預習測驗 02

姓名：＿＿＿＿＿＿＿＿ 序號：＿＿＿ 學號：＿＿＿＿＿＿＿＿ 分數：6 5 4 3 2 1

預習第三講 3.1, 3.2 (41-46 頁); 3.4 (54-56 頁) 並完成下列問題

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

1. 何謂費馬小定理 (Fermat's Little Theorem)？

2. 求 $2^{101} \pmod{13}$ 之值；亦即將 2^{101} 被 13 來除之後，餘數是多少？

3. 將明文信息"happy new year" 依據模 26 之下的仿射密碼 (affine cipher)，加密鑰匙爲 (7,11) 加密之；那麼密文爲何？請用大寫字母表示密碼文

   【解】先數位化明文 $7, 0, 15, 15, 24, 19, 4, 0, 2, 7, 4, 17, 18, 3, 0, 24$

明文	h	a	p	p	y	n	e	w	y	e	a	r
x	7	0	-11	-11	-2	13	4	-4	-2	4	0	-9
y												
密文												

4. 模 26 之下的仿射密碼：加密鑰匙爲 (7,11)，密文爲 XFVLANHRLAO；請破解之

   【解】首先，解同餘式 $y \equiv 7x + 11 \pmod{26}$, 算出解密函數爲

密文	X	F	V	L	A	N	H	R	L	A	O
y	-3	5	-5	11	0	13	7	-9	11	0	-12
x											
明文											