4-2加密解密函數

1

應用：加密與解密 - 加密函數

一個非常簡單的加密程序是按字母順序，
用兩位數來指定每一個文字如下：
$A \to 00$, $B \to 01$, $C \to 02$, ..., $X \to 23$, $Y \to 24$ 與 $Z \to 25$。
定義 一個函數 F(字母值)$\equiv a$(字母值)$+b\,(mod\,26)$，
其中 a 與 b 爲整數，且 a 與 26 無公因數，
同時和被 26 同餘縮小。 例如若 $a=3$ 且 $b=5$，則

$$F(X) \equiv 3(23)+5\,(mod\,26) \equiv 74\,(mod\,26) \equiv 22\,(mod\,26)$$

$F(A) \equiv$

$F(Y) \equiv$

$F(Z) \equiv$

2

應用：加密與解密 – 對射函數

字母	A	B	C	D	E	F	G	H	I	J
字母值	00	01	02	03	04	05	06	07	08	09
F(字母值)	05	08	11	14	17	20	23	00	03	06

字母	K	L	M	N	O	P	Q	R	S	T
字母值	10	11	12	13	14	15	16	17	18	19
F(字母值)	09	12	15	18	21	24	01	04	07	10

字母	U	V	W	X	Y	Z				
字母值	20	21	22	23	24	25				
F(字母值)	13	16	19	22	25	02				

X = {字母值 | 字母值 = 00 ,01 ,02 ,03 ,⋯ ,23 ,24 ,25 }

$F : X \rightarrow X$

F (字母值) ≡ 3(字母值) + 5 (mod 26) 為 1 - 1映成函數

3

應用：加密與解密 - 解密函數

F(字母值)≡ 3(字母值)+ 5 (mod 26) 的反函數爲同形式的另一個函數

G(字母值)≡ a(字母值)+ b (mod 26)，其中 a 與 b 被決定如下：

$$G \circ F(\text{字母值}) \equiv a(3 \cdot \text{字母值} + 5) + b \equiv \text{字母值} \pmod{26}$$

$$3a \cdot \text{字母值} + (5a + b) \equiv \text{字母值} \pmod{26}$$

$$(3a - 1)\,\text{字母值} + (5a + b) \equiv 0 \pmod{26}$$

所以，我們解 $3a - 1 \equiv 0 \pmod{26}$ and $5a + b \equiv 0 \pmod{26}$

得到 $a = 9$ 與 $b = 7$. 反函數則爲 G(字母值)≡ 9(字母值)+ 7(mod 26)。

4

應用：加密與解密 – 例子

例如欲加密傳送字串"HELLO"

HELLO ⇒ 07 04 11 11 14

字母	E	H	L	O
字母值	04	07	11	14
F(字母值)	17	00	12	21

⇓ 加密函數：$F(\text{字母值}) \equiv 3(\text{字母值}) + 5 \pmod{26}$

00 17 12 12 21 (加密後被傳送的訊息)

⇓ 解密函數：$G(\text{字母值}) \equiv 9(\text{字母值}) + 7 \pmod{26}$

07 04 11 11 14 ⇒ HELLO

5

隨堂練習:1

例如欲加密傳送字串"HELLO"

HELLO ⇒ 07 04 11 11 14

字母	E	H	L	O
字母值	04	07	11	14
F(字母值)				

⇓ 加密函數：$F(\text{字母值}) \equiv 5(\text{字母值}) + 7 \pmod{26}$

_____ (加密後被傳送的訊息)

⇓ 解密函數：$G(\text{字母值}) \equiv$ ___(字母值) + ___ $\pmod{26}$

07 04 11 11 14 ⇒ HELLO

6