | | | | | | | | | | | | | | | |
| T: 0.704225% | | | | | | | | | | | | | | | | | | | | | |
| U: 4.225352% | | | | | | | | | | | | | | | | | | | | | |
| V: 4.929577% | | | | | | | | | | | | | | | | | | | | | |
| W: 6.338028% | | | | | | | | | | | | | | | | | | | | | |
| X: 4.225352% | | | | | | | | | | | | | | | | | | | | | |
| Y: 8.450704% | | | | | | | | | | | | | | | | | | | | | |
| Z: 6.338028% | | | | | | | | | | | | | | | | | | | | | |

(b)

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

Table 3: Ciphertext to plaintext mapping

| 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 | J | M | P | S | Q | Y | B | E |
| | 20 | 23 | 0 | 3 | 6 | 9 | 12 | 15 | 18 | 16 | 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 |

The plaintext "v" corresponds to ciphertext "Q", which does not adhere to $f(x) = ax + b$.

The plaintext "Q" corresponds to ciphertext "J", which does not adhere to $f(x) = ax + b$.

(c)

Other than the letters "v" and "Q" in the plaintext, we can observe that each plaintext letter is transformed into its corresponding ciphertext letter with a consistent difference of 9.

(d)

$$\begin{aligned}f(0) &= 0a + b \bmod 2b = 2 \\f(1) &= a + b \bmod 2b = 11 \\f(2) &= 2a + b \bmod 2b = 20 \\&\vdots\end{aligned}$$

$$\Rightarrow a = 9 \quad b = 2$$

$$A: a=9 ; b=2$$

(e)

① 26!

② $26! \approx 2^{88}$. Yes, it becomes difficult. There are so many possible answers that it would take lots of time to make exhaustive search.

(f)

ChatGPT cannot decrypt the ciphertext.



您

decrypt the following ciphertext

C UYGHARMZ IUWMPRWIR GAIR YVRMP MBHMZWMPUM CVMMXWPEYVPRVCZ ZMGYQMD
VZYG CXCGZ YP CPCXKTWPE CPD MBHXYZM RNM VXYD YVCDQCPUMD OPYSXMDEM
SNWUN MCUN KMCZ LZWPEI SWRN WR



ChatGPT

To decrypt the given ciphertext, it appears to be written in a simple substitution cipher, where each letter is replaced by another letter. To decipher it, we need to figure out the mapping between the encrypted letters and their plaintext counterparts. One approach is to analyze the frequency of letters in the ciphertext and compare it with the expected frequency of letters in English text. However, given the limited text provided, we can attempt to manually decipher it based on patterns and common letter frequencies.

So, the corrected plaintext would be:

css

Copy code

TO SEARCHING ALGORITHM AND YOU INTERWOVEN WITH YOURSELF INTRODUCTIONS ARRIVES VERY

This makes more sense and seems like a coherent message.

Then, I found the following website, which can decrypt the ciphertext correctly.

⇒ <https://www.dcode.fr/monoalphabetic-substitution>.

MONOALPHABETIC SUBSTITUTION DECODER

★ ALPHABETIC SUBSTITUTION CIPHERTEXT

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

⇒ CLUDMVENWFOXGPYHJZIRASBKT (Original Encryption Alphabet)
⇒ UXADGJMPSQYBEHKNVTWZCFILOR (Reciprocal Decryption Alphabet)

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

Problem 2

(a)

$1 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$ are coprime with 30

⇒ 8 numbers

$$8 \times 30 = 240 \quad A: 240$$

(b)

- ① $1 \times 1 = 1 \equiv 1 \pmod{30} \Rightarrow$ The inverse of 1 is 1
- ② $7 \times 13 = 91 \equiv 1 \pmod{30} \Rightarrow$ The inverse of 7 is 13
- ③ $11 \times 11 = 121 \equiv 1 \pmod{30} \Rightarrow$ The inverse of 11 is 11
- ④ $13 \times 7 = 91 \equiv 1 \pmod{30} \Rightarrow$ The inverse of 13 is 7
- ⑤ $17 \times 23 = 391 \equiv 1 \pmod{30} \Rightarrow$ The inverse of 17 is 23
- ⑥ $19 \times 19 = 361 \equiv 1 \pmod{30} \Rightarrow$ The inverse of 19 is 19
- ⑦ $23 \times 17 = 391 \equiv 1 \pmod{30} \Rightarrow$ The inverse of 23 is 17
- ⑧ $29 \times 29 = 841 \equiv 1 \pmod{30} \Rightarrow$ The inverse of 29 is 29

⇒ The inverse of other numbers do not exist.

(c)

$$4a + b \bmod 30 = 8 \dots \textcircled{1}$$

$$10a + b \bmod 30 = 2b \dots \textcircled{2}$$

$$27a + b \bmod 30 = 7 \dots \textcircled{3}$$

$$\textcircled{2} - \textcircled{1} : 6a = 18 + 30k \quad (k \in \mathbb{N})$$

$$\textcircled{3} - \textcircled{2} : 17a = -19 + 30n \quad (n \in \mathbb{N})$$

$$\textcircled{3} - \textcircled{1} : 23a = -1 + 30p \quad (p \in \mathbb{N})$$

\Rightarrow When $a = 13$, it fits all the equations

$$\Rightarrow b = 16$$

$$A: k_{\text{enc}} = (13, 16)$$

(d)

$$8c + d \bmod 30 = 4 \dots \textcircled{1}$$

$$26c + d \bmod 30 = 10 \dots \textcircled{2}$$

$$7c + d \bmod 30 = 27 \dots \textcircled{3}$$

$$\textcircled{2} - \textcircled{1} : 18c = 6 + 30k \quad (k \in \mathbb{N})$$

$$\textcircled{1} - \textcircled{3} : c = -23 + 30n \quad (n \in \mathbb{N})$$

$$\textcircled{2} - \textcircled{3} : 19c = -17 + 30p \quad (p \in \mathbb{N})$$

\Rightarrow When $c = 7$, it fits all the equations

$$\Rightarrow d = 8$$

$$A: k_{\text{dec}} = (7, 8)$$