Crytography Engineering student ID: 313553024
Name: 蘇柏叡

Problem 1

Please download `ciphertext.txt` from the new e3 platform.

A message has been encrypted, producing ciphertext characters with ASCII values ranging from 32 to 126.

a) (1 pt) Use frequency analysis to attempt to recover the original plaintext. Fill Table 1 below by mapping each ciphertext character to its corresponding plaintext character. **Include a snapshot of your filled table in your report.** (Leave an entry blank if there is no corresponding plaintext character.)

Hint: The plaintext spans a wide range of ASCII characters (32–126), including lowercase letters, uppercase letters, punctuation, and whitespace.
Hint: Refer to the frequency count information in Table 2 to guide your analysis.

本作答卷將以 作為
標示答案或過程

Ans: 留白處為待定字元!

Ciphertext	(space)	!	"	#	$	%	&	'	(	)	*	+	,	-	.
ASCII	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
Plaintext	F	b		;	W	s		L	h		A		y	6	R
Ciphertext	/	0	1	2	3	4	5	6	7	8	9	:	;	<	=
ASCII	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61
Plaintext	n		G	c	(space)			t	l	M	i	&	B		z
Ciphertext	>	?	@	A	B	C	D	E	F	G	H	I	J	K	L
ASCII	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76
Plaintext	7	S	o	,	H	d				u		N	j	'	C
Ciphertext	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	[
ASCII	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91
Plaintext				T	p	-	I	e				v		O	k
Ciphertext	\	]	^		`	a	b	c	d	e	f	g	h	i	j
ASCII	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106
Plaintext		D				U	q	.	J	f				w	4
Ciphertext	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y
ASCII	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121
Plaintext	P	l		E	a		:		r		K	g			
Ciphertext	z	{	|	}	~										
ASCII	122	123	124	125	126										
Plaintext	x		Q	m											

b) (1 pt) Assume the encryption uses the affine transformation

$$y = (ax + b) \mod 95 + 32,$$

where y is the ciphertext and x is the plaintext (both in the ASCII range). Determine the values of a and b.

Ciphertext	plaintext
S 83	I 73
1 47	n 110
3 51	space 32
@ 64	0 111

首先，將對應之明文-密文其中4組取出用以計算及驗證

$y = ax + b \bmod 95 + 32$

$\Rightarrow y - 32 = ax + b \bmod 95$ 並將右表代以求解

① $83 - 32 \equiv a \cdot 73 + b \bmod 95$

② $47 - 32 \equiv a \cdot 110 + b \bmod 95$

③ $51 - 32 \equiv a \cdot 32 + b \bmod 95$

④ $64 - 32 \equiv a \cdot 111 + b \bmod 95$

---

④ − ③

$\Rightarrow 79a \equiv 13 \bmod 95$

$\therefore a \equiv 13 \times 79 \bmod 95$

$a = 17$ # 代回 ①.②.

$95 = 79 \times 1 + 16$

$79 = 16 \times 4 + 15$

$16 = 15 \times 1 + 1$.

$15 = 15 \times 1 + 0$

$1 = 16 - 15$

$= 16 + 4 \times 16 - 79$

$= 5 \cdot 95 - 6 \times 79$ 即 $79^{-1} \equiv -6$ #

$95 - 6 = 89$ #

$51 \equiv (17 \cdot 1 + b) \bmod 95$ 即 $51 \equiv (b + b) \bmod 95$

$15 \equiv (17 \cdot 90 + b) \bmod 95$ 即 $15 \equiv (b + 5) \bmod 95$

$b = 45$ #

A: $a = 17$, $b = 45$

c) (1 pt) An attacker discovers that the plaintext contains the word `created`. How could this known plaintext be used to break the encryption? What is the name of the technique involved?

Ans:

已知明文攻擊

Attacker在已知 plaintext 中有某个單字為 created 就可以先查找其字母分別对应了哪些密文，並且建立 Affine Transformation ⇒ $y = ax + b \bmod 95 + 32$

並且利用已知的对应去求解 $y = ax + b \bmod 95 + 32$ 中的 a、b.

