1. (a)

Table 1: Ciphertext-to-plaintext mapping (ASCII 32–126)

Ciphertext	(space)	!	"	#	$	%	&	'	(	)	*	+	,	-	.
ASCII	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
Plaintext	F	b		j	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		D	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	g	.	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											

The Declaration of Independence, 酷!

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.

int 才可 mod

	(51)	(84)
cipher	3	T
plain	space	e
	(32)	(101)

a z

$$\begin{cases} 32a + b \mod 95 + 32 = 51 \\ 101a + b \mod 95 + 32 = 84 \end{cases}$$

$$\begin{cases} 32a + b = 19 + 95k_1 \\ 101a + b = 52 + 95k_2 \end{cases}$$

$$69a = 33 + 95(k_2 - k_1)$$

When $k_2 - k_1 = 12$

$$69a = 33 + 95 \cdot 12$$

$$\underline{a = 17} \ *$$

$$133 \cdot 17 + 32b = 71 + 95(k_1 + k_2)$$

$$2261 + 32b = 71 + 95(k_1 + k_2)$$

$$32b + 2190 = 95(k_1 + k_2)$$

let $k_1 + k_2 = 24$

$$\underline{b = 45} \ *$$

P.S. a, b has infinite solution, a = 17, b = 45 is one of them.

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?

(1) As long as attackers find the ciphertext and plaintext, they can analyze the relationship between two texts. They can use some mathematical methods to find out the encryption process.

(2) Known-Plaintext Attack (KPA)

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?

(1)

$126 - 32 + 1 = 95$

from $1 \sim 94$, there are $95(1-\frac{1}{5})(1-\frac{1}{19}) = 72$ numbers coprime with 95.

$72 \cdot 95 = \underline{6840}$ #

(2) Because it contains a small key space, it's easier for the attacker to try all the possible passwords and decipher it.

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?

(1)

$126 - 32 + 1 = 95$

$\underline{95!}$ #

(2) Because 95! is a quite big number, it would cost a lot of time to run 95! possible passwords using brute-force method. Therefore, brute-force method is scarcely feasible on deciphering this password.

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.

First, using the caesar cipher to change the string using the following rule:

- if the char's index i is even: push forward i/2+1 alphabets
- if the char's index i is odd: push backward (i+1)/2 alphabets
- The user can set the scope on ASCII code they want. If the alphabets are pushed over the scope, they would be carried. (e.g. y -> z -> a -> b or b -> a -> z -> y if the scope is limited in the lowercase alphabets)

ex. str = "ilovecryptographyengineering"
for the first char: idx == 0 == even, so i -> j
for the second char: idx == 1 == odd, so l -> k
for the third char: idx == 2 == even, so o -> p -> q
..... etc.

Then, using substitution cipher. The user design their own table to substitute every char in the string. The benefit for this cipher is that only the user can easily solve the password easily since only he/she knows the substitution table. If other people want to decipher it, they need to use the brute-force method and spend a lot of time.

1. This encryption method includes the caesar cipher and substitution cipher.
2. The rule for caesar cipher in first step break the frequency for every char in the string
3. It's quite easy. First, the user use the table to back-substitute the char in the ciphered string. Then we change the push forward into push backward and push backward into push forward while deciphering the caesar cipher. Finally, we can get the original string.

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.

1. 在 Z_n 中，a 必須與 n 互質，以確保每個明文符號皆可映射至唯一密文符號。

$A = \{a \mid 1 \le a < n, \gcd(a, n) = 1, a \in Z^+\}$

∵ n 是 prime，a 有 $n-1$ 種選擇 #

2. b 則是由 n 所決定，因為 b 是取 mod n，

∴ b 有 n 種選擇 $(0 \sim n-1)$ #

$B = \{b \mid 0 \le b \le n-1, b \in N\}$

3. Let $f(n)$ be the size of key space

$f(n) = n(n-1) = n^2 - n$ #

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

在 0~29 中，與 30 互質的數會具有 multiplicative inverse

與 30 互質：1, 7, 11, 13, 17, 19, 23, 29 #

Identify:

$1 \times 1 \equiv 1 \pmod{30}$ $\quad 11 \times 11 \equiv 1 \pmod{30}$ $\quad 23 \times 17 \equiv 1 \pmod{30}$

$7 \times 13 \equiv 1 \pmod{30}$ $\quad 19 \times 19 \equiv 1 \pmod{30}$ $\quad 29 \times 29 \equiv 1 \pmod{30}$

$13 \times 7 \equiv 1 \pmod{30}$ $\quad 17 \times 23 \equiv 1 \pmod{30}$

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 $k_{\text{enc}} = (a, b)$.

$48 = 81a + b \bmod n$

$91 = 14a + b \bmod n$

$72 = 3a + b \bmod n$

$91 < n < 100$

$k_{enc} = (37, 58)$ #

The only valid solution occurs when $n = 97 \rightarrow a = 37, b = 58$

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

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

$81 = 48c + d \mod n$

$14 = 91c + d \mod n$

$3 = 72c + d \mod n$

$81 < n < 100$

The only valid solution occurs when $n = 97 \rightarrow c = 21, d = 43$

$k_{dec} = (21, 43)$ #

e) (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 $k_{\text{enc}} = (a, b)$.

$4? = (12a + b) \mod n$

$72 = (?3a + b) \mod n$

$23 = (45a + b) \mod n$

$39 = (2a + b) \mod n$

$72 < n < 100$

n 可能 73, 79, 83, 89, 97

n	a	b
93	20	72
79	18	3
83	17	5
89	70	77
97	47	42

✓

In these 5 possible solution,

only $n = 83, a = 17, b = 5$ satisfies

"12 → 47 & 73 → 72"

$12 \cdot 17 + 5 \mod 83 = 43$

$43 \cdot 17 + 5 \mod 83 = 72$

$k_{enc} = (17, 5)$ #