

數論與密碼：期中考

系級：_____ 姓名：_____ 序號：_____ 分數：_____

♣♦♠♥ ♣♦♠♥ 每小題15分，共 120分 ♣♦♠♥ ♣♦♠♥

1. 數論：

(a) 將 $2^{23590121}$ 除以23，餘數是多少？

(b) 解同餘式 $5d \equiv 1 \pmod{22}$ 。

(c) 將一信息表示成模23之下的一個整數 $m \pmod{23}$ 再將明文 m 加密為 $c = m^5 \pmod{23}$ 。
請問你如何將密文 $c = 11$ 解密？(提示：解密可將密文 c 在模 23之下取一整次冪來完成。)

2. 仿照第一講第 2節的方法，若用 ZEBRA 為加密鑰匙，我對你的評語為
XMTZPAPAZJJXUAPXBTSА；請問我對你的評語為何？

a	b	c	d	e	f	g	h	i	j	k	l	m
Z	E	B	R	A								
n	o	p	q	r	s	t	u	v	w	x	y	z

英文的 26 個字母其對應的數字如下：

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

3. 下面密文是由位移密碼器所得：LCLLEWLJAZLNNZMVYIYLHRMHZA 試用頻率分析來猜測此密文所用的鑰匙。請問解密之後的明文為何？

4. 使用仿射函數 $7x + 8 \pmod{26}$ 來加密信息，密文為LXSLF。找出明文！

5. 下面密文是由維吉內爾密碼器加密所得，鑰匙是cipher=(2,8,15,7,4,17)。找出明文！

CTATIECZTJVVCBTKIHWIA

6. 希爾密碼：加密鑰匙為 $\begin{pmatrix} 5 & 7 \\ 3 & 8 \end{pmatrix}$ ，密文為WOZGJZQU。找出明文！