如此一來，若是有2組正確的明文、密文对应便可破解出密鑰！

此種攻擊手法可以稱作是「已知明文攻擊」。

也可再加上另一組進行驗証。

---

d) (1 pt) What is the size of the key space for this affine cipher on ASCII characters from 32 to 126? Why does this method provide relatively weak security?

Ans:

首先 a 必須和 n 互質 ⇒ ∵ 95的質因數有：5、19.

∴ a的可能值即 $n \times (1 - \frac{1}{5}) \times (1 - \frac{1}{19}) = 95 \times \frac{4}{5} \times \frac{18}{19} = 72$ #

而 b的數量為 0~n-1 ⇒ n个 ⇒ 95个

故本題 key space for this Affine Cipher 為 $72 \times 95 = 6840$ 組 #

又∵ 6840 組的空間大小其實相对小 ⇝ 易被 Brute-Force 破解

∴ 若是採用 Affine Cipher 易因 key space 過小而被 Brute-Force 破解 #

e) (1 pt) Next, consider a Monoalphabetic Substitution Cipher over ASCII characters from 32 to 126. What is the size of its key space, and how does this size affect the feasibility of a brute-force attack in terms of computational limits?

Ans:

i) ASCII code range 從 32~126 共 95 个，因此每組明文-密文確實既对

$\Rightarrow 95 \times 94 \times 93 \times 92 \times \dots \times 3 \times 2 \times 1 = 95!$ # ⇝ key space 極大

ii) 95! 相較於 bit 的 1840 組在實務上近乎是不會有機会被暴力破解

---

f) (Bonus 1 pt) Propose an enhanced encryption method that is more resilient against frequency analysis. Your design should:

1. Include at least two transformation steps (e.g., affine plus a bitwise operation).
2. Make frequency-based attacks more difficult.
3. Remain fully reversible to allow for accurate decryption.

In your response, explain how your design meets each of these three criteria.

Ans:

step 1: 先一樣使用 Affine Cipher 進行初步加密：$y_1 = ax + b \bmod 95 + 32$

step 2: 利用 XOR operation 把頻率擾亂

具体操作是利用 Pseudo-Random Number Generator 產生和 text 相同長度的亂數字串 ⇒ 接著，我們令該生成的亂數字串為 R ⇒ $y_2 = y_1 \oplus R$ → Ciphertext

驗証是否符合上述 3 大 criteria ⇝ 完全符合 #

(1) 利用 step 1 的 Affine Cipher 再利用 step 2 的 XOR ✓

(2) 因為 step 2 XOR operation 可以擾動原有的訊息字符的頻率 ✓

(3) 因為 XOR 為可逆之操作(自身对稱性) ⇝ 利用相同 key 也可以還原 step 1 的 output ✓

接著，再透过 Affine Cipher 這裡算還原明文

Problem 2

The plaintext is encrypted via an affine cipher over $\mathbb{Z}_n$ where n is a prime number satisfying

$$30 < n < 100.$$

The encryption is given by

$$y = ax + b \mod n,$$

with y the ciphertext and $k_{\text{enc}} = (a, b)$ the encryption key.

a) (1 pt) For a given n, compute the size of the key space by determining:

1. The number of valid a values.
2. The number of possible b values.
3. The total number of possible keys.

Please use standard Discrete Mathematics functions to represent your answer.

Ans:

(a)

已知 $y = ax + b \bmod n$，且 n 是質數及滿足 $30 < n < 100$，

#1. ∵ Affine Cypher 的定義為「a需要和n互質」才可以去求其 Multiplicative Inverses

∵ 在已知 n 是質數 換言之，從 1~(n-1) 都可以是和 n 互質的！

故 the number of valid a values 為 (n-1)個 #

#2. ∵ b mod n 可以任意值 ⇒ 即 b 的範圍是 0~(n-1) 都可以

故 the number of valid b values 為 n 個 #

#3. 所有可能解的空間就是 a·b ⇒ (n-1)×n 個 #

b) (1 pt) List all elements in $\mathbb{Z}_{30}$ that have multiplicative inverses, and identify those inverses.

