112 學年上學期 資訊安全與密碼學第二次作業

繳交方式：程式碼及書面報告都要。書面報告的內容手寫題請附過程，程式題請說明執行的方式，包含輸入與輸出的格式(請自訂)，報告電子檔請依以下方式命名：「HW02_學號_姓名」。
繳交時間：4/10 下午 5:00 前。遲交一週內 7 折，逾一週不計分。

1. (16%) Given an Affine cipher defined as follows:

$$C = \left(P \times K_1 + K_2 \right) \bmod 26$$

$$P = \left(\left(C - K_2 \right) \times K_1^{-1} \right) \bmod 26$$

   (1) Please encrypt the plaintext "**NCHU**" using key (6,3).
   (2) Please decrypt the ciphertext "**HSWZ**" using key (3,2).

2. (12%) Consider a Hill cipher that uses a 2×2 square matrix A as key. The elements of A are integers in Z_{26} that encodes the 26 English alphabets as follows:

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
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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

   Suppose the application of this Hill cipher yields the following results:
   - The plaintext "ba" is encrypted into ciphertext "HC".
   - The plaintext "zz" is encrypted into ciphertext "GT".

   Based on the above known plaintext results, please derive the key A of the given Hill cipher.

3. (10%) Please give an example to illustrate the One-Time Pad (OTP) mechanism and further describe its advantages and disadvantages.

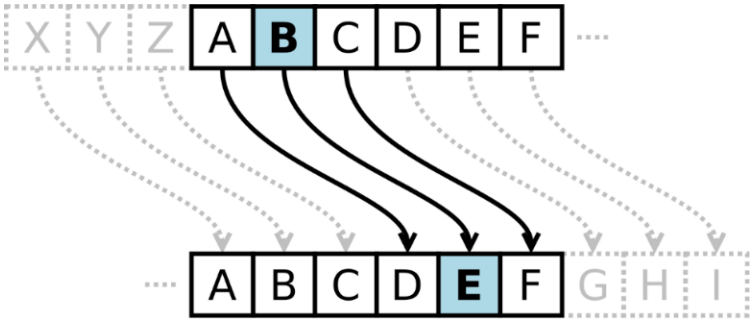
4. (12%) Given a columnar transposition cipher that uses the following permutation table:

1	2	3	4	5	6	7	8
↓	↓	↓	↓	↓	↓	↓	↓
5	8	7	1	6	4	3	2

   (1) Please encrypt the plaintext "**COMPUTER**".
   (2) Please decrypt the ciphertext "**VRPYYHRPITCAUGLO**".

5. (20%) 請用任何程式語言實作一個反轉換位的程式，將使用者所輸入的字串反向顯示。舉例來說，若使用者輸入"5793"，則程式輸出"3975"；若使用者輸入"this is a test"，則程式輸出"tset a si siht"。本程式不得依賴任何字串反轉的 API 來完成，並且須自行設計合適的防呆機制。

6. (30%) 凱撒密碼（Caesar cipher）是一種最簡單且最廣為人知的加密技術，它是一種代換法，將明文中的所有字母都在字母表上向後（或向前）按照一個固定數目進行偏移後取代替換成密文，如下圖所示。



使用者可以輸入一個字串$text$作為明文，及一個整數key作為金鑰。請用任何程式語言實作一個加密函式$encryption(text, key)$進行加密，並輸出密文；再實作一個解密函式$decryption(text, key)$進行解密，並輸出明文。請自行設計程式的防呆機制。（提示：本程式需使用到字元與 ASCII 碼之間的轉換，鍵盤上各字元的 ASCII 碼如下頁附表所示）

Ctrl	Dec	Hex	Char	Code
^@	0	00		NUL
^A	1	01		SOH
^B	2	02		STX
^C	3	03		ETX
^D	4	04		EOT
^E	5	05		ENQ
^F	6	06		ACK
^G	7	07		BEL
^H	8	08		BS
^I	9	09		HT
^J	10	0A		LF
^K	11	0B		VT
^L	12	0C		FF
^M	13	0D		CR
^N	14	0E		SO
^O	15	0F		SI
^P	16	10		DLE
^Q	17	11		DC1
^R	18	12		DC2
^S	19	13		DC3
^T	20	14		DC4
^U	21	15		NAK
^V	22	16		SYN
^W	23	17		ETB
^X	24	18		CAN
^Y	25	19		EM
^Z	26	1A		SUB
^[	27	1B		ESC
^\	28	1C		FS
^]	29	1D		GS
^^	30	1E	▲	RS
^-	31	1F	▼	US

Dec	Hex	Char
32	20	
33	21	!
34	22	"
35	23	#
36	24	$
37	25	%
38	26	&
39	27	'
40	28	(
41	29	)
42	2A	*
43	2B	+
44	2C	,
45	2D	-
46	2E	.
47	2F	/
48	30	0
49	31	1
50	32	2
51	33	3
52	34	4
53	35	5
54	36	6
55	37	7
56	38	8
57	39	9
58	3A	:
59	3B	;
60	3C	<
61	3D	=
62	3E	>
63	3F	?

Dec	Hex	Char
64	40	@
65	41	A
66	42	B
67	43	C
68	44	D
69	45	E
70	46	F
71	47	G
72	48	H
73	49	I
74	4A	J
75	4B	K
76	4C	L
77	4D	M
78	4E	N
79	4F	O
80	50	P
81	51	Q
82	52	R
83	53	S
84	54	T
85	55	U
86	56	V
87	57	W
88	58	X
89	59	Y
90	5A	Z
91	5B	[
92	5C	\
93	5D	]
94	5E	^
95	5F	_

Dec	Hex	Char
96	60	`
97	61	a
98	62	b
99	63	c
100	64	d
101	65	e
102	66	f
103	67	g
104	68	h
105	69	i
106	6A	j
107	6B	k
108	6C	l
109	6D	m
110	6E	n
111	6F	o
112	70	p
113	71	q
114	72	r
115	73	s
116	74	t
117	75	u
118	76	v
119	77	w
120	78	x
121	79	y
122	7A	z
123	7B	{
124	7C	|
125	7D	}
126	7E	~
127	7F	⌂*

* ASCII 碼 127 具有代碼 DEL。在 MS-DOS 下，這個代碼與 ASCII 8 (BS) 的效果相同。DEL 代碼可以由 CTRL + BKSP 鍵產生。