密碼工程 quiz1

111550035 蔡昀錚

Problem 1

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

```
ciphertext = """
C UYGHARMZ IUWMPRWIR GAIR YVRMP MBHMZWMPUM C VMMXWPE YV PYR VCZ ZMGYQMD VZYG CXCZG YP CPCXKTWPE CPD MBHXYZM RNM VXYYD YV CDQCPUM
KMCZ LZWPEI SWRN WR
"""

# Remove spaces and newlines
ciphertext_clean = ciphertext.replace(" ", "").replace("\n", "")

# Calculate frequency of each letter in the ciphertext
frequency = {}
for letter in ciphertext_clean:
    if letter in frequency:
        frequency[letter] += 1
    else:
        frequency[letter] = 1

# Sort the frequency dictionary by value in descending order
sorted_frequency = dict(sorted(frequency.items(), key=lambda item: item[1], reverse=True))

print(sorted_frequency)
```

{'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}

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

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

Plain 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

(c) Assume C is ciphertext, and P is plaintext. Can you find a particular relationship between C and P?

Ans: If we give F and J specific plaintext, we can find that C and P is one to one.

(d) Suppose“f (x) = ax + b mod 26”,where x is plaintext, please solve the value of a and b.

Ans: To find the value of a and b, we first translate the ciphertext-plaintext table into number.

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

By the table, we can have 24 equation:
a * 0 + b mod 26 = 2 a * 1 + b mod 26 = 11 a * 2 + b mod 26 = 20 etc…
After calculation, we can have a = 9 and b = 2.

(e)What is the key size of the Mono-Alphabetic Substitution Cipher? Such a size makes exhaustive search becomes difficult?

Ans: The key size of a Mono-Alphabetic Substitution Cipher refers to the number of possible keys that can be used to encrypt the plaintext. For a simple Mono-Alphabetic Substitution Cipher where each letter in the alphabet is mapped to another unique letter (with no repetitions and no exclusions), the key size is equivalent to the number of possible permutations of the alphabet.

Since there are 26 letters in the English alphabet, the number of possible permutations (and thus the number of possible keys) is 26 factorial (26!), which is calculated as 26!. This number is extremely large. This enormous number of possible keys makes an exhaustive search (trying every possible key until the correct one is found) computationally impractical with current technology, thus providing a significant level of security against brute-force attacks.

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

I ask chatgpt for the solution of (a) and (b). For (a), chatgpt easily solve it, but at the first time it change “ ” and “\n” into “”, this doesn’t affect the result but it may make the following decryption more complex. For (b), chatgpt can’t give the right solution, it often make wrong relationship between ciphertext and plain text. For example, this is the plain text that chatgpt decrypt: “ACIDAGFOETMCNERONMODFMOISOEREYGETNERCEASEELNRHISRIOSATTEDIWEUSTIDALATDIRARALKVNRHARUEYGLITEOPESLLIUISAUWARCEUXRIBLEUHEBPNCPEACPKEATZTNRHMBNOPNO" and this is the table of wrong relationship that chatgpt provided:

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

Problem 2

Plaintext is encrypted using an affine cipher. A plaintext symbol, x, is drawn from Z30 and, hence, encryption is defined as "y = ax + b mod 30", where y is the resulting ciphertext and the encryption key is given by kenc = (a, b).

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

Ans: Possible a can be (coprime with 30): 1, 7, 11, 13, 17, 19, 23, 29. Possible b can be 0~29.
a have 8 possible values, while b have 30 possible values, so the key space is 8 * 30 = 240.

(b) Determine all values in Z30 that have inverses and, by trail-and-error, determine the inverses.

Ans: The values in Z30 that have inverses, along with their respective inverses determined by trial-and-error, are as follows:
1 has an inverse of 1
7 has an inverse of 13
11 has an inverse of 11
13 has an inverse of 7
17 has an inverse of 23
19 has an inverse of 19
23 has an inverse of 17
29 has an inverse of 29

(c) An attacker intercepts the following plaintext/ciphertext pairs:

x	y
4	8
10	26
27	7

Determine the encryption key kenc = (a, b).

Ans: we have following equation:
8 = a * 4 + b mod 30 26 = a * 10 + b mod 30 7 = a * 27 + b mod 30
After trying every possible a and b, we can have a = 13 and b = 16.

(d) Determine the decryption key kdec = (c, d), where “x = cy + d mod 30”.

Ans: To decrypt the text, we have following equation:
4 = c * 8 + d mod 30 10 = c * 26 + d mod 30 27 = c * 7 + d mod 30
After trying every possible c and d, we have c = 7 and d = 8.