Ans:

(b)

首先先找出和 30 互質的數字有 1、7、11、13、17、19、23、29 #

其中根據定義，mod n 中若某數存在 Multiplicative Inverses 則必是唯一！

⇒ 故為符合 $a \cdot a^{-1} \equiv 1 \bmod 30$ 我們將逐一檢查！

$1 \cdot 1 \equiv 1 \bmod 30 \Rightarrow 1^{-1} \equiv 1$

$7 \cdot 13 = 91 \equiv 1 \bmod 30 \Rightarrow 7^{-1} \equiv 13$

$13 \cdot 7 = 91 \equiv 1 \bmod 30 \Rightarrow 13^{-1} \equiv 7$

$11 \cdot 11 = 121 \equiv 1 \bmod 30 \Rightarrow 11^{-1} \equiv 11$

$17 \cdot 23 = 391 \equiv 1 \bmod 30 \Rightarrow 17^{-1} \equiv 23$

$23 \cdot 17 = 391 \equiv 1 \bmod 30 \Rightarrow 23^{-1} \equiv 17$

$29 \cdot 29 = 841 \equiv 1 \bmod 30 \Rightarrow 29^{-1} \equiv 29$

$19 \cdot 19 = 36 \equiv 1 \bmod 30$

$\Rightarrow 19^{-1} \equiv 19$

c) (1 pt) An attacker intercepts the following plaintext-ciphertext pairs.

Plaintext x	Ciphertext y
81	48
14	91
3	72

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

$$\begin{cases} 72 \equiv 3a+b \bmod n \\ 48 \equiv 81a+b \bmod n \end{cases}$$

$$24 \equiv -78a \bmod n$$

$y = ax+b \bmod n$ ↪ 將上表的 x, y 分別代入

$$\begin{cases} 48 \equiv 81a+b \bmod n \\ 91 \equiv 14a+b \bmod n \end{cases} \Rightarrow 43 \equiv -67a \bmod n$$

另外，由題意可知 $30 < n < 100$ 且 n 為質數。

n 可能值為 31、37、41、43、47、53、59、61、67、71、79、83、89、97

$$\begin{cases} 67a+43 \equiv 0 \bmod n \\ 78a+24 \equiv 0 \bmod n \end{cases}$$ ↪ 代表 n 可以整除 $67a+43$ 和 $78a+24$

* ∵ plaintext 和 ciphertext 的 max value 為 81、91，但因為 n 必須不能 ≤ 91
∴ n 必須是比 91 還大的質數 $\Rightarrow$ 97 * 接著把 $n=97$ 代入

接著，將 $43 \equiv -67a \bmod n$，$24 \equiv -78a \bmod n$ 分別改寫成 $\begin{cases} 43 \equiv 30a \bmod 97 \\ 24 \equiv 19a \bmod 97 \end{cases}$

如此一來，$a = 43 \times 30^{-1} \bmod 97$

其中 $30 \times 55 = 1650 \equiv 1 \bmod 97$ ↪ $30^{-1} \equiv 55 \bmod 97$

因此 $30^{-1} \equiv 55 \bmod 97$ ↪ $a \equiv 43 \times 55 \bmod 97 \equiv 37 \bmod 97$

另外將 $a \equiv 37 \bmod 97$ 代入

$48 \equiv 81 \times 37 + b \bmod 97$

又 $48 \equiv 2997 \bmod 97 + b \bmod 97$

$48 \equiv 87 + b \bmod 97$

$b \equiv (48-87) \bmod 97$

$b = 97 - 39 = 58$ *

A: $(a, b) = (37, 58)$

d) (1 pt) Find the decryption key $k_{\text{dec}} = (c, d)$ such that

$$x = cy + d \mod n.$$

原本是 $y = ax + b \bmod n$

$x = a^{-1}(y - b) \bmod n$ ⇝ $x = cy + d \bmod n$，比較係數後可發現，

$x = \underbrace{a^{-1}}_{c} y - \underbrace{(a^{-1} b)}_{d} \bmod n \Rightarrow \begin{cases} c \equiv a^{-1} \bmod n \\ d \equiv -a^{-1} b \bmod n \end{cases}$

$k_{dec} = (c, d) = (a^{-1} \bmod n, -a^{-1} b \bmod n)$ 將(c)算出的 $k_{enc} = (37, 58)$ 和 $n = 97$ 放進去

$37^{-1} \bmod 97$ ⇝ 計算 $\gcd(97, 37) \Rightarrow 97 = 37 \times 2 + 23$

$37 = 23 + 14$.

$23 = 14 + 9$

$9 = 5 + 4$

$5 = 4 \times 1 + 1$

$4 = 1 \times 4 + 0$

並且從 $1 = 5 - 4 \times 1$ 代回

$1 = 5 - (9 - 5) = 2 \times 5 - 9$ ⇝ 依序推回去之後 $\Rightarrow 1 = 5 \times 37 - 8(97 - 37 \times 2)$

$= 21 \times 37 - 8 \times 97 = 1$

$37^{-1} \equiv 21 \bmod 97$

↝ $a^{-1} = 21 \bmod 97$

$d \equiv -21 \times 58 \bmod 97$

$d \equiv -1218 \bmod 97$

$d \equiv (1764 - 1218) \bmod 97$

$d \equiv 43 \bmod 97$

A: $(c, d) = (21, 43)$ #

(1 pt) After a recent attempted breach, Dr. Shieh changed the key $k_{\text{enc}} = (a, b)$ and the prime number modulus n satisfying

$$30 < n < 100.$$

However, the attacker intercept a few plaintext-ciphertext pairs, albeit with some digits obscured. In the intercepted data, a missing digit is denoted by a "?" symbol.

Plaintext x	Ciphertext y
12	4?
?3	72
45	23
2	39

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

$x \to y$

$12 \to 40+k_1$

$10k_2+3 \to 72$

$45 \to 23$

$2 \to 39$

↳ 先從已知的組合找關係

利用 python code 取代繁雜取 a, b 過程

首先，已知密文最大是 72，∴不論如何 n 必須 > 72 故可能值：73, 79, 83, 89, 97

$23 = 45a + b \bmod n$

$39 = 2a + b \bmod n$

$\Rightarrow 16 = -43a \bmod n$

$43a \equiv -16 \bmod n$

接下來一一測試

```
from sympy import mod_inverse

# Given plaintext-ciphertext pairs
known_pairs = [(45, 23), (2, 39)]

# Candidate primes
primes = [73, 79, 83, 89, 97]

# Store results for each prime
results = {}

for n in primes:
    x1, y1 = known_pairs[0]
    x2, y2 = known_pairs[1]

    try:
        # Solve for a using the two equations: (y1 - y2) ≡ a(x1 - x2) mod n
        a = ((y1 - y2) * mod_inverse(x1 - x2, n)) % n
        # Solve for b using any of the known equations: y ≡ ax + b mod n
        b = (y1 - a * x1) % n

        results[n] = (a, b)
    except ValueError as e:
        # If mod_inverse fails, no valid 'a' for this prime
        results[n] = str(e)

results
```

```
{73: (20, 72), 79: (18, 3), 83: (17, 5), 89: (70, 77), 97: (47, 42)}
```

唯一成立的

$n=79$

$y = 18x + 3 \bmod 79$

$x=12$ 代入

$b_1 \equiv 219 \bmod 79$

$b_1 \neq 4?$ 79 刪掉!

$n=83$

$y = 17x + 5 \bmod 83$

$x=12$ 代入 $\Rightarrow y=43$ ✓

$y=12$ 代入

$72 = 170k_1 + 5b \bmod 83$

$170k_1 \bmod 83 = 16$

$k_1 = 4$ 帶 $x=43$ ✓

83 可保留

$n=73$

$y = ax + b \bmod n$

並且將各組合代入 $\Rightarrow y = 20x + 72 \bmod 73$

$x=12$ 代入

$29 \equiv 312 \bmod 73$

$29 \neq 4? \Rightarrow$ 勿刪掉, ✗

n=89

$y = 70x + 77 \bmod 89$

$x=12$ 代入 $\Rightarrow y \equiv 917 \bmod 89 \Rightarrow y \Rightarrow 7$ 不对应于值 x

故 89 删掉！

---

n=99

$y = 47x + 42 \bmod 97$

$x=12$ 代入 $\Rightarrow y \equiv 606 \bmod 97 \Rightarrow y=4$ 不对应于值 x

故 97 删掉

A: Kenc(a,b) $\Rightarrow$ a=17, b=5 时，明文-密文之对应为下表

且题用的 n=83 *

plaintext(x)	Ciphertext(y)
12	43
43	72
45	23
2	39